CHAPITRE 0 : PRESENTATION DU COURS

0.0 Bienvenue dans le cours Présentation des réseaux

0.0.1 Message destiné aux participants

0.0.1.1 Bienvenue

Bienvenue dans le cours CCNA Initiation aux réseaux. L'objectif de ce cours est de vous présenter les concepts et technologies de base liés aux réseaux. Ce contenu pédagogique en ligne vous aidera à développer les compétences nécessaires à l'élaboration et à la mise en oeuvre de petits réseaux sur toute une gamme d'applications. Les connaissances spécifiques à acquérir figurent au début de chaque chapitre.

Vous pouvez utiliser un smartphone, une tablette, un ordinateur portable ou un ordinateur de bureau pour accéder au cours, participer aux discussions avec votre instructeur, consulter vos notes, lire ou réviser des textes et vous entraîner à l'aide de contenus interactifs. Cependant, certains contenus sont très élaborés et doivent être consultés sur un PC, tout comme les questionnaires, les examens et les exercices Packet Tracer.

0.0.1.2 Une communauté internationale

En participant au programme Networking Academy, vous devenez membre d'une communauté mondiale qui partage des objectifs et des technologies similaires. Des établissements scolaires, des établissements d'enseignement supérieur, des universités, ainsi que d'autres entités de plus de 160 pays participent à ce programme. Des informations sur la communauté mondiale Networking Academy sont disponibles à l'adresse http://www.academynetspace.com.

Vous pouvez également consulter les pages Facebook© et LinkedIn© du programme Cisco Networking Academy. Le site Facebook permet de rencontrer et de discuter avec d'autres participants du programme Networking Academy dans le monde entier. La page LinkedIn du programme Cisco Networking Academy vous permet de consulter des offres d'emploi et de voir comment les autres participants communiquent sur leurs compétences.

0.0.1.3 Plus que de simples informations

L'environnement d'apprentissage NetSpace est une composante essentielle de la satisfaction globale des participants et des instructeurs prenant part au programme Networking Academy. Ce contenu pédagogique en ligne comprend des cours et des supports interactifs associés, des activités de simulation sur Packet Tracer, des travaux pratiques sur équipements réels, des travaux pratiques à effectuer à distance, ainsi que de nombreux types de questionnaire. Tous ces supports fournissent de nombreux commentaires vous permettant d'évaluer votre progression tout au long du cours.

Le contenu pédagogique englobe une large gamme de technologies qui facilite la manière dont les personnes travaillent, vivent, jouent et apprennent en communiquant avec la voix, la vidéo et d'autres données. Les réseaux et Internet ont un impact différent dans toutes les régions du monde. Bien que nous ayons travaillé avec des instructeurs du monde entier pour créer ce cours, il est important que vous collaboriez avec votre instructeur et les autres participants pour adapter le contenu du cours à votre situation.

0.0.1.4 Méthode d'enseignement

L'« e-doing » est une philosophie qui repose sur le fait que les personnes apprennent plus facilement grâce à la pratique. Notre cursus comprend des activités d'« e-doing » hautement interactives pour faciliter l'apprentissage, l'assimilation des connaissances et pour enrichir l'apprentissage : il est ainsi plus facile de comprendre le contenu du cours.

0.0.1.5 La pratique mène à la maîtrise

Dans une leçon classique, après avoir étudié un sujet pour la première fois, vous vérifierez votre compréhension grâce à des contenus interactifs. Par exemple, si vous devez apprendre de nouvelles commandes, vous les utiliserez tout d'abord avec le contrôleur de syntaxe avant de configurer ou de dépanner un réseau dans Packet Tracer, l'outil de simulation de réseau de Networking Academy. Ensuite, vous effectuerez des activités pratiques sur le matériel de votre salle de classe ou à distance via Internet.

Packet Tracer peut également être utilisé pour vous entraîner à tout moment, grâce à la création de vos propres activités. Vous pouvez aussi vérifier vos compétences avec les autres participants dans le cadre de jeux à plusieurs. Les travaux pratiques d'intégration des compétences et les évaluations de compétences de Packet Tracer fournissent des commentaires élaborés sur les compétences à assimiler et vous permettent de vous préparer aux examens finaux, de chapitre ou de contrôle.

0.0.1.6 Esprit grand ouvert

L'objectif principal de la formation est d'approfondir vos connaissances en développant ce que vous savez et ce que vous pouvez faire. Il est important de noter, cependant, que le contenu pédagogique et l'instructeur ne servent qu'à faciliter ce processus. L'acquisition de nouvelles compétences dépend de votre engagement. Les pages suivantes contiennent certaines suggestions visant à faciliter votre apprentissage et à vous préparer à appliquer vos nouvelles compétences sur votre lieu de travail.

0.0.1.7 Journaux de conception

Les professionnels du secteur des réseaux tiennent souvent des journaux de conception dans lesquels ils notent les choses qu'ils observent et qu'ils apprennent (comme l'utilisation des protocoles et des commandes). Tenir un journal de conception vous permet de disposer d'une référence que vous pouvez consulter dans le cadre de votre travail. Écrire renforce l'apprentissage, tout comme la lecture, l'observation et la mise en pratique.

Dans le cadre de l'implémentation d'une technologie spécifique, vous pouvez répertorier dans votre journal les commandes logicielles requises, l'objectif de ces commandes, les variables de commande et un schéma de topologie indiquant le contexte d'utilisation des commandes de configuration.

0.0.1.8 Découverte du monde des réseaux

Packet Tracer est un outil d'apprentissage des réseaux qui prend en charge une large gamme de simulations physiques et logiques. Il fournit également des outils de surveillance pouvant vous aider à comprendre le fonctionnement interne d'un réseau.

Les exercices Packet Tracer existants comprennent des simulations de réseau, des jeux, des activités et des défis qui offrent un large éventail d'expériences d'apprentissage. Ces outils vous permettront d'approfondir vos connaissances sur la manière dont les données transitent sur un réseau.

0.0.1.9 Créez vos propres mondes

Vous pouvez également utiliser Packet Tracer pour créer vos propres expériences et scénarios réseau. Nous espérons qu'au fil du temps, vous utiliserez Packet Tracer non seulement pour effectuer les exercices existants, mais également en tant qu'auteur, chercheur, et testeur.

Le contenu pédagogique en ligne comprend des exercices Packet Tracer qui s'exécutent sur des ordinateurs utilisant un système d'exploitation Windows®, si Packet Tracer est installé. Ils peuvent également fonctionner sur d'autres systèmes d'exploitation utilisant une émulation Windows.

0.0.1.10 Comment Packet Tracer permet d'assimiler certains concepts

Jeux éducatifs

Les jeux Packet Tracer multiutilisateurs vous permettent, à vous ou votre équipe, de vous mesurer aux autres participants pour savoir lequel d'entre vous exécute une série de tâches le plus rapidement. C'est un excellent moyen de mettre en pratique les compétences acquises dans les exercices Packet Tracer et les travaux pratiques.

Cisco Aspire est un jeu de simulation et de stratégie qui se joue seul. Les joueurs testent leurs compétences relatives aux réseaux en passant des contrats dans une ville virtuelle. L'édition Networking Academy est spécialement conçue pour vous aider à vous préparer à l'examen de certification CCENT. Elle aborde également les compétences professionnelles et les techniques de communication que les employeurs du secteur des réseaux recherchent activement.

Les évaluations Performance-Based

Les évaluations Performance-Based de Networking Academy vous font effectuer des exercices Packet Tracer comme vous l'avez fait tout au long de la formation, à ceci près que ces exercices sont couplés à un moteur d'évaluation en ligne qui note automatiquement vos performances et vous fournit des commentaires instantanés. Ces commentaires vous aident à identifier plus précisément les connaissances et compétences que vous maîtrisez et celles sur lesquelles vous avez besoin de vous entraîner. Certaines des questions des questionnaires et examens de chapitre utilisent des exercices Packet Tracer pour vous fournir des commentaires supplémentaires sur votre progression

0.0.1.11 Présentation du cours

Comme l'indique le titre du cours, l'objectif principal de cette formation est de vous présenter les notions de base sur les réseaux. Dans ce cours, vous acquerrez à la fois les compétences pratiques et conceptuelles sur lesquelles repose la compréhension des réseaux de base. Le cours se déroulera comme suit :

- Vous comparerez la communication humaine à la communication réseau et ferez des parallèles.
- Vous découvrirez les deux modèles principaux utilisés pour planifier et mettre en œuvre des réseaux : OSI et TCP/IP.
- Vous apprendrez ce qu'est l'approche « en couches » appliquée aux réseaux.
- Vous observerez en détail les couches des modèles OSI et TCP/IP pour comprendre les fonctions et services associés.
- Vous vous familiariserez avec les différents périphériques réseau et schémas d'adressage réseau.
- Vous découvrirez les types de support utilisés pour acheminer les données sur les réseaux.

À la fin de ce cours, vous pourrez créer des LAN simples, effectuer des configurations de base des routeurs et des commutateurs et implémenter des schémas d'adressage IP.

0.1 Navigation dans le cours

0.1.1 Contrôlez votre expérience

0.1.1.1 Didacticiel sur l'interface du cours

CHAPITRE 1 : DECOUVERTE DU RESEAU

1.0 Découverte du réseau

1.0.1 Introduction

1.0.1.1 Introduction

Aujourd'hui, l'utilisation de la technologie pour développer et renforcer notre capacité de communication arrive à un tournant. La généralisation de l'utilisation d'Internet à l'échelle mondiale s'est opérée plus vite que quiconque aurait pu l'imaginer. L'évolution rapide de ce réseau mondial induit un bouleversement des interactions sociales, commerciales, politiques et même personnelles. L'étape suivante de notre développement verra les novateurs se servir d'Internet comme d'un tremplin pour créer de nouveaux produits et services spécialement conçus pour exploiter les capacités des réseaux. Alors que les développeurs repoussent les limites de ce qu'il est possible d'accomplir, les capacités des réseaux interconnectés qui forment Internet sont appelées à jouer un rôle croissant dans le succès de ce projet.

Ce chapitre présente la plateforme de réseaux de données dont nos relations sociales et commerciales sont de plus en plus dépendantes. Cette présentation sert de base à l'étude des services, des technologies et des problèmes rencontrés par les professionnels des réseaux lorsqu'ils conçoivent, élaborent et assurent la maintenance des réseaux modernes.

1.0.1.2 Exercice en classe – Illustrez votre vision d'Internet

Bienvenue dans un nouveau composant de notre cursus Networking Academy : les exercices de conception ! Vous les trouverez au début et à la fin de chaque chapitre.

Certains exercices peuvent être réalisés individuellement (chez vous ou en classe) et certains requièrent une interaction avec des groupes ou des communautés d'apprentissage. Votre instructeur vous aidera à bénéficier pleinement de ces exercices d'introduction.

Ces exercices vous aideront à améliorer votre compréhension en vous donnant la possibilité de visualiser certains des concepts abstraits que vous aborderez dans ce cours. Soyez créatif et profitez de ces exercices !

Voici le premier exercice de conception :

Illustrez votre vision d'Internet

Dessinez une carte d'Internet (et inscrivez les légendes correspondantes) conforme à votre vision actuelle. Indiquez l'emplacement de votre domicile ou de votre école/université ainsi que les informations relatives au câblage, au matériel, aux périphériques, etc. Voici certains des éléments que vous pourriez vouloir inclure :

- Périphériques/Équipement
- Supports (câblage)
- Adresses ou noms de liaison
- Sources et destinations
- Fournisseurs d'accès Internet

Lorsque vous avez terminé, veillez à imprimer votre travail, car il sera utilisé ultérieurement, à la fin de ce chapitre. Si c'est un document électronique, enregistrez-le dans le dossier du serveur fourni par votre instructeur. Préparez-vous à partager et expliquer votre travail en classe.

Pour consulter un exemple, rendez-vous sur http://www.kk.org/internet-mapping/.

Exercice en classe – Illustrez votre vision d'Internet : instructions

1.1 Connecté au monde entier

1.1.1 Les réseaux aujourd'hui

1.1.1.1 Les réseaux dans la vie quotidienne

Parmi les éléments essentiels à l'existence humaine, le besoin de communiquer arrive juste après le besoin de survie. Le besoin de communiquer est aussi important pour nous que l'air, l'eau, la nourriture et le gîte.

Les méthodes que nous utilisons pour communiquer changent et évoluent en permanence. Alors que nous avons été par le passé limités aux interactions en face à face, les innovations technologiques ont considérablement augmenté la portée de nos communications. Des peintures rupestres à la radio et la télévision, en passant par la presse écrite, chaque innovation a développé et amélioré nos possibilités de connexion et de communication avec les autres.

La création et l'interconnexion de réseaux de données fiables ont eu un impact important sur la communication et ces réseaux sont aujourd'hui une nouvelle plate-forme sur laquelle les communications modernes s'effectuent.

Aujourd'hui, grâce aux réseaux, nous sommes plus connectés que jamais. Les personnes qui ont des idées peuvent instantanément communiquer avec d'autres pour les concrétiser. Les événements et les découvertes font le tour du monde en quelques secondes. Nous pouvons nous connecter et jouer avec nos amis dans le monde entier.

Les réseaux permettent aux personnes d'entrer en relation et de communiquer de manière illimitée. Chacun peut se connecter, partager et exploiter au mieux ses opportunités.

1.1.1.2 Évolution des technologies

Imaginez un monde sans Internet. Plus de Google, de YouTube, de messagerie instantanée, de Facebook, de Wikipedia, de jeux en ligne, de Netflix, d'iTunes et d'accès facile aux informations. Plus de sites Web de comparaison de tarifs, plus de shopping en ligne, plus de recherche rapide de numéros de téléphone et d'itinéraires. Dans quelles mesures nos vies seraient-elles différentes sans toutes ces technologies ? En fait, ce serait tout simplement le monde dans lequel nous vivions il y a 15 ou 20 ans. Au fil des années, les réseaux de données se sont développés lentement et ont été redéfinis pour améliorer la qualité de vie de tous.

Au cours d'une seule journée, les ressources disponibles sur Internet peuvent vous aider à :

- publier vos photographies, vidéos personnelles et expériences et les partager avec vos amis ou avec le monde entier.
- accéder à vos devoirs et envoyer vos travaux à l'école ;
- communiquer avec vos amis, votre famille, et vos collègues par messagerie électronique, messagerie instantanée ou appels téléphoniques sur Internet ;
- visionner des vidéos, des films ou des émissions à la demande ;
- jouer sur Internet avec vos amis ;
- choisir en ligne ce que vous allez porter en fonction de la météo ;

- déterminer le trajet le moins embouteillé en visualisant les vidéos du trafic routier et les conditions météo transmises par les webcams ;
- consulter votre compte bancaire et payer vos factures en ligne.

Les innovateurs cherchent des façons d'exploiter au mieux Internet, chaque jour. Alors que les développeurs repoussent les limites du Web, les fonctionnalités d'Internet et le rôle qu'Internet joue dans nos vies se développent de plus en plus. Tenez compte des modifications qui se sont produites depuis 1995, comme indiqué dans la figure. À présent, essayez d'imaginer les modifications qui se produiront pendant les 25 prochaines années. Cet avenir inclut l'Internet of Everything (IoE).

L'IoE rassemble les personnes, les processus, les données, et les périphériques pour mettre en place les connexions réseau les plus adaptées et les plus efficaces. Il exploite les informations en créant de nouvelles fonctionnalités, des expériences plus riches et des opportunités économiques sans précédent pour les utilisateurs, les entreprises et les pays.

Que pensez-vous pouvoir faire d'autre avec le réseau en tant que plate-forme ?

1.1.1.3 La communauté internationale

Les avancées en matière de technologies réseau sont probablement les facteurs d'évolution les plus importants dans le monde actuel. Elles aident à créer un monde dans lequel les frontières, les distances et les obstacles ont de moins en moins d'impact.

Internet a changé la manière avec laquelle les interactions sociales, commerciales, politiques et personnelles se produisent. La nature instantanée des communications sur Internet encourage la création de communautés internationales

Les communautés internationales permettent des interactions sociales qui dépendent des emplacements et des fuseaux horaires. La création de communautés en ligne échangeant idées et informations peut potentiellement accroître les occasions d'améliorer la productivité sur l'ensemble du globe.

Cisco appelle cela le « réseau humain ». Le réseau humain est centré sur l'impact d'Internet et des réseaux sur les individus et les entreprises.

Comment le réseau humain vous affecte-t-il ?

1.1.1.4 Les réseaux facilitent l'apprentissage

Les réseaux et Internet ont fait évoluer notre quotidien : notre façon d'apprendre, notre façon de communiquer, notre façon de travailler et même notre façon de nous divertir.

Changer notre façon d'apprendre

La communication, la collaboration et l'engagement constituent les pierres angulaires de l'enseignement. Les institutions s'efforcent sans cesse d'améliorer ces processus afin d'optimiser la propagation des connaissances. Les méthodes d'apprentissage traditionnelles s'appuient principalement sur deux sources de connaissances pour fournir des informations aux participants : les manuels et les instructeurs. Ces deux sources sont limitées, aussi bien sur le plan du format que sur le plan de la durée des présentations.

Les réseaux ont changé notre façon d'apprendre. L'utilisation de réseaux solides et fiables encourage et enrichit l'expérience didactique des étudiants. Ces réseaux proposent des supports de formation dans de nombreux formats, notamment des exercices, des évaluations, et des commentaires interactifs. Comme l'illustre la Figure 1, les réseaux permettent aujourd'hui :

- la création de classes virtuelles ;
- la diffusion vidéo à la demande ;
- les espaces d'apprentissage collaboratifs ;
- l'apprentissage sur appareils mobiles.

Ainsi, l'accès à un enseignement de qualité n'est plus limité aux personnes résidant à proximité du lieu où l'enseignement est dispensé. L'enseignement à distance en ligne a effacé les obstacles géographiques et augmenté les opportunités. Les cours en ligne (e-learning) peuvent aujourd'hui être diffusés sur un réseau. Ces cours peuvent contenir des données (texte, liens), de l'audio et de la vidéo, disponibles pour les étudiants à tout moment, en tout lieu. Les groupes et forums de discussion en ligne permettent aux participants de collaborer avec leur formateur, avec les autres participants de leur cours et même avec ceux du monde entier. Des cours hybrides associent des leçons dispensées par des instructeurs à des cours en ligne afin d'offrir le meilleur de ces deux méthodes. La Figure 2 présente une vidéo sur les évolutions des salles de classe.

Outre les avantages qu'ils offrent aux participants, les réseaux ont également amélioré la gestion et l'administration des cours. Certaines de ces fonctions en ligne incluent l'inscription des participants, la proposition d'évaluations et le suivi de la progression.

1.1.1.5 Les réseaux facilitent la communication

Changer notre façon de communiquer

L'adoption généralisée d'Internet a entraîné la création de nouvelles formes de communication, qui permettent aux utilisateurs de créer des informations pouvant être lues par le plus grand nombre.

Voici certains types de communication :

- **Messagerie instantanée/messages texte** – la messagerie instantanée et les messages texte facilitent la communication en temps réel entre deux personnes ou plus. De nombreuses applications de messagerie instantanée et de messages texte intègrent des fonctionnalités telles que le transfert de fichiers. Les applications de messagerie instantanée peuvent proposer des fonctions supplémentaires, telles que la communication vocale et vidéo.

- **Réseaux sociaux** – les réseaux sociaux sont des sites Web interactifs où les personnes et communautés créent et partagent du contenu avec leurs amis, leur famille, leurs homologues et le monde entier.

- **Outils collaboratifs** – les outils de collaboration donnent aux utilisateurs la possibilité de travailler ensemble sur des documents partagés. Sans contraintes d'emplacement ou de fuseau horaire, les personnes connectées à un système partagé peuvent communiquer entre eux, souvent grâce à la vidéo interactive en temps réel. Sur tout le réseau, elles peuvent partager du texte et des images, puis modifier les documents ensemble. Avec des outils collaboratifs toujours disponibles, les entreprises peuvent progresser rapidement vers le partage de leurs informations et la réalisation de leurs objectifs. En raison de la large répartition des réseaux de données, les personnes résidant dans des régions reculées peuvent apporter une contribution au même titre que les personnes résidant dans de grands centres urbains.

- **Blogs** – les blogs sont des pages Web qui sont faciles à mettre à jour et à modifier. Contrairement aux sites Web commerciaux qui sont créés par des experts en communication professionnelle, les blogs permettent à n'importe qui de partager des pensées avec un public international sans avoir besoin de posséder des connaissances techniques en matière de conception Web. Il existe des blogs sur pratiquement tous les sujets possibles et imaginables et des communautés se forment souvent autour d'auteurs de blogs populaires.

- **Wikis** – les wikis sont des pages Web que des groupes de personnes peuvent modifier et consulter ensemble. Alors qu'un blog est généralement l'oeuvre d'une seule personne et s'apparente à un journal, un wiki est une création collective. De ce fait, il peut être soumis à des relectures et modifications plus poussées. Comme les blogs, les wikis peuvent être créés en plusieurs phases, par n'importe qui, sans le parrainage d'une grande entreprise commerciale. Wikipédia est devenu une ressource publique complète : une encyclopédie en ligne collaborative. Des organismes privés comme des individus peuvent également développer leurs propres wikis pour rassembler des connaissances sur un sujet particulier. De nombreuses entreprises se servent d'un wiki comme d'un outil collaboratif interne. Avec l'avènement mondial d'Internet, des personnes venues de tous horizons sont en mesure de contribuer à des wikis et d'ajouter leur point de vue et leurs connaissances personnels à une ressource partagée.

- **Podcasts -** les podcasts sont des supports audio qui permettaient initialement d'enregistrer des données audio et de les convertir. Les podcasts permettent aux individus de diffuser leurs enregistrements auprès d'un large public. Le fichier audio est placé sur un site Web (ou sur un blog ou un wiki) sur lequel des tiers peuvent le télécharger pour le lire sur leurs ordinateurs de bureau, ordinateurs portables et autres appareils mobiles.

- **Partage de fichiers en peer-to-peer (P2P)** – le partage en peer-to-peer permet de partager des fichiers sans avoir à les stocker et à les télécharger depuis un serveur central. L'utilisateur se connecte au réseau P2P en installant un logiciel P2P. Cela lui permet de localiser et de partager des fichiers avec d'autres utilisateurs sur le réseau P2P. La numérisation généralisée des fichiers multimédias, tels que la musique et les fichiers vidéo, a amélioré l'intérêt pour le partage de fichiers en peer-to-peer. Le partage de fichiers en peer-to-peer n'a cependant pas été adopté par tout le monde. De nombreuses personnes se soucient par exemple des violations des droits d'auteur.

Quels autres sites ou outils utilisez-vous pour partager vos idées ?

1.1.1.6 Les réseaux facilitent notre travail

Changer notre façon de travailler

Au début, les entreprises exploitaient les réseaux de données pour enregistrer et gérer en interne des informations financières, des renseignements sur les clients et des systèmes de paie des employés. Ces réseaux d'entreprise ont ensuite évolué pour permettre la transmission de nombreux types de service d'informations, parmi lesquels les e-mails, la vidéo, les messageries et la téléphonie.

Le recours aux réseaux en tant que moyen efficace et rentable de former les employés est de plus en plus accepté. Les opportunités de formation en ligne permettent de réduire des déplacements coûteux en termes de temps et d'argent tout en s'assurant que tous les employés sont correctement formés pour accomplir leurs tâches, et ce de façon sûre et productive.

Il existe de nombreux exemples de réussite illustrant la façon dont les réseaux sont utilisés de manière novatrice pour nous permettre d'être plus productifs sur notre lieu de travail. Plusieurs de ces scénarios sont présentés sur le site Web de Cisco, à l'adresse http://www.cisco.com.

1.1.1.7 Les réseaux facilitent le divertissement

Changer notre façon de nous divertir

L'utilisation généralisée d'Internet par l'industrie du loisir et des voyages nous offre le moyen de profiter de nombreuses formes de distraction et de les partager, où que nous nous trouvions. Des présentations interactives nous permettent aujourd'hui d'explorer des lieux dont nous devions nous contenter de rêver autrefois, ou de découvrir des destinations de voyage avant de nous y rendre. Les voyageurs peuvent publier les détails et les photos de leurs aventures en ligne pour qu'ils soient accessibles par tous.

Internet sert également à d'autres formes de divertissement. Internet nous permet d'écouter des artistes, de voir des bandes-annonces ou même des films, de lire des livres et de télécharger des éléments à consulter ultérieurement hors connexion. Des concerts et événements sportifs en direct sont disponibles au moment où ils se produisent, ou sont enregistrés pour être consultés à la demande.

Les réseaux permettent également de créer de nouvelles formes de divertissement comme les jeux en ligne. Les joueurs peuvent participer à tout type de compétitions en ligne imaginées par les concepteurs de jeux. Nous jouons avec nos amis ou affrontons des ennemis du monde entier aussi facilement que s'ils se trouvaient dans la même pièce que nous.

Même des activités réalisées hors connexion se trouvent améliorées par l'utilisation de services collaboratifs en réseau. En effet, des communautés internationales regroupées autour

de centres d'intérêt communs se sont rapidement développées. Nous partageons expériences ou passe-temps communs avec des membres de communautés bien éloignées de notre quartier, ville ou région. Les amateurs de sport échangent opinions et informations sur leurs équipes favorites. Les collectionneurs présentent les collections faisant leur fierté et reçoivent des avis d'experts.

Enfin, des sites de vente et de mise aux enchères en ligne nous offrent la possibilité d'acheter, de vendre ou d'échanger toutes sortes de marchandises.

Quel que soit le type de divertissement que nous apprécions dans notre réseau humain, il peut être amélioré par les réseaux.

Quels sont vos divertissements préférés sur Internet ?

1.1.2 Fourniture de ressources dans un réseau

1.1.2.1 Réseaux de tailles diverses

Les réseaux peuvent être de différentes tailles. Il existe des réseaux élémentaires, constitués de deux ordinateurs, mais également des réseaux extrêmement complexes, capables de connecter des millions de périphériques.

Les réseaux les plus simples permettent de partager des ressources, telles que des imprimantes, des documents, des images et de la musique, entre quelques ordinateurs locaux.

Les réseaux de bureaux à domicile et les réseaux de petits bureaux sont souvent configurés par des personnes qui travaillent à domicile ou à partir d'un bureau distant et qui doivent se connecter à un réseau d'entreprise ou à d'autres ressources centralisées. En outre, de nombreux entrepreneurs indépendants utilisent des réseaux domestiques ou des réseaux de petits bureaux pour faire la promotion et vendre leurs produits, commander des fournitures et communiquer avec les clients. Les communications transmises via un réseau sont généralement plus efficaces et plus économiques que les formes de communication classiques telles que le courrier postal ou les appels téléphoniques interurbains ou internationaux.

Dans les grandes entreprises, des réseaux de très grande envergure peuvent être utilisés pour permettre la consolidation, le stockage, ainsi que l'accès aux données sur des serveurs réseau. Les réseaux permettent également des communications rapides, par exemple grâce aux e-mails, à la messagerie instantanée et à la collaboration entre les employés. Parallèlement aux avantages internes, de nombreuses entreprises utilisent leurs réseaux pour proposer des produits et services aux clients par le biais d'Internet.

Internet est le plus grand réseau existant. En réalité, le terme « Internet » signifie « réseau de réseaux ». Internet est littéralement un ensemble de réseaux privés et publics interconnectés, tels que ceux décrits ci-dessus. Les entreprises, les réseaux de petits bureaux et même les réseaux domestiques fournissent généralement une connexion partagée à Internet.

La rapidité avec laquelle Internet s'est intégré à notre quotidien est tout simplement stupéfiante.

1.1.2.2 Clients et serveurs

Tous les ordinateurs connectés à un réseau et qui participent directement aux communications réseau sont des hôtes ou des périphériques finaux. Les hôtes peuvent envoyer et recevoir des messages sur le réseau. Dans les réseaux actuels, les périphériques finaux peuvent jouer le rôle de client, de serveur, ou les deux. Les logiciels installés sur l'ordinateur déterminent le rôle qu'il tient au sein du réseau.

Les serveurs sont des hôtes équipés des logiciels leur permettant de fournir des informations, comme des messages électroniques ou des pages Web, à d'autres hôtes sur le réseau. Chaque service nécessite un logiciel serveur distinct. Par exemple, un hôte nécessite un logiciel de serveur Web pour pouvoir offrir des services Web au réseau.

Les clients sont des ordinateurs hôtes équipés d'un logiciel qui leur permet de demander des informations auprès du serveur et de les afficher. Un navigateur Web, tel qu'Internet Explorer, est un exemple de logiciel client.

1.1.2.3 Clients et serveurs (suite)

Un ordinateur équipé d'un logiciel serveur peut fournir des services à un ou plusieurs clients en même temps.

De plus, un seul ordinateur peut exécuter différents types de logiciel serveur. Chez les particuliers et dans les petites entreprises, il peut arriver, par nécessité, qu'un ordinateur fasse office à la fois de serveur de fichiers, de serveur Web et de serveur de messagerie.

Un seul ordinateur peut également exécuter différents types de logiciel client. Un logiciel client doit être installé pour chaque type de service requis. Un hôte équipé de plusieurs clients peut se connecter à plusieurs serveurs en même temps. Par exemple, un utilisateur peut consulter sa messagerie électronique et une page Web en même temps qu'il utilise la messagerie instantanée et écoute la radio sur Internet.

1.1.2.4 Peer to peer

Le logiciel client et le logiciel serveur sont généralement exécutés sur des ordinateurs distincts, mais un seul ordinateur peut tenir simultanément ces deux rôles. Dans le cas des réseaux de particuliers et de petites entreprises, il arrive souvent que les ordinateurs fassent à la fois office de serveur et de client sur le réseau. Ce type de réseau est appelé réseau Peer to peer.

Le réseau peer-to-peer le plus simple est constitué de deux ordinateurs connectés directement à l'aide d'une connexion câblée ou sans fil.

Il est également possible d'interconnecter plusieurs PC pour créer un réseau peer-to-peer plus important, mais cela nécessite un périphérique réseau, tel qu'un concentrateur.

L'inconvénient majeur d'un environnement peer-to-peer réside dans le fait que les performances d'un hôte peuvent être amoindries s'il fait office à la fois de client et de serveur.

Dans les grandes entreprises, pour faire face aux importants volumes de trafic réseau, il arrive souvent que des serveurs soient dédiés à la prise en charge des nombreuses demandes de service.

1.2 LAN, WAN et Internet

1.2.1 Composants d'un réseau

1.2.1.1 Composants du réseau

Le chemin emprunté par un message depuis une source jusqu'à une destination peut être aussi simple que la connexion entre deux ordinateurs via un seul câble ou aussi complexe qu'un réseau parcourant le globe terrestre. L'infrastructure réseau constitue la plateforme qui prend en charge le réseau. Elle fournit le canal stable et fiable à travers lequel nos communications peuvent s'établir.

L'infrastructure réseau comprend trois catégories de composant réseau :

- Les périphériques
- Multimédia
- Les services

Cliquez sur chaque bouton de la figure pour mettre en évidence les composants réseau correspondants.

Les périphériques et les supports sont les éléments physiques, ou le matériel, du réseau. Le matériel correspond souvent aux composants visibles de la plateforme réseau, par exemple un ordinateur portable, un ordinateur de bureau, un commutateur, un routeur, un point d'accès sans fil ou le câblage qui sert à relier les périphériques. Parfois, certains composants ne sont pas visibles. Dans le cas d'un support sans fil, les messages sont transmis à travers l'air, à l'aide d'une fréquence radio ou d'ondes infrarouges invisibles.

Les composants réseau sont utilisés pour fournir des services et des processus. Les services et les processus sont les programmes de communication, appelés logiciels, qui sont exécutés sur les périphériques réseau. Un service réseau fournit des informations en réponse à une demande. Les services incluent de nombreuses applications réseau courantes utilisées quotidiennement, comme les services d'hébergement de messagerie et les services d'hébergement Web. Les processus fournissent les fonctionnalités qui dirigent et déplacent les messages à travers le réseau. Les processus nous semblent moins évidents, mais ils sont essentiels au fonctionnement des réseaux.

1.2.1.2 Périphériques finaux

Les périphériques réseau auxquels les gens sont le plus habitués sont appelés périphériques finaux, ou hôtes. Ces périphériques forment l'interface entre les utilisateurs et le réseau de communication sous-jacent.

Voici quelques exemples de périphériques finaux :

- Ordinateurs (stations de travail, ordinateurs portables, serveurs de fichiers, serveurs Web)
- Imprimantes réseau

- Téléphones VoIP
- Terminal TelePresence
- Caméras de surveillance
- Appareils mobiles (tels que les smartphones, tablettes, PDA, les lecteurs de cartes bancaires et les scanners de codes-barres sans fil)

Un périphérique hôte est la source ou la destination d'un message transmis sur le réseau, comme illustré dans l'animation. Pour qu'il soit possible de faire une distinction entre les hôtes, chaque hôte situé sur un réseau est identifié par une adresse. Lorsqu'un hôte démarre une communication, il utilise l'adresse de l'hôte de destination pour indiquer où le message doit être envoyé.

1.2.1.3 Périphériques réseau intermédiaires

Les périphériques intermédiaires relient des périphériques finaux. Ils offrent une connectivité et opèrent en arrière-plan pour s'assurer que les données sont transmises sur le réseau, comme illustré dans l'animation. Les périphériques intermédiaires connectent les hôtes individuels au réseau et peuvent connecter plusieurs réseaux individuels afin de former un interréseau.

Parmi ces périphériques réseau intermédiaires, citons :

- Accès au réseau (commutateurs et points d'accès sans fil)
- Périphériques interréseau (routeurs)
- Sécurité (pare-feu)

La gestion des données lors de leur passage à travers le réseau constitue également l'un des rôles des périphériques intermédiaires. Ces périphériques utilisent l'adresse d'hôte de destination, avec les informations concernant les interconnexions réseau, de manière à déterminer le chemin que doivent emprunter les messages à travers le réseau.

Les processus qui s'exécutent sur les périphériques du réseau intermédiaire remplissent les fonctions suivantes :

- régénérer et retransmettre des signaux de données ;
- gérer des informations indiquant les chemins qui existent à travers le réseau et l'interréseau ;
- indiquer aux autres périphériques les erreurs et les échecs de communication ;
- diriger des données vers d'autres chemins en cas d'échec de liaison ;
- classer et diriger les messages en fonction des priorités de qualité de service ;
- autoriser ou refuser le flux de données, selon des paramètres de sécurité.

1.2.1.4 Supports réseau

La communication à travers un réseau s'effectue sur un support. Ce support fournit le canal via lequel le message se déplace de la source à la destination.

Les réseaux modernes utilisent principalement trois types de supports pour interconnecter des périphériques et fournir le chemin par lequel des données peuvent être transmises. Comme l'illustre la figure, ces supports sont les suivants :

- Fils métalliques dans des câbles
- Fibres de verre ou optiques de plastique (câbles en fibre optique)
- Transmission sans fil

Le codage du signal qui doit se produire afin de transmettre le message diffère selon le type de support. Sur des fils métalliques, les données sont codées en impulsions électriques qui correspondent à des modèles spécifiques. Les transmissions par fibre optique s'effectuent via des impulsions de lumière, dans des plages de lumière infrarouges ou visibles. Dans les transmissions sans fil, des modèles d'ondes électromagnétiques illustrent les différentes valeurs de bit.

Les différents types de supports réseau possèdent divers avantages et fonctionnalités. Tous les supports réseau ne possèdent pas les mêmes caractéristiques et ne conviennent pas pour les mêmes objectifs. Les critères de choix d'un support réseau sont :

- la distance sur laquelle les supports peuvent transporter correctement un signal ;
- l'environnement dans lequel les supports doivent être installés ;
- la quantité de données et le débit de la transmission ;
- Le coût des supports et de l'installation

1.2.1.5 Représentations du réseau

Lors de la transmission d'informations complexes, par exemple l'affichage de tous les équipements et supports dans un interréseau important, il est utile d'utiliser des représentations visuelles. Un schéma constitue un moyen facile de comprendre comment les périphériques d'un grand réseau sont connectés. Un tel schéma utilise des symboles pour représenter les périphériques et les connexions qui composent un réseau. Ce type de schéma de réseau est appelé un diagramme de topologie.

Comme tout autre langage, le langage propre au réseau comprend un ensemble commun de symboles pour représenter les différents périphériques finaux, périphériques réseau et supports (voir la figure). La capacité à reconnaître les représentations logiques des composants réseau physiques est essentielle pour être en mesure de visualiser l'organisation et le fonctionnement d'un réseau. Tout au long de ce cours et des travaux pratiques, vous apprendrez le fonctionnement de ces périphériques et la réalisation de tâches de configuration de base sur ces périphériques.

En plus de ces représentations, une terminologie spécialisée est utilisée pour étudier la manière dont ces périphériques et supports se connectent entre eux. Les termes importants dont il faut se souvenir sont les suivants :

- **Carte réseau** – une carte réseau, ou adaptateur de réseau local, fournit la connexion physique au réseau à partir de l'ordinateur ou d'un autre périphérique hôte. Les supports qui relient l'ordinateur au périphérique réseau se branchent directement à la carte réseau.
- **Port physique** – connecteur ou prise sur un périphérique réseau par lequel/laquelle le support est connecté à un hôte ou à un autre périphérique réseau.
- **Interface** – ports spécifiques d'un périphérique interréseau qui se connectent à des réseaux individuels. Puisque les routeurs sont utilisés pour interconnecter des réseaux, les ports sur un routeur sont appelés interfaces réseau.

1.2.1.6 Schémas de topologie

Les diagrammes de topologie sont obligatoires pour toute personne qui travaille sur un réseau. Ils fournissent une représentation visuelle des connexions réseau.

Il existe deux types de diagrammes de topologie :

- **Diagrammes de topologie physique** – indiquent l'emplacement physique des périphériques intermédiaires, des ports configurés et des câbles.
- **Diagrammes de topologie logique** – illustrent les périphériques, les ports, et le schéma d'adressage IP.

1.2.2 LAN et WAN

1.2.2.1 Types de réseau

Les infrastructures réseau peuvent considérablement varier selon :

- la taille de la zone couverte ;
- le nombre d'utilisateurs connectés ;
- le nombre et les types de service disponibles.

La figure illustre les deux types les plus courants d'infrastructure réseau :

- **Réseau local (LAN)** - infrastructure réseau permettant d'accéder aux périphériques finaux et aux utilisateurs sur une zone peu étendue.
- **Réseau étendu (WAN)** - infrastructure réseau permettant d'accéder à d'autres réseaux sur une vaste zone.

Autres types de réseau :

- **Réseau métropolitain (MAN)** - infrastructure réseau qui couvre une zone plus vaste qu'un LAN, mais moins étendue qu'un WAN (par exemple, une ville). Les MAN sont généralement gérés par une seule entité, comme une grande entreprise.
- **LAN sans fil (WLAN)** - infrastructure similaire à un réseau local, mais sans fil. Elle relie des utilisateurs et des terminaux situés dans une zone peu étendue.
- **Réseau de stockage SAN** - infrastructure réseau conçue pour prendre en charge des serveurs de fichiers et pour fournir des fonctionnalités de stockage, de récupération et de réplication de données. Cette infrastructure comprend des serveurs haut de gamme, plusieurs baies de disques (appelées blocs) et utilise la technologie d'interconnexion Fibre Channel.
-

1.2.2.2 Réseaux locaux

Un réseau local (LAN) est une infrastructure réseau qui couvre une zone peu étendue. Les fonctionnalités spécifiques offertes par les LAN sont les suivantes :

- Les LAN relient des périphériques finaux dans une zone limitée telle qu'une maison, une école, un bureau ou un campus.
- En règle générale, un réseau local est administré par une seule entreprise ou une seule personne. Le contrôle administratif qui gère les stratégies de sécurité et de contrôle d'accès s'applique au niveau du réseau.

- Le réseau local fournit une bande passante très élevée aux périphériques finaux et aux périphériques intermédiaires internes.

1.2.2.3 Réseaux étendus

Un réseau étendu (WAN) est une infrastructure réseau qui couvre une zone étendue. Les réseaux étendus sont généralement gérés par des fournisseurs de services ou des fournisseurs d'accès Internet (FAI).

Les fonctionnalités spécifiques offertes par les WAN sont les suivantes :

- Les WAN relient des LAN sur des zones étendues comme plusieurs villes, des États, des provinces, des pays ou des continents.
- Les WAN sont habituellement gérés par plusieurs fournisseurs de services.
- Les réseaux WAN fournissent généralement des liaisons à plus bas débit entre les réseaux locaux.

1.2.3 Internet

1.2.3.1 Internet

Bien qu'il existe des avantages à utiliser un réseau LAN ou WAN, la plupart des utilisateurs doivent communiquer avec des ressources situées sur un autre réseau, en dehors du réseau local du domicile, du campus ou de l'entreprise. Cela est effectué via Internet.

Comme l'illustre la figure, Internet est un ensemble mondial de réseaux interconnectés (interréseaux ou « Internet ») qui coopèrent pour échanger des informations en utilisant des normes courantes. Les fils téléphoniques, fibres optiques, transmissions sans fil et liaisons satellites permettent aux utilisateurs d'Internet d'échanger des informations sous diverses formes.

Internet est un ensemble de réseaux dont personne n'est propriétaire. Garantir une communication efficace sur cette infrastructure diverse implique l'application de technologies et de normes cohérentes et communément reconnues, ainsi que la coopération entre de nombreux organismes gouvernementaux. Certains organismes ont été créés pour gérer la structure et la normalisation des protocoles et des processus Internet. Ces organismes incluent l'Internet Engineering Task Force (IETF), l'Internet Corporation for Assigned Names and Numbers (ICANN) et l'Internet Architecture Board (IAB), entre autres.

1.2.3.2 Intranet et extranet

Il existe deux autres termes similaires au terme Internet :

- Intranet
- Extranet

Le terme intranet est souvent utilisé pour faire référence à un réseau LAN privé qui appartient à une entreprise ou une administration et auquel peuvent accéder uniquement ses membres, ses employés ou des tierces personnes autorisées. Un intranet est un interréseau qui n'est généralement accessible que depuis le site d'une entreprise.

Les entreprises peuvent publier sur un intranet des pages Web sur les événements internes, les politiques de santé et de sécurité, des lettres d'information destinées au personnel et un

répertoire téléphonique du personnel. Par exemple, une école peut mettre en place un intranet qui inclut des informations sur les programmes de cours, le cursus en ligne et des forums de discussion. Un intranet permet généralement d'éliminer certains documents papier et d'accélérer les workflows. Un intranet peut être utilisé par le personnel travaillant en dehors du site de l'entreprise grâce à des connexions sécurisées au réseau interne.

Une entreprise peut utiliser un extranet pour fournir un accès sécurisé aux personnes qui travaillent pour d'autres entreprises, mais qui ont besoin des données de l'entreprise en question. Voici des exemples d'extranets :

- Une société fournit un accès à des fournisseurs/sous-traitants externes.
- Un hôpital propose un système pour que les médecins puissent planifier les rendez-vous avec leurs patients.
- Un bureau local de formation fournit des informations sur le budget et le personnel aux écoles de la région.

1.2.4 Connexion à Internet

1.2.4.1 Technologies d'accès internet

Il existe plusieurs manières de connecter des utilisateurs et des entreprises à Internet.

Les utilisateurs à domicile, les télétravailleurs (travailleurs à domicile) et les PME ont généralement besoin d'un fournisseur d'accès Internet (FAI) pour se connecter à Internet. Les options de connexion varient considérablement d'un FAI et d'une région à l'autre. Cependant, les options les plus utilisées sont le câble haut débit, la DSL haut débit, les WAN sans fil et les services mobiles.

Les entreprises ont généralement besoin d'un accès aux autres sites professionnels et à Internet. Des connexions rapides sont requises pour prendre en charge les services d'entreprise, notamment les téléphones IP, la vidéoconférence, ainsi que les data centers.

Les connexions professionnelles sont généralement fournies par des fournisseurs de services. Les services professionnels les plus courants sont la DSL, les lignes louées et les solutions Metro Ethernet.

1.2.4.2 Connexion des utilisateurs distants à Internet

La figure ci-contre illustre les options de connexion courantes pour les utilisateurs de petits bureaux et de bureaux à domicile :

- **Câble** – généralement proposé par les fournisseurs de services de télévision par câble, le signal de données Internet est transmis grâce au câble coaxial utilisé pour la télévision par câble. Il offre une connexion permanente à Internet haut débit. Un modem câble spécial sépare le signal Internet des autres signaux transmis sur le câble et fournit une connexion Ethernet à un ordinateur hôte ou à un LAN.

- **DSL** – offre une connexion permanente à Internet haut débit. La ligne DSL utilise un modem spécifique haut débit, qui sépare le signal DSL du signal téléphonique et fournit une connexion Ethernet à un ordinateur hôte ou à un LAN. La DSL fonctionne sur une ligne téléphonique divisée en trois canaux. Un canal est utilisé pour les appels

téléphoniques. Ce canal permet à une personne de recevoir des appels sans se déconnecter d'Internet. Un deuxième canal de téléchargement, plus rapide, est utilisé pour recevoir des informations depuis Internet. Le troisième canal est utilisé pour envoyer des informations. Ce canal est généralement légèrement moins performant que le canal de téléchargement. La qualité et la vitesse de la connexion DSL dépendent essentiellement de la qualité de la ligne téléphonique et de la distance du central de la compagnie de téléphone. Plus vous êtes éloigné du central, plus la connexion est lente.

- **Cellulaire** – l'accès Internet cellulaire utilise un réseau de téléphonie mobile. Partout où vous captez un signal cellulaire, vous pouvez accéder à Internet. Les performances sont cependant limitées par les fonctionnalités du téléphone et de la station de base à laquelle l'appareil est connecté. La disponibilité de l'accès Internet cellulaire constitue un réel avantage dans les régions qui n'ont aucune autre possibilité d'accéder à Internet ou pour les utilisateurs constamment en déplacement.

- **Satellite** – le service par satellite est l'option idéale pour les maisons ou les bureaux qui n'ont pas accès à la DSL ou au câble. Les paraboles nécessitent une visibilité directe sur le satellite et peuvent ne pas fonctionner convenablement dans des zones boisées ou des emplacements entourés d'éléments faisant obstacle aux transmissions. Les débits dépendent du contrat choisi, mais sont en général élevés. Les frais liés au matériel et à l'installation peuvent être élevés (même si les fournisseurs peuvent proposer des promotions), et un forfait mensuel est ensuite mis en place. La disponibilité de l'accès Internet par satellite constitue un réel avantage dans les régions qui n'ont aucune autre possibilité d'accéder à Internet.

- **Ligne commutée** – option peu onéreuse nécessitant une ligne téléphonique et un modem. Pour se connecter au FAI, l'utilisateur appelle le numéro de téléphone d'accès du FAI. La faible bande passante des connexions par ligne commutée n'est généralement pas suffisante pour les transferts de données importants, mais cette solution reste utile pour accéder à Internet lors d'un déplacement. Il ne faut opter pour une connexion par ligne commutée que lorsque les autres options de connexion haut débit ne sont pas disponibles.

Les habitations et les petits bureaux sont de plus en plus connectés directement à Internet par le biais de la fibre optique. Cette infrastructure permet à un fournisseur d'accès Internet de fournir une bande passante très élevée et de prendre en charge plus de services tels qu'Internet, le téléphone et la télévision.

Le choix de la connexion dépend de l'emplacement géographique et de la disponibilité du fournisseur d'accès.

Quelles sont les différentes solutions de connexion à Internet ?

1.2.4.3 Connexion d'une entreprise à Internet

Les options de connexion d'une entreprise sont différentes des options disponibles pour les réseaux à domicile. Les entreprises peuvent nécessiter une bande passante plus élevée, une bande passante spécialisée et des services gérés. Les options de connexion disponibles varient en fonction du nombre de fournisseurs d'accès situés à proximité.

La figure ci-contre illustre les options de connexion courantes pour les entreprises :

- **Ligne louée spécialisée** – connexion dédiée du fournisseur de services sur le site du client. Les lignes louées sont des circuits dédiés qui relient des bureaux distincts pour la transmission de données et/ou de communications vocales privées. Les circuits sont généralement loués sur une base mensuelle ou annuelle, ce qui rend cette solution onéreuse. En Amérique du Nord, les circuits de ligne louée incluent généralement le T1 (1,54 Mbit/s) et le T3 (44,7 Mbit/s), tandis que dans d'autres parties du monde, l'E1 (2 Mbit/s) et l'E3 (34 Mbit/s) sont proposés.

- **Metro Ethernet** – solution généralement fournie par un fournisseur au client par le biais d'une connexion dédiée par câble en cuivre ou par fibre, offrant un débit de 10 Mbit/s à 10 Gbit/s. L'Ethernet over Copper (EoC, Ethernet sur cuivre) est plus économique que le service Ethernet sur fibre optique dans de nombreux cas, est très largement disponible et vous permet d'atteindre des débits de 40 Mbit/s. Cependant, cette solution est limitée en termes de distance. Le service Ethernet sur fibre optique assure les connexions les plus rapides à un prix réduit par mégabit. Malheureusement, il reste encore beaucoup de zones où ce service n'est pas disponible.

- **DSL** – la DSL est disponible dans divers formats. La SDSL (ligne d'abonné numérique à débit symétrique) est largement utilisée. Cette solution est similaire à une ligne ADSL (ligne d'abonné numérique à débit asymétrique), mais présente les mêmes débits ascendant et descendant. L'ADSL est conçue pour fournir une bande passante dont les débits ascendant et descendant sont différents. Par exemple, un client utilisant un accès Internet peut obtenir des débits descendants allant de 1,5 à 9 Mbit/s et des débits ascendants allant de 16 à 640 kbit/s. Les transmissions ADSL fonctionnent à une distance maximale de 5 488 mètres sur un seul câble à paires torsadées en cuivre.

- **Satellite** – le service par satellite peut fournir une connexion lorsqu'aucune solution par câble n'est disponible. Les paraboles nécessitent une visibilité directe sur le satellite. Les frais liés au matériel et à l'installation peuvent être élevés, et un forfait mensuel est ensuite mis en place. Ces connexions ont tendance à être plus lentes et moins fiables que les connexions terrestres, ce qui les rend moins intéressantes que les autres solutions.

Le choix de la connexion dépend de l'emplacement géographique et de la disponibilité du fournisseur d'accès.

1.3 Réseau en tant que plateforme

1.3.1 Réseaux convergents

1.3.1.1 Réseau convergent

Les réseaux modernes sont en constante évolution pour répondre aux exigences des utilisateurs. Si les premiers réseaux de données se limitaient à échanger des informations reposant sur des caractères entre des systèmes informatiques connectés, Les réseaux téléphoniques, radio et de télévision traditionnels ont été gérés séparément des réseaux de données. Auparavant, chacun de ces services nécessitait un réseau dédié, avec des canaux de communication différents et des technologies différentes pour transmettre un signal de communication particulier. Chaque service avait son propre ensemble de règles et de normes, destiné à garantir les communications.

Imaginez une école construite il y a quarante ans. À cette époque, les classes étaient reliées au réseau de données, au réseau téléphonique et au réseau de télévision. Ces réseaux distincts étaient disparates, ce qui signifie qu'ils ne pouvaient pas communiquer entre eux, comme illustré à la Figure 1.

Les progrès technologiques nous permettent aujourd'hui de regrouper ces différents types de réseau sur une plate-forme appelée « réseau convergent ». Contrairement aux réseaux spécialisés, les réseaux convergents peuvent transmettre des sons, des flux vidéo, du texte et des images entre différents types d'appareil, par le biais d'un même canal de communication et d'une même structure réseau, comme illustré à la Figure 2. Des moyens de communication autrefois séparés et bien distincts convergent maintenant sur une plateforme commune. Cette plateforme offre une large gamme de méthodes de communication aussi nouvelles que différentes qui permettent aux individus d'interagir directement, et presque instantanément.

Sur un réseau convergent, il existe encore beaucoup de points de contact et de périphériques spécialisés, comme des ordinateurs, des téléphones, des télévisions et des tablettes, mais il existe une infrastructure réseau commune. Cette infrastructure réseau utilise le même ensemble de règles, de contrats et de normes de mise en œuvre.

1.3.1.2 Planification en prévision de l'avenir

La convergence des différents types de réseaux de communication sur une seule plateforme représente la première phase de l'avènement du réseau d'information intelligent. Nous nous trouvons actuellement dans la phase d'évolution du réseau. La phase suivante sera celle de la consolidation des différents types de message sur un réseau unique, mais également celle des applications générant, transmettant et sécurisant les messages sur des périphériques réseau intégrés.

Non seulement il sera possible de transmettre les éléments audio et vidéo sur le même réseau, mais les périphériques effectuant la commutation téléphonique et la diffusion vidéo seront également ceux qui routent les messages sur le réseau. La plateforme de communication ainsi obtenue offrira des fonctionnalités applicatives de haute qualité pour un coût réduit.

L'extraordinaire vitesse à laquelle de nouvelles applications de réseau convergent prometteuses apparaissent peut s'expliquer par le rapide développement d'Internet. Avec seulement environ 10 milliards d'appareils connectés sur 1,5 trillion d'appareils au total, il existe un potentiel important pour l'IoE. Le public potentiel est donc aujourd'hui très important, quel que soit le message, le produit, ou le service qui peut être fourni.

Les mécanismes et processus sous-jacents qui guident cette croissance exponentielle ont entraîné la création d'une architecture réseau pouvant s'adapter aux évolutions et se développer. Du fait de son rôle de plateforme technologique de prise en charge du mode de vie, d'apprentissage, de travail et de divertissement des hommes, l'architecture réseau d'Internet doit s'adapter à des exigences toujours nouvelles en matière de services et de sécurité.

1.3.2 Réseau fiable

1.3.2.1 Architecture prenant en charge le réseau

Les réseaux doivent prendre en charge une large gamme d'applications et de services, et fonctionner sur de nombreux types de câble et de périphérique, qui constituent l'infrastructure physique. Dans le contexte actuel, l'expression « architecture réseau » désigne aussi bien les technologies prenant en charge l'infrastructure que les services programmés et les règles, ou protocoles, qui font transiter les messages sur le réseau.

Alors que les réseaux évoluent, nous découvrons que les architectures sous-jacentes doivent prendre en considération quatre caractéristiques de base si elles veulent répondre aux attentes des utilisateurs :

- Tolérance aux pannes (Figure 1)
- Évolutivité (Figure 2)
- Qualité de service (QS) (Figure 3)
- Sécurité (Figure 4)

1.3.2.2 Tolérance aux pannes sur les réseaux à à commutation de circuits

Tolérance aux pannes

L'objectif est qu'Internet soit toujours disponible pour ses millions d'utilisateurs. Cela nécessite une architecture réseau conçue pour être tolérante aux pannes. Un réseau tolérant aux pannes est un réseau qui limite l'impact des pannes, de sorte que le plus petit nombre de périphériques possible soit affecté par ces dernières. Il est également conçu de façon à permettre une récupération rapide en cas de panne. De tels réseaux s'appuient sur plusieurs chemins entre la source et la destination d'un message. Si l'un des chemins est défaillant, le message peut instantanément être envoyé par le biais d'une autre liaison. Le fait de disposer de plusieurs chemins vers une destination s'appelle la redondance.

Réseaux à commutation de circuits orientés connexion

Pour comprendre le besoin de redondance, nous pouvons analyser comment fonctionnaient les premiers systèmes téléphoniques. Lorsqu'une personne passait un appel en utilisant un téléphone traditionnel, l'appel passait tout d'abord par un processus de configuration. Ce processus consistait à détecter les centraux de commutation situés entre la personne effectuant l'appel (la source) et le téléphone recevant l'appel (destination). Un chemin, ou circuit temporaire, était créé pendant toute la durée de l'appel téléphonique. En cas de défaillance d'une liaison ou d'un périphérique, l'appel était interrompu. Pour rétablir la connexion, un nouvel appel devait être effectué, en utilisant un nouveau circuit. Cette procédure de connexion est appelée « processus de commutation de circuits » et est illustrée ci-contre.

De nombreux réseaux à commutation de circuits donnent la priorité au maintien des connexions sur les circuits existants aux dépens des requêtes de nouveaux circuits. Une fois qu'un circuit a été établi, il demeure connecté même si aucune communication n'a lieu entre les personnes à chaque extrémité de l'appel, et les ressources sont réservées jusqu'à ce que l'une des parties mette fin à l'appel. Étant donné que le nombre de circuits pouvant être créés est limité, il est possible d'obtenir un message indiquant que tous les circuits sont occupés et

qu'un appel ne peut aboutir. Les coûts liés la création de nombreux chemins alternatifs avec une capacité suffisante pour prendre en charge un grand nombre de circuits simultanés, combinés aux technologies nécessaires pour recréer dynamiquement les circuits rejetés en cas de panne, expliquent pourquoi la technologie de commutation de circuits n'était pas optimale pour Internet.

1.3.2.3 Tolérance aux pannes dans les réseaux à commutation de paquets

Réseaux à commutation de paquets

Dans le cadre de leur recherche d'un réseau tolérant aux pannes, les premiers concepteurs d'Internet ont étudié les réseaux à commutation de paquets. Le principe de ce type de réseaux est qu'un message peut être scindé en plusieurs blocs, chacun de ces blocs contenant les informations d'adressage indiquant l'origine et la destination finale du message. Grâce à ces informations intégrées, les blocs de message, appelés paquets, peuvent être envoyés sur le réseau en empruntant des chemins variés avant d'être réassemblés pour recomposer le message d'origine une fois parvenus à destination (voir la figure).

Les périphériques du réseau ne connaissent en général pas le contenu des paquets individuels. Seules les adresses de la source et de la destination finale sont visibles. Ces adresses sont souvent appelées adresses IP, exprimées en notation décimale (par exemple, 10.10.10.10). Chaque paquet est envoyé d'un emplacement à un autre de façon indépendante. À chaque emplacement, une décision de routage est prise pour déterminer le chemin qui sera emprunté pour transmettre le paquet vers sa destination finale. Cela revient en fait à envoyer un long message à un ami en utilisant dix cartes postales. Chaque carte postale comporte l'adresse du destinataire. Lorsque les cartes postales sont transférées par la poste, l'adresse de destination est utilisée pour déterminer le chemin que la carte postale doit suivre. Par la suite, les cartes sont acheminées vers l'adresse indiquée.

Si un chemin précédemment utilisé n'est plus disponible, la fonction de routage peut choisir dynamiquement le meilleur chemin suivant disponible. Comme les messages sont fragmentés au lieu d'être envoyés sous forme de message unique complet, il est possible de retransmettre via un chemin différent les quelques paquets qui pourraient s'être perdus. Dans bien des cas, le périphérique de destination ignore les défaillances ou modifications de routages qui sont intervenues. Pour revenir à notre exemple de cartes postales, si l'une des cartes postales est perdue le long du chemin, seule cette carte postale doit être renvoyée.

Dans ce type de réseau, il est inutile de réserver un circuit unique de bout en bout. Chaque morceau du message peut être envoyé sur le réseau par l'intermédiaire de n'importe quel chemin disponible. De plus, des paquets contenant des morceaux de messages provenant de sources différentes peuvent emprunter simultanément le réseau. Parce qu'il permet d'utiliser dynamiquement des chemins redondants sans intervention de l'utilisateur, Internet est devenu un moyen de communication tolérant aux pannes. Dans notre exemple utilisant des cartes postales, comme celles-ci transitent par le système postal, elles utilisent le même réseau que d'autres cartes postales, lettres et paquets. Par exemple, l'une des cartes postales peut être transportée en avion, avec beaucoup d'autres colis et lettres qui sont acheminés vers leur destination finale.

Bien que les réseaux à commutation de paquets sans connexion soient l'infrastructure de base d'Internet aujourd'hui, un système orienté connexion comme le système téléphonique à

commutation de circuits peut présenter des avantages. Étant donné que les ressources des divers emplacements de commutation ont pour vocation de fournir un nombre précis de circuits, la qualité et la cohérence des messages transmis sur un réseau orienté connexion peuvent être garanties. En outre, le fournisseur du service peut facturer la période de temps pendant laquelle la connexion est active aux utilisateurs du réseau, ce qui est un autre avantage. Pouvoir facturer aux utilisateurs les connexions actives sur le réseau est un élément essentiel de l'industrie des services de télécommunication.

1.3.2.4 Réseaux évolutifs

Évolutivité

Chaque semaine, des milliers de nouveaux utilisateurs et fournisseurs de services se connectent à Internet. Pour qu'Internet puisse supporter cette croissance rapide, il doit être évolutif. Un réseau évolutif est en mesure de s'étendre rapidement afin de prendre en charge de nouveaux utilisateurs et applications sans que cela n'affecte les performances du service fourni aux utilisateurs existants. Les figures ci-contre illustrent la structure d'Internet.

Si Internet est capable de s'étendre au rythme que nous connaissons sans que ceci n'ait d'impact sérieux sur ses performances au niveau des utilisateurs individuels, c'est grâce à la conception des protocoles et des technologies sous-jacentes sur lesquels il repose. Internet dispose d'une structure en couches hiérarchisée pour l'adressage, l'attribution de noms et pour les services de connectivité. En conséquence, le trafic réseau destiné à des services locaux ou régionaux n'a pas besoin de transiter par un point central pour être distribué. Les services communs peuvent être dupliqués dans différentes régions, ce qui écarte le trafic des réseaux fédérateurs de niveau supérieur.

L'évolutivité correspond également à la possibilité d'accepter de nouveaux produits et de nouvelles applications. Bien qu'Internet ne soit pas régulé par une organisation unique, les nombreux réseaux individuels qui assurent la connectivité d'Internet collaborent et respectent des normes et protocoles établis. Le respect de ces normes permet aux fabricants de matériel et de logiciels de se concentrer sur le développement de leurs produits ainsi que sur l'amélioration des performances et de la capacité, en sachant que les nouveaux produits pourront s'intégrer à l'infrastructure existante et l'améliorer.

En dépit de sa grande évolutivité, l'architecture actuelle d'Internet ne sera peut-être pas toujours en mesure de suivre le rythme de la demande des utilisateurs. De nouveaux protocoles et structures d'adressage sont en cours de développement pour faire face au rythme toujours plus rapide auquel de nouveaux services et applications Internet sont ajoutés.

1.3.2.5 Qualité de service (QS)

QS (qualité de service)

La qualité de service (QS) est une exigence de plus en plus répandue qui repose sur les réseaux actuels. Les nouvelles applications disponibles via des interréseaux, telles que les applications de communication vocale et vidéo en direct (voir la Figure 1), entraînent des attentes plus poussées en termes de qualité des services fournis. Avez -vous déjà tenté de visionner une vidéo saccadée ?

Les réseaux doivent fournir des services prévisibles, mesurables et, parfois, garantis. L'architecture réseau à commutation de paquets ne garantit pas que tous les paquets composant un message particulier arriveront à temps, dans l'ordre voulu, ni même qu'ils arriveront.

Les réseaux ont également besoin de processus leur permettant de gérer l'encombrement du réseau. La bande passante d'un réseau est la mesure de sa capacité à transporter de données. En d'autres termes, quelle quantité de données peut être transmise en un temps donné ? La bande passante réseau est mesurée en bits pouvant être transmis en une seconde, soit en « bits par seconde » (bit/s). Lorsque plusieurs communications sont initiées simultanément sur le réseau, la demande de bande passante peut excéder la quantité disponible, créant ainsi un encombrement du réseau. Le réseau a simplement plus de bits à transmettre que ce que la bande passante du canal de communication peut prendre en charge.

Dans la plupart des cas, lorsque le volume de paquets est supérieur au volume pouvant être transporté sur le réseau, les périphériques placent les paquets en file d'attente dans la mémoire en attendant que des ressources se libèrent (voir la Figure 2). La mise en file d'attente des paquets entraîne des retards, car les nouveaux paquets ne peuvent pas être transmis avant que les paquets précédents ne soient traités. Si le nombre de paquets devant être placés en file d'attente continue à augmenter, les files d'attente dans la mémoire se remplissent et des paquets sont abandonnés.

Assurer le niveau de qualité de service (QS) requis en gérant les retards et les paramètres de perte de paquets sur un réseau devient la clé du succès d'une solution destinée à garantir la qualité d'une application de bout en bout. L'une des méthodes permettant d'y parvenir est la classification. Pour créer des classifications de qualité de service pour les données, il faut se baser sur les caractéristiques des communications et sur l'importance relative affectée à l'application (voir la Figure 3). Toutes les données appartenant à la même classe sont ensuite traitées selon les mêmes règles. Par exemple, une communication pour laquelle la vitesse d'acheminement est importante, telle qu'une communication vocale, est classée différemment d'une communication qui peut tolérer les retards, telle qu'un transfert de fichiers.

Dans une entreprise, il faut établir des priorités. Par exemple :

- **les communications pour lesquelles la vitesse d'acheminement est importante** – augmenter la priorité des services tels que la téléphonie ou la distribution vidéo ;
- **les communications pour lesquelles la vitesse d'acheminement n'est pas importante** – réduire la priorité du téléchargement des pages Web ou des e-mails ;
- **les communications revêtant une grande importance pour l'entreprise** – accroître la priorité des données de contrôle de la production ou de transactions commerciales ;
- les **communications indésirables** (réduire leur priorité ou bloquer les activités indésirables, comme le partage de fichiers en peer-to-peer ou la transmission multimédia en continu).

1.3.2.6 Assurer la sécurité du réseau

Sécurité

Autrefois simple interréseau d'organisations éducatives et gouvernementales strictement contrôlées, Internet a évolué pour devenir un moyen de transmission de communications professionnelles et personnelles largement accessible. Les exigences du réseau en matière de sécurité ont donc évidemment changé. L'infrastructure réseau, les services et les données

contenus dans les périphériques reliés au réseau sont des ressources personnelles et professionnelles essentielles. Compromettre l'intégrité de ces ressources pourrait avoir de graves conséquences, notamment :

- des pannes du réseau qui empêchent les communications et les transactions, entraînant donc une perte d'activité ;
- le vol d'éléments de propriété intellectuelle (idées de recherche, brevets ou dessins de conception) ensuite utilisés par un concurrent ;
- la divulgation ou la compromission de données personnelles ou privées sans le consentement des utilisateurs ;
- une mauvaise utilisation ou une perte de fonds personnels ou de l'entreprise ;
- la perte de données importantes, très difficiles à remplacer ou irremplaçables.

Deux aspects de la sécurité réseau doivent être pris en compte : la sécurité de l'infrastructure réseau et la protection des données.

Sécuriser l'infrastructure réseau implique de sécuriser matériellement les périphériques qui assurent la connectivité réseau et d'empêcher tout accès non autorisé aux logiciels de gestion qu'ils hébergent.

Sécuriser les données consiste à protéger les informations contenues dans les paquets transmis sur le réseau, ainsi que les informations stockées sur des périphériques reliés au réseau. Les mesures de sécurité prises sur un réseau doivent :

- Empêcher la divulgation d'informations confidentielles
- Éviter le vol d'informations (Figure 1)
- Empêcher toute modification non autorisée des informations
- Empêcher les dénis de service (DoS)

Pour atteindre ces objectifs de sécurité réseau, il faut respecter trois exigences, comme illustré à la Figure 2 :

- **Assurer la confidentialité** : garantir la confidentialité des données consiste à limiter l'accès aux données aux destinataires autorisés (individus, processus ou périphériques). Pour cela, il est nécessaire de disposer d'un système fiable d'authentification des utilisateurs, qui met en place des mots de passe difficile à deviner et demande aux utilisateurs de les modifier fréquemment. Le chiffrement des données, qui fait en sorte que seul le destinataire autorisé peut accéder aux informations, fait également partie des mesures de confidentialité.
- **Garantir l'intégrité des données** : garantir l'intégrité des données consiste à veiller à ce que les informations ne soient pas modifiées lors de leur transmission de leur point d'origine à leur destination. L'intégrité des données peut être compromise quand des informations ont été corrompues (sciemment ou accidentellement). L'intégrité des données est garantie en exigeant la validation de l'expéditeur et en utilisant des mécanismes permettant de vérifier que le paquet n'a pas été modifié pendant la transmission.
- **Assurer la disponibilité** : garantir la disponibilité consiste à veiller à ce que les utilisateurs autorisés puissent accéder en temps voulu et de façon fiable aux services de données. Les pare-feu matériels d'un réseau, ainsi que les logiciels antivirus pour ordinateurs et pour serveurs, peuvent garantir la fiabilité et la protection du système afin de détecter, d'empêcher et de repousser les attaques. L'élaboration d'infrastructures réseau entièrement redondantes, avec peu de points d'échec uniques, peut réduire l'impact de ces menaces.

1.4 Évolution de l'environnement réseau

1.4.1 Tendances relatives au réseau

1.4.1.1 Nouvelles tendances

Lorsque vous examinez l'impact d'Internet sur nos tâches quotidiennes, il est difficile de croire que cet outil n'est disponible que depuis 20 ans pour le grand public. Internet a vraiment transformé la façon dont les individus et les entreprises communiquent. Par exemple, avant qu'Internet ne se démocratise, les grandes entreprises et les PME s'appuyaient principalement sur le marketing papier pour informer les consommateurs sur leurs produits. Il était difficile pour elles de savoir quels ménages étaient des clients potentiels : il leur fallait donc imprimer en masse leurs documents de marketing. Ces campagnes de communication étaient chères et leurs résultats incertains. Comparez cela à la manière dont les consommateurs sont informés aujourd'hui. La plupart des entreprises sont présentes sur Internet : les consommateurs peuvent obtenir des informations sur les produits, lire les commentaires d'autres clients et commander des produits directement sur le site Web. Les réseaux sociaux collaborent avec les entreprises pour la promotion des produits et services. Les blogueurs travaillent en partenariat avec les entreprises pour mettre en avant et promouvoir des produits et services. La majeure partie de ce placement de produits est destinée aux consommateurs potentiels, plutôt qu'à un grand nombre de personnes au hasard. La Figure 1 présente plusieurs prévisions relatives à Internet pour ces prochaines années.

Comme de nouvelles technologies et de nouveaux périphériques sont disponibles sur le marché, les entreprises et les consommateurs doivent continuer à s'adapter à cet environnement en constante évolution. Le rôle du réseau est de se transformer pour permettre aux personnes et aux périphériques d'échanger des informations. Il existe plusieurs nouvelles tendances relatives au réseau, qui affecteront les entreprises et les clients. Les plus répandues incluent :

- « Tous les périphériques, tous les contenus, toutes les méthodes de connexion »
- La collaboration en ligne
- Vidéos
- Le cloud computing

Ces tendances sont interdépendantes et continueront à se développer ces prochaines années, les unes se basant sur les autres. Les deux prochains sujets couvriront ces tendances plus en détail.

Cependant, gardez à l'esprit que des nouvelles tendances naissent et sont conceptualisées chaque jour. Comment pensez-vous qu'Internet va évoluer ces 10 prochaines années ? Ces 20 prochaines années ? La Figure 2 est une vidéo présentant certaines des réflexions de Cisco concernant les prochaines évolutions des réseaux.

1.4.1.2 BYOD

Le BYOD (Bring Your Own Device)

Le concept de « tous les périphériques, tous les contenus et toutes les méthodes de connexion » est une tendance majeure qui nécessite des modifications importantes au niveau de l'utilisation des périphériques. Cette tendance est appelée « Bring Your Own Device » (BYOD).

Le BYOD consiste à offrir aux utilisateurs finaux la liberté d'utiliser leurs propres outils pour accéder aux informations et communiquer au sein d'une entreprise ou d'un réseau de campus. Avec la croissance des appareils personnels et la réduction de leur coût, les employés et les étudiants peuvent disposer des meilleurs outils informatiques et de réseau pour leur usage personnel. Ces outils personnels incluent notamment des ordinateurs portables, des netbooks, des tablettes, des smartphones et des liseuses. Il peut s'agir de périphériques achetés par l'entreprise ou l'école, achetés par l'utilisateur, ou dont le coût a été partagé.

Le BYOD, c'est pour n'importe quel appareil, quel que soit son propriétaire, n'importe où. Par exemple, dans le passé, un étudiant qui avait besoin d'accéder au réseau du campus ou à Internet devait utiliser l'un des ordinateurs de l'école. Ces périphériques sont généralement limités et considérés comme des outils réservés au travail en classe ou à la bibliothèque. Une connectivité étendue grâce à l'accès mobile et à l'accès à distance au réseau du campus donne aux étudiants plus de flexibilité et d'opportunités d'apprentissage.

Le BYOD est une tendance importante, qui concerne ou concernera tous les services informatiques.

1.4.1.3 Collaboration en ligne

Collaboration en ligne

Les gens souhaitent se connecter au réseau, non seulement pour accéder aux applications de données, mais également pour travailler ensemble. La collaboration est définie comme « le fait de travailler avec une ou plusieurs autres personnes sur un projet commun ».

Pour les entreprises, la collaboration est une priorité vitale et stratégique. Pour rester compétitives, les entreprises doivent répondre à trois questions principales relatives à la collaboration :

- Comment peut-on faire en sorte que tout le monde soit sur la même longueur d'onde ?
- Disposant de budgets et d'un personnel réduits, comment peut-on répartir nos ressources pour qu'elles soient disponibles partout en même temps ?
- Comment peut-on continuer d'organiser des réunions en face à face étant donné la croissance du réseau de collègues, de clients, de partenaires et d'homologues dans un environnement qui dépend de plus en plus de la connectivité 24 h/24 ?

La collaboration est également une priorité au niveau de la formation. Les étudiants doivent collaborer pour s'aider les uns les autres durant leur formation, développer des compétences d'équipe nécessaires pour leurs prochains postes et travailler ensemble sur des projets d'équipe.

Un moyen de répondre à ces questions et à ces exigences dans le contexte actuel est d'utiliser les outils de collaboration en ligne. Dans les espaces de travail traditionnels, tout comme dans les environnements BYOD, les personnes exploitent des services de communication vocale, vidéo et de conférence sécurisés dans une optique collaborative.

La possibilité de collaborer en ligne modifie les processus métier. Les nouveaux outils de collaboration permettent aux employés de collaborer rapidement et facilement, indépendamment de leur emplacement physique. Les entreprises peuvent s'organiser de manière plus flexible. Les utilisateurs ne rencontrent plus de limitations liées à leur emplacement physique. Il est plus facile d'accéder à des informations très précises. Les

évolutions de la collaboration permettent aux entreprises d'améliorer la collecte d'informations, l'innovation et la productivité. La figure ci-contre présente quelques-uns des avantages de la collaboration en ligne.

Les outils de collaboration permettent aux employés, aux étudiants, aux enseignants, aux clients et aux partenaires de se connecter immédiatement, d'interagir et d'effectuer leurs tâches sur le canal de communication qu'ils préfèrent, et ainsi d'atteindre leurs objectifs.

1.4.1.4 Communication vidéo

Communication vidéo

La vidéo est une autre tendance relative au réseau. Elle est indispensable pour la communication et la collaboration. La vidéo est utilisée pour la communication, la collaboration et le divertissement. Les appels vidéo sont de plus en plus populaires et facilitent les communications dans le cadre du réseau humain. Les appels vidéo peuvent être émis et reçus n'importe où via Internet, notamment depuis son domicile ou son bureau.

Les appels vidéo et les vidéoconférences s'avèrent particulièrement efficaces pour les processus de vente et les communications professionnelles. La vidéo est un outil utile pour travailler à distance, au niveau régional ou international. Aujourd'hui, les entreprises utilisent la vidéo pour transformer la manière dont elles gèrent leurs activités. La vidéo aide les entreprises à développer un avantage concurrentiel, à réduire les coûts et à diminuer l'impact sur l'environnement grâce à la réduction du nombre de déplacements. La Figure 1 illustre la tendance relative à la vidéo dans le cadre de la communication.

Cette évolution provient à la fois des consommateurs et des entreprises. La vidéo devient essentielle pour collaborer efficacement à mesure que les entreprises se développent au-delà des frontières géographiques et culturelles. Les utilisateurs de vidéos souhaitent pouvoir visualiser tous les contenus, où qu'ils se trouvent, et sur n'importe quel périphérique.

Les entreprises sont également conscientes de l'importance de la vidéo pour améliorer le réseau humain. La croissance du multimédia, ainsi que ses nouvelles applications, implique la nécessité d'intégrer l'audio et la vidéo dans de nombreuses formes de communication. La conférence audio coexistera avec la conférence vidéo. Les outils de collaboration conçus pour permettre aux employés dispersés sur le territoire de communiquer intègrent peu à peu la vidéo, pour permettre aux équipes de collaborer facilement.

L'intégration d'une stratégie pour l'utilisation de la vidéo présente de nombreux avantages. Chaque entreprise est unique. Les différentes raisons d'adopter la vidéo varient d'une entreprise à l'autre et dépendent des différentes fonctions professionnelles. Le service Marketing, par exemple, peut se concentrer sur la mondialisation et l'évolution des demandes des consommateurs, alors que le responsable informatique peut se concentrer sur les économies réalisées grâce à la diminution du nombre de déplacements. La Figure 2 répertorie quelques-unes des raisons pour lesquelles les entreprises doivent développer et mettre en œuvre une stratégie de solution vidéo.

La Figure 3 est une vidéo qui présente plus précisément la manière dont la technologie de vidéo TelePresence peut être utilisée au quotidien, au bureau comme à son domicile.

Une autre tendance relative à la vidéo est la vidéo à la demande et la vidéo en direct et en continu. Grâce à la vidéo sur le réseau, nous pouvons regarder des films et des programmes TV à n'importe quel moment, n'importe où.

1.4.1.5 Cloud computing

Cloud computing

Le cloud computing consiste à utiliser des ressources informatiques (matérielles et logicielles) sous forme de service sur un réseau. Une société utilise le matériel et les logiciels dans le cloud et des frais de service lui sont imputés.

Les ordinateurs locaux n'ont plus à effectuer de tâches complexes lorsqu'il s'agit d'exécuter des applications réseau. Les ordinateurs en réseau qui constituent le cloud s'en chargent. Le matériel et les logiciels requis par l'utilisateur sont réduits. L'ordinateur de l'utilisateur doit interagir avec le cloud grâce à un logiciel, qui peut être un navigateur Web, et le réseau du cloud se charge du reste.

Le cloud computing est également une tendance globale qui fait évoluer l'accès aux données et leur stockage. Le terme « cloud computing » fait référence à tout service disponible en temps réel sur Internet, impliquant un paiement sous forme d'abonnement ou en fonction de l'utilisation. Le cloud computing nous permet de stocker des fichiers personnels, voire de sauvegarder tout le contenu d'un disque dur sur des serveurs via Internet. Des applications telles que le traitement de texte et la retouche photo peuvent être accessibles via le cloud.

Pour les entreprises, le cloud computing offre de nouvelles fonctionnalités sans nécessiter d'investissement dans une nouvelle infrastructure, une nouvelle formation du personnel ou de nouveaux logiciels. Ces services sont disponibles à la demande et sont fournis à moindre coût à n'importe quel périphérique, partout dans le monde, sans compromettre la sécurité ou les fonctionnalités.

Le terme « cloud computing » fait en fait référence à l'informatique sur le Web. Les opérations bancaires en ligne, les magasins en ligne et les sites de téléchargement de musique sont des exemples courants de cloud computing. Les utilisateurs accèdent aux applications du cloud via un navigateur Web. Aucun logiciel supplémentaire n'est nécessaire sur leurs ordinateurs. Cela permet à de nombreux types de périphérique d'accéder au cloud.

Le cloud computing peut offrir les avantages suivants :

- **Flexibilité organisationnelle** – les utilisateurs peuvent accéder aux informations à tout moment et partout via un navigateur Web.
- **Réactivité et rapidité de déploiement** – le service informatique peut se concentrer sur la fourniture d'outils pour extraire, analyser et partager les informations provenant de bases de données, de fichiers, et de données utilisateur.
- **Coûts d'infrastructure réduits** – l'infrastructure technologique, précédemment sur site, est gérée par le fournisseur de services cloud : les coûts liés au matériel et aux applications sont nuls.
- **Recadrage des ressources informatiques** – l'argent économisé sur le matériel et les applications peut être attribué à d'autres secteurs.
- **Création de nouveaux business models** – les applications et les ressources sont facilement accessibles. Les entreprises peuvent donc réagir rapidement aux besoins

des clients. Elles peuvent ainsi développer des stratégies pour promouvoir l'innovation tout en pénétrant de nouveaux marchés.

Il existe quatre types principaux de cloud, comme illustré à la Figure 2. Cliquez sur chaque type de cloud pour obtenir des informations supplémentaires.

1.4.1.6 Data centers

Le cloud computing fonctionne grâce aux data centers. Un data center héberge des systèmes informatiques et les composants associés :

- Connexions de communication de données redondantes
- Serveurs virtuels haut débit (parfois appelés batteries de serveurs ou clusters de serveurs)
- Systèmes de stockage redondants (généralement, technologie SAN)
- Alimentations redondantes ou de secours
- Systèmes de contrôle de l'environnement (par exemple, climatisation, système d'extinction des incendies)
- Dispositifs de sécurité

Un data center peut occuper une pièce, un ou plusieurs étages, voire un bâtiment entier. Les data centers modernes utilisent le cloud computing et la virtualisation pour gérer efficacement les transactions de données importantes. La virtualisation consiste à créer une version virtuelle d'une plate-forme matérielle, d'un système d'exploitation, d'un périphérique de stockage ou de ressources réseau. Alors qu'un ordinateur physique est un périphérique matériel autonome, un ordinateur virtuel est composé d'un ensemble de fichiers et de programmes s'exécutant sur un système physique réel. À la différence du multitâche, qui implique d'exécuter plusieurs programmes sur le même système d'exploitation, la virtualisation exécute plusieurs systèmes d'exploitation en parallèle sur un seul processeur. Cela réduit considérablement les frais généraux et d'administration.

Les data centers sont en général très coûteux à construire et à prendre en charge. C'est pour cela que les grandes entreprises utilisent des data centers privés pour stocker leurs données et fournir des services aux utilisateurs. Par exemple, un grand hôpital peut posséder un data center distinct où les informations sur les patients sont gérées de manière électronique. Les entreprises de plus petite taille, qui ne peuvent pas se permettre de posséder leur propre data center privé, peuvent réduire le coût total de possession en louant des services de stockage et de serveur cloud à une entreprise proposant des data centers.

La figure est une vidéo sur l'utilisation accrue des services de cloud computing et de data center.

1.4.2 Technologies réseau domestiques

1.4.2.1 Tendances technologiques domestiques

Les tendances relatives au réseau affectent non seulement la façon dont nous communiquons au travail et à l'école, mais modifient également chaque aspect de la maison.

Les nouvelles tendances domestiques incluent les « technologies domestiques intelligentes ». Les technologies domestiques intelligentes sont intégrées aux appareils de la maison, pour leur permettre de se connecter à d'autres périphériques et ainsi les rendre plus « intelligents » ou automatisés. Imaginez : vous préparez un plat et le placez dans votre four avant de quitter la maison pour la journée. Le four « sait » quel plat il doit faire cuire et est connecté à votre

« calendrier des événements » pour déterminer à quelle heure vous prendrez votre repas. Il peut ainsi configurer l'heure de début de cuisson ainsi que le temps de cuisson en fonction de ces informations. Il peut même régler les heures et les températures de cuisson en fonction des changements apportés à votre calendrier. De plus, une connexion depuis un smartphone ou une tablette vous permet de vous connecter directement au four pour effectuer tous les réglages souhaités. Une fois votre plat prêt, le four vous envoie un message pour vous indiquer que votre plat est terminé et maintenu au chaud.

Ce scénario ne sera bientôt plus de la science-fiction. Les technologies domestiques intelligentes sont en cours de développement et s'intègreront bientôt à toutes les pièces de la maison. Les technologies domestiques intelligentes deviennent une réalité à mesure que les technologies de réseau domestique et d'Internet haut débit se développent. De nouvelles technologies de réseau domestique sont développées chaque jour pour répondre à ces types de besoin technologique en pleine croissance.

1.4.2.2 Réseau sur courant électrique

Le réseau sur courant électrique est une tendance émergente dans le domaine des réseaux domestiques. Il permet d'utiliser le câblage électrique existant pour connecter des périphériques, comme l'illustre la figure. Le concept « pas de nouveaux câbles » repose sur la possibilité de connecter un périphérique au réseau grâce à n'importe quelle prise électrique. Cela permet d'éliminer les coûts d'installation de câbles de données, sans coûts supplémentaires sur la facture d'électricité. Grâce au câblage électrique, le réseau sur courant électrique transmet des informations en envoyant les données sur des fréquences spécifiques, tout comme la technologie utilisée pour la DSL.

À l'aide d'un adaptateur HomePlug standard, les périphériques peuvent se connecter au LAN en utilisant n'importe quelle prise de courant. Le réseau sur courant électrique est particulièrement utile lorsque les points d'accès sans fil ne peuvent pas être utilisés ou ne peuvent pas couvrir tous les périphériques d'un domicile. Le réseau sur courant électrique n'est pas conçu pour remplacer les câblages dédiés aux réseaux de données. Cependant, c'est une alternative viable lorsque les câbles ou les communications sans fil du réseau de données ne sont pas utilisables.

1.4.2.3 Haut débit sans fil

Une connexion à Internet est essentielle pour les technologies domestiques intelligentes. Les connexions DSL et par câble sont des technologies courantes utilisées pour connecter des particuliers et des petites entreprises à Internet. Cependant, la technologie sans fil est une alternative viable dans de nombreux cas.

Fournisseur d'accès Internet sans fil

Un fournisseur d'accès Internet sans fil est un FAI qui permet à ses abonnés de se connecter à un point d'accès spécifique en utilisant des technologies sans fil similaires à celles utilisées dans les réseaux locaux sans fil (WLAN). Les fournisseurs d'accès Internet sans fil opèrent généralement dans les régions rurales où la DSL et les services par câble ne sont pas disponibles.

Bien qu'une tour de transmission distincte puisse être érigée pour installer l'antenne, il est courant que l'antenne soit fixée à une structure élevée existante, telle qu'un château d'eau ou

un pylône radio. Une petite parabole ou antenne est installée sur le toit de la maison de l'abonné, à portée de l'émetteur du fournisseur d'accès Internet sans fil. L'unité d'accès de l'abonné est connectée au réseau câblé à l'intérieur de la maison. Pour l'utilisateur, cette configuration n'est pas très différente de la DSL ou du câble. La principale différence est en fait la connexion entre la maison et le FAI : celle-ci se fait sans fil et n'utilise pas de câble.

Service haut débit sans fil

Le haut débit sans fil est une autre solution pour disposer d'une connexion sans fil chez soi. Cette technologie utilise la même technologie cellulaire de connexion à Internet qu'un smartphone ou une tablette. Une antenne est installée à l'extérieur de la maison pour offrir une connectivité avec ou sans fil aux périphériques du domicile. Dans de nombreuses régions, le haut débit sans fil domestique est en concurrence directe avec la DSL et le câble.

1.4.3 Sécurité du réseau

1.4.3.1 Menaces de sécurité

La sécurité du réseau est une partie intégrante des réseaux informatiques, qu'il s'agisse d'un simple environnement domestique avec une seule connexion à Internet ou d'une entreprise avec des milliers d'utilisateurs. La sécurité réseau mise en œuvre doit prendre en compte l'environnement, ainsi que les outils et les besoins du réseau. Le réseau doit être capable de sécuriser les données, tout en garantissant en permanence la qualité de service attendue.

La sécurisation d'un réseau implique l'utilisation de protocoles, de technologies, de périphériques, d'outils, et de techniques pour sécuriser les données et limiter les risques. De nombreuses menaces externes sur la sécurité réseau se diffusent aujourd'hui par Internet. Les menaces externes les plus courantes pour les réseaux sont les suivantes :

- **Virus, vers, et chevaux de Troie** – logiciels malveillants et code arbitraire s'exécutant sur un périphérique utilisateur.
- **Logiciels espions et publicitaires** – logiciels installés sur un périphérique utilisateur qui collectent secrètement des informations sur l'utilisateur.
- **Attaques zero-day, également appelées attaques zero-hour** – attaques qui se produisent le jour où une vulnérabilité est détectée.
- **Attaques de pirates** – attaques lancées sur des périphériques utilisateur ou des ressources réseau par une personne qui possède de solides connaissances en informatique.
- **Attaques par déni de service** – attaques conçues pour ralentir ou bloquer les applications et les processus d'un périphérique réseau.
- **Interception et vol de données** – attaques visant à acquérir des informations confidentielles à partir du réseau d'une entreprise.
- **Usurpation d'identité** - attaques visant à recueillir les informations de connexion d'un utilisateur afin d'accéder à des données privées.

Il est également important de prendre en compte les menaces internes. Il existe de nombreuses études démontrant que la plupart des violations de données se produisent par la faute des utilisateurs internes du réseau. Ces violations peuvent découler d'une perte ou d'un vol de périphériques, d'une mauvaise utilisation d'un périphérique par un employé et, dans un contexte professionnel, d'un employé malveillant. En raison de la croissance des stratégies BYOD, les données d'entreprise sont beaucoup plus vulnérables. Par conséquent, lors du développement d'une stratégie de sécurité, il est important de prendre en compte les menaces externes et internes.

1.4.3.2 Solutions de sécurité

Aucune solution unique ne peut protéger le réseau contre les diverses menaces existantes. Pour cette raison, la sécurité doit être implémentée en plusieurs couches, avec plusieurs solutions de sécurité. Si un composant de sécurité ne parvient pas à identifier et à protéger le réseau, d'autres peuvent alors prendre la relève.

La mise en œuvre de la sécurité du réseau domestique est généralement plutôt simple. Les fonctions de sécurité sont généralement mises en place sur les périphériques hôtes de connexion, ainsi qu'au niveau du point d'accès à Internet. Elles peuvent même exploiter les services proposés par le FAI.

En revanche, la mise en œuvre de la sécurité du réseau d'une entreprise implique généralement de nombreux composants intégrés dans le réseau afin de contrôler et de filtrer le trafic. Dans l'idéal, tous les composants fonctionnent ensemble, ce qui réduit les opérations de maintenance et renforce la sécurité.

Les composants de sécurité réseau d'un réseau domestique ou d'un réseau de petit bureau doivent inclure, au minimum :

- **Un antivirus et un logiciel anti-espion** – pour protéger les périphériques des utilisateurs contre les logiciels malveillants.

- **Un pare-feu** – pour bloquer les accès non autorisés au réseau. Il peut s'agir d'un système de pare-feu sur l'hôte qui est mis en œuvre pour empêcher l'accès non autorisé au périphérique hôte, ou d'un service de filtrage sur le routeur de la maison pour empêcher l'accès non autorisé depuis l'extérieur du réseau.

De plus, les réseaux plus étendus et les réseaux des grandes entreprises ont souvent d'autres exigences relatives à la sécurité :

- **Des systèmes de pare-feu spécialisés** – pour fournir des fonctionnalités de pare-feu plus avancées et filtrer un trafic plus important avec plus de précision.
- **Des listes de contrôle d'accès (ACL)** – pour filtrer davantage les accès et le transfert de trafic.
- **Des systèmes de prévention contre les intrusions** – pour identifier des menaces immédiates telles que les attaques zero-day ou zero-hour.
- **Des réseaux privés virtuels (VPN)** – pour fournir un accès sécurisé aux télétravailleurs.

Les exigences de sécurité réseau doivent prendre en compte l'environnement réseau, ainsi que les différentes applications et les exigences informatiques. Les réseaux domestiques et professionnels doivent être sécurisés, tout en garantissant en permanence la qualité de service attendue. En outre, la solution de sécurité mise en œuvre doit être capable de s'adapter aux nouvelles tendances et à l'évolution du réseau.

L'étude des menaces de sécurité réseau et des techniques permettant de limiter les risques nécessite toute d'abord une parfaite compréhension de l'infrastructure de routage et de commutation sous-jacente, qui permet d'organiser les services réseau.

1.4.4 Architectures réseau

1.4.4.1 Architectures réseau Cisco

Le rôle du réseau a changé : auparavant simple réseau de données, il constitue désormais un système qui permet aux personnes et aux périphériques d'échanger des informations dans le cadre d'un réseau multimédia et convergent. Pour que les réseaux fonctionnent efficacement et se développent dans ce type d'environnement, ils doivent s'appuyer sur une architecture réseau standard.

L'architecture réseau désigne les périphériques, les connexions et les produits intégrés permettant de prendre en charge les technologies et applications nécessaires. Une architecture de technologie réseau efficace permet de garantir la connexion de n'importe quel périphérique à n'importe quel réseau. Tout en garantissant la connectivité, elle augmente également la rentabilité en intégrant des fonctionnalités de sécurité et de gestion du réseau, et améliore les processus commerciaux. À la base de toutes les architectures réseau, et en fait, à la base d'Internet lui-même, on trouve les routeurs et les commutateurs. Ces périphériques transmettent des données, des communications vocales et des communications vidéo, et permettent un accès sans fil tout en assurant la sécurité.

La conception de réseaux prenant en charge nos besoins actuels et nos demandes futures implique une parfaite compréhension de l'infrastructure de routage et de commutation sous-jacente. Après avoir conçu une infrastructure de routage et de commutation de base, les utilisateurs individuels, les PME et les grandes entreprises peuvent développer leur réseau au fil du temps, en ajoutant de nouvelles fonctionnalités au sein d'une solution intégrée.

1.4.4.2 CCNA

À mesure que l'usage de ces réseaux intégrés et évolutifs se développe, il en va de même pour les besoins en formation des personnes qui implémentent et gèrent des solutions réseau. Ces formations doivent commencer par les principes de base du routage et de la commutation. L'obtention de la certification Cisco Certified Network Associate (CCNA) est la première étape de la préparation à une carrière dans le domaine des réseaux.

La certification CCNA atteste de la capacité à installer, configurer, exploiter et dépanner des réseaux routés et commutés de taille moyenne, ainsi que de la maîtrise de la mise en œuvre et de la vérification des connexions à des sites distants dans un WAN. Le cursus CCNA inclut également des informations de base sur la réduction des menaces, une introduction aux concepts et à la terminologie des réseaux sans fil, ainsi que des évaluations axées sur les performances. Ce cursus CCNA inclut l'utilisation de différents protocoles : IP, Open Shortest Path First (OSPF), Serial Line Interface Protocol, Frame Relay, VLAN, Ethernet, listes de contrôle d'accès (ACL), etc.

Ce cours permet de présenter les concepts de réseau et les configurations de routage et de commutation de base, et est le point de départ de la certification CCNA.

CHAPITRE 2: **CONFIGURATION D'UN SYSTEME D'EXPLOITATION DE RESEAU**

2.0 Configuration d'un système d'exploitation de réseau

2.0.1 Introduction

2.0.1.1 Initiation à Cisco IOS

Les réseaux domestiques relient généralement une grande variété de périphériques finaux, notamment des ordinateurs de bureau, des ordinateurs portables, des tablettes, des smartphones, des télévisions connectées, des lecteurs multimédias réseau compatibles DLNA (Xbox 360, PlayStation 3), etc.

Tous ces périphériques finaux se connectent généralement à un routeur domestique. Les routeurs domestiques regroupent en fait 4 périphériques en un :

- **Router -** Transfère les paquets de données vers Internet et reçoit des paquets depuis Internet
- **Switch -** Connecte des périphériques finaux à l'aide de câbles réseau
- **Point d'accès sans fil -** Se compose d'un émetteur radio capable de connecter des périphériques finaux sans fil
- **Pare-feu -** Sécurise le trafic sortant et contrôle le trafic entrant

À une échelle plus importante, dans les réseaux d'entreprise comportant beaucoup plus de périphériques et gérant plus de trafic, ces périphériques sont souvent intégrés comme des périphériques indépendants et autonomes, assurant un service spécifique. Des périphériques finaux, tels que des PC et des ordinateurs portables, sont connectés aux commutateurs réseau par le biais de connexions câblées. Pour envoyer des paquets en dehors du réseau local, les commutateurs réseau se connectent aux routeurs du réseau. Les points d'accès sans fil et les dispositifs de sécurité dédiés, tels que des pare-feu, sont également des périphériques d'infrastructure réseau.

Chaque périphérique est très différent en termes de matériel, d'utilisation et de fonctionnalités. Cependant, dans tous les cas, c'est le système d'exploitation qui permet au matériel de fonctionner.

Les systèmes d'exploitation sont utilisés sur presque tous les périphériques utilisateur et réseau connectés à Internet. Les périphériques utilisateur incluent les smartphones, les tablettes, les ordinateurs de bureau et les ordinateurs portables. Les périphériques réseau, ou périphériques intermédiaires, sont utilisés pour transporter les données sur l'ensemble du réseau et comprennent les commutateurs, les routeurs, les points d'accès sans fil et les pare-feu. Le système d'exploitation d'un périphérique réseau est appelé système d'exploitation réseau.

Cisco Internetwork Operating System (IOS) est un terme générique utilisé pour désigner l'ensemble des systèmes d'exploitation réseau utilisés sur les périphériques réseau Cisco. Cisco IOS est utilisé par la plupart des périphériques Cisco, quels que soient leur taille et leur type.

Ce chapitre fait référence à une topologie de réseau de base, comportant deux commutateurs et deux PC, pour illustrer l'utilisation de Cisco IOS.

2.0.1.2 Exercice en classe – Ce n'est qu'un système d'exploitation

Sur la plateforme CISCO

2.1 IOS Bootcamp

2.1.1 Cisco IOS

2.1.1.1 Systèmes d'exploitation

Tous les périphériques finaux et tous les périphériques réseau connectés à Internet nécessitent un système d'exploitation pour pouvoir remplir leur fonction.

Lorsqu'un ordinateur est mis sous tension, il charge le système d'exploitation dans la mémoire vive (RAM), en principe à partir d'un disque dur. La partie du code du système d'exploitation directement liée au matériel informatique s'appelle le noyau. La partie liée aux applications et à l'utilisateur s'appelle l'interpréteur de commandes. L'utilisateur accède à l'interpréteur de commandes à l'aide de l'interface de ligne de commande (CLI) ou de l'interface graphique utilisateur.

Lorsqu'il utilise l'interface de ligne de commande, l'utilisateur accède directement au système dans un environnement textuel, en entrant des commandes au clavier, dans une invite de commande. En règle générale, le système exécute la commande en fournissant une sortie textuelle. L'interface graphique permet à l'utilisateur d'accéder au système dans un environnement qui offre des images, du contenu multimédia et du texte. Les actions sont exécutées par le traitement des images à l'écran. Pour interagir avec le système, l'interface graphique est plus conviviale que l'interface de ligne de commande et ne requiert pas de connaissances approfondies. C'est pour cette raison que de nombreux utilisateurs préfèrent des environnements basés sur une interface graphique. La plupart des systèmes d'exploitation offrent ces deux types d'interface.

Cliquez sur le matériel, le noyau et l'interpréteur de commandes sur la figure pour obtenir plus d'informations.

La plupart des systèmes d'exploitation des périphériques finaux sont accessibles via une interface graphique, y compris MS Windows, MAC OS X, Linux, Apple iOS, Android, etc.

Le système d'exploitation des routeurs domestiques est généralement appelé « firmware ». La méthode la plus courante pour configurer un routeur domestique est d'utiliser un navigateur Web pour accéder à une interface graphique conviviale. La plupart des routeurs domestiques permettent la mise à jour du firmware à mesure que de nouvelles fonctions sont implémentées ou que des failles de sécurité sont détectées.

Les périphériques réseau d'infrastructure utilisent un système d'exploitation réseau. Le système d'exploitation réseau utilisé sur les périphériques Cisco est appelé Cisco Internetwork Operating System (IOS). Cisco IOS est un terme générique utilisé pour désigner l'ensemble des systèmes d'exploitation réseau utilisés sur les périphériques réseau Cisco. Cisco IOS est utilisé par la plupart des périphériques Cisco, quels que soient leur taille et leur type. La méthode la plus courante pour accéder à ces périphériques est d'utiliser la CLI.

Ce chapitre fait référence à une topologie de petit réseau d'entreprise. Cette topologie est composée de deux commutateurs et de deux PC, et sera utilisée pour illustrer l'utilisation de Cisco IOS à l'aide de la CLI.

2.1.1.2 Utilité du système d'exploitation

Les systèmes d'exploitation réseau comportent de nombreux points communs avec les systèmes d'exploitation des PC. Un système d'exploitation exécute plusieurs fonctionnalités techniques en arrière-plan qui permettent aux utilisateurs :

- d'utiliser une souris ;
- d'afficher des images sur un écran ;
- d'entrer des commandes ;
- de sélectionner des options dans une boîte de dialogue.

Les fonctions en arrière-plan des commutateurs et des routeurs sont très similaires. L'IOS d'un commutateur ou d'un routeur offre au technicien réseau une interface. Le technicien peut entrer des commandes pour configurer ou programmer le périphérique, afin qu'il exécute diverses fonctions réseau. Les détails du fonctionnement d'IOS dépendent des périphériques interréseau, de l'objectif des périphériques et des fonctions prises en charge.

Cisco IOS est un terme faisant référence aux différents systèmes d'exploitation qui s'exécutent sur divers périphériques réseau. Il existe de nombreuses versions différentes de Cisco IOS :

- IOS pour les commutateurs, les routeurs et les autres périphériques réseau Cisco
- Versions numérotées d'IOS pour un périphérique réseau Cisco précis
- Ensembles de fonctionnalités IOS offrant différentes fonctions et différents services

De la même façon qu'un PC peut exécuter Microsoft Windows 8 et qu'un MacBook peut exécuter OS X, un périphérique réseau Cisco exécute une version spécifique de Cisco IOS. La version de l'IOS dépend du type de périphérique utilisé et des fonctions nécessaires. Alors que tous les périphériques possèdent un IOS et un ensemble de fonctionnalités par défaut, il est possible de mettre à niveau l'IOS ou l'ensemble de fonctionnalités, afin d'obtenir des fonctions supplémentaires.

Dans ce cours, vous vous concentrerez principalement sur Cisco IOS version 15.x. La Figure 1 répertorie les versions logicielles d'IOS disponibles pour un commutateur Cisco Catalyst 2960. La Figure 2 répertorie les versions logicielles d'IOS disponibles pour un routeur à services intégrés Cisco 2911.

2.1.1.3 Emplacement de Cisco IOS

Le fichier IOS proprement dit, dont la taille atteint plusieurs méga-octets, est stocké dans une zone de mémoire semi-permanente appelée Flash. La figure illustre une carte CompactFlash. La mémoire Flash assure un stockage non volatil. En d'autres termes, cette mémoire conserve son contenu lorsque le périphérique n'est plus sous tension. Bien que le contenu de la mémoire Flash ne soit pas perdu en cas de perte d'alimentation, il peut être modifié ou remplacé si nécessaire. Cela permet de mettre à niveau l'IOS ou de disposer de nouvelles fonctionnalités sans remplacer le matériel. En outre, la mémoire Flash peut être utilisée pour stocker plusieurs versions du logiciel IOS simultanément.

Dans de nombreux périphériques Cisco, l'IOS est copié de la mémoire Flash vers la mémoire vive lorsque le périphérique est mis sous tension. L'IOS s'exécute alors depuis la mémoire vive lorsque le périphérique fonctionne. La mémoire vive a de nombreuses utilités, notamment le stockage des données utilisées par le périphérique pour prendre en charge les fonctions réseau. L'exécution de l'IOS sur la mémoire vive augmente les performances du périphérique. Cependant, la mémoire vive est considérée comme de la mémoire volatile car les données sont perdues en cas de cycle d'alimentation. Le terme « cycle d'alimentation » fait référence à la mise hors tension (accidentelle ou non) puis sous tension d'un périphérique.

Les quantités de mémoire Flash et de mémoire vive requises varient selon la version de l'IOS. Dans le cadre de la maintenance et de la planification réseau, il est important de déterminer les exigences relatives à la mémoire Flash et à la mémoire vive pour chaque périphérique, notamment les quantités maximales de mémoire Flash et de mémoire vive. Il est possible que les nouvelles versions d'IOS requièrent plus de mémoire vive et de mémoire Flash que la quantité disponible sur les périphériques.

2.1.1.4 Fonctions IOS

Les routeurs et commutateurs Cisco IOS exécutent des fonctions dont les professionnels réseau ont besoin pour faire en sorte que les réseaux fonctionnent comme prévu. Les routeurs et les commutateurs Cisco assurent principalement les fonctions suivantes, ou permettent de les effectuer :

- Garantir la sécurité du réseau
- L'adressage IP des interfaces virtuelles et physiques
- Les configurations spécifiques aux interfaces pour optimiser la connectivité des supports respectifs
- Routage
- Les technologies de qualité de service (QS)
- La prise en charge des technologies de gestion de réseau

Chaque fonction ou service possède un groupe associé de commandes de configuration qui permettent à un technicien réseau d'effectuer sa mise en œuvre.

Pour accéder aux services fournis par Cisco IOS, l'interface de ligne de commande (CLI) est généralement utilisée.

2.1.1.5 Démonstration vidéo –Découverte des comptes CCO et de l'image IOS

Cette vidéo présente Cisco Connection Online (CCO). CCO contient une foule d'informations sur les produits et services Cisco.
Suivez la vidéo

2.1.2 Accès à un périphérique Cisco IOS

2.1.2.1 La méthode d'accès par une console

Il y a plusieurs moyens d'accéder à l'interface CLI. Voici les méthodes les plus répandues :

- Console
- Telnet ou SSH
- Port AUX

Console

Le port de console est un port de gestion permettant un accès hors réseau à un périphérique Cisco. L'accès hors réseau désigne l'accès via un canal de gestion dédié qui est utilisé uniquement pour la maintenance des périphériques. L'avantage d'utiliser un port de console est que le périphérique est accessible même si aucun service réseau n'a été configuré, par exemple en effectuant la configuration initiale du périphérique réseau. Pour effectuer la configuration initiale, un ordinateur exécutant un logiciel d'émulation de terminal est connecté au port de console du périphérique à l'aide d'un câble spécial. Ainsi, il est possible d'entrer au clavier de l'ordinateur connecté les commandes de configuration du routeur ou du commutateur.

Le port de console peut également être utilisé lorsque les services réseau ont échoué et lorsque l'accès à distance au périphérique Cisco IOS est impossible. Dans ce cas, une connexion à la console peut permettre à un ordinateur de déterminer l'état du périphérique. Par défaut, la console transmet les messages de démarrage, de débogage et d'erreur du périphérique. Une fois le technicien réseau connecté au périphérique, il peut exécuter toutes les commandes de configuration nécessaires à l'aide de la session en mode console.

Pour de nombreux périphériques IOS, l'accès console ne requiert par défaut aucune forme de sécurité. Il convient toutefois de configurer un mot de passe pour la console afin d'empêcher l'accès non autorisé au périphérique. En cas de perte du mot de passe, des procédures spéciales permettent d'accéder malgré tout au périphérique. Il est recommandé de placer le périphérique dans une pièce ou une armoire fermée à clé pour éviter les accès non autorisés.

2.1.2.2 Méthodes d'accès : Telnet, SSH et AUX

Telnet

Telnet est une méthode permettant de créer à distance une session CLI sur un périphérique, par le biais d'une interface virtuelle, via un réseau. À la différence des connexions console, les sessions Telnet requièrent des services réseau actifs sur le périphérique. Le périphérique réseau doit disposer d'au moins une interface active configurée avec une adresse Internet, par exemple une adresse IPv4. Les périphériques Cisco IOS comportent un processus serveur Telnet qui permet aux utilisateurs d'entrer des commandes de configuration à partir d'un client Telnet. En plus de prendre en charge le processus serveur Telnet, les périphériques Cisco IOS contiennent également un client Telnet. Cela permet à un administrateur réseau d'établir une connexion Telnet à partir de la CLI du périphérique Cisco vers tout autre périphérique prenant en charge un processus serveur Telnet.

SSH

Le protocole Secure Shell (SSH) fournit une connexion à distance semblable à Telnet, sauf qu'il utilise des services réseau plus sécurisés. SSH fournit une authentification par mot de passe plus résistante que celle de Telnet et emploie un chiffrement lors du transport des données de la session. Ceci préserve la confidentialité de l'ID d'utilisateur, du mot de passe et des détails de la session de gestion. Il est fortement conseillé d'utiliser SSH plutôt que Telnet dans la mesure du possible.

La plupart des versions de Cisco IOS comprennent un serveur SSH. Dans certains périphériques, ce service est activé par défaut. D'autres périphériques requièrent une activation manuelle du serveur SSH. Les périphériques IOS incluent également un client SSH permettant d'établir des sessions SSH avec d'autres périphériques.

Port

Il est possible d'établir une session CLI à distance par le biais d'une connexion téléphonique commutée, à l'aide d'un modem connecté au port auxiliaire (AUX) d'un routeur (mis en surbrillance dans la figure). Tout comme la connexion console, la méthode d'accès AUX est une connexion hors réseau et ne nécessite aucun service réseau pour être configurée ou disponible sur le périphérique. En cas de défaillance des services réseau, un administrateur à distance peut accéder au commutateur ou au routeur par le biais d'une ligne téléphonique.

Le port AUX peut également s'utiliser localement, comme le port de console, avec une connexion directe à un ordinateur exécutant un programme d'émulation de terminal. Cependant, il est préférable d'utiliser le port de console plutôt que le port AUX pour le dépannage, car celui-ci affiche par défaut les messages de démarrage, de débogage et d'erreur du routeur.

Remarque : les commutateurs Cisco Catalyst ne prennent pas en charge les connexions auxiliaires.

2.1.2.3 Programmes d'émulation de terminal

Il existe d'excellents programmes d'émulation de terminal disponibles pour se connecter à un périphérique réseau via une connexion série sur un port de console ou via une connexion Telnet/SSH. Voici quelques exemples :

- PuTTY (Figure 1)
- Tera Term (Figure 2)
- SecureCRT (Figure 3)
- HyperTerminal
- Terminal OS X

Ces programmes vous permettent d'améliorer votre productivité grâce à différentes fonctionnalités comme la personnalisation de la taille de fenêtres, de la taille des polices ou des jeux de couleurs.

2.1.3 Navigation à travers IOS

2.1.3.1 Modes de fonctionnement de Cisco IOS

Une fois l'ingénieur réseau connecté à un périphérique, il peut le configurer. Le technicien réseau doit parcourir plusieurs modes de l'IOS. Les modes de Cisco IOS sont assez similaires pour les commutateurs et les routeurs. L'interface en ligne de commande (CLI) est organisées selon une structure hiérarchique des modes.

En partant de la configuration la plus simple à la plus spécialisée, les modes principaux sont les suivants :

- Mode d'exécution utilisateur
- Mode d'exécution privilégié
- Mode de configuration globale
- Autres modes de configuration spécifiques tels que le mode de configuration d'interface

Chaque mode présente une invite distincte et permet d'effectuer des tâches particulières grâce à des commandes spécifiques disponibles uniquement dans ce mode. Par exemple, le mode de configuration globale permet à un technicien de configurer les paramètres du périphérique concernant le périphérique dans son ensemble, comme le nom du périphérique. Cependant, un autre mode doit être utilisé si le technicien réseau veut configurer les paramètres de sécurité sur un port spécifique d'un commutateur, par exemple. Dans ce cas, le technicien réseau doit en effet passer en mode de configuration d'interface pour ce port spécifique. Toutes les configurations entrées en mode de configuration d'interface ne s'appliquent qu'au port en question.

Il est possible de configurer la structure hiérarchique des modes à des fins de sécurité. Une authentification différente peut être requise pour chaque mode. Cela permet de contrôler les droits d'accès accordés au personnel réseau.

La figure montre la structure hiérarchique des modes IOS, ainsi que des invites et des fonctionnalités représentatives.

2.1.3.2 Modes principaux

Les deux modes de fonctionnement principaux sont le mode d'exécution utilisateur et le mode d'exécution privilégié. Par mesure de sécurité, Cisco IOS prévoit deux modes d'accès distincts pour les sessions d'exécution. Comme le montre la figure, le mode d'exécution privilégié a un haut niveau d'autorité dans ce qu'il permet à l'utilisateur de faire avec le périphérique.

Mode d'exécution utilisateur

Le mode d'exécution utilisateur offre des fonctionnalités limitées, mais est utile pour certaines opérations de base. Le mode d'exécution utilisateur est à la base de la structure hiérarchique des modes IOS. C'est le premier mode sélectionné dans l'interface en ligne de commande d'un périphérique IOS.

Le mode d'exécution utilisateur n'autorise qu'un nombre limité de commandes de surveillance de base. Il est souvent qualifié de mode « affichage seul ». Il n'autorise aucune commande susceptible de modifier la configuration du périphérique.

Par défaut, aucune authentification n'est requise pour accéder au mode d'exécution utilisateur depuis la console. Il est donc conseillé de définir une méthode d'authentification lors de la configuration initiale.

Le mode d'exécution utilisateur se reconnaît facilement dans l'interface en ligne de commande : l'invite se termine par le symbole >. Voici un exemple montrant le symbole > dans l'invite :

Switch>

Mode d'exécution privilégié

Pour exécuter les commandes de configuration et de gestion, l'administrateur réseau doit utiliser le mode d'exécution privilégié ou un mode plus spécifique. Cela signifie qu'un utilisateur doit d'abord passer en mode d'exécution utilisateur, puis accéder au mode d'exécution privilégié.

Le mode d'exécution privilégié se reconnaît à l'invite qui se termine par le symbole # :

Switch#

Par défaut, le mode d'exécution privilégié ne requiert pas d'authentification. Il est donc recommandé de s'assurer qu'une authentification est configurée.

Pour accéder au mode de configuration globale et aux autres modes de configuration plus spécifiques, il est nécessaire de passer par le mode d'exécution privilégié. Nous traiterons en détail la configuration des périphériques et quelques-uns des modes de configuration plus loin dans ce chapitre.

2.1.3.3 Mode de configuration globale et sous-modes

Pour accéder au mode de configuration globale et aux modes de configuration d'interface, il est nécessaire de passer par le mode d'exécution privilégié.

Mode de configuration globale

Le principal mode de configuration est appelé mode de configuration globale. Les modifications de la configuration effectuées dans la CLI en mode de configuration globale affectent le fonctionnement du périphérique dans son ensemble. Le mode de configuration globale est sélectionné avant d'accéder à des modes de configuration spécifiques.

La commande IOS suivante permet de faire passer le périphérique du mode d'exécution privilégié au mode de configuration globale et d'autoriser l'entrée de commandes de configuration à partir d'un terminal :

Switch# **configure terminal**

Une fois la commande exécutée, l'invite change pour indiquer que le commutateur se trouve en mode de configuration globale.

Switch(config)#

Modes de configuration spécifiques

À partir du mode de configuration globale, l'utilisateur peut accéder à différents sous-modes de configuration. Ceux-ci permettent tous de configurer une partie ou une fonction spéciale du périphérique IOS. La liste ci-dessous en présente quelques-uns :

- **Mode interface** - pour configurer l'une des interfaces réseau (Fa0/0, S0/0/0)
- **Mode ligne** - pour configurer l'une des lignes physiques ou virtuelles (console, AUX, VTY)

La Figure 1 illustre les invites de certains de ces modes. Pour quitter un mode de configuration spécifique et retourner au mode de configuration globale, entrez **exit** à une invite. Pour quitter complètement le mode de configuration et retourner au mode d'exécution privilégié, entrez **end** ou utilisez la combinaison de touches **Ctrl-Z**.

Invites de commandes

Dans la CLI, le mode dans lequel vous travaillez est reconnaissable à son invite de commandes unique. Par défaut, toute invite commence par le nom du périphérique. Après le nom du périphérique, le reste de l'invite précise le mode. Par exemple, l'invite par défaut pour le mode de configuration globale d'un commutateur est :

Switch(config)#

Comme le montre la Figure 2, lorsque vous entrez des commandes et passez d'un mode à l'autre, l'invite change pour refléter le mode en cours d'utilisation.

2.1.3.4 Sélection des différents modes IOS

Basculement entre mode d'exécution utilisateur et mode d'exécution privilégié

Les commandes **enable** et **disable** permettent d'aller et venir entre le mode d'exécution utilisateur et le mode d'exécution privilégié de la CLI.

Pour accéder au mode d'exécution privilégié, utilisez la commande **enable**. Cette commande est la raison pour laquelle le mode d'exécution privilégié est parfois appelé mode actif.

La syntaxe de la commande **enable** est la suivante :
Switch> **enable**
Cette commande est exécutée sans argument ni mot-clé. Après avoir appuyé sur la touche Entrée, l'invite change :

Switch#

Le symbole # à la fin de l'invite indique que le commutateur est désormais en mode d'exécution privilégié.

Si une authentification par mot de passe a été configurée pour le mode d'exécution privilégié, l'IOS vous invite à entrer le mot de passe.

Par exemple :
Switch> **enable**
Password:
Switch#
La commande **disable** permet de repasser du mode d'exécution privilégié au mode d'exécution utilisateur.
Par exemple :
Switch# **disable**
Switch>
Comme l'illustre la figure, les commandes permettant d'accéder au mode d'exécution privilégié et de revenir au mode d'exécution utilisateur sur un routeur Cisco sont identiques à celles utilisées sur un commutateur Cisco.

2.1.3.5 Sélection des différents modes IOS (suite)

Lancer et quitter le mode de configuration globale et les sous-modes

Pour quitter le mode de configuration globale et retourner au mode d'exécution privilégié, entrez la commande **exit**.

Notez qu'entrer la commande **exit** en mode d'exécution privilégié entraîne l'interruption de la session en mode console. Autrement dit, en saisissant la commande **exit** en mode d'exécution privilégié, l'écran que vous pouvez voir lorsque vous lancez pour la première fois une session en mode console s'affiche. Une fois cet écran affiché, vous devez appuyer sur la touche Entrée pour passer en mode d'exécution utilisateur.

Pour passer de n'importe quel sous-mode du mode de configuration globale au mode situé un niveau plus haut dans la hiérarchie des modes, saisissez la commande **exit**. La Figure 1 illustre le passage du mode d'exécution utilisateur au mode d'exécution privilégié, puis au mode de configuration globale, au mode de configuration d'interface, avant le retour au mode de configuration globale et à nouveau au mode d'exécution privilégié, le tout en utilisant la commande **exit**.

Pour passer de n'importe quel sous-mode du mode d'exécution privilégié au mode d'exécution privilégié, entrez la commande **end** ou utilisez la combinaison de touches **Ctrl + Z.** La Figure 2 illustre le passage du mode de configuration VLAN au mode d'exécution privilégié en utilisant la commande **end**.

Pour passer de n'importe quel sous-mode du mode de configuration globale à un autre sous-mode « adjacent » du mode de configuration globale, entrez simplement la commande correspondante, qui est normalement entrée à partir du mode de configuration globale. La Figure 3 illustre le passage du mode de configuration de ligne, Switch(config-line)#, au mode de configuration d'interface, Switch(config-if)#, sans quitter le mode de configuration de ligne.

2.1.3.6 Démonstration vidéo – Navigation à travers IOS

Cette vidéo explique la navigation dans les différents modes de commande de la CLI des routeurs et des commutateurs à l'aide de Cisco IOS.

2.1.4 Structure des commandes

2.1.4.1 Structure de commande IOS

Structure des commandes IOS de base

Un périphérique Cisco IOS prend en charge de nombreuses commandes. Chaque commande IOS a un format ou une syntaxe spécifique et ne peut être exécutée que dans le mode approprié. En général, vous entrez une commande en tapant un nom de commande suivi des mots-clés et des arguments appropriés. En effet, certaines commandes offrent un sous-ensemble de mots-clés et d'arguments qui étendent leurs fonctionnalités. Une commande sert à effectuer une action et les mots-clés permettent de préciser où ou comment l'exécuter.

Comme l'illustre la Figure 1, la commande est le premier mot entré (ou les premiers mots entrés) dans la ligne de commande suivant l'invite. Il n'y a pas de distinction entre les majuscules et les minuscules. La commande est suivie d'un ou plusieurs mots clés et arguments. Après avoir saisi une commande complète suivie des mots-clés et des arguments adéquats, appuyez sur la touche Entrée pour envoyer la commande à l'interpréteur de commandes.

Les mots-clés décrivent des paramètres spécifiques à l'interpréteur de commandes. Par exemple, la commande **show** affiche des informations sur le périphérique. Cette commande admet divers mots-clés permettant de préciser le type d'informations à afficher. Par exemple :

Switch# **show running-config**
La commande **show** est suivie du mot-clé **running-config**. Ce mot-clé spécifie que vous voulez afficher la configuration en cours.

Conventions des commandes IOS

Une commande peut exiger un ou plusieurs arguments. Un argument n'est généralement pas un mot prédéfini, contrairement à un mot clé. Un argument est une valeur ou une variable définie par l'utilisateur. Pour connaître les mots-clés et arguments requis pour une commande, consultez la section sur la syntaxe des commandes. La syntaxe indique le modèle ou le format devant être utilisé lorsque vous saisissez une commande.

Par exemple, la syntaxe d'une commande **description** est :
Switch(config-if)# **description** *chaîne*
Comme l'illustre la Figure 2, le texte en gras indique les commandes et les mots-clés à saisir tels quels et le texte en italique indique un argument pour lequel vous devez fournir une valeur. Pour la commande **description**, l'argument est une chaîne de charactères. La valeur de la chaîne peut être toute chaîne de texte de 80 caractères maximum.
Par exemple, pour associer une description à une interface à l'aide de la commande **description**, entrez une ligne telle que la suivante :
Switch(config-if)# **description Commutateur du QG**
La commande est **description** et l'argument défini par l'utilisateur est **Commutateur du QG.**
Les exemples suivants illustrent certaines conventions utilisées pour documenter et utiliser les commandes IOS.
Pour la commande **ping** :
Syntaxe :
Switch> **ping** *Adresse IP*
Exemple avec des valeurs :

Switch> **ping 10.10.10.5**
La commande est **ping** et l'argument défini par l'utilisateur est **10.10.10.5**.
De même, la syntaxe de la commande **traceroute** est la suivante :
Syntaxe :
Switch> **traceroute** *Adresse IP*
Exemple avec des valeurs :
Switch> **traceroute 192.168.254.254**
La commande est **traceroute** et l'argument défini par l'utilisateur est **192.168.254.254**.

2.1.4.2 Cisco IOS Command Référence

La liste des commandes Cisco IOS est un ensemble de documentation en ligne qui décrit en détail les commandes IOS utilisées sur les périphériques Cisco. La liste des commandes est la source d'informations de référence pour trouver une commande IOS particulière, de la même manière qu'un dictionnaire est la source de référence pour obtenir des informations sur un mot particulier.

La liste des commandes est une ressource essentielle qu'utilisent les ingénieurs réseau pour vérifier diverses caractéristiques d'une commande IOS donnée. Voici certaines des caractéristiques les plus courantes :

- **Syntaxe** - version la plus détaillée de la syntaxe d'une commande
- **Par défaut –** manière dont la commande est mise en œuvre sur un périphérique avec une configuration par défaut
- **Mode** - mode de configuration du périphérique sur lequel la commande est entrée
- **Historique** – description de la manière dont la commande est mise en œuvre en fonction de la version de l'IOS
- **Instructions d'utilisation** – instructions spécifiques décrivant comment mettre en œuvre la commande
- **Exemples** – exemples utiles illustrant les scénarios d'utilisation de la commande

Pour accéder à la liste des commandes et trouver une commande particulière, suivez les étapes ci-dessous :
Étape 1. Rendez-vous à l'adresse www.cisco.com.
Étape 2. Cliquez sur **Support**.
Étape 3. Cliquez sur **Networking Software** (IOS & NX-OS).
Étape 4. Cliquez sur **15.2M&T** (par exemple).
Étape 5. Cliquez sur **Reference Guides**.
Étape 6. Cliquez sur **CommandReferences**.
Étapes 7. Cliquez sur la technologie correspondant à la commande que vous recherchez.
Étape 8. Cliquez sur le lien à gauche (ordre alphabétique) correspondant à la commande concernée.
Étape 9. Cliquez sur le lien de la commande.
Par exemple, la commande **description** est disponible sous *Cisco IOS Interface and Hardware Component Command Reference*, sous le lien *D through E*.
Remarque : des versions PDF complètes des listes de commandes peuvent être téléchargées grâce à des liens sur la page affichée lorsque vous avez terminé l'étape 7 ci-dessus.

2.1.4.3 Aide contextuelle

IOS propose plusieurs types d'aide :

- Aide contextuelle
- Contrôle de la syntaxe des commandes
- Touches d'accès rapide et raccourcis

Aide contextuelle

L'aide contextuelle fournit la liste des commandes, des mots-clés et des arguments disponibles dans le contexte du mode en vigueur. Pour afficher l'aide contextuelle, saisissez un point d'interrogation **?** à une invite. Vous recevez une réponse immédiate sans qu'il soit nécessaire d'appuyer sur la touche Entrée.

L'aide contextuelle peut s'utiliser pour obtenir une liste des commandes disponibles. Ceci s'avère utile lorsque vous n'êtes pas sûr du nom d'une commande ou que vous voulez voir si IOS autorise une commande particulière dans un certain mode.

Par exemple, pour consulter les commandes disponibles dans le mode d'exécution utilisateur, tapez un point d'interrogation **?** à l'invite Switch>.

Vous pouvez aussi utiliser l'aide contextuelle pour afficher une liste des commandes ou des mots-clés débutant par des caractères spécifiques. Si vous entrez un point d'interrogation immédiatement après une suite de caractères (sans espace), IOS affiche la liste des commandes ou des mots-clés disponibles dans ce contexte, qui débutent par les caractères entrés.

Par exemple, entrez **sh?** pour obtenir la liste des commandes qui commencent par les caractères **sh**.

Enfin, vous pouvez vous servir de l'aide contextuelle pour déterminer les options, les mots-clés ou les arguments disponibles pour une commande donnée. À la suite d'une commande, entrez un espace suivi d'un **?** pour savoir ce qui peut ou doit être saisi.

Comme l'illustre la figure, après avoir tapé la commande **clock set 19:50:00**, il est possible de saisir **?** pour connaître les options ou les mots-clés supplémentaires disponibles pour la commande.

2.1.4.4 Contrôle de la syntaxe des commandes

Contrôle de la syntaxe des commandes

Lorsque vous soumettez une commande en appuyant sur la touche Entrée, l'interpréteur de commandes analyse la commande de gauche à droite pour déterminer l'action demandée. En général, l'IOS fournit uniquement des retours négatifs, comme illustré à la Figure 1. Si l'interpréteur comprend la commande, IOS exécute l'action demandée et l'invite appropriée reparaît dans l'interface CLI. Par contre, s'il ne comprend pas la commande entrée, l'interpréteur affiche des commentaires décrivant le problème rencontré.

La Figure 2 présente trois types de messages d'erreur :

- Commande ambiguë
- Commande incomplète
- Commande incorrecte

La commande **clock set** est une commande IOS conçue pour vous familiariser avec les messages de vérification de la syntaxe des commandes, comme illustré à la Figure 1. La Figure 2 décrit les trois types de messages d'erreur.

2.1.4.5 Touches d'accès rapide et raccourcis

Touches d'accès rapide et raccourcis

Dans l'interface CLI, des touches d'accès rapide et des raccourcis facilitent la configuration, la surveillance et le dépannage du système d'exploitation IOS.

La figure présente les principaux raccourcis. Les raccourcis suivants méritent des précisions :

- **Flèche Bas** – permet à l'utilisateur de faire défiler les commandes précédentes, de la plus ancienne à la plus récente
- **Flèche Haut** – permet à l'utilisateur de faire défiler les commandes précédentes, de la plus récente à la plus ancienne
- **Tab** - termine une commande ou un mot-clé partiellement saisis
- **Ctrl + A** – place le curseur au début de la ligne
- **Ctrl + E** – place le curseur à la fin de la ligne
- **Ctrl-R** - Affiche à nouveau une ligne.
- **Ctrl + Z** – permet de passer du mode de configuration au mode d'exécution utilisateur
- **Ctrl + C** - quitte le mode de configuration ou annule la commande actuelle
- **Ctrl + Maj + 6** (avec un clavier QWERTY) - permet à l'utilisateur d'interrompre un processus IOS comme ping ou traceroute. Avec un clavier AZERTY, il faudra utiliser le raccourci Ctrl + Maj + 9.

Examinons certains de ces raccourcis plus en détail :

Tabulation

La touche Tab permet de compléter automatiquement une commande ou un paramètre abrégés, si l'abréviation contient suffisamment de lettres pour exclure toute ambiguïté par rapport aux autres commandes ou paramètres disponibles. Après avoir tapé assez de caractères pour identifier la commande ou le mot-clé sans ambiguïté, appuyez sur la touche **Tab** pour afficher le reste de la commande ou du mot-clé.

Cette technique s'avère particulièrement utile pendant votre apprentissage parce qu'elle vous permet de voir en entier le mot servant de commande ou de mot-clé.

Ctrl + R

Afficher à nouveau la ligne permet d'actualiser la ligne qui vient d'être saisie. Utilisez **Ctrl-R** pour faire reparaître cette ligne. Par exemple, il peut arriver qu'un message IOS s'affiche dans l'interface CLI juste au moment où vous tapez une ligne. Vous pouvez alors utiliser **Ctrl-R** pour rappeler votre ligne afin d'éviter de la retaper.

Dans l'exemple suivant, un message concernant une interface défaillante interrompt l'entrée d'une commande.

Switch# **show mac-**
16w4d: %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to down
16w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to down
Pour rappeler la ligne que vous étiez en train de taper, utilisez **Ctrl + R** :
Switch# **show mac**
Ctrl + Z
Quitter le mode de configuration permet de sortir du mode de configuration et de revenir au mode d'exécution privilégié. Du fait de la structure hiérarchique des modes IOS, vous risquez de vous retrouver plusieurs niveaux plus bas lorsque vous quittez un mode. Pour cette raison, au lieu de quitter chaque mode séparément, utilisez le raccourci **Ctrl + Z** afin de retourner directement à l'invite du mode d'exécution privilégié au plus haut niveau.

Flèches Haut et Bas

Les touches de commandes précédentes permettent de consulter l'historique des commandes saisies. Comme le logiciel Cisco IOS conserve en mémoire tampon plusieurs commandes et caractères entrés par l'utilisateur, vous pouvez rappeler des entrées antérieures. La mémoire tampon s'avère utile pour saisir à nouveau des commandes sans avoir à les retaper.

Il est possible de parcourir les commandes stockées en mémoire tampon à l'aide de combinaisons de touches. Utilisez la flèche **Haut** (**Ctrl + P**) pour afficher les commandes entrées antérieurement. Chaque fois que vous appuyez sur cette touche, IOS affiche la commande précédente. À l'inverse, utilisez la flèche **Bas** (**Ctrl + N**) pour afficher la commande mémorisée suivante.

Ctrl + Maj + 6

Appuyer sur la touche Escape permet d'interrompre le processus en cours. Lorsque vous lancez un processus IOS à partir de l'interface en ligne de commande, par exemple ping ou traceroute, la commande s'exécute jusqu'à ce qu'elle se termine ou qu'elle soit interrompue. Pendant ce temps, l'interface en ligne de commande ne répond plus. Pour interrompre l'affichage des résultats et interagir avec la CLI, appuyez sur **Ctrl-Maj-6** (avec un clavier QWERTY). Avec un clavier AZERTY, il faudra utiliser le raccourci : Ctrl-Maj-9.

Ctrl + C

Interrompt l'entrée d'une commande et quitte le mode de configuration. Cela est utile si vous entrez une commande qui doit être annulée.

Commandes ou mots-clés abrégés

Il est possible d'abréger les commandes et les mots-clés jusqu'au nombre minimal de caractères formant un ensemble de caractères unique. Par exemple, vous pouvez abréger la commande **configure** en entrant **conf** parce que **configure** est la seule commande qui commence par **conf**. Par contre, l'abréviation **con** ne fonctionne pas parce que plusieurs commandes débutent par **con**.

Vous pouvez aussi abréger les mots-clés.
À titre d'exemple, **show interfaces** peut s'abréger de la façon suivante :
Switch# **show interfaces**
Switch# **show int**
Il est également possible d'abréger la commande et les mots-clés, comme le montre l'exemple suivant :

Switch# **sh int**

2.1.4.6 Commandes d'analyse d'IOS

Pour contrôler et dépanner le réseau, il est nécessaire d'examiner le fonctionnement des périphériques. La commande d'examen de base est la commande **show**.

Il existe plusieurs variantes de cette commande. À mesure que vous vous familiariserez avec IOS, vous apprendrez à utiliser les commandes **show** et à interpréter leurs résultats. Utilisez la commande **show ?** pour afficher la liste des commandes disponibles dans un contexte ou un mode donné.

Une commande **show** type peut fournir des informations sur la configuration, l'utilisation et l'état des pièces d'un commutateur ou d'un routeur Cisco. La figure illustre certaines des commandes IOS standard.

Dans ce cours, nous nous concentrons principalement sur les commandes **show** de base.

Une commande **show** très répandue est la commande **show interfaces**. Elle affiche des statistiques relatives à toutes les interfaces du périphérique. Pour afficher les statistiques d'une interface spécifique, entrez la commande **show interfaces** suivie du type d'interface et du numéro de port/slot. Par exemple :

Switch# **show interfaces fastethernet 0/1**
Voici d'autres commandes **show** fréquemment utilisées par les techniciens réseau :
show startup-config - affiche la configuration sauvegardée dans la mémoire vive non volatile.
show running-config - affiche le contenu du fichier de configuration en cours.
Commandes disponibles à l'invite More
Lorsque les résultats d'une commande ne tiennent pas dans un seul écran, l'invite **--More--** apparaît en bas de l'écran. Quand l'invite **--More--** apparaît, vous pouvez appuyer sur la touche **Espace** pour afficher la suite des résultats. Pour afficher seulement la ligne suivante, appuyez sur la touche **Entrée**. Si vous appuyez sur une autre touche, l'affichage des résultats est annulé et vous retournez à l'invite de commandes.

2.1.4.7 Commande show version

L'une des commandes les plus utilisées sur un commutateur ou un routeur est :

Switch# **show version**

Cette commande affiche des informations sur la version d'IOS actuelle ainsi que des renseignements sur le matériel et le périphérique. Si vous êtes connecté à un routeur ou à un commutateur à distance, la commande **show version** est un excellent moyen de trouver

rapidement des informations utiles sur le périphérique auquel vous êtes connecté. Cette commande affiche, entre autres, les informations suivantes :

- **Version du logiciel** - Version du logiciel IOS (stocké en mémoire Flash)
- **Version du bootstrap** - Version du programme de démarrage (stocké en mémoire ROM de démarrage)
- **Durée de l'activité du système** - Temps écoulé depuis le dernier redémarrage
- **Informations sur le redémarrage du système** - Méthode de redémarrage (par exemple en cas de cycle d'alimentation ou d'incident)
- **Nom de l'image du logiciel** - Nom du fichier IOS stocké en mémoire Flash
- **Type de routeur et type de processeur** - Numéro de modèle et type de processeur
- **Type et allocation de la mémoire (partagée/principale)** - Mémoire vive principale du processeur et mémoire partagée servant de tampon pour les paquets d'E/S
- **Fonctionnalités du logiciel** - Protocoles/ensembles de fonctionnalités pris en charge
- **Interfaces matérielles** - Interfaces disponibles sur le périphérique
- **Registre de configuration** - Définit les spécifications du démarrage, la vitesse de la console et des paramètres connexes

La Figure 1 présente le résultat pour un routeur à services intégrés Cisco 1941, tandis que la Figure 2 présente le résultat pour un commutateur Cisco Catalyst 2960.

2.2 Bases

2.2.1 Noms d'hôtes

2.2.1.1 Pourquoi utiliser un commutateur ?

Comme expliqué ci-dessus, les commutateurs et les routeurs Cisco ont beaucoup de points communs. Ils prennent en charge le même système d'exploitation de modes, les mêmes structures de commandes et comptent de nombreuses commandes similaires. En outre, les étapes de configuration initiale sont identiques pour les deux périphériques lors de la mise en œuvre dans un réseau.

Toutefois, un commutateur Cisco IOS est l'un des périphériques les plus simples pouvant être configurés sur un réseau. En effet, aucune configuration n'est nécessaire avant d'utiliser le périphérique. Dans sa configuration la plus simple, un commutateur peut être connecté sans être configuré. Dans ce cas, il effectuera tout de même la commutation des données entre les périphériques connectés.

Un commutateur est également l'un des éléments fondamentaux utilisés lors de la création d'un petit réseau. En reliant deux PC à un commutateur, ces ordinateurs disposeront d'une interconnectivité instantanée.

Pour ces raisons, le reste de ce chapitre porte sur la création d'un petit réseau composé de deux PC connectés via un commutateur configuré avec les paramètres d'origine. Les paramètres initiaux comprennent l'attribution d'un nom pour le commutateur, la limitation de l'accès à la configuration du périphérique, la configuration des messages de bannière et l'enregistrement de la configuration.

2.2.1.2 Noms de périphériques

Lors de la configuration d'un périphérique réseau, l'une des premières étapes est la configuration d'un nom de périphérique unique, ou nom d'hôte. Les noms d'hôte apparaissent

dans les invites de la CLI, peuvent être utilisés dans différents processus d'authentification entre les périphériques et doivent être utilisés dans les diagrammes de topologie.

Les noms d'hôtes sont configurés sur le périphérique réseau actif. Si le nom du périphérique n'est pas explicitement configuré, un nom de périphérique par défaut est utilisé par Cisco IOS. Le nom par défaut d'un commutateur Cisco IOS est « Switch ».

Imaginez un interréseau disposant de plusieurs commutateurs portant le nom par défaut « Switch » (comme illustré sur la figure). Il en résulterait une grande confusion lors de la configuration et de la maintenance du réseau. En accédant à un périphérique distant avec une connexion SSH, il est important d'être sûr que vous êtes connecté au périphérique approprié. Si tous les périphériques ont conservé leurs noms par défaut, il est difficile d'identifier le bon périphérique.

En revanche, si vous choisissez et notez les noms intelligemment, vous n'aurez aucune peine à mémoriser, expliquer et utiliser les noms des périphériques réseau. Pour nommer les périphériques de façon cohérente et utile, il est nécessaire d'établir une convention d'attribution de noms applicable dans toute l'entreprise ou tout au moins à l'emplacement géographique des périphériques. Il est conseillé de créer la convention d'attribution de noms en même temps que le schéma d'adressage afin d'assurer l'homogénéité au sein de l'entreprise.

Les conventions d'attribution des noms doivent par exemple imposer que ceux-ci :

- Commencent par une lettre
- Ne contiennent pas d'espaces
- Se terminent par une lettre ou un chiffre
- Ne comportent que des lettres, des chiffres et des tirets
- Comportent moins de 64 caractères

IOS distingue les majuscules des minuscules dans les noms d'hôte utilisés pour les périphériques. Vous pouvez donc utiliser des majuscules comme vous le feriez normalement pour un nom. Contrairement à IOS, la plupart des systèmes d'attribution de noms Internet ne font aucune distinction entre majuscules et minuscules.

2.2.1.3 Noms d'hôtes

Les noms d'hôte permettent aux administrateurs réseau d'identifier les périphériques sur un réseau ou sur Internet.

Exemples d'attribution de noms

Prenons un exemple de trois commutateurs interconnectés dans un réseau qui couvre trois étages différents.

Pour créer une convention d'attribution de noms pour les commutateurs, vous devez prendre en compte leur emplacement et le rôle qu'ils jouent.

Par exemple, dans la figure, nous avons nommé les commutateurs Sw-Floor-1, Sw-Floor-2 et Sw-Floor-3.

Il convient de consigner ces noms dans la documentation du réseau en expliquant les raisons de leur choix, afin d'assurer la continuité dans l'attribution de noms lorsque de nouveaux périphériques seront ajoutés au réseau.

Une fois la convention d'attribution de noms établie, l'étape suivante consiste à associer ces noms aux périphériques à l'aide de la CLI.

2.2.1.4 Configuration des noms d'hôtes

Configuration du nom d'hôte IOS

En mode d'exécution privilégié, accédez au mode de configuration globale en entrant la commande **configure terminal** :

Switch# **configure terminal**
Après exécution de cette commande, l'invite devient :
Switch(config)#
Comme l'illustre la figure, en mode de configuration globale, entrez le nom d'hôte :
Switch(config)# **hostname Sw-Floor-1**
Après exécution de cette commande, l'invite devient :
Sw-Floor-1 (config)#

Observez que le nom d'hôte apparaît dans l'invite. Pour quitter le mode de configuration globale, utilisez la commande **exit**.

N'oubliez pas de mettre à jour votre documentation chaque fois que vous ajoutez ou modifiez un périphérique. Dans la documentation, identifiez les périphériques par leur emplacement, leur rôle et leur adresse.

Remarque : pour annuler ou inverser les effets d'une commande, faites-la précéder du mot-clé **no**.

Par exemple, pour supprimer le nom attribué à un périphérique, utilisez :
Sw-Floor-1 (config)# **no hostname**
Switch(config)#
Notez que la commande **no hostname** rétablit sur le commutateur le nom d'hôte par défaut « Switch ».

À l'aide de la figure, essayez d'attribuer un nom d'hôte à un commutateur.

2.2.2 Limitation de l'accès aux configurations de périphérique

2.2.2.1 Sécurisation de l'accès au périphérique

Il est recommandé de limiter physiquement l'accès aux périphériques réseau en les plaçant dans des pièces et des armoires fermées à clé ; toutefois, les mots de passe sont la principale défense contre l'accès non autorisé à ces périphériques. Tous les périphériques, même des routeurs domestiques, doivent être configurés localement avec des mots de passe pour limiter l'accès au réseau. Plus tard, nous expliquerons comment renforcer la sécurité en demandant un nom d'utilisateur et un mot de passe à la connexion. Pour l'instant, nous allons présenter des

précautions de base en matière de sécurité qui reposent uniquement sur l'emploi de mots de passe.

Comme vous le savez, IOS utilise des modes organisés hiérarchiquement pour faciliter la protection des périphériques. Dans le cadre de ce dispositif de sécurité, IOS peut accepter plusieurs mots de passe, ce qui vous permet d'établir différents privilèges d'accès au périphérique.

Caractéristiques des mots de passe présentés ici :

- **Mot de passe d'activation (enable)** – limite l'accès au mode d'exécution privilégié.
- **Mot de passe secret actif** – chiffré, limite l'accès au mode d'exécution privilégié.
- **Mot de passe de console** – limite l'accès au périphérique par une connexion console.
- **Mot de passe VTY** – limite l'accès au périphérique par une connexion Telnet.

Il est recommandé d'utiliser des mots de passe différents pour chacun de ces niveaux d'accès. En effet, bien que l'utilisation de plusieurs mots de passe différents ne facilite pas l'ouverture d'une session, cette précaution est nécessaire pour protéger convenablement l'infrastructure réseau contre l'accès non autorisé.

En outre, utilisez des mots de passe forts qui ne sont pas faciles à deviner. L'utilisation de mots de passe faibles ou faciles à deviner demeure un véritable problème de sécurité dans de nombreuses entreprises.

Pour choisir les mots de passe, respectez les règles suivantes :

- Utilisez des mots de passe de plus de 8 caractères.
- Utilisez une combinaison de lettres majuscules et minuscules, des chiffres, des caractères spéciaux et/ou des séquences de chiffres dans les mots de passe.
- Évitez d'utiliser le même mot de passe pour tous les périphériques.
- Abstenez-vous d'employer des mots communs tels que mot de passe ou administrateur, parce qu'ils sont faciles à deviner.

Remarque : dans la plupart des travaux pratiques de ce cours, nous utiliserons des mots de passe simples tels **que cisco** ou **class**. Il faut éviter ces mots de passe dans un environnement de production, car ils sont considérés comme faibles et faciles à deviner. Nous n'utilisons ces mots de passe que pour une utilisation dans une salle de cours ou pour illustrer des exemples de configuration.

2.2.2.2 Sécurisation de l'accès au mode d'exécution privilégié

Pour sécuriser l'accès au mode d'exécution privilégié, utilisez la commande **enable secret** *mot_de_passe*. Une variante de cette commande, plus ancienne et moins sécurisée, est la commande **enable password** *mot_de_passe*. Bien que l'une de ces commandes puisse être utilisée pour établir l'authentification avant l'accès au mode d'exécution privilégié (enable), il est recommandé d'utiliser la commande **enable secret**. En effet, la commande **enable secret** offre une plus grande sécurité dans la mesure où le mot de passe est chiffré.
Exemple de commande permettant de définir les mots de passe :
Switch(config)# **enable secret class**
La figure illustre le fait qu'un mot de passe n'est pas requis lors de la première utilisation de la commande **enable**. Ensuite, la commande **enable secret class** est configurée et l'accès au mode d'exécution privilégié est sécurisé. Notez que pour des raisons de sécurité, le mot de passe ne s'affiche pas lorsqu'il est saisi.

2.2.2.3 Sécurisation de l'accès au mode d'exécution utilisateur

Pour cette raison, vous devez sécuriser le port de console des périphériques réseau en exigeant, au minimum, que l'utilisateur fournisse un mot de passe fort. Cela réduit les chances qu'un personnel non autorisé branche physiquement un câble sur le port de console de l'appareil et accède ainsi au périphérique.

Vous utilisez les commandes suivantes en mode de configuration globale pour définir un mot de passe pour la ligne de console :

Switch(config)# **line console 0**
Switch(config-line)# **password cisco**
Switch(config-line)# **login**
À partir du mode de configuration globale, la commande **line console 0** permet d'entrer en mode de configuration de ligne pour la console. Le zéro sert à représenter la première (et le plus souvent, la seule) interface de console.

La deuxième commande, **password cisco** définit un mot de passe pour la ligne de console.

Enfin, la commande **login** permet de configurer le commutateur pour qu'il exige une authentification à l'ouverture de session. Lorsque la connexion est activée et qu'un mot de passe est défini, l'utilisateur de la console est invité à saisir un mot de passe avant d'accéder à la CLI.

Mot de passe VTY

Les lignes vty permettent d'accéder à un routeur Cisco via Telnet. Par défaut, de nombreux commutateurs Cisco prennent en charge jusqu'à 16 lignes vty, numérotées de 0 à 15. Le nombre de lignes vty prises en charge par un routeur Cisco varie selon le type de routeur et la version de l'IOS. Cependant, en général, cinq lignes vty sont configurées. Ces lignes sont numérotées de 0 à 4 par défaut, bien que des lignes supplémentaires puissent être configurées. Vous devez définir un mot de passe pour toutes les lignes vty disponibles. Vous pouvez certes définir le même mot de passe pour toutes les connexions. Toutefois, il est souvent souhaitable d'associer un mot de passe unique à une certaine ligne afin de réserver un accès à un administrateur lorsque les autres connexions sont utilisées.

Exemples de commandes permettant de définir un mot de passe sur les lignes vty :
Switch(config)# **line vty 0 15**
Switch(config-line)# **password cisco**
Switch(config-line)# **login**

Par défaut, l'IOS inclut la commande **login** sur les lignes VTY. Cela permet d'interdire les accès Telnet au périphérique sans authentification préalable. Si vous avez exécuté par inadvertance la commande **no login**, rien n'empêche des personnes non autorisées de se connecter à la ligne avec Telnet puisque l'authentification n'est plus obligatoire. Il s'agit d'un risque majeur en matière de sécurité.

La figure illustre la sécurisation de l'accès au mode d'exécution utilisateur sur les lignes de console et Telnet.

2.2.2.4 Chiffrement de l'affichage des mots de passe

Une autre commande utile permet d'empêcher l'affichage des mots de passe en clair lorsqu'un utilisateur consulte les fichiers de configuration. Il s'agit de la commande **service password-encryption**.

Cette commande provoque le chiffrement des mots de passe déjà configurés. La commande **service password-encryption** applique un chiffrement simple à tous les mots de passe non chiffrés. Ce chiffrement ne s'applique qu'aux mots de passe du fichier de configuration et non aux mots de passe transmis sur le support. Le but de cette commande est d'empêcher les personnes non autorisées de lire les mots de passe dans le fichier de configuration.

Si vous exécutez la commande **show running-config** ou **show startup-config** avant la commande **service password-encryption**, les mots de passe non chiffrés sont visibles dans les informations fournies par le périphérique sur sa configuration. Dès que vous exécutez la commande service password-encryption, IOS applique le chiffrement aux mots de passe. Par la suite, les mots de passe déjà chiffrés le restent même si vous supprimez le service password-encryption (en annulant la commande).

À l'aide de la figure, essayez d'entrer une commande permettant de configurer le chiffrement des mots de passe.

2.2.2.5 Messages de bannière

Bien que les mots de passe soient l'un des moyens dont vous disposez pour empêcher l'accès non autorisé à un réseau, il est vital de mettre en place une méthode pour déclarer que l'accès à un périphérique est réservé aux personnes autorisées. À cet effet, ajoutez une bannière aux informations affichées par le périphérique.

Les bannières peuvent constituer une pièce importante dans un procès intenté à une personne qui aurait accédé illégalement à un périphérique. En effet, dans certains systèmes juridiques, il n'est pas possible de poursuivre des utilisateurs, ni même de les surveiller, sauf s'ils ont reçu une notification appropriée.

La formulation utilisée dans une bannière dépend des lois en vigueur localement et des stratégies d'entreprise. Voici quelques exemples d'informations à inclure dans une bannière :

- « L'utilisation du périphérique est strictement réservée au personnel autorisé. »
- « Vos interactions avec le périphérique peuvent faire l'objet d'une surveillance. »
- « Toute utilisation non autorisée fera l'objet de poursuites judiciaires. »

Comme les bannières peuvent être vues par quiconque essaie d'ouvrir une session, le message doit être formulé avec la plus grande prudence. Par exemple, il faut éviter de laisser entendre que l'utilisateur qui ouvre la session est « bienvenu » ou « invité » à le faire. En effet, il est difficile de prouver la responsabilité d'une personne qui perturbe le fonctionnement du réseau après un accès non autorisé s'il apparaît qu'elle a été invitée à le faire.

La création de bannières est un processus simple, à condition de respecter un minimum de règles dans leur rédaction. Si vous utilisez une bannière, abstenez-vous de souhaiter la bienvenue à l'utilisateur accédant au routeur. Votre bannière doit préciser que seul le personnel autorisé a le droit d'accéder au périphérique. Enfin, la bannière peut contenir des

informations sur les arrêts programmés du système et d'autres renseignements concernant tous les utilisateurs du réseau.

IOS fournit plusieurs types de bannières. L'une des bannières communes est le message du jour (MOTD). Ce message s'utilise souvent pour les mentions légales parce qu'il s'affiche sur tous les terminaux connectés.

Configurez le message du jour en entrant la commande **banner motd** en mode de configuration globale.

La commande **banner motd** nécessite l'emploi de délimiteurs pour identifier le contenu du message de bannière. La commande **banner motd** est suivie d'un espace et d'un caractère de délimitation. Ensuite, une ou plusieurs lignes de texte constituent le message de bannière. Enfin, le caractère de délimitation apparaît une seconde fois pour marquer la fin du message. Vous pouvez utiliser comme délimiteur tout caractère ne figurant pas dans le message. C'est la raison pour laquelle les symboles tels que « # » sont souvent employés comme délimiteurs.

La syntaxe permettant de configurer un message du jour, en mode de configuration globale, est :
Switch(config)# **banner motd #** *le message* **#**
Une fois cette commande exécutée, la bannière s'affichera lors de toutes les tentatives d'accès au périphérique suivantes jusqu'à ce que vous la supprimiez.

2.2.3 Enregistrement des configurations

2.2.3.1 Fichiers de configuration

Le fichier de configuration en cours reflète la configuration actuelle appliquée à un périphérique Cisco IOS. Il contient les commandes utilisées pour déterminer comment le périphérique fonctionne sur le réseau, comme indiqué à la Figure 1. Modifier une configuration en cours affecte le fonctionnement d'un périphérique Cisco immédiatement.

Le fichier de configuration en cours est stocké dans la mémoire vive du périphérique (RAM). Cela signifie que le fichier de configuration en cours est temporairement actif lorsque le périphérique Cisco fonctionne (sous tension). Cependant, en cas de panne de courant ou de redémarrage du routeur, toutes les modifications de la configuration que vous n'avez pas enregistrées sont perdues.

Après avoir apporté des modifications à un fichier de configuration en cours, trois possibilités s'offrent à vous :

- restaurer la configuration d'origine du périphérique ;
- supprimer toutes les configurations du périphérique ;
- adopter la configuration modifiée comme nouvelle configuration initiale.

Le fichier de configuration initiale reflète la configuration utilisée par le périphérique lors du redémarrage. Le fichier de configuration initiale est stocké dans la mémoire vive non volatile. Lorsqu'un périphérique réseau est configuré et que la configuration en cours est modifiée, il est important d'enregistrer ces modifications dans le fichier de configuration initiale. Ainsi, vous ne risquez pas de perdre des modifications à la suite d'une panne de courant ou d'un redémarrage intentionnel.

Avant de pérenniser une configuration modifiée, utilisez les commandes **show** adéquates pour vérifier le fonctionnement du périphérique. Comme le montre la figure, vous pouvez entrer la

commande **show running-config** pour afficher le contenu d'un fichier de configuration en cours. Après avoir vérifié que les modifications sont correctes, utilisez la commande **copy running-config startup-config** à l'invite du mode d'exécution privilégié. La commande permettant d'enregistrer la configuration en cours dans le fichier de configuration initiale est la suivante :

Switch# **copy running-config startup-config**

Après avoir été exécuté, le fichier de configuration en cours met à jour le fichier de configuration initiale.

Si les modifications apportées à la configuration en cours n'ont pas l'effet souhaité, il peut s'avérer nécessaire de revenir à la configuration antérieure du périphérique. Dans l'hypothèse où vous n'avez pas recouvert la configuration initiale avec les modifications, vous pouvez remplacer la configuration en cours par la configuration initiale. Le meilleur moyen de le faire consiste à redémarrer le périphérique en entrant la commande **reload** en mode d'exécution privilégié.

Quand il reçoit une commande de rechargement, IOS vérifie si la configuration en cours comporte des modifications qui n'ont pas été enregistrées dans la configuration initiale. Dans l'affirmative, IOS affiche une invite vous demandant s'il doit enregistrer les modifications. Pour abandonner les modifications, entrez **n** ou **no**.

Une autre invite apparaît pour vous permettre de confirmer le rechargement. Pour confirmer, appuyez sur Entrée. Toute autre touche annule la commande.

Par exemple :
Switch# **reload**
System configuration has been modified. Save? [yes/no]: **n**
Proceed with reload? [confirm]
*Apr 13 01:34:15.758: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2009 by cisco Systems, Inc.
PLD version 0x10
GIO ASIC version 0x127
c1841 processor with 131072 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled

Si des modifications indésirables sont enregistrées dans la configuration initiale, il peut s'avérer nécessaire de supprimer toutes les configurations. Pour ce faire, vous devez effacer la configuration initiale et redémarrer le périphérique.

La commande **erase startup-config** permet de supprimer la configuration initiale.

Pour supprimer le fichier de configuration initiale, entrez **erase NVRAM:startup-config** ou **erase startup-config** à l'invite du mode d'exécution privilégié :

Switch# **erase startup-config**
Quand vous entrez cette commande, le commutateur vous demande confirmation :

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
Confirm est la réponse par défaut. Pour confirmer la suppression du fichier de configuration initiale, appuyez sur la touche Entrée. Toute autre touche annule la commande.

Attention : utilisez la commande **erase** avec précaution. En effet, erase permet de supprimer tous les fichiers du périphérique. Une utilisation incorrecte peut donc aboutir à effacer IOS lui-même ou un autre fichier important.

Sur un commutateur, vous devez également exécuter la commande **delete vlan.dat** en plus de la commande **erase startup-config**, afin de restaurer la configuration initiale du périphérique par défaut (comparable à une restauration de la configuration d'usine) :

Switch# **delete vlan.dat**
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch# **erase startup-config**
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
Après la suppression de la configuration initiale de la mémoire vive non volatile (et la suppression du fichier vlan.dat dans le cas d'un commutateur), rechargez le périphérique pour supprimer le fichier de configuration en cours de la mémoire vive. Le périphérique charge alors la configuration initiale par défaut et l'adopte comme configuration en cours.

À l'aide de la Figure 2, essayez d'entrer des commandes permettant d'enregistrer la configuration en cours dans la mémoire vive sur la mémoire vive non volatile.

2.2.3.2 Légende

Sauvegarde des configurations par capture de texte

Il est possible d'enregistrer des configurations en cours en tant que configurations initiales, mais les fichiers de configuration peuvent également être sauvegardés et archivés sous forme de document texte. Cette procédure permet de s'assurer qu'une copie de travail des fichiers de configuration est disponible en vue d'une modification ou une réutilisation ultérieure.

Comme l'illustre la Figure 1, les fichiers de configuration peuvent être stockés et archivés sur un document texte à l'aide de Tera Term.

Les étapes sont les suivantes :

- Dans le menu File, cliquez sur **Log**.
- Choisissez l'emplacement. Tera Term commence à capturer le texte.
- Après avoir démarré la capture, exécutez la commande **show running-config** ou **show startup-config** à l'invite du mode d'exécution privilégié. Le texte affiché dans la fenêtre du terminal est alors placé dans le fichier choisi.
- Une fois la capture terminée, sélectionnez **Close** dans la fenêtre Tera Term:Log.
- Affichez le contenu du fichier de sortie pour vérifier qu'il s'agit bien des informations voulues.

De même, la Figure 2 montre comment les fichiers peuvent être enregistrés et archivés dans un document texte à l'aide de HyperTerminal.

Restauration des configurations sauvegardées dans un document texte

Il est possible de copier un fichier de configuration à partir d'un support de stockage vers un périphérique. IOS considère chaque ligne du texte de configuration copié dans le terminal comme une commande et l'exécute. Des modifications du fichier seront probablement nécessaires avant de copier ledit fichier. Il est conseillé de passer du chiffrement des mots de passe à des mots de passe en clair et de supprimer le paramètre, numéro 5 ou 7, qui indique que le mot de passe est chiffré. Le texte ne faisant pas partie de commandes, par exemple les messages IOS ou « --More-- », doit être supprimé. Ce processus est expliqué dans les travaux pratiques.

En outre, dans l'interface en ligne de commande, le périphérique doit être en mode de configuration globale, sinon il ne recevra pas les commandes du fichier texte copié.

Avec Tera Term, la procédure est la suivante :

- Modifiez le texte pour supprimer les mots ne faisant pas partie des commandes, puis enregistrez le fichier.
- Dans le menu **File**, cliquez sur **Send**.
- Recherchez le fichier à copier sur le périphérique et cliquez sur **Open**.
- Tera Term colle alors le fichier dans le périphérique.

Le texte contenu dans le fichier est appliqué sous forme de commandes dans l'interface en ligne de commande et devient la configuration en cours du périphérique. Cette méthode s'avère pratique pour configurer manuellement un périphérique.

2.3 Schémas d'adressage

2.3.1 Ports et adresses

2.3.1.1 Adressage IP des périphériques

L'utilisation d'adresses IP, IPv4 ou IPv6, est le principal moyen permettant aux périphériques de se localiser les uns les autres et d'établir la communication de bout en bout sur Internet. En fait, dans tout interréseau, les adresses IP sont essentielles pour que les périphériques communiquent de la source à la destination et inversement.

Chaque périphérique final d'un réseau doit comporter une adresse IP. Voici quelques exemples de périphériques finaux :

- Ordinateurs (stations de travail, ordinateurs portables, serveurs de fichiers, serveurs Web)
- Imprimantes réseau
- Téléphones VoIP
- Caméras de surveillance
- Smartphones
- Périphériques mobiles (par exemple, lecteurs de codes-barres sans fil)

La structure d'une adresse IPv4 est appelée « notation décimale à point » et est composée de quatre nombres décimaux compris entre 0 et 255. Les adresses IPv4 sont des numéros affectés à des périphériques connectés à un réseau. Ces adresses sont logiques par nature, dans la mesure où elles fournissent des informations sur l'emplacement des périphériques.

En plus d'une adresse IP, un masque de sous-réseau est également nécessaire. Un masque de sous-réseau est un type spécial d'adresse IPv4 qui, allié à l'adresse IP, détermine à quel sous-réseau spécifique (qui fait partie d'un réseau plus grand) le périphérique appartient.

Les adresses IP peuvent être attribuées aux ports physiques et aux interfaces virtuelles des périphériques. Une interface virtuelle signifie qu'il n'y a aucun matériel physique sur le périphérique qui lui est associé.

2.3.1.2 Interfaces et Port

Les communications réseau dépendent des interfaces des périphériques utilisateur, des interfaces des périphériques réseau et des câbles de connexion.

Chaque interface a des caractéristiques, ou des normes, qui la définissent : un câble de connexion à l'interface doit donc être adapté aux normes physiques de l'interface. Ces supports réseau incluent les câbles en cuivre à paires torsadées, les câbles à fibres optiques, les câbles coaxiaux ou la technologie sans fil. Les différents types de supports réseau possèdent divers avantages et fonctionnalités. Tous les supports réseau ne possèdent pas les mêmes caractéristiques et ne conviennent pas pour les mêmes objectifs. Quelques différences entre les supports de transmission :

- la distance sur laquelle les supports peuvent transporter correctement un signal ;
- l'environnement dans lequel les supports doivent être installés ;
- la quantité de données et le débit de la transmission ;
- le coût des supports et de l'installation.

Chaque liaison à Internet requiert un type de support réseau spécifique, ainsi qu'une technologie réseau particulière. L'Ethernet est la technologie de réseau local (LAN) la plus répandue aujourd'hui. Les ports Ethernet sont présents sur les périphériques des utilisateurs finaux, les commutateurs et d'autres périphériques réseau pouvant se connecter physiquement au réseau à l'aide d'un câble. Pour qu'un câble puisse connecter des périphériques à l'aide d'un port Ethernet, celui-ci doit disposer du connecteur approprié, RJ-45.

Les commutateurs Cisco IOS sont équipés de ports physiques pour la connexion, mais intègrent également une ou plusieurs interfaces virtuelles de commutateur (SVI). Ce sont des interfaces virtuelles car il n'existe aucun matériel sur le périphérique associé : une interface SVI est créée au niveau logiciel. L'interface virtuelle est un moyen de gérer à distance un commutateur sur un réseau grâce à l'IPv4. Chaque commutateur dispose d'une interface SVI apparaissant dans la configuration initiale par défaut prête à l'emploi . L'interface SVI par défaut est l'interface VLAN1.

2.3.2 Adressage des périphériques

2.3.2.1 Configuration d'une interface virtuelle de commutateur

Pour accéder à distance au commutateur, une adresse IP et un masque de sous-réseau doivent être configurés sur l'interface SVI :

- **Adresse IP** - combinée au masque de sous-réseau, identifie le périphérique final sur l'interréseau de manière unique.

- **Masque de sous-réseau** – détermine quelle partie d'un réseau plus étendu est utilisée par une adresse IP.

Pour l'instant, le cours est axé sur l'IPv4. Vous étudierez l'IPv6 plus tard.

Vous apprendrez ultérieurement le fonctionnement de toutes ces adresses IP, mais pour l'instant, l'objectif est de configurer rapidement le commutateur pour gérer l'accès distant. La figure présente la commande permettant d'activer la connectivité IP au périphérique S1, via l'adresse IP 192.168.10.2 :

- **interface vlan 1** - Utilisé pour accéder au mode de configuration d'interface à partir du mode de configuration globale
- **ip address 192.168.10.2 255.255.255.0** - Configure l'adresse IP et le masque de sous-réseau pour le commutateur (ce n'est que l'une des nombreuses combinaisons possibles d'adresse IP et de masque de sous-réseau)
- **no shutdown** - Active l'interface par voie administrative

Une fois ces commandes configurées, le commutateur dispose de tous les éléments IP adaptés pour la communication sur le réseau.

Remarque : le commutateur doit toujours disposer d'un ou de plusieurs ports physiques configurés, ainsi que des lignes VTY, pour qu'il soit possible de terminer la configuration qui permet une gestion distante du commutateur.

Essayez de configurer une interface virtuelle de commutateur en entrant les commandes de la figure.

2.3.2.2 Configuration manuelle des adresses IP des périphériques finaux

Pour qu'un périphérique final puisse communiquer sur le réseau, les informations correctes d'adresse IP doivent lui être attribuées. Tout comme une interface SVI de commutateur, le périphérique final doit disposer d'une adresse IP et d'un masque de sous-réseau. Ces informations sont définies sur les paramètres de l'ordinateur.

Tous ces paramètres doivent être configurés sur un périphérique final pour qu'il puisse se connecter correctement au réseau. Ces informations sont configurées dans les paramètres réseau de l'ordinateur. Outre l'adresse IP et le masque de sous-réseau, il est également possible de configurer les informations de passerelle par défaut et de serveur DNS, comme illustré dans la figure.

L'adresse de passerelle par défaut est l'adresse IP de l'interface de routeur utilisée pour que le trafic réseau sorte du réseau local. La passerelle par défaut est l'adresse IP qui est souvent attribuée par l'administrateur réseau et est utilisée lorsque le trafic doit être acheminé vers un autre réseau.

L'adresse du serveur DNS est l'adresse IP du serveur de noms de domaine (DNS), qui est utilisé pour convertir des adresses IP en adresses Web, par exemple www.cisco.com. Sur Internet, tous les périphériques possèdent une adresse IP. C'est cette adresse qui est utilisée pour les joindre. Cependant, il est plus facile pour les utilisateurs de se souvenir de noms plutôt que de numéros. Par conséquent, les sites Web se voient attribuer des noms pour simplifier ce processus. Le serveur DNS est utilisé pour garantir le mappage entre les adresses IP et les noms de différents périphériques

2.3.2.3 Configuration automatique des adresses IP des périphériques finaux

Les informations d'adresse IP peuvent être entrées manuellement sur le PC, ou attribuées automatiquement à l'aide du protocole DHCP (Dynamic Host Configuration Protocol). Le protocole DHCP permet aux périphériques finaux de disposer d'informations IP configurées automatiquement.

Le protocole DHCP est une technologie utilisée sur presque tous les réseaux d'entreprise. Le meilleur moyen de comprendre pourquoi le DHCP est tellement répandu est de prendre en compte tout le travail supplémentaire qui doit être effectué sans celui-ci.

Le protocole DHCP permet la configuration automatique des adresses IPv4 pour chaque périphérique final sur un réseau utilisant DHCP. Imaginez que chaque fois que vous vous connectez au réseau, vous devez entrer manuellement l'adresse IP, le masque de sous-réseau, la passerelle par défaut, et le serveur DNS. Multipliez cette opération par le nombre d'utilisateurs et de périphériques sur le réseau : vous avez saisi le problème.

Le protocole DHCP est un exemple de technologie fonctionnant de manière optimale. L'un des principaux objectifs de toute technologie est de faciliter les opérations. Grâce au protocole DHCP, les utilisateurs entrent dans la zone couverte par un réseau donné, connectent un câble Ethernet ou activent une connexion sans fil, et les informations IPv4 nécessaires à la communication sur le réseau leur sont attribuées automatiquement.

Comme l'illustre la Figure 1, pour configurer le protocole DHCP sur un ordinateur Windows, vous devez sélectionner « Obtenir une adresse IP automatiquement » et « Obtenir les adresses des serveurs DNS automatiquement ». Votre ordinateur reçoit automatiquement les informations en provenance d'un pool d'adresses IP et les informations IP associées sont configurées sur le serveur DHCP.

Il est possible d'afficher les paramètres de configuration IP d'un PC Windows à l'aide de la commande **ipconfig** à l'invite de commande. Le résultat affiche l'adresse IP, le masque de sous-réseau et la passerelle que le PC a reçus du serveur DHCP.

Essayez de consulter l'adresse IP d'un ordinateur Windows en entrant les commandes de la Figure 2.

2.3.2.4 Conflits d'adresses IP

Si une adresse IP statique (manuelle) est configurée pour un périphérique réseau, par exemple, une imprimante, et qu'un serveur DHCP est activé, des conflits d'adresses IP dupliquées peuvent survenir entre le périphérique réseau et un ordinateur obtenant automatiquement son adresse IP à partir du serveur DHCP. Un conflit peut également se produire lorsque vous attribuez manuellement une adresse IP statique à un périphérique réseau pendant une défaillance du réseau impliquant le serveur DHCP : une fois les défaillances du réseau résolues et le serveur DHCP accessible, le conflit survient.

Pour résoudre ce type de conflits d'adressage IP, configurez le périphérique réseau avec l'adresse IP statique d'un client DHCP, ou excluez l'adresse IP statique du périphérique final de la plage d'adresses DHCP sur le serveur DHCP.

Cette dernière solution nécessite de disposer de droits d'administrateur sur le serveur DHCP et de bien connaître la configuration du protocole DHCP sur un serveur.

Vous pouvez également rencontrer des problèmes de conflit d'adressage IP en configurant manuellement l'adresse IP d'un périphérique final sur un réseau qui utilise uniquement des adresses IP statiques. Dans ce cas, vous devez déterminer quelles adresses IP sont disponibles sur le sous-réseau IP en question et appliquer une configuration en conséquence. Cet exemple montre pourquoi il est important qu'un administrateur réseau tienne à jour une documentation détaillée, comprenant les attributions d'adresses IP, pour les périphériques utilisateur.

Remarque : généralement, des adresses IP statiques sont utilisées pour les serveurs et les imprimantes d'un réseau de PME, tandis que les périphériques des employés utilisent des informations d'adresses IP attribuées par DHCP.

2.3.3 Vérification de la connectivité

2.3.3.1 Test de l'adresse de bouclage sur un périphérique final

Test de la boucle

La figure représente la première étape de la série de tests. La commande **ping** permet de vérifier la configuration IP interne d'un hôte local. Ce test s'effectue en exécutant la commande **ping** sur une adresse réservée appelée adresse de bouclage (127.0.0.1). L'adresse de bouclage, 127.0.0.1, est définie par le protocole TCP/IP comme adresse réservée renvoyant les paquets vers l'hôte.

Les commandes ping sont entrées sur une ligne de commande sur l'hôte local en utilisant la syntaxe suivante :

C:\> **ping 127.0.0.1**
La réponse que vous obtenez présente l'aspect suivant :
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Durée approximative des boucles en millisecondes :
Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms
Le résultat indique que quatre paquets de test de 32 octets chacun ont été envoyés, puis renvoyés par l'hôte 127.0.0.1 en moins de 1 ms. Cette requête ping vérifie que la carte réseau, les pilotes et la mise en œuvre TCP/IP fonctionnent correctement.

Essayez de tester une adresse de bouclage en entrant les commandes de la Figure 2.

2.3.3.2 Test de l'affectation des interfaces

Tout comme il est possible d'utiliser des commandes et des utilitaires pour vérifier la configuration d'un hôte, vous pouvez utiliser des commandes pour vérifier les interfaces des

périphériques intermédiaires. IOS fournit plusieurs commandes pour vérifier le fonctionnement des interfaces de routeur et de commutateur.

Vérification des interfaces de commutateur

Dans le cadre de l'examen des périphériques S1 et S2, utilisez la commande **show ip interface brief** pour vérifier l'état des interfaces de commutateur, comme illustré dans la figure. L'adresse IP attribuée à l'interface VLAN 1 sur le périphérique S1 est 192.168.10.2. L'adresse IP attribuée à l'interface VLAN 1 sur le périphérique S2 est 192.168.10.3. Les interfaces physiques F0/1 et F0/2 sur le périphérique S1 sont opérationnelles, de même que les interfaces physiques F0/1 et F0/2 du périphérique S2.

Essayez de vérifier une interface VLAN en entrant les commandes de la figure.

2.3.3.3 Vérification de la connectivité de bout en bout

Test de la connectivité PC-commutateur

La commande **ping** peut être utilisée sur un PC, de la même manière que sur un périphérique Cisco IOS. La figure montre qu'une requête ping du PC1 sur l'adresse IP de l'interface VLAN 1 du périphérique S1, 192.168.10.2, doit aboutir.

Vérification de la connectivité de bout en bout

L'adresse IP de PC1 est 192.168.10.10, avec le masque de sous-réseau 255.255.255.0 et la passerelle par défaut 192.168.10.1.

L'adresse IP de PC2 est 192.168.10.11, avec le masque de sous-réseau 255.255.255.0 et la passerelle par défaut 192.168.10.1.

Une requête ping de PC1 vers PC2 doit également aboutir. Une requête ping de PC1 vers PC2 permet de vérifier la connectivité de bout en bout sur le réseau.

CHAPITRE 3: COMMUNICATIONS ET PROTOCOLES RESEAU

3.0 Communications et protocoles réseau

3.0.1 Introduction

3.0.1.1 Introduction

De plus en plus, ce sont les réseaux qui nous relient. Nous communiquons en ligne où que nous soyons. Les conversations des salles de classe débouchent sur des sessions de chat et les débats en ligne se poursuivent à l'école. De nouveaux services sont développés au quotidien pour tirer parti du réseau.
Au lieu de développer des systèmes uniques et distincts pour chaque nouveau service, le secteur du réseau dans son ensemble a adopté une structure de développement permettant aux développeurs de comprendre les plates-formes réseau actuelles et d'en assurer la maintenance. Parallèlement, cette structure permet de simplifier le développement de nouvelles technologies qui doivent répondre aux futurs besoins de communication et permettre des améliorations technologiques.

L'utilisation de modèles unanimes décrivant les règles et les fonctions du réseau est au cœur de cette architecture de développement.

Dans ce chapitre, vous découvrirez ces modèles, ainsi que les normes qui permettent aux réseaux de fonctionner. Vous connaîtrez également les processus de communication sur un réseau.

3.0.1.2 Exercice en classe - Conception d'un système de communication

Parlons un peu...

Vous venez d'acheter une nouvelle automobile pour votre usage personnel. Après avoir utilisé votre voiture pendant une semaine, vous découvrez qu'elle ne fonctionne pas correctement.

Après avoir discuté du problème avec plusieurs amis, vous décidez d'amener la voiture à un centre de réparation qui vous a été vivement recommandé. C'est le seul garage proche de chez vous.

Lorsque vous arrivez au garage, vous constatez que tous les mécaniciens parlent une autre langue. Vous avez des difficultés à expliquer les problèmes de performances de l'automobile, mais les réparations doivent vraiment être effectuées. Vous n'êtes pas sûr de pouvoir rentrer chez vous pour trouver une autre solution.

Vous devez trouver un moyen de vous faire comprendre pour vous assurer que votre automobile sera réparée correctement.

Comment allez-vous communiquer avec les mécaniciens ? Créez un modèle de communication permettant de vous assurer que la voiture soit bien réparée.

Instructions de l'exercice en classe - Parlons un peu...

3.1 Règles de communication

3.1.1 Les règles

3.1.1.1 Qu'est-ce que la communication ?

Un réseau peut être très complexe et consister en des périphériques connectés à Internet, ou alors très simple, comme deux ordinateurs connectés directement entre eux par un seul câble. Tous les niveaux de complexité sont possibles. La taille, la forme et la fonction des réseaux peuvent varier. Cependant, il ne suffit pas de connecter physiquement des périphériques finaux pour permettre la communication. Les périphériques doivent également savoir comment communiquer.

Les personnes échangent des idées par de nombreuses méthodes de communication différentes. Cependant, quelle que soit la méthode choisie, tous les modes de communication ont en commun trois éléments. Le premier de ces éléments est la source du message, ou l'expéditeur. Les sources d'un message sont les personnes, ou les périphériques électroniques, qui doivent envoyer un message à d'autres personnes ou périphériques. Le deuxième élément de communication est la destination ou le récepteur du message. La destination reçoit le message et l'interprète. Le troisième élément, appelé canal, est constitué par le support qui fournit la voie par laquelle le message se déplace depuis la source vers la destination.

La communication commence par un message (ou des informations) qui doit être envoyé d'une source à une destination. L'envoi de ce message, soit lors d'une conversation en face à face soit sur un réseau, est régi par des règles appelées protocoles. Ces protocoles sont propres au mode de communication. Dans nos communications personnelles quotidiennes, les règles que nous utilisons pour communiquer à travers un support (par exemple, un appel téléphonique) ne sont pas nécessairement identiques aux protocoles liés à d'autres moyens de transmission, par exemple l'envoi d'une lettre.

Imaginez deux personnes communiquant face à face comme dans la Figure 1. Avant de communiquer, elles doivent se mettre d'accord sur la façon de communiquer. Si la communication fait appel à la voix, les partenaires doivent d'abord définir la langue. Ensuite, lorsqu'elles ont un message à partager, elles doivent pouvoir mettre ce message en forme de sorte qu'il soit compréhensible. Par exemple, si une personne utilise l'anglais, mais que la structure de sa phrase est mauvaise, le message peut facilement être mal compris. Chacune de ces tâches décrit les protocoles mis en place pour permettre la communication. Cela s'applique à la communication entre les ordinateurs, comme le montre la Figure 2.

Pensez au nombre de règles et de protocoles différents qui régissent l'ensemble des différentes méthodes de communication existant actuellement dans le monde.

3.1.1.2 Détermination des règles

Détermination des règles

Pour pouvoir communiquer entre elles, les personnes doivent utiliser des règles établies ou des conventions qui régissent la conversation. Par exemple, examinez la Figure 1 qui montre que les protocoles sont indispensables à une communication efficace. Les protocoles utilisés dépendent des caractéristiques du mode de communication, notamment la source, la destination et le canal. Ces règles ou protocoles doivent être respectés pour que le message soit correctement transmis et compris. Il existe de nombreux protocoles qui régissent la communication humaine. Une fois qu'une méthode de communication a été convenue (en face à face, par téléphone, par lettre, à travers une photographie), les protocoles mis en place doivent répondre aux conditions suivantes :

- Expéditeur et destinataire identifiés
- Même langue et syntaxe
- Vitesse et rythme d'élocution
- Demande de confirmation ou d'accusé de réception

Les protocoles utilisés dans les communications réseau partagent de nombreuses caractéristiques fondamentales avec les protocoles utilisés pour régir les conversations humaines. Reportez-vous à la Figure 2. En plus d'identifier la source et la destination, les protocoles informatiques et réseau définissent la manière dont un message est transmis sur un réseau pour répondre aux conditions ci-dessus. Il existe de nombreux protocoles qui doivent interagir, mais les protocoles informatiques courants sont les suivants :

- Codage des messages
- Mise en forme et encapsulation des messages
- Taille des messages
- Synchronisation des messages
- Options de remise des messages

Nous allons étudier chacun de ces protocoles plus en détail.

3.1.1.3 Codage des messages

Codage des messages

Pour envoyer un message, il faut tout d'abord le coder. Le codage est le processus de conversion des informations vers un autre format acceptable, à des fins de transmission. Le décodage est le processus inverse ; il permet d'interpréter les informations.

Imaginez une personne qui prévoit de partir en vacances avec un ami et qui appelle cette personne pour discuter de leur destination, comme illustré à la Figure 1. Pour communiquer son message, l'expéditeur doit tout d'abord convertir ses pensées et ses perceptions en mots (ou les « coder »). Les mots sont dits au téléphone au moyen de sons et d'inflexions du langage qui véhiculent le message. À l'autre bout du téléphone, la personne qui écoute la description reçoit et décode les sons afin de visualiser l'image du coucher de soleil décrit par l'expéditeur.

Le codage intervient également dans la communication informatique, comme illustré à la Figure 2. Le format du codage entre les hôtes doit être adapté au support. Les messages envoyés sur le réseau sont d'abord convertis en bits par l'hôte émetteur. Chaque bit est codé en modèle de sons, d'ondes lumineuses ou d'impulsions électriques, selon le support sur lequel les bits sont transmis. L'hôte de destination reçoit et décode les signaux pour interpréter le message.

3.1.1.4 Format et encapsulation des messages

Format et encapsulation des messages

Lorsqu'un message est envoyé de la source à la destination, il doit respecter un format ou une structure spécifique. Les formats des messages dépendent du type de message et du type de canal utilisés pour remettre le message.

La lettre est l'une des formes les plus communes de communication écrite. Durant des siècles, le format convenu pour les lettres personnelles n'a pas changé. Dans de nombreuses cultures, une lettre personnelle comprend les éléments suivants :

- Le nom du destinataire
- Une formule de politesse
- Le contenu du message
- Une phrase de conclusion
- Le nom de l'expéditeur

Outre le format approprié, la plupart des lettres personnelles doivent également être insérées ou contenues dans une enveloppe pour être acheminées, comme illustré à la Figure 1. L'enveloppe comporte l'adresse de l'expéditeur et celle du destinataire, chacune étant écrite à l'endroit prévu à cet effet. Si l'adresse de destination et le format ne sont pas corrects, la lettre n'est pas remise. Le processus consistant à placer un format de message (la lettre) dans un autre (l'enveloppe) s'appelle « encapsulation ». Une désencapsulation a lieu lorsque le processus est inversé par le destinataire et que la lettre est retirée de l'enveloppe.

L'auteur d'une lettre utilise un format convenu pour s'assurer que la lettre est remise, et ensuite comprise par le destinataire. De la même manière, un message qui est envoyé via un réseau informatique suit des règles de format spécifiques en vue de sa livraison et de son traitement. Les messages informatiques sont encapsulés, de la même manière qu'une lettre est placée dans une enveloppe. Chaque message informatique est encapsulé dans un format spécifique, appelé trame, avant d'être transmis sur le réseau. La trame fait office d'enveloppe. Elle fournit l'adresse de la destination souhaitée et celle de l'hôte source, comme le montre la Figure 2.

Le format et le contenu de la trame sont déterminés par le type de message envoyé et par le canal sur lequel ce dernier est transmis. Les messages qui ne sont pas correctement formatés ne sont ni livrés ni traités par l'hôte de destination.

3.1.1.5 Taille des messages

Taille des messages

La taille fait également l'objet d'une règle de communication. Lorsque les personnes communiquent, les messages qu'elles envoient sont généralement décomposés en petites parties ou phrases. Ces phrases sont limitées, en termes de taille, à ce que le destinataire peut comprendre ou traiter en une fois, comme le montre la Figure 1. Une conversation personnelle peut être composée de plusieurs petites phrases pour que chaque partie du message soit reçue et comprise. Imaginons que ce cours tienne en une seule et longue phrase. Il serait difficile à lire et à comprendre.

De même, lorsqu'un long message est envoyé par un hôte à un autre hôte sur le réseau, il est nécessaire de décomposer le message en plusieurs petites parties, comme illustré à la Figure 2. Les règles qui régissent la taille des parties ou « trames » transmises au réseau sont très strictes. Elles peuvent également être différentes selon le canal utilisé. Les trames trop longues ou trop courtes ne sont pas livrées.

En raison des restrictions imposées pour la taille des trames, l'hôte source doit décomposer les messages longs en portions répondant aux impératifs de taille minimale et maximale. C'est ce que l'on appelle la segmentation. Chaque portion est encapsulée dans une trame distincte avec

les informations d'adresse, puis transmise sur le réseau. Au niveau de l'hôte destinataire, les messages sont désencapsulés et recomposés pour être traités et interprétés.

3.1.1.6 Synchronisation des messages

Synchronisation des messages

La synchronisation affecte également la qualité de la réception et de la compréhension d'un message. Les personnes utilisent la synchronisation pour déterminer le moment de la prise de parole, le débit de parole et le temps d'attente d'une réponse. Ce sont les règles de tout engagement.

Méthode d'accès

La méthode d'accès détermine le moment où un individu peut envoyer un message. Ces règles de synchronisation dépendent de l'environnement. Par exemple, vous pouvez parler si vous avez quelque chose à dire. Dans cet environnement, avant de prendre la parole, l'intervenant doit attendre que tout le monde ait fini de parler. Si deux personnes parlent en même temps, une collision d'informations se produit et elles doivent s'arrêter et recommencer, comme illustré à la Figure 1. De même, il est nécessaire pour les ordinateurs de définir une méthode d'accès. Les hôtes d'un réseau ont besoin d'une méthode d'accès pour savoir à quel moment ils doivent commencer à envoyer des messages et comment réagir en cas d'erreurs.

Contrôle de flux

La synchronisation affecte également la quantité d'informations pouvant être envoyées, ainsi que leur vitesse d'acheminement. Si une personne parle trop rapidement, l'autre personne éprouve des difficultés à entendre et à comprendre le message, comme illustré à la Figure 2. Le destinataire doit demander à l'expéditeur de parler moins vite. Dans une communication réseau, il arrive que l'hôte émetteur transmette des messages plus rapidement que l'hôte de destination ne peut en recevoir et traiter. Les hôtes source et de destination utilisent le contrôle de flux pour négocier une synchronisation correcte en vue d'établir une communication.

Délai d'attente de la réponse

Si une personne pose une question et qu'elle n'entend pas de réponse dans un délai acceptable, elle suppose qu'aucune réponse n'a été donnée et réagit en conséquence, comme illustré à la Figure 3. La personne peut répéter la question ou continuer à converser. Les hôtes du réseau sont également soumis à des règles qui spécifient le délai d'attente des réponses et l'action à entreprendre en cas de dépassement du délai d'attente.

3.1.1.7 Options de remise des messages

Options de remise des messages

Un message peut être transmis de différentes manières selon les besoins, comme illustré à la Figure 1. Il arrive qu'une personne souhaite communiquer des informations à un seul individu. La même personne peut aussi vouloir envoyer des informations à tout un groupe de personnes ou à toutes les personnes d'une même zone géographique. Une conversation entre deux individus est un exemple de communication « un à un ». Lorsqu'un groupe de destinataires

doit recevoir simultanément le même message, un message de type « un à plusieurs » ou « un à tous » est nécessaire.

Parfois, l'expéditeur d'un message doit également s'assurer que le message a bien été reçu par son destinataire. Dans ce cas, le destinataire doit renvoyer un accusé de réception à l'expéditeur. Si aucun accusé de réception n'est requis, l'option de remise est dite « sans accusé de réception ».

Les hôtes d'un réseau utilisent des options similaires de remise des messages pour communiquer, comme illustré à la Figure 2.

Une option de livraison « un à un » est appelée monodiffusion, ce qui signifie qu'il n'existe qu'une seule destination pour le message.

Lorsqu'un hôte envoie des messages selon une option de livraison de type « un à plusieurs », il s'agit d'une multidiffusion. La multidiffusion est la livraison simultanée du même message à un groupe d'hôtes de destination.

Si tous les hôtes du réseau doivent recevoir le message en même temps, une diffusion est utilisée. La diffusion correspond à une option de remise de type « un à tous ». De plus, les hôtes requièrent des messages avec accusés de réception.

3.2 Normes et protocoles réseau

3.2.1 Protocoles

3.2.1.1 Protocoles : règles qui régissent les communications

Comme dans les communications humaines, les différents protocoles réseau et informatiques doivent pouvoir interagir et œuvrer ensemble à faire aboutir la communication réseau. Un groupe de protocoles interreliés et nécessaires pour remplir une fonction de communication est appelé suite de protocoles. Les suites de protocoles sont mises en œuvre par les hôtes et les périphériques réseau dans le logiciel, le matériel ou les deux.

Pour mieux visualiser l'interaction des protocoles d'une suite, imaginez que celle-ci est une pile. Une pile de protocoles indique comment chacun des protocoles de la suite est mis en œuvre. Les protocoles sont représentés par des couches et chaque service de niveau supérieur dépend de la fonctionnalité définie par les protocoles constituant les niveaux inférieurs. Les couches inférieures de la pile s'occupent du déplacement de données sur le réseau et de la fourniture de services aux couches supérieures, qui elles, se concentrent sur le contenu du message en cours d'envoi. Comme l'illustre la figure, nous pouvons utiliser des couches pour décomposer l'activité qui intervient dans notre exemple de communication en face à face. À la couche inférieure, la couche physique, se trouvent deux personnes, chacune douée de la parole et capables de prononcer des mots à haute voix. À la deuxième couche, celle des règles, nous disposons d'un accord pour parler dans une langue commune. À la couche supérieure, la couche du contenu, des mots sont effectivement prononcés. Il s'agit du contenu de la communication.

Si nous devions assister à cette conversation, nous ne pourrions pas réellement voir ces couches flotter dans l'air. L'utilisation de couches permet de décomposer une tâche complexe en différentes parties simples et de décrire leur fonctionnement.

3.2.1.2 Protocoles réseau

Au niveau humain, certaines règles de communication sont formelles et d'autres sont simplement comprises en fonction de la coutume et de la pratique. Afin que des périphériques puissent communiquer correctement, une suite de protocoles réseau doit décrire des exigences et des interactions précises. Les protocoles réseau définissent un format et un ensemble communs de règles d'échange des messages entre les périphériques. Les protocoles IP, HTTP et DHCP sont des exemples de protocoles réseau courants.

Les figures illustrent les protocoles réseau qui décrivent les processus suivants :

- Format ou structure du message, comme illustré à la Figure 1
- Le processus de partage d'informations à propos des chemins entre les périphériques réseau et d'autres réseaux, comme illustré à la Figure 2
- Le mode et le moment de transmission de messages d'erreur et de messages systèmes entre les périphériques, comme illustré à la Figure 3
- L'initialisation et la fin des sessions de transfert de données, comme illustré à la Figure 4

Par exemple, le protocole IP définit la façon dont un paquet de données est acheminé au sein d'un réseau ou à un réseau distant. Les informations du protocole IPv4 sont transmises dans un format spécifique de sorte que le récepteur puisse les interpréter correctement. Ce protocole n'est pas très différent de celui utiliser pour noter l'adresse sur une enveloppe lorsque vous envoyez une lettre. Les informations doivent respecter un certain format pour que la lettre puisse être livrée à la destination par la poste.

3.2.1.3 Interaction des protocoles

L'interaction entre un serveur Web et un client Web constitue un exemple de l'utilisation d'une suite de protocoles dans des communications réseau. Cette interaction utilise plusieurs protocoles et normes dans le processus d'échange d'informations entre ceux-ci. Les différents protocoles fonctionnent entre eux pour garantir que les messages sont reçus et compris par les deux parties. Exemples de tels protocoles :

- **Protocole d'application** : le protocole de transfert hypertexte (Hypertext Transfer Protocol, protocole HTTP) régit la manière dont un serveur Web et un client Web interagissent. Le protocole HTTP décrit le contenu et la mise en forme des requêtes et des réponses échangées entre le client et le serveur. Les logiciels du client et du serveur Web implémentent le protocole HTTP dans le cadre de l'application. Le protocole HTTP dépend d'autres protocoles pour gérer le transport des messages entre le client et le serveur.

- **Protocole de transport** : le protocole de contrôle de transmission (Transmission Control Protocol, TCP) est le protocole de transport qui gère les conversations individuelles entre les serveurs Web et les clients Web. Le protocole TCP divise les messages HTTP en petites parties appelées segments. Ces segments sont envoyés entre les processus du serveur Web et du client exécutés sur l'hôte de destination. Ce protocole est également responsable du contrôle de la taille et du débit d'échange de messages entre le serveur et le client.

- **Protocole Internet** : le protocole IP se charge d'encapsuler en paquets les segments mis en forme par le protocole TCP, de les attribuer aux adresses appropriées et de les remettre à l'hôte de destination en utilisant le meilleur chemin.

- **Protocoles d'accès au réseau** : les protocoles d'accès au réseau décrivent deux fonctions principales, d'une part la communication sur une liaison de données et d'autre part la transmission physique des données sur le support réseau. Les protocoles de gestion de liaison de données prennent les paquets depuis le protocole IP et les formatent pour les transmettre à travers les supports. Les normes et les protocoles des supports physiques régissent la manière dont les signaux sont envoyés, ainsi que leur interprétation par les clients destinataires. Ethernet est un exemple de protocole d'accès au réseau.

3.2.2 Suites de protocoles

3.2.2.1 Suites de protocoles et normes de l'industrie

Comme nous l'avons vu, une suite de protocoles est un ensemble de protocoles qui fonctionnent ensemble pour fournir des services de communication réseau complets. Une suite de protocoles peut être définie par un organisme de normalisation ou développée par un constructeur.

Les protocoles IP, HTTP et DHCP font tous partie de la suite de protocoles Internet connue sous le nom de Transmission Control Protocol/IP (TCP/IP). La suite de protocoles TCP/IP est une norme ouverte, ce qui signifie que ces protocoles peuvent être utilisés gratuitement par tous et que tous les constructeurs ont la possibilité de les mettre en œuvre sur leur matériel ou leurs logiciels.

Les protocoles basés sur des normes sont des processus ou des protocoles qui ont été validés par le secteur des réseaux et ratifiés, ou approuvés, par un organisme de normalisation. L'utilisation de normes dans le développement et la mise en œuvre de protocoles garantit que les produits provenant de différents fabricants fonctionnent ensemble. Si un fabricant spécifique n'adhère pas strictement à un protocole, son équipement ou ses logiciels risquent de ne pas communiquer correctement avec les produits des autres fabricants.

Dans les communications de données, par exemple, si l'un des participants à une conversation utilise un protocole pour gérer une communication unidirectionnelle et que l'autre participant suppose qu'il s'agit d'un protocole décrivant une communication bidirectionnelle, en toute probabilité, aucune information ne sera échangée.

Certains protocoles sont propriétaires. Propriétaire, dans ce contexte, signifie qu'une société ou qu'un fournisseur contrôle la définition du protocole et la manière dont il fonctionne. Certains protocoles propriétaires peuvent être utilisés par différentes organisations avec l'autorisation du propriétaire. D'autres peuvent uniquement être implémentés sur du matériel fabriqué par le fournisseur propriétaire. AppleTalk et Novell NetWare sont des exemples de protocoles propriétaires.

Plusieurs entreprises peuvent même créer ensemble un protocole propriétaire. Il n'est pas rare qu'un constructeur (voire un groupe de constructeurs) développe un protocole propriétaire pour répondre aux besoins de ses clients, puis contribue à faire de ce protocole propriétaire une norme ouverte. Par exemple, Ethernet était un protocole propriétaire développé initialement par Bob Metcalfe au centre de recherche XEROX de Palo Alto (PARC) dans les années 1970. En 1979, Bob Metcalfe a créé sa propre entreprise, 3COM, et a collaboré avec Digital Equipment Corporation (DEC), Intel et Xerox en vue de promouvoir la norme « DIX » d'Ethernet. En 1985, l'IEEE (Institute of Electrical and Electronics Engineers) a publié la norme IEEE 802.3 qui était quasiment identique à Ethernet. Aujourd'hui, 802.3 est la

norme de fait utilisée sur les réseaux locaux (LAN). Autre exemple plus récent : Cisco a ouvert le protocole de routage EIGRP sous forme de RFC informatif afin de répondre aux besoins des clients souhaitant utiliser le protocole sur un réseau multifournisseur.

3.2.2.2 Création d'Internet et développement de la suite de protocoles TCP/IP

La suite IP est une suite de protocoles nécessaire pour transmettre et recevoir des informations via Internet. Elle est plus connue sous le nom de TCP/IP, car les deux premiers protocoles réseau définis pour cette norme étaient TCP et IP. La suite TCP/IP basée sur des normes ouvertes a remplacé d'autres suites de protocoles propriétaires, telles qu'AppleTalk d'Apple et IPX/SPX (Internetwork Packet Exchange/sequenced Packet Exchange) de Novell.

Le premier réseau à commutation de paquets, prédécesseur de l'Internet actuel, était l'ARPANET (Advanced Research Projects Agency Network), né en 1969 de la connexion d'ordinateurs centraux situés sur quatre sites différents. L'ARPANET a été financé par le département de la défense américain et était destiné aux universités et aux laboratoires de recherche. Le sous-traitant BBN (Bolt, Beranek et Newman) a réalisé une grande partie du développement initial de l'ARPANET, notamment en créant le premier routeur alors appelé processeur de message d'interface (IMP).

En 1973, Robert Kahn et Vinton Cerf ont commencé leurs travaux sur le protocole TCP afin de développer la nouvelle génération de l'ARPANET. Le protocole TCP devait remplacer le programme de contrôle du réseau (NCP) alors utilisé par l'ARPANET. En 1978, le protocole TCP a été divisé en deux protocoles : TCP et IP. D'autres protocoles ont ensuite été ajoutés à la suite de protocoles TCP/IP, notamment Telnet, FTP et DNS.

Cliquez sur la chronologie de la figure pour afficher les détails relatifs au développement d'autres protocoles et applications réseau.

3.2.2.3 Suite de protocoles TCP/IP et processus de communication

Actuellement, la suite inclut des dizaines de protocoles, comme illustré à la Figure 1. Cliquez sur chaque protocole pour afficher sa description. Ils sont organisés sous forme de couches à l'aide du modèle de protocole TCP/IP. Dans le modèle TCP/IP, les protocoles TCP/IP sont inclus de la couche Internet à la couche application. Les protocoles de couche inférieure de la couche de liaison de données ou d'accès au réseau sont chargés d'acheminer le paquet IP sur un support physique. Ces protocoles de couche inférieure sont développés par des organismes de normalisation, tels que l'IEEE.

La suite de protocoles TCP/IP est mise en œuvre comme une pile TCP/IP à la fois sur les hôtes expéditeurs et récepteurs pour assurer l'acheminement de bout en bout des applications sur un réseau. Les protocoles 802.3 ou Ethernet sont utilisés pour transmettre le paquet IP sur le support physique utilisé par le réseau local.

Les Figures 2 et 3 présentent le processus de communication complet grâce à un exemple d'une transmission de données d'un serveur Web à un client.

Cliquez sur le bouton Lire pour afficher les animations :

1. La page HTML (Hypertext Markup Langage) du serveur Web correspond aux données à envoyer.
2. L'en-tête HTTP du protocole d'application est ajouté à l'avant des données HTML. L'en-tête contient différentes informations, y compris la version HTTP utilisée par le serveur et un code d'état indiquant qu'il dispose d'informations destinées au client Web.
3. Le protocole de couche application HTTP fournit les données de la page Web au format HTML à la couche transport. Le protocole de couche transport TCP est utilisé pour gérer cette conversation entre le serveur et le client Web.
4. Ensuite, les informations IP sont ajoutées à l'avant des informations TCP. Le protocole IP attribue les adresses IP source et de destination appropriées. Ces informations représentent le paquet IP.
5. Le protocole Ethernet ajoute les informations aux deux extrémités du paquet IP, qui forment la trame de liaison de données. Cette trame est transmise au routeur le plus proche du chemin vers le client Web. Ce routeur supprime les informations Ethernet, analyse le paquet IP, détermine le meilleur chemin de transmission du paquet, insère le paquet dans une nouvelle trame et l'envoie au routeur voisin suivant en direction de la destination. Chaque routeur supprime des informations de liaison de données et en ajoute de nouvelles avant de transférer le paquet.
6. Ces données sont maintenant transportées via l'interréseau, qui se compose de supports et de périphériques intermédiaires.
7. Le client reçoit les trames de liaison de données qui contiennent les informations et chaque en-tête de protocole est traité, puis supprimé dans l'ordre inverse de son ajout. Les informations Ethernet sont traitées et supprimées. Elles sont suivies des informations du protocole IP, puis des informations TCP, et enfin des informations HTTP.
8. Les informations de la page Web sont ensuite transmises jusqu'au navigateur Web du client.

3.2.3 Organismes de normalisation

3.2.3.1 Normes ouvertes

Les normes ouvertes favorisent la concurrence et l'innovation. Elles empêchent également qu'un seul produit d'une entreprise monopolise le marché ou puisse bénéficier d'un avantage inique sur ses concurrents. Pour illustrer ceci, prenons l'exemple de l'achat d'un routeur sans fil par un particulier. Il existe de nombreux appareils proposés par divers constructeurs, qui intègrent tous des protocoles standard tels que IPv4, DHCP, 802.3 (Ethernet) et 802.11 (réseau local sans fil). Ces normes ouvertes permettent également à un client exécutant le système d'exploitation OS X d'Apple de télécharger une page Web à partir d'un serveur Web exécutant le système d'exploitation Linux. Cela s'explique par le fait que les deux systèmes d'exploitation mettent en œuvre les mêmes protocoles de norme ouverte, notamment ceux de la suite TCP/IP.

Les organismes de normalisation jouent un rôle important en assurant qu'Internet reste ouvert, que ses spécifications et protocoles soient accessibles librement et puissent être mis en œuvre par tous les constructeurs. Un organisme peut rédiger un ensemble de règles de A à Z ou il peut se baser sur un protocole propriétaire. Si un protocole propriétaire est utilisé, il implique généralement le constructeur à l'origine de sa création.

Les organismes de normalisation sont généralement des associations à but non lucratif qui ne sont liées à aucun constructeur. Leur objectif est de développer et de promouvoir le concept des normes ouvertes.

Voici les principaux organismes de normalisation :

- Internet Society (ISOC)
- Internet Architecture Board (IAB)
- Internet Engineering Task Force (IETF)
- IEEE (Institute of Electrical and Electronics Engineers)
- ISO (International Organization for Standardization)

Chacun de ces organismes est abordé plus en détail dans les prochaines pages.

Sur la figure, cliquez sur chaque logo pour afficher les informations sur les normes.

3.2.3.2 ISOC, IAB et IETF

L'ISOC (Internet Society) est chargée de promouvoir le développement, l'évolution et l'utilisation ouverts d'Internet dans le monde entier. L'ISOC favorise le développement ouvert de normes et de protocoles relatifs à l'infrastructure technique d'Internet, y compris la supervision de l'IAB (Internet Architecture Board).

L'IAB (Internet Architecture Board) s'occupe de la gestion et du développement généraux des normes Internet. Il assure la surveillance des protocoles et des procédures d'architecture utilisés par Internet. L'organisme se compose de 13 membres, dont le président de l'IETF (Internet Engineering Task Force). Les membres de l'IAB agissent en qualité de personne privée et ne représentent aucune entreprise, aucune institution ni aucune autre organisation.

La mission de l'IETF est de développer, de mettre à jour et d'assurer la maintenance d'Internet et les technologies TCP/IP. L'une des principales responsabilités de l'IETF est de produire des documents RFC (Request for Comments), c'est-à-dire des notes décrivant les protocoles, les processus et les technologies d'Internet. L'IETF se compose de groupes de travail (WG pour « working groups » en anglais) qui constituent les principales entités de développement des spécifications et des recommandations de l'organisme. Les groupes de travail sont constitués à des fins précises et dès que leurs objectifs sont remplis, ils sont dissous. L'IESG (Internet Engineering Steering Group) est chargé de la gestion technique de l'IETF et du processus des normes Internet.

L'IRTF (Internet Research Task Force) se concentre sur la recherche à long terme liée à Internet et aux protocoles TCP/IP, aux applications, à l'architecture et aux technologies. Si l'IETF s'intéresse surtout aux besoins à court terme en matière de normes, l'IRTF se compose de groupes de recherche centrés sur le développement à long terme. Les groupes de recherche actuels sont notamment l'ASRG (Anti-Spam Research Group), le CFRG (Crypto Forum Research Group), le P2PRG (Peer-to-Peer Research Group) et le RRG (Router Research Group).

3.2.3.3 IEEE

L'IEEE (Institute of Electrical and Electronics Engineers) est une association américaine professionnelle s'adressant aux spécialistes du génie électrique et de l'électronique qui souhaitent se consacrer à l'innovation technologique et à la création de normes. En 2012, l'IEEE se composait de 38 sociétés, avait publié 130 journaux et parrainé plus de 1 300 conférences par an dans le monde entier. L'IEEE compte actuellement plus de 1 300 normes et projets en cours de développement.

L'organisme rassemble plus de 400 000 membres dans plus de 160 pays, dont plus de 107 000 étudiants. L'IEEE offre des opportunités de formation et de valorisation professionnelle dans l'optique de promouvoir les compétences et les connaissances du domaine de l'électronique.

Il s'agit d'un organisme de normalisation majeur sur le plan international. Il crée et gère des normes affectant un grand nombre de secteurs, notamment l'électricité et l'énergie, la santé, les télécommunications et les réseaux. Les normes 802 de l'IEEE traitent des réseaux locaux et des réseaux métropolitains, y compris les réseaux filaires et sans fil. Comme l'illustre la figure, chaque norme IEEE correspond à un groupe de travail chargé de créer et d'améliorer des normes.

Les normes 802.3 et 802.11 de l'IEEE jouent un rôle de premier plan dans les réseaux informatiques. La norme 802.3 définit le contrôle d'accès au support (MAC ou Media Access Control) de l'Ethernet filaire. Cette technologie sert généralement aux réseaux locaux, mais certaines de ses applications concernent également le réseau étendu (WAN). La norme 802.11 définit un ensemble de normes relatives à la mise en œuvre des réseaux locaux sans fil (WLAN). Elle définit la couche physique et la sous-couche de liaison de données MAC du modèle OSI (Open Systems Interconnection) pour les communications sans fil.

3.2.3.4 ISO

L'ISO, l'organisation internationale de normalisation, est le plus grand concepteur de normes internationales pour une large gamme de produits et services. ISO n'est pas l'acronyme du nom de l'organisation. En réalité, le terme ISO provient du mot grec « isos » qui signifie « égal ». L'organisation internationale de normalisation a choisi le terme ISO pour affirmer sa volonté d'égalité envers tous les pays.

Dans le domaine des réseaux, elle est surtout célèbre pour son modèle de référence OSI (Open Systems Interconnection), publié en 1984 dans le but de développer un cadre composé de couches pour les protocoles réseau. L'objectif initial de ce projet était non seulement de créer un modèle de référence, mais également de servir de base à une suite de protocoles applicables à Internet. Celle-ci a été appelée suite de protocoles OSI. Toutefois, en raison de la popularité croissante de la suite TCP/IP développée par Robert Kahn, Vinton Cerf et d'autres spécialistes, le choix de la suite de protocoles Internet ne s'est pas porté sur le modèle OSI, mais sur la suite TCP/IP. La suite de protocoles OSI a tout de même été implémentée sur des équipements de télécommunications et existe toujours dans des réseaux de télécommunications d'ancienne génération.

Vous connaissez peut-être déjà certains produits qui font appel aux normes ISO. L'extension de fichier ISO est attribuée à de nombreuses images de CD pour indiquer l'utilisation de la norme ISO 9660 dans le système de fichiers. L'organisme ISO est également chargé de créer des normes relatives aux protocoles de routage.

3.2.3.5 Autres organismes de normalisation

Les normes réseau font appel à plusieurs autres organismes de normalisation, dont voici les plus courants :

- **L'EIA** (Electronic Industries Alliance), anciennement Electronics Industries Association, est une alliance commerciale internationale de normalisation dont le rôle concerne les entreprises d'électronique. L'EIA est connue pour ses normes associées au câblage électrique, aux connecteurs et aux racks 19 pouces utilisés pour monter l'équipement réseau.

- **La TIA** (Telecommunications Industry Association) est responsable du développement des normes de communication dans un grand nombre de domaines, incluant les équipements radio, les tours cellulaires, les dispositifs de voix sur IP (VoIP) et les communications par satellite. Plusieurs de ses normes sont élaborées en collaboration avec l'EIA.

- **L'ITU-T** (secteur de la normalisation des télécommunications de l'Union internationale des télécommunications) figure parmi les organismes de normalisation les plus grands et les plus anciens. L'ITU-T définit des normes de compression vidéo, de télévision sur IP (IPTV) et de communication haut débit, telles que la ligne d'abonné numérique (DSL). Par exemple, lorsque vous appelez un correspondant dans un autre pays, les codes de pays de l'ITU sont utilisés pour établir la connexion.

- **L'ICANN** (Internet Corporation for Assigned Names and Numbers) est une association à but non lucratif basée aux États-Unis qui coordonne l'attribution des adresses IP, la gestion des noms de domaine utilisés par le protocole DNS et les identificateurs de protocole ou numéros de ports utilisés par les protocoles TCP et UDP. L'ICANN crée des politiques et assume la responsabilité totale de ces attributions.

- **L'IANA** (Internet Assigned Numbers Authority) est une composante de l'ICANN chargée de superviser et de gérer l'affectation des adresses IP, la gestion des noms de domaine et les identificateurs de protocole pour le compte de l'ICANN.

Le fait de connaître les organismes à l'origine des normes utilisées dans les réseaux vous aidera à mieux comprendre en quoi ces normes assurent un réseau Internet ouvert et non lié à des entreprises. Vous pourrez également découvrir les nouvelles normes à mesure de leur élaboration.

3.2.4 Modèles de référence

3.2.4.1 Avantage de l'utilisation d'un modèle en couches

On utilise souvent un modèle sous forme de couches, tel que le modèle TCP/IP pour aider à visualiser l'interaction entre les différents protocoles. Ce modèle illustre le fonctionnement des protocoles intervenant dans chaque couche, ainsi que leur interaction avec les couches supérieures et inférieures.

L'utilisation d'un modèle en couches présente certains avantages pour décrire des protocoles et des opérations sur un réseau. L'utilisation d'un modèle en couches :

- Aide à la conception d'un protocole, car des protocoles qui fonctionnent à un niveau de couche spécifique disposent d'informations définies à partir desquelles ils agissent, ainsi que d'une interface définie par rapport aux couches supérieures et inférieures.

- Il encourage la concurrence, car les produits de différents fournisseurs peuvent fonctionner ensemble.
- Il permet d'éviter que des changements technologiques ou fonctionnels dans une couche ne se répercutent sur d'autres couches, supérieures et inférieures.
- Il fournit un langage commun pour décrire les fonctions et les fonctionnalités réseau.

Il existe deux types de modèles de réseau de base :

- **Le modèle de protocole**, qui suit la structure d'une suite de protocoles donnée. L'ensemble hiérarchique des protocoles associés dans une suite représente généralement toutes les fonctionnalités requises à l'interface entre le réseau humain et le réseau de données. Le modèle TCP/IP est un modèle de protocole, car il décrit les fonctions qui interviennent à chaque couche des protocoles au sein de la suite TCP/IP.

- **Le modèle de référence** assure la cohérence de tous les types de protocoles et services réseau en décrivant les opérations à effectuer à chaque couche, mais n'indique pas leur mise en œuvre. Un modèle de référence n'est pas destiné à être une spécification d'implémentation, ni à fournir un niveau de détail suffisant pour définir précisément les services de l'architecture réseau. Le principal objectif d'un modèle de référence est d'assurer une compréhension plus claire des fonctions et des processus impliqués.

Le modèle OSI (Open System Interconnection) est le modèle de référence interréseau le plus connu. Il est utilisé pour la conception de réseaux de données, des spécifications d'opérations et la résolution des problèmes.

Comme l'illustre la figure, les modèles OSI et TCP/IP sont les principaux modèles utilisés en matière de fonctionnalités réseau. Les concepteurs des protocoles, services ou périphériques réseau peuvent créer leurs propres modèles représentant leurs produits. Enfin, les concepteurs doivent communiquer avec l'industrie en associant leurs produits ou leurs services aux modèles OSI ou TCP/IP ou aux deux.

3.2.4.2 Modèle de référence OSI

À l'origine, le modèle OSI a été conçu par l'organisation ISO pour fournir un cadre dans lequel concevoir une suite de protocoles système ouverts. L'idée était que cet ensemble de protocoles serait utilisé pour développer un réseau international qui ne dépendrait pas de systèmes propriétaires.

Finalement, du fait de la rapidité avec laquelle Internet basé sur TCP/IP a été adopté et de sa vitesse de développement, l'élaboration et l'acceptation de la suite de protocoles OSI sont restées à la traîne. Même si peu de protocoles développés à l'aide des spécifications OSI font l'objet d'une utilisation répandue aujourd'hui, le modèle OSI à sept couches a apporté des contributions essentielles au développement d'autres protocoles et produits pour tous les types de nouveaux réseaux.

Il fournit une liste exhaustive de fonctions et de services qui peuvent intervenir à chaque couche. Il décrit également l'interaction de chaque couche avec les couches directement supérieures et inférieures. Bien que le contenu de ce cours soit structuré autour du modèle de référence OSI, la discussion traitera essentiellement des protocoles identifiés dans le modèle de protocole TCP/IP. Cliquez sur le nom de chaque couche pour afficher les détails.

Remarque : si les couches du modèle TCP/IP sont désignées par leur nom uniquement, les sept couches du modèle OSI sont plus fréquemment désignées par un numéro. Par exemple, la couche physique est appelée Couche 1 dans le modèle OSI.

3.2.4.3 Le modèle de référence TCP/IP

Le modèle de protocole TCP/IP pour les communications interréseau fut créé au début des années 1970 et est appelé modèle Internet. Comme l'illustre la figure, il définit quatre catégories de fonctions qui doivent intervenir pour que les communications aboutissent. L'architecture de la suite de protocoles TCP/IP suit la structure de ce modèle. Pour cette raison, le modèle Internet est généralement appelé modèle TCP/IP.

La plupart des modèles de protocole décrivent une pile de protocoles spécifique au fournisseur. Cependant, comme le modèle TCP/IP est une norme ouverte, aucune entreprise ne contrôle la définition du modèle. Les définitions de la norme et des protocoles TCP/IP sont traitées dans un forum public et définies dans un ensemble de documents RFC disponible au public. Les documents RFC contiennent les spécifications formelles des protocoles de communication de données ainsi que des ressources qui décrivent l'utilisation des protocoles.

Ils contiennent également des documents techniques et organisationnels concernant Internet, y compris les spécifications techniques et les documents relatifs aux politiques élaborés par l'IETF.

3.2.4.4 Comparaison des modèles OSI et TCP/IP

Les protocoles qui constituent la suite de protocoles TCP/IP peuvent être décrits selon les termes du modèle de référence OSI. Dans le modèle OSI, la couche d'accès au réseau et la couche application du modèle TCP/IP sont subdivisées pour décrire les fonctions distinctes qui doivent intervenir sur ces couches.

Au niveau de la couche d'accès au réseau, la suite de protocoles TCP/IP ne spécifie pas quels protocoles utiliser lors de la transmission à travers un support physique ; elle décrit uniquement la remise depuis la couche Internet aux protocoles réseau physiques. Les couches OSI 1 et 2 traitent des procédures nécessaires à l'accès aux supports et des moyens physiques permettant d'envoyer des données à travers un réseau.

Comme l'illustre la figure, les principaux points communs entre les deux modèles de réseau se situent aux couches OSI 3 et 4. La couche 3 du modèle OSI, c'est-à-dire la couche réseau, est utilisée de manière presque universelle pour décrire l'éventail de processus qui interviennent dans tous les réseaux de données afin d'adresser et d'acheminer les messages à travers un interréseau. Le protocole IP est le protocole de la suite TCP/IP qui contient la fonctionnalité décrite à la couche 3 du modèle OSI.

La couche 4, c'est-à-dire la couche transport du modèle OSI décrit les services et les fonctionnalités de base qui assurent l'ordre et la fiabilité des données acheminées entre les hôtes source et de destination. Ces fonctions incluent l'accusé de réception, la reprise après erreur et le séquencement. Au niveau de cette couche, les protocoles TCP et UDP de la suite TCP/IP fournissent les fonctionnalités nécessaires.

La couche application TCP/IP inclut plusieurs protocoles qui fournissent des fonctionnalités spécifiques à plusieurs applications d'utilisateur final. Les couches 5, 6 et 7 du modèle OSI servent de références aux développeurs et aux éditeurs de logiciels d'application pour créer des produits qui fonctionnent sur les réseaux.

3.3.1 Encapsulation de données

3.3.1.1 Communication des messages

En théorie, une communication unique, comme une vidéo musicale ou un e-mail pourrait être transmise à travers un réseau depuis une source vers une destination sous la forme d'un flux ininterrompu et volumineux de bits. Si des messages étaient réellement transmis de cette manière, alors aucun autre périphérique ne serait en mesure d'envoyer ou de recevoir des messages sur ce même réseau pendant le transfert de ces données. Ces flux de données volumineux entraîneraient des retards conséquents. En outre, si un lien dans l'infrastructure du réseau interconnecté échouait durant la transmission, la totalité du message serait perdue et devrait être retransmise dans son intégralité.

Il existe une meilleure approche, qui consiste à diviser les données en parties de taille moins importante et plus facilement gérables pour les envoyer sur le réseau. Cette division du flux de données en parties plus petites est appelée segmentation. La segmentation des messages présente deux avantages principaux :

- Par l'envoi de parties individuelles de plus petite taille depuis une source vers une destination, de nombreuses conversations différentes peuvent s'entremêler sur le réseau. Le processus qui sert à entremêler les parties des différentes conversations entre elles sur le réseau est appelé multiplexage. Cliquez sur chaque bouton de la Figure 1, puis sur le bouton Lire pour afficher les animations sur la segmentation et le multiplexage.

- La segmentation peut augmenter la fiabilité des communications réseau. Les différentes parties de chaque message n'ont pas besoin de parcourir le même chemin sur le réseau depuis la source jusqu'à la destination. Si un chemin particulier devient encombré en raison du trafic de données ou qu'il connaît une défaillance, les parties individuelles du message peuvent toujours être adressées à la destination via d'autres chemins. Si une partie du message ne parvient pas à sa destination, seules les parties manquantes doivent être transmises à nouveau.

L'inconvénient de l'utilisation de la segmentation et du multiplexage pour la transmission des messages à travers un réseau réside dans le niveau de complexité ajouté au processus. Imaginez que vous deviez envoyer une lettre de 100 pages, mais que chaque enveloppe ne peut contenir qu'une seule page. Le processus d'adressage, d'étiquetage, d'envoi, de réception et d'ouverture de la totalité des 100 enveloppes prendrait beaucoup de temps à l'expéditeur et au destinataire.

Dans les communications réseau, chaque partie du message doit suivre un processus similaire permettant de s'assurer qu'elle arrive à la bonne destination et qu'elle peut être réassemblée pour former le contenu du message d'origine, comme le montre la Figure 2.

À travers le réseau, plusieurs types de périphériques contribuent à garantir que les parties du message arrivent de manière fiable à leur destination.

3.1.2 Unités de données de protocole (PDU)

Lorsque les données d'application descendent la pile de protocoles en vue de leur transmission sur le support réseau, différents protocoles ajoutent des informations à chaque niveau. C'est ce qu'on appelle communément l'encapsulation.

La forme que prend une donnée sur n'importe quelle couche est appelée unité de données de protocole. Au cours de l'encapsulation, chaque couche suivante encapsule l'unité de données de protocole qu'elle reçoit de la couche supérieure en respectant le protocole utilisé. À chaque étape du processus, une unité de données de protocole possède un nom différent qui reflète ses nouvelles fonctions. Bien qu'il n'existe aucune convention universelle d'attribution des noms pour les unités de données de protocole, dans ce cours, les unités de données de protocole sont nommées en fonction des protocoles de la suite TCP/IP, comme illustré dans la figure :

- **Donnée** : terme générique attribué à l'unité de données de protocole utilisée à la couche application
- **Segment** : unité de données de protocole de la couche transport
- **Paquet** : unité de données de protocole de la couche réseau
- **Trame :** unité de données de protocole de la couche liaison de données
- **Bits** : unité de données de protocole de la couche physique utilisée lors de la transmission physique des données via le support

3.3.1.3 Encapsulation

L'encapsulation de données est le processus qui ajoute aux données des informations d'en-tête de protocole supplémentaires avant leur transmission. Dans la plupart des formes de communication de données, les données d'origine sont encapsulées ou enveloppées dans plusieurs protocoles avant d'être transmises.

Lors de l'envoi de messages sur un réseau, la pile de protocoles sur un hôte fonctionne de haut en bas. Dans l'exemple du serveur Web, nous pouvons utiliser le modèle TCP/IP pour illustrer le processus d'envoi d'une page Web HTML à un client.

Le protocole de la couche application, HTTP, démarre le processus en remettant à la couche transport les données de la page Web au format HTML. Dans la couche transport, les données de la couche application sont divisées en segments TCP. Chaque segment TCP reçoit une étiquette, appelée en-tête, qui contient des informations pour désigner le processus s'exécutant sur l'ordinateur de destination qui doit recevoir le message. Il contient également les informations qui permettent au processus de destination de réassembler les données selon leur format d'origine.

La couche transport encapsule les données HTML de la page Web au sein du segment et les envoie à la couche Internet, où est implémenté le protocole IP. Dans cette couche, la totalité du segment TCP est encapsulée dans ce paquet IP, qui ajoute une autre étiquette, appelée en-tête IP. L'en-tête IP contient des adresses IP d'hôtes source et de destination, ainsi que des informations nécessaires à la livraison du paquet à son processus de destination correspondant.

Ensuite, le paquet IP est envoyé à la couche d'accès au réseau, où il est encapsulé dans un en-tête de trame et une fin de trame (code de fin). Chaque en-tête de trame contient une adresse

physique source et de destination. L'adresse physique identifie de manière unique les périphériques sur le réseau local. Le code de fin contient des informations de vérification d'erreur. Enfin, les bits sont codés sur le support par la carte réseau du serveur. Cliquez sur le bouton Lire de la figure pour visualiser le processus d'encapsulation.

3.3.1.4 Désencapsulation

Ce processus est inversé sur l'hôte récepteur. Il est alors appelé désencapsulation. La désencapsulation est le processus utilisé par un périphérique récepteur pour supprimer un ou plusieurs des en-têtes de protocole. Les données sont désencapsulées au fur et à mesure qu'elles se déplacent vers la partie supérieure de la pile et l'application d'utilisateur final. Cliquez sur le bouton Lire de la figure pour visualiser le processus de désencapsulation.

3.3.2 Accès aux ressources locales

3.3.2.1 Adresses réseau et adresses de liaison de données

Le modèle OSI décrit des processus de codage, de mise en forme, de segmentation et d'encapsulation de données pour la transmission sur le réseau. La couche réseau et la couche liaison de données sont chargées de transmettre les données du périphérique source ou expéditeur au périphérique de destination ou récepteur. Les protocoles de ces deux couches contiennent les adresses source et de destination, mais ils ne les utilisent pas aux mêmes fins.

Adresse réseau

Sur la couche réseau ou couche 3, l'adresse logique contient les informations nécessaires à l'acheminement du paquet IP du périphérique source au périphérique de destination. Une adresse IP de couche 3 se compose de deux parties, le préfixe réseau et la partie hôte. Le préfixe réseau est utilisé par les routeurs pour transférer le paquet au réseau approprié. La partie hôte est utilisée par le dernier routeur du chemin pour livrer le paquet au périphérique de destination.

Un paquet IP contient deux adresses IP :

- **L'adresse IP source** : il s'agit de l'adresse IP du périphérique expéditeur.
- **L'adresse IP de destination** : elle correspond à l'adresse IP du périphérique récepteur. L'adresse IP de destination est utilisée par les routeurs pour transférer un paquet vers sa destination.

Adresse de liaison de données

Sur la couche liaison de données ou couche 2, l'adresse physique joue un rôle différent. L'objectif de l'adresse de liaison de données est de transmettre la trame liaison de données d'une interface réseau à une autre, sur un même réseau. Pour qu'un paquet IP puisse être envoyé via un réseau câblé ou sans fil, il doit être encapsulé dans une trame de liaison de données qui peut être transmise à travers le support physique, c'est-à-dire le réseau réel. Les réseaux locaux Ethernet et sans fil sont par exemple des réseaux dont les supports physiques sont différents, chacun ayant son propre type de protocole de liaison de données.

Le paquet IP est encapsulé dans une trame de liaison de données à remettre au réseau de destination. Les adresses de liaison de données source et de destination sont ajoutées, comme illustré dans la figure :

- **Adresse de liaison de données source** : adresse physique du périphérique qui envoie le paquet. Initialement, c'est la carte réseau qui est la source du paquet IP.

- **Adresse de liaison de données de destination** : adresse physique de l'interface réseau du routeur du tronçon suivant ou de l'interface réseau du périphérique de destination.

3.3.2.2 Communication avec un périphérique sur le même réseau

Pour comprendre à quels éléments tient la réussite des communications dans le réseau, il est important de comprendre les rôles des adresses de couche réseau et des adresses de liaison de données lorsqu'un périphérique communique avec un autre sur le même réseau. Dans cet exemple, nous avons un ordinateur client (PC1) communiquant avec un serveur de fichiers (serveur FTP) sur le même réseau IP.

Adresses réseau

Les adresses de couche réseau ou adresses IP indiquent le réseau et l'adresse de l'hôte de la source et de la destination. La partie réseau de l'adresse est la même, seule la partie hôte ou périphérique de l'adresse diffère.

- **Adresse IP source** : adresse IP du périphérique expéditeur, l'ordinateur client PC1 : 192.168.1.110.
- **Adresse IP de destination** : adresse IP du périphérique récepteur, le serveur FTP : 192.168.1.9.

Adresses de liaison de données

Lorsque l'expéditeur et le récepteur du paquet IP se trouvent sur le même réseau, la trame de liaison de données est envoyée directement au périphérique récepteur. Sur un réseau Ethernet, les adresses de liaison de données sont appelées adresses MAC Ethernet. Les adresses MAC sont des adresses formées de 48 bits qui sont physiquement intégrées à la carte réseau Ethernet. L'adresse MAC est également appelée « adresse physique » ou « adresse rémanente ».

- **Adresse MAC source** : il s'agit de l'adresse de liaison de données ou adresse MAC Ethernet du périphérique qui envoie le paquet IP, c'est-à-dire PC1. L'adresse MAC de la carte réseau Ethernet de PC1 est AA-AA-AA-AA-AA-AA.
- **Adresse MAC de destination** : lorsque le périphérique récepteur se trouve sur le même réseau que le périphérique expéditeur, il s'agit de l'adresse de liaison de données du périphérique récepteur. Dans cet exemple, l'adresse MAC de destination est l'adresse MAC du serveur FTP : CC-CC-CC-CC-CC-CC.

Les adresses source et de destination sont ajoutées à la trame Ethernet. La trame contenant le paquet IP encapsulé peut maintenant être transmise par PC1 directement au serveur FTP.

3.3.2.3 Adresses MAC et IP

Vous devriez maintenant savoir que pour envoyer des données à un autre hôte situé sur le même réseau local, l'hôte source doit connaître les adresses logique et physique de l'hôte de destination. Une fois ces informations acquises, il peut créer une trame et l'envoyer sur le support réseau. L'hôte source peut obtenir l'adresse IP de destination de différentes manières. Par exemple, il peut l'obtenir en utilisant le système de noms de domaine (DNS) ou il peut connaître l'adresse IP de destination parce qu'elle est indiquée manuellement dans l'application, notamment lorsque l'utilisateur saisit l'adresse IP d'un serveur FTP de destination. Mais comment un hôte détermine-t-il l'adresse MAC Ethernet d'un autre périphérique ?

La plupart des applications réseau utilisent l'adresse IP logique de destination pour identifier l'emplacement des hôtes intervenant dans la communication. L'adresse MAC de liaison de données est nécessaire pour acheminer le paquet IP encapsulé dans la trame Ethernet sur tout le réseau, jusqu'à la destination.

L'hôte expéditeur utilise un protocole IP appelé « protocole ARP » pour connaître l'adresse MAC d'un hôte sur le même réseau local. L'hôte expéditeur envoie un message de requête ARP à l'ensemble du réseau local. La requête ARP est un message de diffusion qui contient l'adresse IP du périphérique de destination. Chaque périphérique du réseau local examine la requête ARP pour voir si elle contient sa propre adresse IP. Seul le périphérique dont l'adresse IP est présente dans la requête ARP envoie une réponse ARP. Celle-ci contient l'adresse MAC associée à l'adresse IP de la requête ARP.

3.3.3 Accès aux ressources distantes

3.3.3.1 Passerelle par défaut

La méthode utilisée par un hôte pour envoyer des messages à une destination sur un réseau distant est différente de celle qu'il utilise pour envoyer des messages à une destination sur le même réseau local. Lorsqu'un hôte doit envoyer un message à un autre hôte du même réseau, il transfère directement le message. Un hôte utilisera le protocole ARP pour connaître l'adresse MAC de l'hôte de destination. Il inclut l'adresse IP de destination dans l'en-tête du paquet et encapsule le paquet dans une trame contenant l'adresse MAC de la destination, puis le transfère.

Lorsqu'un hôte doit envoyer un message à un réseau distant, il doit utiliser le routeur, également appelé « passerelle par défaut ». La passerelle par défaut est l'adresse IP d'une interface d'un routeur se trouvant sur le même réseau que l'hôte expéditeur.

Il est important que l'adresse de la passerelle par défaut soit configurée sur chaque hôte du réseau local. Si aucune adresse de passerelle par défaut n'est configurée dans les paramètres TCP/IP de l'hôte ou si une passerelle par défaut incorrecte est spécifiée, les messages adressés aux hôtes des réseaux distants ne peuvent pas être acheminés.

Sur la figure, les hôtes du réseau local utilisent R1 comme passerelle par défaut et son adresse 192.168.1.1 est configurée dans leurs paramètres TCP/IP. Si la destination d'une unité de données de protocole se trouve sur un autre réseau IP, les hôtes envoient les unités de données de protocole à la passerelle par défaut sur le routeur qui devra à son tour les transmettre.

3.3.3.2 Communication avec un périphérique sur un réseau distant

Mais quels sont les rôles de l'adresse de couche réseau et de l'adresse de couche liaison de données lorsqu'un périphérique communique avec un autre périphérique situé sur un réseau distant ? Dans cet exemple, nous avons un ordinateur client (PC1) communiquant avec un serveur appelé « serveur Web », situé sur un autre réseau IP.

Adresses réseau

Les adresses IP indiquent les adresses des réseaux et des périphériques source et de destination. Lorsque l'expéditeur du paquet appartient à un réseau différent de celui du récepteur, les adresses IP source et de destination représentent des hôtes sur différents réseaux. Cette information est indiquée par la partie réseau de l'adresse IP de l'hôte de destination.

- **Adresse IP source** : adresse IP du périphérique expéditeur, l'ordinateur client PC1 : 192.168.1.110.
- **Adresse IP de destination** : adresse IP du périphérique récepteur, ici le serveur Web : 172.16.1.99.

Adresses de liaison de données

Lorsque l'expéditeur et le récepteur du paquet IP se trouvent sur des réseaux différents, la trame liaison de données Ethernet ne peut pas être envoyée directement à l'hôte de destination, car celui-ci n'est pas directement accessible sur le réseau de l'expéditeur. La trame Ethernet doit être envoyée à un autre périphérique appelé routeur ou passerelle par défaut. Dans notre exemple, la passerelle par défaut est R1. R1 dispose d'une interface, et d'une adresse IP qui se trouve sur le même réseau que PC1. Cela permet à PC1 d'accéder directement au routeur.

- **Adresse MAC source** : adresse MAC Ethernet du périphérique expéditeur, PC1. L'adresse MAC de l'interface Ethernet de PC1 est AA-AA-AA-AA-AA-AA.

Adresse MAC de destination : lorsque le périphérique récepteur se trouve sur un réseau différent de celui du périphérique expéditeur, il s'agit de l'adresse MAC Ethernet de la passerelle par défaut ou routeur. Dans cet exemple, l'adresse MAC de destination est l'adresse MAC de l'interface Ethernet de R1 qui est reliée au réseau de PC1, 11-11-11-11-11-11.

La trame Ethernet contenant le paquet IP encapsulé peut être transmise à R1. R1 achemine le paquet vers la destination, le serveur Web. R1 peut transmettre le paquet à un autre routeur ou bien directement au serveur Web si la destination se trouve sur un réseau connecté à R1.

Comment le périphérique destinataire détermine-t-il l'adresse MAC du routeur ?

Chaque périphérique obtient l'adresse IP du routeur à travers l'adresse de la passerelle par défaut configurée dans ses paramètres TCP/IP. L'adresse de la passerelle par défaut est l'adresse de l'interface du routeur connectée au même réseau local que le périphérique source. Tous les périphériques du réseau local utilisent l'adresse de la passerelle par défaut pour envoyer des messages au routeur. Une fois que l'hôte connaît l'adresse IP de la passerelle par

défaut, il peut utiliser le protocole ARP pour en déterminer l'adresse MAC. L'adresse MAC de la passerelle par défaut est ensuite incluse dans la trame.

CHAPITRE 4: ACCES RESEAU

4.0 Accès réseau

4.0.1 Introduction

4.0.1.1 Introduction

Pour permettre aux utilisateurs de communiquer, le modèle OSI divise les fonctions d'un réseau de données en couches. Chaque couche fonctionne avec les couches supérieures et inférieures afin de transmettre des données. Deux couches du modèle OSI sont si étroitement liées que, selon le modèle TCP/IP, elles ne forment presque qu'une seule couche. Il s'agit de la couche liaison de données et de la couche physique.

Sur le périphérique émetteur, il appartient à la couche liaison de données de préparer les données à transmettre et de contrôler l'accès de ces données aux supports physiques. Cependant, la couche physique contrôle la manière dont les données sont transmises sur les supports physiques en codant sous forme de signaux les chiffres binaires qui représentent des données.

Au niveau du destinataire, la couche physique reçoit des signaux à travers les supports connectés. Après avoir décodé le signal pour obtenir à nouveau des données, la couche physique transmet les données à la couche liaison de données pour acceptation et traitement.

Ce chapitre décrit d'abord les fonctions générales de la couche physique et les normes et protocoles qui gèrent la transmission de données sur le support local. Il présente également les fonctions de la couche liaison de données et des protocoles qui lui sont associés.

4.0.1.2 Exercice - Gestion du support

Gestion du support

Vous et votre collègue participez à un congrès sur les réseaux. De nombreuses conférences et présentations sont proposées pour l'occasion, mais comme elles se chevauchent, chacun d'entre vous doit choisir un nombre limité de sessions auxquelles assister.

Par conséquent, vous décidez de vous séparer et de participer chacun à des présentations différentes. Vous partagerez ensuite les documents reçus et les connaissances acquises à la fin de l'événement.

Essayez de répondre aux questions suivantes :

- Comment organiseriez-vous un congrès dans lequel plusieurs sessions se tiennent en parallèle ? Les placeriez-vous toutes dans une même salle de conférence ou utiliseriez-vous plusieurs salles ? Pourquoi ?

- Supposons que la salle de conférence est équipée de matériel audiovisuel permettant d'afficher des vidéos grands formats et d'amplifier la voix de l'orateur. Si une personne souhaite participer à une session spécifique, la place qu'elle choisit a-t-elle une importance ou suffit-il qu'elle se trouve dans la salle de conférence correspondante ?

- Si le discours prononcé dans une salle était perceptible dans une autre salle, cela aurait-il des retombées positives ou négatives ?

- Si des questions ou des demandes d'information apparaissent pendant une présentation, le participant doit-il simplement crier sa question ou est-il nécessaire de mettre en place des moyens de gestion des questions, par exemple les noter et les remettre à un animateur ? Que se passerait-il sans ce processus ?

- Une session peut-elle arriver à échéance sans que tout le contenu prévu ait été communiqué si un sujet intéressant donne lieu à une discussion plus poussée qui soulève de nombreuses questions ? Pourquoi ?

- Imaginez la session comme une table ronde, c'est-à-dire une discussion plus libre entre les participants et les intervenants, voire entre les participants eux-mêmes. Si une personne souhaite s'adresser à une autre personne dans la même salle, peut-elle le faire directement ? Quelles actions seraient nécessaires pour qu'un orateur puisse inviter une personne non présente dans la salle à le rejoindre ?

- À quoi servirait la répartition des différentes sessions dans plusieurs salles de conférence si, à l'issue de la manifestation, les personnes peuvent se rencontrer et partager des informations ?

Instructions de l'exercice en classe - Laisse-moi te raconter ce que j'ai appris à la conférence

4.1 Protocoles de couche physique

4.1.1 Mise en place de la connexion

4.1.1.1 Connexion au réseau

Que vous vous connectiez à une imprimante locale chez vous ou à un site Web dans un autre pays, avant que toute communication réseau puisse se produire, une connexion physique à un réseau local doit être établie. Une connexion physique peut être une connexion filaire par câble ou une connexion sans fil passant par les ondes radio.

Le type de connexion physique utilisé dépend entièrement de la configuration du réseau. Par exemple, dans de nombreuses entreprises, les employés ont des ordinateurs portables ou de bureau qui sont connectés physiquement à un commutateur partagé par l'intermédiaire d'un câble. Ce type de configuration correspond à un réseau filaire, dans lequel les données sont transmises à travers un câble physique.

Outre les connexions filaires, certaines entreprises proposent également des connexions sans fil pour les ordinateurs portables, les tablettes et les smartphones. Avec les périphériques sans fil, les données sont transmises par des ondes radio. Les connexions sans fil se développent à mesure que les particuliers comme les entreprises découvrent les avantages des services sans fil. Pour qu'il puisse proposer une connectivité sans fil, un réseau doit intégrer un point d'accès sans fil (WAP) permettant aux équipements de se connecter.

Les commutateurs et les points d'accès sans fil sont souvent deux périphériques dédiés distincts dans une configuration de réseau. Cependant, certains équipements proposent à la fois une connectivité filaire et sans fil. Par exemple, la plupart des particuliers utilisent des routeurs à services intégrés (ISR) chez eux, comme illustré à la Figure 1. Les ISR proposent un composant de commutation équipé de plusieurs ports, ce qui permet la connexion de plusieurs périphériques au réseau local (LAN) à l'aide de câbles, comme illustré à la Figure 2.

En outre, de nombreux ISR intègrent un WAP qui permet également la connexion des périphériques sans fil.

4.1.1.2 Cartes réseau

Les cartes réseau (NIC en anglais) connectent un périphérique au réseau. Les cartes réseau Ethernet sont utilisées dans les connexions filaires, tandis que les cartes réseau WLAN (réseau local sans fil) sont utilisées dans les connexions sans fil. Un périphérique utilisateur peut comporter l'un de ces deux types de carte réseau ou les deux. Une imprimante réseau, par exemple, peut ne comporter qu'une carte réseau Ethernet et doit, dans ce cas, être connectée au réseau à l'aide d'un câble Ethernet. D'autres périphériques, tels que les tablettes et les smartphones peuvent n'être équipés que d'une carte réseau WLAN et doivent donc utiliser une connexion sans fil.

Le niveau de performance n'est pas le même dans toutes les connexions physiques à un réseau.

Par exemple, un périphérique sans fil subit une dégradation des performances en fonction de sa distance au point d'accès sans fil. Plus le périphérique est éloigné du point d'accès, plus faible est le signal sans fil qu'il reçoit. Il peut donc bénéficier d'une bande passante inférieure ou encore perdre la connexion sans fil. La figure montre qu'un amplificateur de signal sans fil peut être utilisé pour régénérer le signal sans fil afin d'en faire bénéficier d'autres parties de la maison qui sont trop éloignées du point d'accès sans fil. Au contraire, les connexions filaires ne dégradent pas les performances, mais limitent grandement les mouvements au point de nécessiter généralement une position statique.

Tous les périphériques sans fil doivent partager un accès aux ondes assurant la connexion au point d'accès sans fil. Cela signifie que les performances du réseau peuvent être ralenties si plusieurs périphériques sans fil accèdent simultanément au réseau. Un périphérique filaire n'a pas besoin de partager son accès au réseau avec d'autres périphériques. Chaque périphérique filaire dispose d'un canal de communication distinct à travers son câble Ethernet. Cet aspect a son importance pour certaines applications telles que les jeux vidéo, la vidéo en streaming et la visioconférence qui nécessitent davantage de bande passante dédiée que d'autres applications.

Au fil des prochains thèmes abordés, vous en saurez davantage sur les connexions de la couche physique et sur les effets de ces connexions sur le transport des données.

4.1.2 Objectif de la couche physique

4.1.2.1 La couche physique

La couche physique OSI fournit un moyen de transporter sur le support réseau les bits constituant une trame de couche liaison de données. Cette couche accepte une trame complète de la couche liaison de données et la code sous la forme d'une série de signaux transmis sur les supports locaux. Les bits codés composant une trame sont reçus par un périphérique final ou intermédiaire.

Le processus subi par les données, du nœud source au nœud de destination, est le suivant :

- Les données utilisateur sont segmentées par la couche transport, placées dans des paquets par la couche réseau, puis encapsulées sous forme de trames par la couche liaison de données.
- La couche physique code les trames et crée les signaux électriques, optiques ou ondulatoires (radio) qui représentent les bits dans chaque trame.
- Ces signaux sont alors envoyés sur le support individuellement.
- La couche physique du nœud de destination récupère ces signaux individuels sur les supports, les convertit en représentations binaires et transmet les bits à la couche liaison de données sous forme de trame complète.

4.1.2.2 Supports de couche physique

Il existe trois formes élémentaires de support réseau. La couche physique produit la représentation et les groupements de bits pour chaque type de support comme suit :

- **Câble en cuivre** : les signaux sont des variations d'impulsions électriques.
- **Câble à fibre optique** : les signaux sont des variations lumineuses.
- **Sans fil** : les signaux sont des variations de transmission d'hyperfréquences.

La figure illustre des exemples de signalisation pour le cuivre, la fibre optique et le sans fil.

Pour permettre l'interopérabilité sur la couche physique, tous les aspects de ces fonctions sont régis par les organismes de normalisation.

4.1.2.3 Normes de couche physique

Les protocoles et les opérations des couches OSI supérieures sont exécutés dans des logiciels conçus par des développeurs et des ingénieurs informaticiens. Par exemple, les services et les protocoles de la suite TCP/IP sont définis par l'IETF (Internet Engineering Task Force) dans des documents RFC, comme illustré à la Figure 1.

La couche physique est constituée de circuits électroniques, de supports et de connecteurs développés par des ingénieurs. Il est par conséquent approprié que les normes régissant ces matériels soient définies par les organisations d'ingénierie électrique et de communications correspondantes.

De nombreux organismes internationaux et nationaux, organisations gouvernementales de réglementation et entreprises privées sont impliqués dans l'établissement et la mise à jour des normes de couche physique. Par exemple, les normes relatives au matériel, aux supports, au codage et à la signalisation de la couche physique sont définies et régies par les organismes suivants :

- ISO (International Standards Organization)
- TIA/EIA (Telecommunications Industry Association/Electronic Industries Association)
- Union Internationale des Télécommunications (UIT)
- ANSI (American National Standards Institute)
- Institute of Electrical and Electronics Engineers (IEEE)
- Des autorités réglementaires nationales des télécommunications, notamment la FCC (Federal Communication Commission, États-Unis) et l'ETSI (European Telecommunications Standards Institute)

Il existe également certains groupes régionaux de normalisation du câblage tels que la CSA (Canadian Standards Association), le CENELEC (European Committee for Electrotechnical Standardization) et le JSA/JIS (Japanese Standards Association) qui établissent des spécifications locales.

La Figure 2 présente les principaux contributeurs et certaines des normes de couche physique utilisées.

4.1.3 Principes fondamentaux de la couche 1

4.1.3.1 Principes fondamentaux de la couche physique

Les normes de couche physique correspondent à trois zones fonctionnelles :

Composants physiques

Les composants physiques sont les périphériques électroniques, les supports et les connecteurs qui transportent et transmettent les signaux pour représenter les bits. Les composants matériels, tels que les cartes réseau, les interfaces et les connecteurs, les matériaux et les types de câble, sont tous répertoriés dans les normes associées à la couche physique. Les différents ports et interfaces d'un routeur Cisco 1941 sont également des exemples de composants physiques équipés de connecteurs et de brochage spécifiques définis dans des normes.

Codage

Le codage, ou codage de ligne, est une méthode permettant de convertir un flux de bits de données en un code prédéfini. Les codes sont des groupements de bits utilisés pour fournir un modèle prévisible pouvant être reconnu à la fois par l'expéditeur et le récepteur. Dans le cas du réseau, le codage correspond à des variations de tension ou de courant utilisées pour représenter les bits (les 0 et les 1).

Outre la création de codes pour les données, les méthodes de codage au niveau de la couche physique peuvent également fournir des codes à des fins de contrôle comme l'identification du début et de la fin d'une trame.

Les méthodes de codage réseau les plus répandues sont les suivantes :

- **Le codage Manchester** : le 0 est représenté par une baisse de tension et le 1 par une hausse de tension. Ce type de codage est utilisé dans des versions précédentes d'Ethernet, de radio-identification et de communication en champ proche.
- **La méthode NRZ (Non-Return to Zero)** : méthode commune de codage des données utilisant deux états appelés « zéro » et « un » et aucune position neutre ou de repos. Un 0 peut être représenté par un niveau de tension et un 1 par une autre tension sur les supports.

Remarque : les débits plus élevés nécessitent un codage plus complexe, par exemple de type 4B/5B, mais ces méthodes sortent du cadre de ce cours.

Signalisation

La couche physique doit générer les signaux électriques, optiques ou sans fil qui représentent le 1 et le 0 sur les supports. La méthode de représentation des bits est appelée méthode de signalisation. Les normes de couche physique doivent définir le type de signal représentant un 1 et celui représentant un 0. Il peut s'agir simplement d'un changement de niveau du signal électrique ou de l'impulsion optique. Par exemple, une impulsion longue peut représenter un 1, alors qu'une impulsion courte représente un 0.

Ce code utilise le même principe de communication que le code Morse. Le code Morse est une autre méthode de signalisation qui utilise une série de tonalités, de signaux lumineux ou de clics pour envoyer du texte sur une ligne téléphonique ou entre les bateaux en mer.

Il existe deux types de transmission des signaux :

- **Asynchrone** : les signaux de données sont transmis sans signal d'horloge associé. L'intervalle de temps entre les caractères ou les blocs de données peut être défini arbitrairement, ce qui signifie qu'il n'est pas normalisé. Par conséquent, les trames doivent comporter des indicateurs de début et de fin.
- **Synchrone** : les signaux de données sont envoyés avec un signal d'horloge qui se produit à des intervalles réguliers appelés temps bits.

Il existe plusieurs manières de transmettre des signaux. L'utilisation de techniques de modulation pour envoyer des données est courante. La modulation est le processus par lequel la caractéristique d'une onde (signal) modifie une autre onde (porteuse). Les techniques de modulation suivantes sont largement utilisées dans la transmission de données sur un support :

- **Modulation de fréquence (FM)** : méthode de communication dans laquelle la fréquence porteuse varie selon le signal.
- **Modulation d'amplitude (AM)** : technique de transmission dans laquelle l'amplitude de la porteuse varie selon le signal.
- **Modulation par impulsions et codage (PCM)** : technique dans laquelle un signal analogique, tel que la voix est converti en un signal numérique en échantillonnant l'amplitude du signal et en exprimant les différentes amplitudes sous forme binaire. La fréquence d'échantillonnage doit être au moins deux fois supérieure à la plus haute fréquence du signal.

La nature des signaux réels représentant les bits sur le support dépend de la méthode de signalisation utilisée. Certaines méthodes peuvent utiliser un attribut de signal pour représenter un seul 0 et un autre pour représenter un seul 1.

La Figure 2 illustre l'utilisation des techniques AM et FM lors de l'envoi d'un signal.

4.1.3.2 Bande passante

Différents supports physiques prennent en charge le transfert de bits à différentes vitesses. Le transfert des données est généralement décrit par la bande passante et le débit.

La bande passante est la capacité d'un support à transporter des données. La bande passante numérique mesure la quantité de données pouvant circuler d'un emplacement à un autre

pendant une période donnée. Elle est généralement exprimée en kilobits par seconde (kbit/s) ou en mégabits par seconde (Mbit/s).

La bande passante pratique d'un réseau est déterminée par une combinaison de facteurs :

- Les propriétés des supports physiques
- Les technologies choisies pour signaliser et détecter les signaux réseau

Les propriétés du support physique, les technologies courantes et les lois de la physique jouent toutes un rôle dans la détermination de la bande passante disponible.

Le tableau décrit les principales unités de mesure de la bande passante.

4.1.3.3 Débit

Le débit est la mesure du transfert de bits sur le support pendant une période donnée.

En raison de différents facteurs, le débit ne correspond généralement pas à la bande passante spécifiée dans les mises en œuvre de couche physique. De nombreux facteurs influencent le débit, notamment :

- la quantité de trafic
- le type de trafic
- la latence créée par le nombre de périphériques réseau rencontrés entre la source et la destination

La latence désigne le temps nécessaire (délais inclus) aux données pour voyager d'un point A à un point B.

Dans un interréseau ou un réseau avec des segments multiples, le débit ne peut pas être plus rapide que la liaison la plus lente du chemin de la source à la destination. Même si la totalité ou la plupart des segments ont une bande passante élevée, il suffit d'un segment dans le chemin ayant un faible débit pour créer un goulot d'étranglement dans le débit de l'ensemble du réseau.

Il existe de nombreux tests de débit en ligne qui peuvent indiquer le débit d'une connexion Internet. La figure présente des exemples de résultats d'un test de débit.

Remarque : il existe une troisième mesure qui indique le transfert de données utilisables, appelée débit applicatif. Le débit applicatif mesure les données utilisables transférées sur une période donnée. Le débit applicatif correspond donc au débit moins la surcharge de trafic pour l'établissement de sessions, les accusés de réception et l'encapsulation.

4.1.3.4 Types de supports physiques

La couche physique produit la représentation et les groupements de bits sous forme de tensions, de radiofréquences ou d'impulsions lumineuses. Divers organismes de normalisation ont contribué à la définition des propriétés physiques, électriques et mécaniques des supports disponibles pour différentes communications de données. Ces spécifications garantissent que les câbles et les connecteurs fonctionnent comme prévu avec différentes mises en œuvre de la couche liaison de données.

Par exemple, des normes pour les supports en cuivre sont définies pour :

- Le type de câblage en cuivre utilisé
- La bande passante de la communication
- Le type de connecteurs utilisés
- Le brochage et les codes couleur des connexions avec le support
- La distance maximale du support

La figure présente différents types d'interfaces et de ports disponibles sur un routeur 1941.

4.2 Supports réseau

4.2.1 L'utilisation de câbles en cuivre

4.2.1.1 Caractéristiques des supports en cuivre

Les supports en cuivre sont utilisés sur certains réseaux, car ils sont bon marché, faciles à installer et qu'ils présentent une faible résistance au courant électrique. Cependant, les supports en cuivre sont limités par la distance et les interférences du signal.

Les données sont transmises sur les câbles en cuivre sous forme d'impulsions électriques. Un détecteur dans l'interface réseau d'un périphérique de destination doit recevoir un signal pouvant être décodé correctement pour correspondre au signal envoyé. Toutefois, plus la distance de transmission du signal est longue, plus il se détériore selon un phénomène dit d'atténuation du signal. Pour cette raison, tous les supports en cuivre sont soumis à des restrictions de distance strictes spécifiées par les normes en la matière.

La durée et la tension des impulsions électriques sont également susceptibles de subir des interférences de deux sources :

- **Interférences électromagnétiques (EMI) ou interférences radioélectriques (RFI) :** les signaux électromagnétiques et radioélectriques peuvent déformer et détériorer les signaux de données transportés par les supports en cuivre. Les sources potentielles d'interférences EMI et RFI sont notamment les ondes radio et les appareils électromagnétiques tels que les éclairages fluorescents ou les moteurs électriques comme illustré sur la figure.
- **Diaphonie** : la diaphonie est une perturbation causée par les champs électriques ou magnétiques d'un signal dans un câble au signal traversant le câble adjacent. Dans les circuits téléphoniques, les interlocuteurs peuvent entendre une partie d'une autre conversation vocale provenant d'un circuit adjacent. Plus précisément, lorsque le courant électrique circule dans un câble, il crée un petit champ magnétique circulaire autour du câble qui peut être capté par le fil adjacent.

4.2.1.2 Supports en cuivre

Lancez l'animation de la figure pour voir l'effet des interférences sur la transmission de données.

Pour contrer les effets négatifs des perturbations électromagnétiques et radioélectriques, certains types de câbles en cuivre sont entourés d'un blindage métallique et nécessitent des connexions de mise à la terre appropriées.

Pour contrer les effets négatifs de la diaphonie, certains types de câbles en cuivre utilisent des paires de fils opposés torsadés qui annulent la perturbation.

La sensibilité des câbles en cuivre aux parasites électroniques peut également être limitée :

Il existe trois principaux types de supports en cuivre utilisés dans les réseaux :

- **les câbles à paires torsadées non blindées (UTP)**
- **les câbles à paires torsadées blindées (STP)**
- **les câbles coaxiaux**

Ces câbles sont utilisés pour interconnecter des nœuds d'un réseau local et des périphériques d'infrastructure tels que des commutateurs, des routeurs et des points d'accès sans fil. Chaque type de connexion et les périphériques associés possèdent des exigences de câblage stipulées par les normes de couche physique.

Diverses normes de couche physique spécifient l'utilisation de différents connecteurs. Ces normes définissent les dimensions mécaniques des connecteurs et les propriétés électriques acceptables de chaque type. Les supports réseau utilisent des connecteurs et des fiches modulaires qui facilitent la connexion et la déconnexion. De plus, un même type de connecteur physique peut servir à plusieurs types de connexions. Par exemple, le connecteur RJ-45 est largement employé dans les réseaux locaux avec un type de support et dans certains réseaux étendus avec un autre type de support.

4.2.1.3 Câble à paires torsadées non blindé

Le câblage à paires torsadées non blindées (UTP) est le support réseau le plus répandu. Ces câbles terminés par des connecteurs RJ-45 sont utilisés pour relier des hôtes réseau à des périphériques réseau intermédiaires, tels que des commutateurs et des routeurs.

Dans les réseaux locaux, chaque câble UTP se compose de quatre paires de fils à code-couleur qui ont été torsadés, puis placés dans une gaine en plastique souple qui les protège des dégâts matériels mineurs. Le fait de torsader les fils permet de limiter les interférences causées par les signaux d'autres fils.

Comme l'illustre la figure, les codes de couleur identifient les paires individuelles et les fils des paires afin de faciliter le raccordement des câbles.

4.2.1.4 Câble à paires torsadées blindées (STP)

Les câbles à paires torsadées blindées (STP) offrent une meilleure protection parasitaire que le câblage UTP. Toutefois, par rapport aux UTP, les câbles STP sont bien plus onéreux et plus difficiles à installer. Comme les câbles UTP, les câbles STP utilisent un connecteur RJ-45.

Les câbles à paires torsadées blindées allient la technique de blindage pour contrer les interférences électromagnétiques et radioélectriques, et les torsades pour éviter la diaphonie. Pour tirer entièrement parti des avantages du blindage, les câbles STP sont terminés par des connecteurs de données STP blindés spécifiques. Si le câble n'est pas correctement mis à la terre, le blindage peut agir comme une antenne et capter des signaux parasites.

Différents types de câbles STP sont disponibles, chacun avec des caractéristiques différentes. Il existe toutefois deux variantes principales de ces câbles :

- Le câble STP entoure de feuilles de blindage l'ensemble du faisceau de fils et élimine ainsi presque toutes les interférences (version la plus répandue).
- Le câble STP entoure de feuilles de blindage l'ensemble du faisceau de fils ainsi que chaque paire de fils, et élimine ainsi toute interférence.

Le câble STP représenté utilise quatre paires de fils, chacune enveloppée dans une feuille de blindage. Le tout est ensuite entouré dans une torsade ou une feuille métallique.

Pendant de nombreuses années, le câblage STP a constitué la structure de câblage spécifiée pour les installations réseau Token Ring. Les réseaux de type Token Ring étant de moins en moins employés, la demande de câblage à paires torsadées blindées a également décliné. Cependant, la nouvelle norme relative à 10 Gigabit Ethernet prévoit l'utilisation de câblage STP, ce qui crée un certain regain d'intérêt envers ce type de câble.

4.2.1.5 Câble coaxial

Le câble coaxial (parfois abrégé coax) tire son nom du fait qu'il contient deux conducteurs qui partagent le même axe. Comme l'illustre la figure, le câble coaxial est composé des éléments suivants :

- Un conducteur en cuivre utilisé pour transmettre les signaux électroniques.
- Le conducteur en cuivre est entouré d'une couche de matériau isolant souple en plastique.
- Sur ce matériau isolant, une torsade de cuivre ou une feuille métallique constitue le second fil du circuit et fait office de protection pour le conducteur intérieur. Cette seconde couche, ou blindage, réduit également les interférences électromagnétiques externes.
- Le câble dans son entier est ensuite entouré d'une gaine qui le protège contre les dommages physiques mineurs.

Remarque : différents types de connecteurs sont utilisés avec les câbles coaxiaux.

Les câbles coaxiaux étaient traditionnellement utilisés pour la télévision par câble et permettaient la transmission dans une seule direction. Ils ont également été largement utilisés dans les premières installations Ethernet.

Bien que les câbles UTP aient pratiquement remplacé les câbles coaxiaux dans les installations Ethernet modernes, la conception du câble coaxial a été adaptée aux fins suivantes :

- **Installations sans fil** : les câbles coaxiaux relient les antennes aux périphériques sans fil. Le câble coaxial transporte de l'énergie en radiofréquence (RF) entre les antennes et le matériel radio.
- **Installations Internet par le câble** : les fournisseurs d'accès câblé convertissent actuellement leurs systèmes unidirectionnels en systèmes bidirectionnels afin de fournir une connectivité Internet à leurs clients. Afin de fournir ces services, des portions du câble coaxial et des éléments d'amplification associés sont remplacés par du câble à fibre optique. Cependant, la connexion finale avec le site du client et le

câblage à l'intérieur de ses locaux restent coaxiaux. Cette utilisation mixte de fibre et de coaxial est appelée réseau hybride fibre et coaxial (HFC).

4.2.1.6 Sécurité des supports en cuivre

Les trois types de supports en cuivre présentent des risques d'incendie et des risques électriques.

L'isolation et les gaines du câble peuvent être inflammables ou dégager des émanations toxiques lorsqu'elles sont chauffées ou brûlées, d'où le risque d'incendie. Les organismes de construction peuvent stipuler des normes de sécurité pour le câblage et les installations matérielles.

Des risques électriques peuvent également exister puisque les fils de cuivre peuvent conduire l'électricité dans des directions non souhaitables. Personnel et matériel peuvent alors être exposés à une série de risques électriques. Par exemple, un périphérique réseau défectueux peut conduire le courant dans le châssis d'autres périphériques du réseau. De plus, le câblage réseau peut présenter des niveaux de tension indésirables lorsqu'il sert à connecter des périphériques dont les sources d'alimentation ont des mises à la terre différentes. De telles situations sont possibles lorsque le câblage en cuivre est utilisé pour connecter des réseaux dans des bâtiments ou à des étages de bâtiments différents, qui utilisent des installations d'alimentation différentes. Pour finir, le câblage en cuivre peut conduire des tensions causées par la foudre vers des périphériques réseau.

Les tensions et courants indésirables peuvent endommager les périphériques réseau et les ordinateurs connectés, ou encore blesser le personnel. Il est essentiel que le câblage en cuivre soit installé de manière appropriée, conformément aux spécifications et normes de construction, pour éviter des situations potentiellement dangereuses et dommageables.

4.2.2 Câblage à paires torsadées non blindées (UTP)

4.2.2.1 Propriétés du câblage à paires torsadées non blindées

Lorsqu'il est utilisé comme support réseau, le câblage à paires torsadées non blindées (UTP) se compose de quatre paires de fils à code-couleur qui ont été torsadées, puis entourées d'une gaine en plastique souple. Un câble UTP réseau est constitué de quatre paires de fils en cuivre de 22 ou 24 AGW. Il présente un diamètre extérieur d'environ 0,43 cm (0,17 pouce) et sa petite taille peut constituer un avantage lors de l'installation.

Le câble UTP n'utilise pas de blindage pour contrer les effets des perturbations électromagnétiques et radioélectriques. En revanche, les concepteurs de câbles se sont rendu compte qu'il était possible de limiter les effets négatifs de la diaphonie des manières suivantes :

- **Annulation** : les concepteurs apparient désormais les fils du circuit. Lorsque deux fils d'un circuit électrique sont proches l'un de l'autre, leurs champs magnétiques sont exactement opposés l'un à l'autre. Par conséquent, les deux champs magnétiques s'annulent et annulent également tous les signaux extérieurs d'EMI et de RFI.
- **Variation du nombre de torsades par paire de fils** : pour renforcer l'effet d'annulation des paires de fils, les concepteurs utilisent un nombre différent de

torsades pour chaque paire de fils d'un câble. Le câble UTP doit respecter des caractéristiques précises qui définissent le nombre de torsades autorisées par mètre (3,28 pieds) de câble. Sur la figure, vous observez que la paire orange/orange et blanc est moins torsadée que la paire bleu/bleu et blanc. Chaque couleur de paire présente un nombre de torsades différent.

Le câble UTP utilise uniquement l'effet d'annulation produit par les paires de fils torsadées pour limiter la dégradation du signal et pour protéger mutuellement les paires de fils des supports réseau.

4.2.2.2 Normes de câblage UTP

Le câblage UTP respecte les normes établies conjointement par la TIA et l'EIA. Plus précisément, la norme TIA/EIA-568A, le plus souvent utilisée dans les environnements de câblage LAN, définit le câblage commercial pour les installations de réseau local. Elle définit des éléments tels que :

- Les types de câbles
- Les longueurs de câbles
- Connecteurs
- Le raccordement des câbles
- Les méthodes de test des câbles

Les caractéristiques électriques du câblage en cuivre sont définies par l'IEEE (Institute of Electrical and Electronics Engineers). L'IEEE classe le câblage UTP suivant ses performances. Les câbles sont placés dans des catégories selon leur capacité à prendre en charge des débits supérieurs de bande passante. Par exemple, un câble de catégorie 5 (Cat5) est généralement utilisé dans les installations FastEthernet 100BASE-TX. Les autres catégories comprennent le câble de catégorie 5 renforcée (Cat5e), la catégorie 6 (Cat6) et la catégorie 6a.

Les câbles des catégories supérieures sont conçus pour prendre en charge des débits de données plus élevés. À mesure que de nouvelles technologies Ethernet avec des débits exprimés en gigabits sont mises au point et adoptées, Cat5e constitue désormais le type de câble minimum acceptable, Cat6 étant recommandé pour les installations de nouveaux bâtiments.

La figure illustre les différentes catégories de câbles UTP.

Remarque : certains fabricants produisent des câbles dont les caractéristiques dépassent celles de la catégorie 6a définies par la TIA et l'EIA. Ils parlent alors de catégorie 7.

4.2.2.3 Connecteurs UTP

Le câble UTP est généralement terminé par un connecteur RJ-45 spécifié ISO 8877. Ce connecteur est utilisé pour de nombreuses spécifications de couche physique, dont Ethernet. La norme TIA/EIA 568 décrit la correspondance des codes couleur des fils avec les broches (brochage) pour les câbles Ethernet.

La vidéo proposée dans la Figure 1 montre un câble UTP terminé par un connecteur RJ-45.

Comme l'illustre la Figure 2, le connecteur RJ-45 est le composant mâle qui pince les fils à l'extrémité du câble. La prise (ou le port) est le composant femelle d'un périphérique réseau, d'une prise murale ou fixée sur une cloison ou d'un tableau de connexions.

Chaque fois qu'un câblage en cuivre est raccordé, cela implique le risque de perte de signal et l'introduction de parasites dans le circuit de communication. S'il est mal raccordé, chaque câble constitue une source potentielle de dégradation des performances de la couche physique. Il est essentiel que tous les raccordements de supports en cuivre soient de qualité supérieure pour garantir des performances optimales avec les technologies réseau actuelles et futures.

La Figure 3 présente un exemple d'un câble UTP mal raccordé et d'un câble UTP correct.

4.2.2.4 Types de câble à paires torsadées non blindées

D'autres situations peuvent nécessiter des câbles UTP répondant à différentes conventions de câblage. Cela signifie que les fils du câble doivent être connectés dans des ordres différents avec diverses séries de broches des connecteurs RJ-45.

Les principaux types de câbles obtenus en utilisant des conventions de câblage spécifiques sont les suivants :

- **Câble Ethernet droit** : le type le plus courant de câbles réseau. Il est généralement utilisé pour connecter un hôte à un commutateur et un commutateur à un routeur.
- **Câble Ethernet croisé** : câble peu utilisé permettant de relier des périphériques similaires. Par exemple, pour connecter un commutateur à un commutateur, un hôte à un autre hôte ou un routeur à un routeur.
- **Câble de renversement** : câble propriétaire Cisco permettant d'établir une connexion avec un routeur ou un port de console de commutateur.

L'utilisation incorrecte d'un câble croisé ou droit entre des périphériques ne peut pas les endommager, mais la connectivité et la communication entre les périphériques deviennent alors impossibles. Il s'agit d'une erreur courante dans les TP et la vérification des connexions de périphériques doit constituer la première action de dépannage en cas de problème de connectivité.

La figure indique le type de câble UTP, les normes associées et l'application la plus courante de ces câbles. Elle identifie également les paires de fils selon les normes TIA 568A et TIA 568B.

4.2.2.5 Test de câbles à paires torsadées non blindées

Après l'installation, un contrôleur de câble UTP doit être utilisé pour vérifier les paramètres suivants :

- Schéma du câblage
- Longueur des câbles
- Perte de signal due à l'atténuation
- Interférences

Il est recommandé de vérifier minutieusement que toutes les conditions d'installation UTP sont respectées.

4.2.3 Fibre optique

4.2.3.1 Propriétés de la fibre optique

La fibre optique est de plus en plus utilisée pour interconnecter des périphériques réseau d'infrastructure. Elle permet la transmission de données sur de longues distances et à des débits plus élevés qu'avec les autres supports réseau.

La fibre optique est un fil en verre très pur (silice) transparent, à la fois flexible et très fin. Son diamètre n'est pas beaucoup plus grand que celui d'un cheveu humain. Les bits sont codés sur la fibre sous forme d'impulsions lumineuses. Le câble à fibre optique sert de guide d'ondes ou « tuyau lumineux » qui transmet la lumière entre les deux extrémités avec un minimum de perte de signal.

Pour mieux vous le représenter, imaginez un rouleau d'essuie-tout vide de plusieurs milliers de mètres de long, dont l'intérieur est recouvert d'un miroir. Un petit pointeur laser serait utilisé pour envoyer des signaux en code Morse à la vitesse de la lumière. Un câble à fibre optique utilise le même principe, mais son diamètre est inférieur et utilise des technologies sophistiquées d'émission et de réception des signaux lumineux.

Contrairement aux fils de cuivre, la fibre optique peut transmettre des signaux qui subissent moins d'atténuation et est entièrement insensible aux perturbations électromagnétiques et radioélectriques.

Actuellement, les câbles à fibre optique sont utilisés dans quatre domaines d'application :

- **Les réseaux d'entreprise** : la fibre est utilisée pour les applications de câblage du réseau fédérateur et pour relier les périphériques d'infrastructure.
- **Les réseaux FTTH et d'accès** : la technologie FTTH (fiber to the home ou fibre optique jusqu'au domicile) est utilisée pour fournir des services haut débit disponibles en permanence aux particuliers et aux petites entreprises. Les réseaux FTTH permettent un accès Internet haut débit abordable, le télétravail, la télémédecine et la vidéo à la demande.
- **Les réseaux longue distance** : les fournisseurs d'accès utilisent des réseaux terrestres longue distance à fibre optique pour connecter les pays et les villes. Ces réseaux vont généralement de quelques dizaines à quelques milliers de kilomètres et utilisent des systèmes proposant jusqu'à 10 Gbit/s.
- **Les réseaux sous-marins** : des câbles à fibre spéciaux sont utilisés pour fournir des solutions haut débit et haute capacité fiables, à l'épreuve des environnements sous-marins sur des distances à l'échelle d'un océan.

Nous nous intéressons principalement à l'utilisation de la fibre au sein de l'entreprise.

4.2.3.2 Éléments d'un câble en fibre optique

Bien que la fibre optique soit très fine, elle se compose de deux types de verre et d'une protection extérieure. Les différentes couches sont les suivantes :

- **Le cœur** : il se compose de verre pur et est en contact direct avec la lumière.
- **La gaine optique** : il s'agit d'une couche de verre qui entoure le cœur et fonctionne comme un miroir. Les impulsions lumineuses se propagent dans le cœur tandis que la

gaine les reflète. Ainsi, les impulsions lumineuses sont contenues dans le cœur de la fibre selon un phénomène appelé réflexion totale interne.

- **La protection** : il s'agit généralement d'une gaine en PVC qui protège le cœur et la gaine optique. Elle peut également contenir des matériaux de renforcement et un gainage (revêtement) destinés à protéger le verre des rayures et de l'humidité.

Bien qu'ils puissent être abimés s'ils sont pliés, le cœur et le gainage ont subi une modification de leur propriété au niveau moléculaire qui les rend très résistants. La qualité de la fibre optique est testée par un processus de fabrication rigoureux et doit résister à une traction d'au moins 100 000 livres par pouce carré. La fibre optique est assez résistante pour être manipulée lors de l'installation et du déploiement dans les conditions environnementales difficiles des réseaux du monde entier.

4.2.3.3 Types de fibre optique

Les impulsions lumineuses représentant les données transmises sous forme de bits sur le support sont générées par l'un des deux moyens suivants :

- Lasers
- Diodes électroluminescentes (LED/DEL)

Des dispositifs à semi-conducteur électronique appelés photodiodes détectent les impulsions lumineuses et les convertissent en tensions qui peuvent ensuite être reconstituées en trames de données.

Remarque : la lumière laser transmise via le câblage à fibre optique peut endommager l'œil humain. Ne regardez pas l'extrémité d'une fibre optique active.

Les câbles à fibre optique peuvent être classés en deux grands types :

- **La fibre optique monomode (SMF)** : son cœur présente un très faible diamètre et elle fait appel à la technologie coûteuse qu'est le laser pour envoyer un seul rayon lumineux. Elle est répandue dans les réseaux longue distance (plusieurs centaines de kilomètres) nécessaires pour les applications de téléphonie et de télévision par câble longue distance.
- **La fibre multimode (MMF)** : la taille de son cœur est supérieure et elle utilise des émetteurs LED pour envoyer des impulsions lumineuses. La lumière d'une LED entre dans la fibre multimode selon différents angles. Elle est généralement utilisée dans les réseaux locaux, car elle permet l'utilisation de LED, dont le coût est faible. Elle fournit une bande passante allant jusqu'à 10 Gbit/s sur des liaisons pouvant atteindre 550 mètres de long.

Les Figures 1 et 2 mettent en évidence les caractéristiques de la fibre multimode et monomode. L'une de ces différences est le niveau de dispersion. La dispersion correspond à la propagation d'une impulsion lumineuse au fil du temps. Plus la dispersion est importante, plus la perte de puissance du signal est importante.

4.2.3.4 Connecteurs de fibre réseau

Un connecteur fibre optique termine l'extrémité d'un câble à fibre optique. Divers connecteurs de ce type sont disponibles. Les principales différences entre les types de connecteurs sont les

dimensions et les méthodes de couplage mécanique. Généralement, les entreprises fixent chacune un type de connecteur à utiliser dans l'ensemble des installations, selon le matériel qu'elles emploient globalement, ou alors elles choisissent les connecteurs en fonction du type de fibre (un pour la fibre multimode et un pour la fibre multimode). En tenant compte de toutes les générations de connecteurs, environ 70 types de connecteur sont actuellement utilisés.

Comme l'illustre la Figure 1, les trois connecteurs fibre optique réseau les plus répandus sont les suivants :

- **Connecteur ST (Straight-Tip)** : connecteur à baïonnette d'ancienne version couramment utilisé avec la fibre monomode.
- **Connecteur SC (Subscriber Connector)** : parfois appelé connecteur carré ou connecteur standard. Il s'agit d'un connecteur largement utilisé dans les réseaux locaux et étendus qui fait appel à un mécanisme de clipsage permettant de vérifier l'insertion. Ce type de connecteur est utilisé avec la fibre optique multimode et monomode.
- **Connecteur LC (Lucent Connector)** : parfois appelé petit connecteur ou connecteur local, il est de plus en plus répandu en raison de sa petite taille. Il est utilisé avec la fibre monomode et prend également en charge la fibre multimode.

Remarque : d'autres connecteurs fibre optique tels que les connecteurs FC (Ferrule Connector) et SMA (Sub Miniature A) servent peu dans les déploiements de réseaux locaux et étendus. Certains connecteurs, tels que les connecteurs biconiques et D4 sont à présent obsolètes. Ils ne sont donc pas abordés dans ce chapitre.

La lumière pouvant uniquement voyager dans une direction par la fibre optique, deux fibres sont requises pour prendre en charge le fonctionnement bidirectionnel simultané. C'est pour cette raison que les câbles de brassage en fibre optique regroupent deux câbles à fibre optique raccordés par une paire de connecteurs monovoies standard. Certains connecteurs à fibres optiques acceptent à la fois les fibres de transmission et de réception. Ce sont des connecteurs bidirectionnels (voir figure 1).

Les câbles de brassage en fibre optique sont nécessaires pour interconnecter des périphériques d'infrastructure. Par exemple, la Figure 2 illustre différents câbles de brassage courants :

- Câble de brassage multimode SC-SC
- Câble de brassage monomode LC-LC
- Câble de brassage multimode ST-LC
- Câble de brassage monomode SC-ST

Les câbles à fibre optique doivent être protégés par un petit embout en plastique lorsqu'ils ne sont pas utilisés.

Notez également l'utilisation de couleurs permettant de différencier les câbles de brassage monomode et multimode. C'est la norme TIA 598 qui recommande l'utilisation d'une gaine jaune pour les câbles à fibre optique monomode et d'une gaine orange (ou bleue) pour les câbles à fibre multimode.

4.2.3.5 Test des fibres

Le raccordement et l'épissage des câbles en fibre optique exigent une formation et un matériel adapté. Le raccordement incorrect de supports en fibre optique diminue les distances de signalisation ou entraîne l'échec complet de la transmission.

Trois types courants d'erreurs de raccordement de fibre optique et d'épissage sont :

- **Mauvais alignement** : les supports en fibre optique ne sont pas alignés précisément lors de la jonction.
- **Écart à l'extrémité** : les supports ne se touchent pas complètement à l'épissure ou à la connexion.
- **Finition de l'extrémité** : les extrémités des supports ne sont pas bien polies ou de la poussière est présente au niveau du raccordement.

Un test sur site peut être effectué rapidement et facilement. Il suffit d'allumer une lampe de poche puissante à une extrémité de la fibre optique tout en observant l'autre extrémité. Si la lumière est visible, la fibre est capable de la transporter. Même si cela ne garantit pas les performances de la fibre, il s'agit d'un moyen rapide et économique de repérer une fibre cassée.

Il est conseillé d'utiliser un appareil de vérification tel que celui représenté dans la figure pour tester les câbles à fibre optique. Un réflectomètre optique (OTDR) permet de tester chaque segment de câble à fibre optique. Ce dispositif injecte une impulsion test de lumière dans le câble et mesure la rétrodiffusion et la réflexion de lumière détectées en fonction du temps. Le réflectomètre optique calcule la distance approximative à laquelle ces défauts sont détectés le long du câble.

4.2.3.6 Fibre ou cuivre

Les câbles à fibre optique présentent de nombreux avantages par rapport aux câbles en cuivre.

Les fibres utilisées dans les supports en fibre optique n'étant pas des conducteurs électriques, le support est à l'abri des interférences électromagnétiques et ne peut pas conduire de courant électrique indésirable suite à des problèmes de mise à la terre. Les fibres optiques étant fines et subissant une perte de signal relativement faible, elles peuvent fonctionner à des longueurs bien supérieures aux supports en cuivre, sans nécessiter de régénération des signaux. Certaines spécifications de couche physique en fibre optique autorisent des distances pouvant atteindre plusieurs kilomètres.

Les problèmes de mise en oeuvre de support en fibre optique comprennent :

- Un coût plus élevé (généralement) que les supports en cuivre pour la même distance (mais pour une capacité supérieure)
- Des compétences et matériel différents pour raccorder et épisser l'infrastructure de câblage
- Une manipulation plus délicate que les supports en cuivre

Actuellement, dans la plupart des environnements d'entreprise, la fibre optique est utilisée principalement comme câblage du réseau fédérateur pour les connexions point à point de trafic élevé entre des points de distribution de données et pour l'interconnexion des bâtiments des grands complexes. La fibre optique ne conduisant pas l'électricité et subissant une perte de signal inférieure, elle est bien adaptée à ces usages.

4.2.4 Supports sans fil

4.2.4.1 Propriétés des supports sans fil

Les supports sans fil transportent les signaux électromagnétiques qui représentent les bits des communications de données via des fréquences radio ou micro-ondes.

En tant que support réseau, la transmission sans fil n'est pas limitée aux conducteurs ou voies d'accès, comme les supports en cuivre et à fibre optique. Ce sont les supports sans fil qui offrent le plus d'options de mobilité. De plus, le nombre de périphériques sans fil augmente sans cesse. De ce fait, la technologie sans fil est devenue le support de choix pour les réseaux domestiques. Alors que les options de bande passante augmentent, le sans fil gagne rapidement du terrain dans les réseaux d'entreprise.

La figure illustre les différents symboles associés à la technologie sans fil.

Toutefois, le sans fil présente également quelques contraintes :

- **Zone de couverture** : les technologies de communication de données sans fil fonctionnent bien dans les environnements ouverts. Cependant, certains matériaux de construction utilisés dans les bâtiments et structures, ainsi que le terrain local, limitent la couverture effective.
- **Interférences** : la transmission sans fil est sensible aux interférences et peut être perturbée par des appareils aussi courants que les téléphones fixes sans fil, certains types d'éclairages fluorescents, les fours à micro-ondes et d'autres communications sans fil.
- **Sécurité** : la connexion à un réseau sans fil ne nécessite aucun accès physique à un support. Par conséquent, les périphériques et les utilisateurs non autorisés à accéder au réseau peuvent tout de même se connecter. La sécurité du réseau constitue donc un composant essentiel de l'administration des réseaux sans fil.

Bien que la technologie sans fil soit de plus en plus utilisée sur les ordinateurs de bureau, le cuivre et la fibre sont les supports de couche physique les plus répandus dans les déploiements réseau.

4.2.4.2 Types de support sans fil

L'IEEE et les normes de l'industrie des télécommunications en matière de communication de données sans fil couvrent à la fois les couches liaison de données et physique.

Trois normes de communications de données courantes s'appliquent aux supports sans fil :

- **Norme IEEE 802.11** : la technologie LAN sans fil (WLAN), plus communément appelée Wi-Fi, utilise un système avec gestion des conflits ou non déterministe et un processus d'accès au support CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance).
- **Norme IEEE 802.15** : la norme relative au réseau personnel sans fil (WPAN), couramment appelée Bluetooth, utilise un processus de jumelage de périphériques pour communiquer sur des distances de 1 à 100 mètres.

- **Norme IEEE 802.16** : la technologie d'accès couramment appelée WiMAX (Worldwide Interoperability for Microwave Access) utilise une topologie point-à-multipoint pour fournir un accès à large bande sans fil.

La figure présente certaines des différences qui existent entre les supports sans fil.

Remarque : d'autres technologies sans fil telles que les communications par satellite ou cellulaires peuvent également fournir une connectivité au réseau de données. Cependant, ces technologies sans fil ne sont pas traitées dans ce chapitre.

Dans chacun des exemples ci-dessus, des spécifications de couche physique sont appliquées à des domaines :

- Codage des données en signal radio
- Fréquence et puissance de transmission
- Besoins relatifs à la réception et au décodage des signaux
- Conception et mise en service des antennes

Remarque : Wi-Fi est une marque déposée de la de Wi-Fi Alliance. L'appellation Wi-Fi est utilisée sur des produits certifiés appartenant à des périphériques WLAN basés sur les normes IEEE 802.11.

4.2.4.3 LAN sans fil

Une mise en oeuvre courante de réseau de données sans fil est la possibilité pour des périphériques de se connecter sans fil via un réseau local. Un réseau local sans fil exige généralement les périphériques réseau suivants :

- **Point d'accès sans fil** : il concentre les signaux sans fil des utilisateurs et se connecte, en général via un câble en cuivre, à une infrastructure réseau en cuivre existante telle qu'Ethernet. Les routeurs sans fil pour particuliers et petites entreprises intègrent à la fois les fonctions d'un routeur, d'un commutateur et d'un point d'accès, comme illustré dans la figure.
- **Adaptateurs de carte réseau sans fil** : ils fournissent à chaque hôte du réseau la possibilité de communiquer sans fil.

Au fur et à mesure de la mise au point de cette technologie, un certain nombre de normes Ethernet WLAN ont émergé. L'acquisition de périphériques sans fil doit s'effectuer avec soin pour garantir la compatibilité et l'interopérabilité.

Les avantages des technologies de communication de données sans fil sont évidents, en particulier les économies sur le câblage coûteux des locaux et le côté pratique lié à la mobilité des hôtes. Cependant, les administrateurs réseau doivent mettre au point et appliquer des processus et politiques de sécurité stricts pour protéger les réseaux locaux sans fil contre tout accès non autorisé et endommagement.

4.2.4.4 Normes Wi-Fi 802.11

Les différentes normes 802.11 ont évolué au fil des années. Exemples de normes :

- **IEEE 802.11a** : fonctionne dans la bande de fréquences de 5 GHz et permet des débits allant jusqu'à 54 Mbit/s. Cette norme s'appliquant à des fréquences élevées, elle possède une zone de couverture plus petite et est moins efficace pour pénétrer des structures de bâtiments. Il n'y a pas d'interopérabilité entre les périphériques fonctionnant sous cette norme et les normes 802.11b et 802.11g décrites ci-dessous.
- **IEEE 802.11b** : fonctionne dans la bande de fréquences de 2,4 GHz et permet des débits allant jusqu'à 11 Mbit/s. Les périphériques mettant en oeuvre cette norme ont une portée plus longue et sont davantage capables de pénétrer les structures de bâtiments que les périphériques basés sur la norme 802.11a.
- **IEEE 802.11g :** fonctionne dans la bande de fréquences de 2,4 GHz et offre des débits allant jusqu'à 54 Mbit/s. Les périphériques mettant en oeuvre cette norme fonctionnent par conséquent aux mêmes portée et radiofréquence que la norme 802.11b mais avec la bande passante de la norme 802.11a.
- **IEEE 802.11n** : fonctionne dans les bandes de fréquences 2,4 GHz et 5 GHz. Les débits de données standard attendus vont de 150 Mbit/s à 600 Mbit/s sur une distance maximale de 70 mètres. Cette norme est rétrocompatible avec les périphériques 802.11a/b/g.
- **IEEE 802.11ac** : fonctionne dans la bande de fréquence de 5 GHz offrant des débits de données de 450 Mbit/s à 1,3 Gbit/s (1 300 Mbit/s). Cette norme est rétrocompatible avec les périphériques 802.11a/n.
- **IEEE 802.11ad** : également appelée « WiGig ». Cette norme utilise une solution Wi-Fi tribande sur les bandes de fréquences de 2,4 GHz, 5 GHz et 60 GHz et permet des débits théoriques jusqu'à 7 Gbit/s.

La figure illustre certaines de ces différences.

4.3.1 Objectif de la couche liaison de données

4.3.1.1 Couche liaison de données

La couche d'accès au réseau TCP/IP correspond dans le modèle OSI aux couches suivantes :

- Liaison de données (couche 2)
- Physique (couche 1)

Comme l'illustre la figure, la couche liaison de données est responsable de l'échange des trames entre les nœuds via un support réseau physique. Elle permet aux couches supérieures d'accéder aux supports et contrôle la manière dont les données sont placées et reçues sur les supports.

Remarque : la notation de couche 2 des périphériques réseau connectés à un support commun est appelée un nœud.

Plus précisément, la couche liaison de données assure ces deux services de base :

- Elle accepte les paquets de couche 3 et les encapsule dans des unités de données appelées des trames.

- Elle contrôle l'accès au support et détecte les erreurs.

La couche liaison de données sépare efficacement les transitions de support qui se produisent lorsque le paquet est transféré à partir des processus de communication des couches supérieures. La couche liaison de données reçoit des paquets provenant d'un protocole de couche supérieure et les achemine également vers un protocole de couche supérieure, ici IPv4 ou IPv6. Ce protocole de couche supérieure n'a pas besoin de savoir quel support de communication sera utilisé.

Remarque : dans ce chapitre, le terme « support » n'est pas lié à du contenu numérique ou multimédia tel que l'audio, l'image, la télévision et la vidéo. Il fait référence au matériel qui transporte les signaux de données, tels que les câbles en cuivre et à fibre optique.

4.3.1.2 Sous-couches liaison de données

La couche liaison de données se divise en fait en deux sous-couches :

- **Contrôle de liaison logique (LLC)** : cette sous-couche supérieure définit les processus logiciels qui fournissent des services aux protocoles de couche réseau. Elle place les informations dans la trame qui indique le protocole de couche réseau utilisé pour la trame. Ces informations permettent à plusieurs protocoles de couche 3 (par exemple, IPv4 et IPv6) d'utiliser la même interface réseau et les mêmes supports.
- **Contrôle d'accès au support (MAC)** : cette sous-couche inférieure définit les processus d'accès au support exécutés par le matériel. Elle assure l'adressage de couche liaison de données et la délimitation des données en fonction des exigences de signalisation physique du support et du type de protocole de couche liaison de données utilisé.

Diviser la couche liaison de données en sous-couches permet à un type de trame défini par la couche supérieure d'accéder à différents types de supports définis par la couche inférieure. Il en est ainsi avec de nombreuses technologies de réseau local, y compris Ethernet.

Cette figure illustre la division de la couche liaison de données en sous-couches LLC et MAC. La sous-couche LLC communique avec la couche réseau alors que la sous-couche MAC autorise différentes technologies d'accès au réseau. Par exemple, la sous-couche MAC communique avec la technologie de réseau local Ethernet pour envoyer et recevoir des trames via des câbles en cuivre ou à fibre optique. La sous-couche MAC communique également avec les technologies sans fil telles que le Wi-Fi et le Bluetooth pour envoyer et recevoir des trames sans fil.

4.3.1.3 Contrôle d'accès au support

Les protocoles de couche 2 spécifient l'encapsulation d'un paquet dans une trame et les techniques permettant de placer le paquet encapsulé sur chaque support et de le récupérer. La technique utilisée pour placer la trame sur les supports et la récupérer à partir des supports est dite méthode de contrôle d'accès au support.

Lorsque les paquets voyagent de l'hôte source à l'hôte de destination, ils traversent généralement différents réseaux physiques. Ces réseaux physiques peuvent être basés sur différents types de supports physiques tels que des câbles en cuivre, des câbles a fibre optique

et des supports sans fil constitués de signaux électromagnétiques, à fréquences radio ou hyperfréquences et des liaisons par satellite.

Les paquets ne sont pas en mesure d'accéder directement à ces différents supports. Le rôle de la couche liaison de données OSI est de préparer les paquets de couche réseau en vue de leur transmission et de contrôler l'accès aux supports physiques. Les méthodes de contrôle d'accès au support décrites par les protocoles de couche liaison de données définissent les processus qui permettent aux périphériques réseau d'accéder aux supports réseau et de transmettre des trames dans divers environnements réseau.

Sans la couche liaison de données, les protocoles de couche réseau (par exemple, IP) devraient prévoir d'établir une connexion à chaque type de support pouvant se trouver sur le chemin. En outre, le protocole IP devrait s'adapter à chaque développement d'une nouvelle technologie réseau ou d'un nouveau support. Cela freinerait l'innovation et le développement des protocoles et des supports réseau. C'est une des raisons majeures de l'approche en couches appliquée aux réseaux.

L'animation de la figure présente un exemple d'un ordinateur situé à Paris qui se connecte à un ordinateur portable au Japon. Bien que les deux hôtes communiquent en utilisant exclusivement le protocole IP, il est probable que de nombreux protocoles de couche liaison de données soient utilisés pour transmettre les paquets IP sur différents types de réseau locaux et étendus. Chaque transition effectuée au niveau d'un routeur peut nécessiter un protocole de couche liaison de données différent en vue du transport sur un nouveau support.

4.3.1.4 Accès aux supports

Différentes méthodes de contrôle d'accès au support peuvent être requises au cours d'une même communication. Chaque environnement réseau que les paquets rencontrent alors qu'ils voyagent d'un hôte local à un hôte distant peut présenter différentes caractéristiques. Par exemple, un réseau local Ethernet se compose de plusieurs hôtes qui sont en concurrence pour accéder au support réseau de façon ad hoc. Les liaisons série consistent uniquement en une connexion directe entre deux périphériques via lesquels les données circulent sous forme d'une suite organisée de bits.

Les interfaces de routeur encapsulent le paquet dans la trame appropriée et une méthode adéquate de contrôle d'accès au support est utilisée pour accéder à chaque liaison. Un échange de paquets de couche réseau peut impliquer de nombreuses transitions de support et de couche liaison de données. Au niveau de chaque tronçon le long du chemin, un routeur :

- Accepte une trame d'un support
- Désencapsule la trame
- Réencapsule le paquet dans une nouvelle trame
- Achemine la nouvelle trame appropriée jusqu'au support de ce segment du réseau physique

Le routeur présenté dans la figure comporte une interface Ethernet pour se connecter au réseau local et une interface série pour se connecter au réseau étendu. Pour traiter les trames, le routeur utilise des services de couche liaison de données afin de recevoir la trame d'un support, de désencapsuler cette trame dans l'unité de données de protocole de la couche 3, de réencapsuler l'unité de données de protocole dans une nouvelle trame et de placer la trame sur le support de la liaison suivante du réseau.

4.3.2 Structure de trame de couche 2

4.3.2.1 Formatage des données à transmettre

La couche liaison de données prépare un paquet pour le transport à travers les supports locaux en l'encapsulant avec un en-tête et un code de fin pour créer une trame. La description d'une trame est un élément clé de chaque protocole de couche liaison de données.

Pour fonctionner, les protocoles de couche liaison de données nécessitent des informations de contrôle. Les informations de contrôle répondent généralement aux questions suivantes :

- Quels nœuds sont en communication ?
- Quand la communication entre les nœuds individuels commence-t-elle et quand se termine-t-elle ?
- Quelles erreurs se sont produites lorsque les nœuds communiquaient ?
- Quels nœuds communiqueront ensuite ?

Contrairement aux autres unités de données de protocoles décrites dans ce cours, la trame de couche liaison de données comprend les éléments suivants :

- **Un en-tête** : il contient des informations de contrôle telles que l'adressage et est situé au début de l'unité de données de protocole.
- **Des données** : elles contiennent l'en-tête IP, l'en-tête de la couche transport et les données d'application.
- **La fin de trame** : elle contient des informations de contrôle pour la détection d'erreurs, ajoutées à la fin de l'unité.

Ces éléments de trame sont représentés sur la figure et sont décrits plus en détail dans la suite du cours.

4.3.2.2 Création d'une trame

Lorsque les données voyagent sur les supports, elles sont converties en un flux de bits, ou de 1 et de 0. Si un nœud reçoit de longs flux de bits, comment détermine-t-il où commence et où finit une trame, ou quels bits représentent l'adresse ?

Le verrouillage de trame divise le flux en regroupements déchiffrables, des informations de contrôle étant insérées dans l'en-tête et dans le code de fin en tant que valeurs situées dans différents champs. Ce format attribue aux signaux physiques une structure pouvant être reçue par les noeuds et décodée en paquets au niveau de la destination.

Comme l'illustre la figure, les types de champ de trame générique sont les suivants :

- **Indicateurs de début et de fin de trame** : ils sont utilisés par la sous-couche MAC pour identifier les limites de début et de fin de la trame.
- **Adressage** : utilisé par la sous-couche MAC pour identifier les nœuds source et de destination.
- **Type** : ce champ permet à la sous-couche LLC d'identifier le protocole de couche 3.
- **Contrôle** : ce champ permet d'identifier les services de contrôle de flux spécifiques.

- **Données** : ce champ contient les données utiles de la trame (c'est-à-dire l'en-tête de paquet, l'en-tête de segment et les données).
- **Détection d'erreur** : inclus après les données pour constituer la fin de trame, ces champs de trame sont utilisés pour la détection des erreurs.

Tous les protocoles n'incluent pas tous ces champs. Les normes d'un protocole de liaison de données spécifique définissent le format de trame réel.

Remarque : des exemples de formats de trames sont décrits à la fin de ce chapitre.

4.3.3 Normes de couche 2

4.3.3.1 Normes de couche liaison de données

Contrairement aux protocoles des couches supérieures de la suite TCP/IP, les protocoles de couche liaison de données ne sont généralement pas définis par des documents RFC (Request For Comments). Bien que le groupe IETF (Internet Engineering Task Force) maintienne les protocoles et les services fonctionnels de la suite de protocoles TCP/IP dans les couches supérieures, il ne définit pas les fonctions ni le fonctionnement de la couche d'accès réseau de ce modèle.

Les services et les spécifications de couche liaison de données sont définis par plusieurs normes reposant sur une variété de technologies et de supports auxquels sont appliqués les protocoles. Certaines de ces normes intègrent les services de couche 1 et de couche 2.

Les protocoles et services fonctionnels de la couche liaison de données sont décrits par :

- Les organismes d'ingénierie qui définissent les normes et protocoles publics et ouverts.
- Les sociétés du secteur des communications qui définissent et utilisent des protocoles propriétaires pour tirer parti de nouvelles avancées technologiques ou d'opportunités commerciales.

Les organismes d'ingénierie qui définissent des normes et des protocoles ouverts s'appliquant à la couche liaison de données incluent :

- Institute of Electrical and Electronics Engineers (IEEE)
- Union Internationale des Télécommunications (UIT)
- ISO (International Standards Organization)
- ANSI (American National Standards Institute)

Le tableau de la figure présente quelques organismes de normalisation et leurs principaux protocoles de la couche liaison de données.

4.4 Contrôle d'accès au support

4.4.1 Topologies

4.4.1.1 Contrôle d'accès au support

C'est la sous-couche de contrôle d'accès au support qui régit le placement des trames de données sur les supports.

Le contrôle d'accès au support est l'équivalent des règles de trafic régulant l'accès des véhicules à une autoroute. L'absence d'un contrôle d'accès au support serait comparable à des véhicules ignorant le trafic et accédant à la route sans se préoccuper des autres véhicules. Cependant, toutes les routes et tous les accès ne sont pas identiques. Un véhicule peut accéder à la route en se fondant dans la circulation, en attendant son tour à un stop ou en obéissant à des feux de circulation. Le conducteur suit des règles différentes selon chaque type d'accès à la circulation.

De même, il existe différentes manières de réguler le placement des trames sur les supports. Les protocoles opérant au niveau de la couche liaison de données définissent les règles d'accès aux différents supports. Certaines méthodes de contrôle d'accès au support utilisent des processus hautement contrôlés pour s'assurer que les trames sont placées sur le support en toute sécurité. Ces méthodes sont définies par des protocoles sophistiqués, qui nécessitent des mécanismes à l'origine d'une surcharge sur le réseau.

Parmi les différentes mises en œuvre des protocoles de couche liaison de données, il existe différentes méthodes de contrôle d'accès au support. Ces techniques de contrôle d'accès au support indiquent si et comment les noeuds partagent les supports.

La méthode de contrôle d'accès au support utilisée dépend des critères suivants :

- **Topologie** : comment la connexion établie entre les nœuds apparaît à la couche liaison de données.
- **Partage de support** : comment les nœuds partagent les supports. Le partage de supports peut être de type point à point comme dans les réseaux étendus, ou partagé comme dans les réseaux locaux.

4.4.1.2 Topologies physique et logique

La topologie d'un réseau constitue l'organisation ou la relation des périphériques réseau et les interconnexions existant entre eux. Les topologies LAN et WAN peuvent être présentées de deux manières :

- **Topologie physique** : désigne les connexions physiques et identifie la façon dont les périphériques finaux et les périphériques d'infrastructure tels que les routeurs, les commutateurs et les points d'accès sans fil sont interconnectés. Les topologies physiques sont généralement de type point-à-point ou en étoile. Voir la Figure 1.
- **Topologie logique** : désigne la manière dont un réseau transfère les trames d'un nœud à l'autre. Cette configuration est composée de connexions virtuelles entre les nœuds d'un réseau. Ces chemins de signaux logiques sont définis par les protocoles de couche liaison de données. La topologie logique des liaisons point à point est relativement simple tandis que les supports partagés proposent des méthodes de contrôle d'accès au support déterministes et non déterministes. Reportez-vous à la figure 2.

La couche liaison de données « voit » la topologie logique d'un réseau lorsqu'elle contrôle l'accès des données aux supports. C'est la topologie logique qui influence le type de trame réseau et de contrôle d'accès au support utilisé.

4.4.2 Topologies de réseau étendu

4.4.2.1 Topologies physiques de réseau étendu courantes

Les réseaux étendus sont généralement interconnectés selon les topologies physiques suivantes :

- **Point à point** : c'est la topologie la plus simple, composée d'une liaison permanente entre deux terminaux. Elle est donc très répandue.
- **Hub and Spoke** : version WAN de la topologie en étoile, dans laquelle un site central connecte entre eux les sites des filiales à l'aide de liaisons point à point.
- **Maillée** : cette topologie offre une haute disponibilité, mais nécessite que tous les systèmes finaux soient connectés entre eux. Les coûts d'administration et physiques peuvent donc être élevés. En essence, chaque liaison est une liaison point à point avec l'autre nœud. Il existe plusieurs variantes de cette topologie, notamment le maillage partiel qui consiste à relier uniquement certains périphériques finaux entre eux.

Les trois principales topologies physiques de réseau étendu sont représentées sur la figure.

4.4.2.2 Topologie physique point à point

Les topologies point-à-point physiques connectent directement deux nœuds comme illustré sur la figure.

Dans cette configuration, deux nœuds n'ont pas besoin de partager le support avec d'autres hôtes. En outre, le nœud n'a pas besoin de déterminer si une trame entrante est lui est destinée ou si elle est destinée à un autre nœud. Par conséquent, les protocoles de liaison de données logiques peuvent être très simples puisque toutes les trames sur le support peuvent uniquement transiter vers ou depuis les deux nœuds. Les trames sont placées sur le support par le noeud situé à une extrémité et retirées du support par celui situé à l'autre extrémité du circuit point à point.

Les protocoles de couche liaison de données pourraient fournir des processus plus sophistiqués de contrôle d'accès au support pour les topologies point à point logiques, mais ceci ne créerait qu'une surcharge de protocole inutile.

4.4.2.3 Topologie point à point logique

Les noeuds finaux communiquant dans un réseau point à point peuvent être physiquement connectés via des périphériques intermédiaires. Cependant, l'utilisation de périphériques physiques sur un réseau n'affecte pas la topologie logique.

Comme l'illustre la Figure 1, les nœuds source et de destination peuvent être indirectement connectés l'un à l'autre sur une certaine distance géographique. Dans certains cas, la connexion logique établie entre les noeuds forme un circuit nommé circuit virtuel. Un circuit virtuel est une connexion logique établie au sein d'un réseau entre deux périphériques réseau.

Les deux noeuds situés aux extrémités du circuit virtuel s'échangent les trames. Ceci se produit même si les trames sont dirigées via des périphériques intermédiaires. Les circuits virtuels sont d'importants composants de communication logiques qu'utilisent certaines technologies de couche 2.

La méthode d'accès au support qu'utilise le protocole de liaison de données est déterminée par la topologie point-à-point logique et non par la topologie physique. Cela signifie que la connexion point à point logique établie entre deux noeuds peut ne pas être nécessairement établie entre deux noeuds physiques à chaque extrémité d'une liaison physique.

La Figure 2 illustre les équipements physiques situés entre les deux routeurs.

4.4.2.4 Modes bidirectionnel simultané et bidirectionnel non simultané

La Figure 1 illustre une topologie point à point. Dans les réseaux point à point, les données peuvent circuler de deux manières :

- **Communication bidirectionnelle non simultanée** : les deux périphériques peuvent transmettre et recevoir des données sur les supports, mais pas simultanément. La norme Ethernet a choisi de traiter le cas d'un support non partagé bidirectionnel non simultané comme le cas d'un support partagé. La Figure 2 illustre la communication bidirectionnelle non simultanée.
- **Communication bidirectionnelle simultanée** : les deux périphériques peuvent simultanément transmettre et recevoir des données sur les supports. La couche liaison de données considère que le support est à tout moment disponible pour les deux noeuds en vue d'une transmission de données. De ce fait, aucune règle d'arbitrage des supports n'est nécessaire au niveau de la couche liaison de données. La Figure 3 illustre la communication bidirectionnelle simultan

4.4.3 Topologies LAN

4.4.3.1 Topologies LAN physiques

La topologie physique définit la façon dont les systèmes finaux sont physiquement interconnectés. Sur les réseaux locaux à supports partagés, les périphériques finaux peuvent être interconnectés selon les topologies physiques suivantes :

- **Topologie en étoile** : les périphériques finaux sont connectés à un périphérique intermédiaire central. Dans les premières topologies en étoile, les périphériques finaux étaient interconnectés à l'aide de concentrateurs. Actuellement, des commutateurs sont utilisés. La topologie en étoile est la topologie LAN physique la plus courante, surtout parce qu'elle est facile à installer, très évolutive (il est facile d'ajouter et de retirer des périphériques finaux) et facile à dépanner.
- **Étoile étendue ou hybride** : dans une topologie en étoile étendue, les périphériques intermédiaires centraux sont interconnectés avec d'autres topologies en étoile. Dans une topologie hybride, des réseaux en étoile peuvent être interconnectés via une topologie en bus.
- **Topologie en bus** : tous les systèmes finaux sont enchaînés entre eux et le réseau est terminé à chaque extrémité. Les périphériques d'infrastructure tels que les commutateurs ne sont pas nécessaires pour interconnecter les périphériques finaux.

Les topologies en bus étaient utilisées dans les réseaux Ethernet en raison de leur faible coût et de leur simplicité d'installation.

- **Topologie en anneau** : les systèmes finaux sont connectés à leur voisin respectif et forment ainsi un anneau. Contrairement à la topologie en bus, l'anneau n'a pas besoin d'être terminé. Les topologies en anneau étaient utilisées dans les réseaux FDDI (Fiber Distributed Data Interface). Ces réseaux utilisent un deuxième anneau pour la tolérance aux pannes ou l'amélioration des performances.

La figure illustre l'interconnexion des périphériques finaux sur les réseaux locaux.

4.4.3.2 Topologie logique des supports partagés

La topologie logique d'un réseau est étroitement liée au mécanisme utilisé pour gérer l'accès au réseau. Les méthodes d'accès fournissent les procédures permettant de gérer l'accès au réseau de sorte que toutes les stations de travail puissent accéder au réseau. Lorsque plusieurs entités partagent le même support, un mécanisme doit être mis en place pour contrôler l'accès à ce support. Les méthodes d'accès sont appliquées aux réseaux pour réguler l'accès aux supports.

Certaines topologies réseau partagent un support commun avec plusieurs noeuds. À tout moment, des périphériques peuvent tenter d'envoyer et de recevoir des données à l'aide des supports réseau. Il existe des règles qui régissent la manière dont ces périphériques partagent les supports.

Deux méthodes élémentaires de contrôle d'accès au support sont utilisées pour les supports partagés :

- **Accès avec gestion des conflits** : tous les nœuds sont en concurrence pour utiliser le support, mais savent comment réagir en cas de conflit. La Figure 1 illustre l'accès avec gestion des conflits.
- **Accès contrôlé** : chaque nœud peut utiliser le support à son tour. La Figure 2 illustre l'accès contrôlé.

Le protocole de couche liaison de données spécifie la méthode de contrôle d'accès au support qui équilibrera correctement le contrôle de trame, la protection de trame et la surcharge réseau.

4.4.3.3 Accès avec gestion des conflits

Lorsqu'une méthode non déterministe avec gestion des conflits est utilisée, un périphérique réseau peut tenter d'accéder au support chaque fois qu'il doit envoyer des données. Pour éviter que le chaos total ne règne sur les supports, ces méthodes utilisent un processus d'accès multiple avec écoute de porteuse (CSMA) pour d'abord détecter si le support véhicule un signal.

Si un signal de porteuse issu d'un autre noeud et circulant sur le support est détecté, alors un autre périphérique est en train de transmettre des données. Lorsque le périphérique qui tente de transmettre des données constate que le support est occupé, il attend et essaie de nouveau au bout d'un court laps de temps. Si aucun signal n'est détecté, le périphérique transmet ses données. Les réseaux Ethernet et sans fil utilisent un contrôle d'accès au support basé sur le conflit.

Il est possible que le processus CSMA échoue et que deux périphériques transmettent des données en même temps, créant ainsi une collision de données. Dans ce cas, les données envoyées par les deux périphériques sont corrompues et doivent être envoyées de nouveau.

Les méthodes de contrôle d'accès au support basé sur le conflit n'impliquent pas la surcharge provoquée par les méthodes d'accès contrôlé. Aucun mécanisme établissant quel périphérique en attente peut accéder au support n'est requis. Cependant, les systèmes d'accès basé sur le conflit évoluent mal lorsque les supports sont très sollicités. À mesure que l'utilisation des supports s'intensifie et que le nombre de noeuds augmente, il est de moins en moins probable que l'accès aux supports s'effectue sans collision de données. En outre, les mécanismes de récupération nécessaires pour résoudre les erreurs liées à ces collisions de données diminuent encore plus le débit.

Le processus CSMA est généralement mis en oeuvre conjointement avec une méthode de résolution des conflits de supports. Les deux méthodes les plus courantes sont :

- **Méthode CSMA/CD (Carrier sense multiple access with collision detection)** : le périphérique final établit si le support comporte un signal de données. Si aucun signal de données n'est détecté et donc que le support est libre, le périphérique transmet ses données. Si des signaux sont alors détectés indiquant qu'un autre périphérique était au même moment en train de transmettre des données, tous les périphériques arrêtent de transmettre leurs données et réessayent ultérieurement. Les formes traditionnelles d'Ethernet utilisent cette méthode.
- **Méthode CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)** : le périphérique final détermine si le support comporte un signal de données. Si le support est libre, le périphérique envoie une notification à travers le support pour indiquer son intention de l'utiliser. Dès qu'il reçoit une autorisation de transmission, le périphérique envoie les données. Cette méthode est utilisée par les technologies de réseau sans fil 802.11.

La figure illustre ce qui suit :

- Principe de fonctionnement des méthodes d'accès avec gestion des conflits
- Caractéristiques des méthodes d'accès avec gestion des conflits
- Exemples de méthodes d'accès avec gestion des conflits

4.4.3.4 Topologie d'accès multiple

Une topologie d'accès multiple permet à des nœuds de communiquer en utilisant le même support partagé. Les données uniquement issues d'un seul noeud peuvent être placées sur le support à tout moment. Chaque noeud voit toutes les trames qui se trouvent sur le support, mais seul le noeud auquel la trame est destinée en traite le contenu.

Lorsque de nombreux noeuds partagent un accès au support, une méthode de contrôle d'accès au support de liaison de données est nécessaire pour contrôler la transmission des données et réduire ainsi les collisions entre différents signaux.

Lancez l'animation pour savoir comment les noeuds accèdent aux supports dans une topologie d'accès multiple.

4.4.3.5 Accès contrôlé

Lorsque la méthode d'accès contrôlé est utilisée, les périphériques réseau accèdent tour à tour au support. Si un périphérique final n'a pas besoin d'accéder au support, le périphérique final suivant prend le relai. Ce processus est facilité par l'utilisation d'un jeton. Un périphérique final acquiert le jeton et place une trame sur le support. Aucun autre périphérique ne peut faire de même jusqu'à ce que la trame soit arrivée et ait été traitée par la destination, libérant ainsi le jeton.

Remarque : cette méthode est également appelée accès programmé ou déterministe.

Bien que la méthode d'accès contrôlé soit bien organisée et offre un débit prévisible, les méthodes déterministes peuvent être inefficaces car les périphériques doivent attendre leur tour pour pouvoir utiliser le support.

Voici quelques exemples d'accès contrôlé :

- Token Ring (IEEE 802.5)
- FDDI (Fiber Distributed Data Interface), interface basée sur le protocole de bus à jeton IEEE 802.4.

Remarque : les deux méthodes de contrôle d'accès au support sont considérées comme obsolètes.

La figure illustre ce qui suit :

- Principe de fonctionnement des méthodes d'accès contrôlé
- Caractéristiques des méthodes d'accès contrôlé
- Exemples de méthodes d'accès contrôlé

4.4.3.6 Topologie en anneau

Dans une topologie en anneau logique, chaque nœud reçoit une trame tour à tour. Si la trame n'est pas adressée au noeud, ce dernier la transmet au noeud suivant. Un anneau peut ainsi utiliser une technique de contrôle d'accès au support contrôlé appelée passage de jeton.

Les noeuds d'une topologie en anneau logique suppriment la trame de l'anneau, examinent l'adresse et font suivre la trame si elle n'est pas adressée à ce noeud. Dans un anneau, tous les nœuds situés autour de l'anneau (entre les nœuds source et de destination) examinent la trame.

Plusieurs techniques de contrôle d'accès au support peuvent être utilisées avec un anneau logique. Cela dépend du niveau de contrôle requis. Par exemple, une seule trame à la fois est généralement véhiculée par le support. Si aucune donnée n'est en cours de transmission, un signal (appelé jeton) peut être placé sur le support et un noeud ne peut placer une trame de données sur le support que s'il dispose du jeton.

N'oubliez pas que la couche liaison de données « voit » une topologie en anneau logique. La topologie de câblage physique réelle peut être une autre topologie.

Lancez l'animation pour savoir comment les noeuds accèdent aux supports dans une topologie en anneau logique.

4.4.4 Trame liaison de données

4.4.4.1 Trame

Même si de nombreux protocoles de couche liaison de données différents décrivent les trames de couche liaison de données, chaque type de trame comprend trois parties élémentaires :

- En-tête
- Données
- Code de fin

Tous les protocoles de couche liaison de données encapsulent l'unité de données de protocole de couche 3 dans le champ de données de la trame. Cependant, la structure de la trame et les champs contenus dans l'en-tête et le code de fin varient selon le protocole.

Le protocole de couche liaison de données décrit les fonctionnalités nécessaires au transport des paquets à travers différents supports. Ces fonctionnalités du protocole sont intégrées à l'encapsulation de la trame. Lorsque la trame arrive à destination et que le protocole de liaison de données la retire du support, les informations de trame sont lues et supprimées.

Il n'existe aucune structure de trame répondant aux besoins de tout le transport de données sur tous les types de supports. En fonction de l'environnement, la quantité d'informations de contrôle requises dans la trame varie selon les exigences du contrôle d'accès au support et de la topologie logique.

Comme l'illustre la Figure 1, un environnement fragile nécessite plus de contrôle. Au contraire, un environnement protégé (Figure 2) requiert moins de contrôles.

4.4.4.2 En-tête

L'en-tête de trame contient les informations de contrôle spécifiées par le protocole de couche liaison de données pour la topologie logique et les supports spécifiques utilisés.

Les informations de contrôle de trame sont propres à chaque type de protocole. Le protocole de couche 2 les utilise pour fournir les fonctionnalités demandées par l'environnement.

La figure représente les champs d'en-tête de trame Ethernet :

- **Champ du délimiteur de début de trame** : indique le début de la trame.
- **Champs d'adresse source et de destination** : ils indiquent les nœuds source et de destination sur les supports.
- **Champ de type** : indique le service de couche supérieure contenu dans la trame.

Différents protocoles de couche liaison de données peuvent utiliser d'autres champs que ceux mentionnés. Voici quelques autres exemples de champs de trame d'en-tête de protocole de couche 2 :

- **Champ de priorité/qualité du service** : indique un type particulier de service de communication pour le traitement.
- **Champ de contrôle de connexion logique** : permet d'établir une connexion logique entre des noeuds.

- **Champ de contrôle de liaison physique** : permet d'établir la liaison aux supports.
- **Champ de contrôle de flux** : permet de lancer et d'arrêter le trafic sur les supports.
- **Champ de contrôle d'encombrement** : indique l'encombrement sur les supports.

Le but et les fonctions des protocoles de couche liaison de données étant liés aux topologies et aux supports spécifiques, il est nécessaire d'examiner chaque protocole pour acquérir une compréhension complète de sa structure de trame. À mesure que les protocoles sont décrits dans ce cours, plus d'informations sur la structure de trame seront fournies.

4.4.4.3 Adresse de couche 2

La couche liaison de données assure l'adressage utilisé pour acheminer la trame à travers les supports locaux partagés. Au niveau de cette couche, les adresses de périphérique sont appelées adresses physiques. L'adressage de couche liaison de données est spécifié dans l'en-tête de trame et indique le noeud de destination de trame sur le réseau local. L'en-tête de la trame peut également contenir son adresse source.

Contrairement aux adresses logiques de couche 3, qui sont des adresses hiérarchiques, les adresses physiques n'indiquent pas le réseau sur lequel le périphérique se situe. Au contraire, l'adresse physique est une adresse unique spécifique du périphérique. Si le périphérique est déplacé vers un autre réseau ou sous-réseau, il opère encore avec la même adresse physique de couche 2.

Une adresse spécifique du périphérique et non hiérarchique ne peut pas être utilisée pour localiser un périphérique sur des réseaux de grande envergure ou sur Internet. Cela reviendrait à chercher une certaine maison dans le monde entier, en ne connaissant que la rue et le numéro de celle-ci. En revanche, l'adresse physique permet de localiser un périphérique dans une zone limitée. Pour cette raison, l'adresse de la couche liaison de données est utilisée uniquement pour l'acheminement local. Au niveau de cette couche, les adresses n'ont une signification que sur le réseau local. Comparons ce scénario à celui de la couche 3, où les adresses présentes dans l'en-tête de paquet sont acheminées de l'hôte source à l'hôte de destination quel que soit le nombre de tronçons réseau figurant sur le chemin.

Si les données doivent passer sur un autre segment du réseau, alors un périphérique intermédiaire tel qu'un routeur est requis. Le routeur doit accepter la trame en fonction de son adresse physique et la désencapsuler afin d'en examiner l'adresse hiérarchique, ou adresse IP. Grâce à l'adresse IP, le routeur peut déterminer l'emplacement réseau du périphérique de destination et le meilleur chemin pour l'atteindre. Une fois qu'il sait où transférer le paquet, le routeur crée une nouvelle trame pour le paquet, laquelle est envoyée sur le segment suivant en direction de sa destination finale.

La figure présente les exigences applicables aux adresses de couche 2 dans les topologies à accès multiple et point à point.

4.4.4.4 La fin de trame

Les protocoles de couche liaison de données ajoutent un code de fin à la fin de chaque trame. Ce code permet de déterminer si la trame est arrivée sans erreur. Ce processus est appelé la détection d'erreurs et s'effectue par le placement dans la fin de trame d'un résumé logique ou mathématique des bits qui constituent la trame. La détection d'erreurs est ajoutée à la couche liaison de données, car les signaux sur les supports peuvent être soumis à des interférences,

une distorsion ou une perte qui modifierait de manière significative les valeurs binaires qu'ils représentent.

Un nœud de transmission crée un résumé logique du contenu de la trame. Ce résumé est appelé valeur de contrôle par redondance cyclique (CRC). Cette valeur est placée dans le champ de séquence de contrôle de trame de la trame pour représenter le contenu de la trame.

Cliquez sur les champs FCS et Stop Frame de la figure pour afficher plus d'informations.

Lorsque la trame arrive au niveau du noeud de destination, le noeud de réception calcule son propre résumé logique (ou CRC) de la trame. Le noeud de réception compare les deux valeurs CRC. Si les deux valeurs sont les mêmes, la trame est considérée comme arrivée telle que transmise. Si la valeur CRC du champ de séquence de contrôle de trame diffère de la valeur CRC calculée au niveau du noeud de réception, la trame est ignorée.

Par conséquent, le champ de séquence de contrôle de trame permet de déterminer si des erreurs se sont produites lors de la transmission et de la réception de la trame. Le mécanisme de détection d'erreur mis en oeuvre par le champ de séquence de contrôle de trame détecte la plupart des erreurs survenant sur le support.

Il existe toujours un faible risque qu'une trame ayant un résultat CRC correct soit en fait endommagée. Des erreurs de bits peuvent s'annuler mutuellement lorsque la valeur CRC est calculée. Les protocoles de couche supérieure seraient alors requis pour détecter et corriger cette perte de données.

4.4.4.5 Trames LAN et WAN

Dans un réseau TCP/IP, tous les protocoles de couche 2 OSI fonctionnent avec le protocole IP sur la couche OSI 3. Cependant, le protocole de couche 2 utilisé dépend de la topologie logique du réseau et de la mise en œuvre de la couche physique. En raison du large éventail de supports physiques utilisés sur l'ensemble des topologies de réseaux, un nombre élevé de protocoles de couche 2 est utilisé.

Chaque protocole effectue un contrôle d'accès au support pour les topologies logiques de couche 2 spécifiées. Cela signifie que différents périphériques réseau peuvent opérer comme des noeuds fonctionnant au niveau de la couche liaison de données lorsqu'ils mettent en oeuvre ces protocoles. Ces périphériques incluent l'adaptateur réseau ou les cartes réseau des ordinateurs, ainsi que les interfaces des routeurs et les commutateurs de couche 2.

Le protocole de couche 2 utilisé pour une topologie réseau spécifique dépend de la technologie mettant en oeuvre cette topologie. La technologie dépend à son tour de la taille du réseau (définie par le nombre d'hôtes et l'étendue géographique) et des services à fournir sur le réseau.

Un réseau local fait généralement appel à une technologie de bande passante élevée capable de prendre en charge de nombreux hôtes. Cette technologie est économique en raison de l'étendue géographique relativement faible (un bâtiment ou un campus) des réseaux locaux et de leur densité élevée d'utilisateurs.

Cependant, il n'est généralement pas rentable d'utiliser une technologie de bande passante élevée dans le cas de réseaux étendus couvrant de grandes zones géographiques (par exemple,

une ou plusieurs villes). La capacité de la bande passante est généralement moindre en raison du coût des liaisons physiques longue distance et de la technologie utilisées pour transporter les signaux à travers ces étendues.

La différence de bande passante a normalement pour résultat l'utilisation de différents protocoles pour les réseaux locaux et les réseaux étendus.

Voici quelques protocoles courants de couche liaison de données :

- Ethernet
- PPP (Point-to-Point Protocol)
- 802.11 sans fil

D'autres protocoles sont abordés dans le cursus CCNA : HDLC (High-Level Data Link Control) et le relais de trames.

Cliquez sur Lecture pour voir des exemples de protocoles de couche 2.

4.4.4.6 Trame Ethernet

Ethernet

Ethernet est la technologie de réseau local prédominante. Ethernet est une famille de technologies réseau définies par les normes IEEE 802.2 et 802.3.

Les normes Ethernet définissent à la fois les protocoles de la couche 2 et les technologies de la couche 1. Ethernet est la technologie de réseau local la plus utilisée et prend en charge des bandes passantes de données de 10 Mbit/s, 100 Mbit/s, 1 Gbit/s (1 000 Mbit/s) ou 10 Gbit/s (10 000 Mbit/s).

Le format de trame de base et les sous-couches IEEE des couches OSI 1 et 2 restent cohérents quelle que soit la forme d'Ethernet. Cependant, les méthodes de détection et de placement des données sur les supports varient selon les mises en oeuvre.

Ethernet fournit un service non orienté connexion sans accusé de réception sur un support partagé en utilisant les méthodes CSMA/CD comme méthodes d'accès au support. Le support partagé nécessite que l'en-tête de trame Ethernet utilise une adresse de couche liaison de données pour identifier les nœuds source et de destination. Comme avec la plupart des protocoles de réseau local, cette adresse est nommée adresse MAC du noeud. Une adresse MAC Ethernet comporte 48 bits et est généralement représentée dans un format hexadécimal.

La figure présente les nombreux champs de la trame Ethernet. Au niveau de la couche liaison de données, la structure de trame est presque la même pour tous les débits Ethernet. Cependant, au niveau de la couche physique, les différentes versions d'Ethernet ne placent pas les bits de la même manière sur les supports. Ethernet est traité plus en détail dans le chapitre suivant.

4.4.4.7 Trame PPP

Protocole point à point

Le protocole PPP (Point-to-Point Protocol) est également un protocole de couche liaison de données. Il est utilisé pour acheminer des trames entre deux nœuds. Contrairement à de nombreux protocoles de couche liaison de données définis par des organismes d'ingénierie électrique, la norme PPP est définie par des RFC. Le protocole PPP a été développé en tant que protocole de réseau étendu et demeure le protocole de choix pour mettre en oeuvre de nombreux réseaux étendus série. Il peut être utilisé sur différents supports physiques, notamment les câbles à paires torsadées, la fibre optique ou la transmission par satellite, ainsi que pour les connexions virtuelles.

Le protocole PPP utilise une architecture multicouche. Pour prendre en compte les différents types de supports, le protocole PPP établit des connexions logiques, nommées sessions, entre deux noeuds. La session PPP masque au protocole PPP supérieur les supports physiques sous-jacents. Ces sessions fournissent également au protocole PPP une méthode permettant d'encapsuler plusieurs protocoles sur une liaison point à point. Chaque protocole encapsulé sur la liaison établit sa propre session PPP.

Le protocole PPP permet également aux deux noeuds de négocier des options au sein de la session PPP. Cela inclut l'authentification, la compression et les liaisons multiples (l'utilisation de plusieurs connexions physiques).

Reportez-vous à la figure pour connaître les champs de base d'une trame PPP.

4.4.4.8 Trame 802.11 sans fil

802.11 sans fil

La norme IEEE 802.11 utilise la même sous-couche LLC 802.2 et le même schéma d'adressage à 48 bits que les autres réseaux locaux 802. Cependant, il existe de nombreuses différences au niveau de la sous-couche MAC et de la couche physique. Un environnement sans fil nécessite une attention particulière. Il n'existe aucune connectivité physique définissable. De ce fait, les facteurs externes peuvent interférer avec le transfert des données et le contrôle de l'accès est difficile. Pour relever ces défis, les normes sans fil comportent des contrôles supplémentaires.

La norme IEEE 802.11 est généralement appelée Wi-Fi. Il s'agit d'un système avec gestion des conflits qui fait appel à un processus d'accès au support de type CSMA/CA. CSMA/CA spécifie une procédure d'interruption aléatoire pour tous les noeuds qui attendent de transmettre des données. Le risque de conflit de support se pose surtout juste après que le support devienne disponible. La mise en retrait des noeuds pendant une période aléatoire réduit considérablement les risques de collision de données.

Les réseaux 802.11 utilisent également les accusés de réception de liaison de données pour confirmer la bonne réception d'une trame. Si la station de travail d'envoi ne détecte pas la trame d'accusé de réception, car la trame de données d'origine ou l'accusé de réception n'a pas été reçu intact, la trame est retransmise. Cet accusé de réception explicite corrige les interférences et autres problèmes de transmission radio.

Les autres services pris en charge par les réseaux 802.11 sont l'authentification, l'association (connectivité à un périphérique sans fil) et la confidentialité (chiffrement).

Comme l'illustre la figure, une trame 802.11 contient les champs suivants :

- **Version de protocole** : version de la trame 802.11 utilisée
- **Type et sous-type** : identifient une des trois fonctions et sous-fonctions de la trame (contrôle, données et gestion)
- **Vers DS** : défini sur 1 bit dans les trames de données destinées au système de distribution (périphériques de la structure sans fil)
- **À partir de DS** : défini sur 1 bit dans les trames de données quittant le système de distribution
- **Fragments supplémentaires** : défini sur 1 bit pour les trames comportant un autre fragment
- **Réessayer** : défini sur 1 bit si la trame est une retransmission d'une trame antérieure
- **Gestion de l'alimentation**: défini sur 1 bit pour indiquer qu'un nœud sera en mode économie d'énergie
- **Données supplémentaires** : défini sur 1 bit pour indiquer à un nœud en mode économie d'énergie que d'autres trames sont mises en mémoire tampon pour ce nœud
- **WEP (Wired Equivalent Privacy)** : défini sur 1 bit si la trame contient des informations chiffrées WEP à des fins de sécurité
- **Ordre** : défini sur 1 bit dans une trame de type de données qui utilise une classe de services strictement ordonnée (pas de réorganisation nécessaire)
- **Durée/ID** : selon le type de trame, indique le temps (en microsecondes) nécessaire pour transmettre la trame ou l'identité d'association (AID, Association Identity) de la station de travail ayant transmis la trame
- **AD (adresse de destination)** : adresse MAC du nœud de destination final sur le réseau
- **AS (adresse source)** : adresse MAC du nœud qui a lancé la trame
- **AR (adresse du récepteur)** : adresse MAC qui identifie le périphérique sans fil constituant le destinataire immédiat de la trame
- **Numéro de fragment** : indique le numéro de chaque fragment d'une trame
- **Numéro d'ordre** : indique le numéro d'ordre attribué à la trame ; les trames retransmises sont identifiées par des numéros d'ordre dupliqués
- **AE (adresse de l'émetteur)** : adresse MAC qui identifie le périphérique sans fil ayant transmis la trame
- **Corps de trame** : contient les informations transportées ; généralement un paquet IP pour les trames de données
- **FCS (séquence de contrôle de trame)** : contient un contrôle par redondance cyclique (CRC) 32 bits de la trame

CHAPITRE 5: Ethernet

Objectif :

- Décrire le fonctionnement des sous-couches Ethernet
- Identifier les principaux champs de la trame Ethernet
- Décrire l'objectif et les caractéristiques de l'adresse MAC Ethernet
- Décrire l'objectif du protocole ARP
- Expliquer l'impact qu'ont les requêtes ARP sur le réseau et les performances des hôtes
- Expliquer les concepts de commutation de base
- Comparer les commutateurs à configuration fixe et modulaires
- Configurer un commutateur de couche 3

5.0 Ethernet

5.0.1 Introduction

5.0.1.1 Introduction

La couche physique OSI fournit un moyen de transporter sur le support réseau les bits constituant une trame de couche liaison de données.

Ethernet est désormais la technologie de réseau local prédominante dans le monde. Ethernet fonctionne au niveau de la couche liaison de données et de la couche physique. Les normes du protocole Ethernet définissent de nombreux aspects de la communication réseau dont le format et la taille des trames, la synchronisation et le codage. Lorsque des messages sont transmis entre hôtes sur un réseau Ethernet, ces derniers formatent les messages dans la structure de la trame spécifiée par les normes. Les trames sont également désignées par le terme PDU (Protocol Data Unit).

Puisqu'Ethernet est constitué de normes au niveau de ces couches inférieures, la référence au modèle OSI peut permettre de mieux comprendre le protocole. Le modèle OSI sépare les fonctionnalités d'adressage, de tramage et d'accès aux supports entre la couche liaison de données et les normes de la couche physique des supports. Les normes Ethernet définissent à la fois les protocoles de la couche 2 et les technologies de la couche 1. Bien que les spécifications Ethernet prennent en charge différents supports, bandes passantes et autres variantes de la couche 1 et de la couche 2, le format de trame et le schéma d'adressage de base sont les mêmes pour toutes les formes d'Ethernet.

Dans ce chapitre, nous nous intéresserons aux caractéristiques et au fonctionnement d'Ethernet en suivant son évolution depuis la technologie de communication de données, basée sur des supports partagés et sur la restriction de l'accès aux supports jusqu'à la technologie moderne de large bande haut débit, bidirectionnelle simultanée.

5.0.1.2 Exercice - Rejoignez mon réseau social !

Rejoignez mon réseau social !

La plupart de nos communications réseau prennent la forme de messages (SMS ou messages instantanés), d'un contact visuel, de publications sur des réseaux sociaux, etc.

Pour cet exercice, choisissez l'un des réseaux de communication que vous utilisez le plus :

- SMS ou messagerie instantanée
- Conférence audio/vidéo
- Envoi d'e-mails
- Jeux

Maintenant que vous avez sélectionné un moyen de communication réseau, répondez aux questions suivantes :

- Existe-t-il une procédure à suivre pour enregistrer d'autres personnes et vous-même afin de former un groupe de communications ?
- Comment prenez-vous contact avec la ou les personnes avec lesquelles vous souhaitez communiquer ?

- Comment limitez-vous vos conversations pour vous assurer qu'elles sont reçues uniquement par les utilisateurs avec lesquels vous souhaitez communiquer ?

Soyez prêt à expliquer en classe les réponses que vous avez notées.

5.1 Protocole Ethernet

5.1.1 Fonctionnement du protocole Ethernet

5.1.1.1 Sous-couches LLC et MAC Protocole Ethernet

Fonctionnement du protocole Ethernet

Ethernet est la technologie LAN la plus répandue aujourd'hui.

Ethernet fonctionne au niveau de la couche liaison de données et de la couche physique. Ethernet est une famille de technologies réseau définies par les normes IEEE 802.2 et 802.3. Ethernet prend en charge des bandes passantes de données de :

- 10 Mbit/s
- 100 Mbit/s
- 1 000 Mbit/s (1 Gbit/s)
- 10 000 Mbit/s (10 Gbit/s)
- 40 000 Mbit/s (40 Gbit/s)
- 100 000 Mbit/s (100 Gbit/s)

Comme illustré à la Figure 1, les normes Ethernet définissent à la fois les protocoles de la couche 2 et les technologies de la couche 1. Pour les protocoles de couche 2, tout comme pour chacune des normes IEEE 802, Ethernet s'appuie sur les deux sous-couches distinctes de la couche liaison de données pour fonctionner : les sous-couches LLC et MAC.

La sous-couche LLC

La sous-couche LLC Ethernet gère la communication entre les couches supérieures et les couches inférieures. Celle-ci a généralement lieu entre les logiciels et les matériels réseaux du périphérique. La sous-couche LLC extrait les données des protocoles réseau, en principe un paquet IPv4, et leur ajoute des informations de contrôle pour faciliter la transmission du paquet jusqu'au noeud de destination. Elle est utilisée pour communiquer avec les couches supérieures de l'application et pour faire passer le paquet aux couches inférieures en vue de son acheminement.

La mise en œuvre de la sous-couche LLC se fait au niveau logiciel et est indépendante du matériel. Dans un ordinateur, la sous-couche LLC est en quelque sorte le pilote de la carte réseau. Le pilote de la carte réseau est un logiciel qui interagit directement avec le matériel de la carte réseau pour transmettre les données entre la sous-couche MAC et les supports physiques.

5.1.1.2 Sous-couche MAC

La sous-couche MAC est la sous-couche inférieure de la couche liaison de données. Elle est mise en œuvre au niveau matériel, généralement sur la carte réseau de l'ordinateur. Les spécifications sont décrites par les normes IEEE 802.3. La Figure 2 présente la liste des normes Ethernet courantes de l'IEEE

Comme l'illustre la figure, la sous-couche MAC Ethernet a deux fonctions principales :

- Encapsulation des données
- Contrôle d'accès au support

Encapsulation des données

L'encapsulation des données consiste à assembler les trames avant de les transmettre et à les désassembler à leur réception. Lorsqu'elle assemble une trame, la couche MAC ajoute un en-tête et une fin à l'unité de données de protocole de la couche réseau.

Elle assure trois fonctions de base :

- **Délimitation des trames** : le processus de tramage fournit des délimiteurs importants utilisés pour identifier un groupe de bits qui composent une trame. Ce processus permet la synchronisation entre les noeuds de transmission et ceux de réception.
- **Adressage** : l'encapsulation fournit également un adressage pour la couche liaison de données. Chaque en-tête Ethernet ajouté à la trame contient l'adresse physique (MAC) qui permet de remettre celle-ci au nœud de destination.
- **Détection d'erreur** : chaque trame Ethernet contient une fin avec un contrôle de redondance cyclique (CRC, Cyclic Redundancy Check) du contenu des trames. Après réception d'une trame, le noeud récepteur crée un CRC pour le comparer à celui de la trame. Si ces deux calculs de CRC correspondent, cela signifie probablement que la trame a été reçue sans erreur.

L'utilisation de trames facilite la transmission des bits lors de leur placement sur le support et le regroupement des bits sur le noeud récepteur.

Contrôle d'accès au support

La deuxième fonction de la sous-couche MAC consiste à contrôler l'accès aux supports. Le contrôle d'accès au support gère le placement des trames sur les supports et leur suppression. Comme son nom l'indique, il contrôle l'accès aux supports. Cette sous-couche communique directement avec la couche physique.

La topologie logique sous-jacente d'Ethernet est un bus à accès multiple. Par conséquent, tous les nœuds (périphériques) d'un même segment de réseau doivent partager le support. Ethernet est une méthode réseau avec gestion des conflits. Rappelez-vous qu'une méthode avec gestion des conflits ou méthode non déterministe permet à tous les périphériques de transmettre des données à travers le support partagé chaque fois qu'il doit en envoyer. Cependant, comme lorsque deux personnes essaient de parler en même temps, si plusieurs périphériques essaient de transmettre des données simultanément sur un même support, ces données entrent en collision et deviennent corrompues, et donc inexploitables. C'est pourquoi la technologie

Ethernet offre une méthode de contrôle de la manière dont les nœuds partagent l'accès, par l'utilisation de la technologie CSMA (Carrier Sense Multiple Access).

5.1.1.3 Contrôle d'accès au support

Le processus CSMA détecte d'abord si le support transporte un signal. Si un signal de porteuse issu d'un autre noeud et circulant sur le support est détecté, alors un autre périphérique est en train de transmettre des données. Lorsque le périphérique qui tente de transmettre des données constate que le support est occupé, il attend et essaie de nouveau au bout d'un court laps de temps. Si aucun signal n'est détecté, le périphérique transmet ses données. Il est possible que le processus CSMA échoue et que deux périphériques transmettent des données en même temps. Ce scénario est nommé collision de données. Dans ce cas, les données envoyées par les deux périphériques sont endommagées et doivent être envoyées de nouveau.

Les méthodes de contrôle d'accès aux supports avec gestion des conflits n'ont pas besoin de suivre l'accès au support à tour de rôle. Par conséquent, elles ne surchargent pas le réseau comme les méthodes d'accès contrôlé. Cependant, les systèmes d'accès basé sur le conflit évoluent mal lorsque les supports sont très sollicités. À mesure que l'utilisation des supports s'intensifie et que le nombre de noeuds augmente, il est de moins en moins probable que l'accès aux supports s'effectue sans collision de données. En outre, les mécanismes de récupération nécessaires pour résoudre les erreurs liées à ces collisions de données diminuent encore plus le débit.

Comme l'illustre la figure, le processus CSMA est généralement mis en œuvre conjointement avec une méthode de résolution des conflits de support. Les deux méthodes les plus courantes sont :

CSMA/CD (CSMA/Collision Detection)

Avec la méthode CSMA/CD , le périphérique contrôle le support pour établir si celui-ci comporte un signal de données. Si aucun signal de données n'est détecté, à savoir si le support est libre, le périphérique transmet ses données. Si des signaux sont alors détectés, ce qui indique qu'un autre périphérique était en train de transmettre des données, tous les périphériques arrêtent de transmettre leurs données et réessayent ultérieurement. Les formes traditionnelles d'Ethernet ont été développées pour utiliser cette méthode.

L'intégration généralisée des technologies commutées dans les réseaux modernes a largement éliminé la nécessité de mettre en œuvre la méthode CSMA/CD dans les réseaux locaux. Actuellement, la quasi-totalité des connexions filaires entre les périphériques d'un réseau local sont des connexions bidirectionnelles simultanées. C'est-à-dire qu'un périphérique peut envoyer et recevoir des données simultanément. Par conséquent, même si les réseaux Ethernet actuels sont conçus avec la technologie CSMA/CD, avec les périphériques intermédiaires récents, aucune collision ne se produit et les processus CSMA/CD sont devenus inutiles.

Toutefois, les collisions doivent toujours être envisagées sur les connexions sans fil des environnements de réseau local. Les périphériques des réseaux locaux sans fil utilisent la méthode CSMA/CA (CSMA/Collision Avoidance).

CSMA/CA (CSMA/Collision Avoidance)

Avec la méthode CSMA/CA, le périphérique examine le support pour établir si celui-ci comporte un signal de données. Si le support est libre, le périphérique envoie une notification à travers le support pour indiquer son intention de l'utiliser. Le périphérique transmet alors ses données Cette méthode est utilisée par les technologies de réseau sans fil 802.11

5.1.1.4 Adresse MAC : identité Ethernet

Comme nous l'avons vu précédemment, la topologie logique sous-jacente d'Ethernet est un bus à accès multiple. Chaque périphérique réseau est connecté au même support partagé et tous les nœuds reçoivent toutes les trames transmises. La question est donc la suivante : si tous les périphériques reçoivent toutes les trames, comment chaque périphérique peut-il déterminer si elles lui sont destinées sans devoir passer par tout le processus de traitement et de désencapsulation pour accéder à l'adresse IP ? La question devient encore plus problématique dans les grands réseaux dont le volume de trafic est élevé et où un grand nombre de trames sont transférées.

Pour éviter la surcharge excessive liée au traitement de chaque trame, un identifiant unique appelé adresse MAC a été créé. Il permet d'identifier les nœuds source et de destination sur un réseau Ethernet. Quel que soit le type de réseau Ethernet utilisé, l'adressage MAC fournit une méthode d'identification des périphériques au niveau inférieur du modèle OSI. Vous vous souvenez sûrement que l'adressage MAC est ajouté dans l'unité de données de protocole de la couche 2. Une adresse MAC Ethernet est une valeur binaire de 48 bits constituée de 12 chiffres hexadécimaux (4 bits par chiffre hexadécimal).

Structure de l'adresse MAC

Les adresses MAC doivent être uniques au monde. La valeur de l'adresse MAC est un résultat direct des règles mises en application par l'IEEE auprès des revendeurs pour garantir l'attribution d'adresses uniques à chaque périphérique Ethernet, et ce, à l'échelle mondiale. Les règles établies par l'IEEE exigent de chaque revendeur de périphérique Ethernet qu'il s'enregistre auprès de l'IEEE. L'IEEE attribue au constructeur un code de 3 octets (24 bits) appelé OUI (Organizationally Unique Identifier).

L'IEEE demande aux constructeurs de respecter deux règles simples représentées sur la figure :

- Toutes les adresses MAC attribuées à une carte réseau ou à un autre périphérique Ethernet doivent utiliser, comme 3 premiers octets, l'identifiant OUI attribué au revendeur correspondant.

Toutes les adresses MAC qui ont le même identifiant OUI doivent recevoir une valeur unique (référence du revendeur ou numéro de série) dans les 3 derniers octets.

5.1.1.5 Traitement des trames

L'adresse MAC est souvent dite rémanente, car elle était au départ stockée dans la mémoire morte (ROM) de la carte réseau. Cela signifie que l'adresse est codée dans la puce de mémoire morte (ROM) définitivement, et qu'elle ne peut pas être modifiée à l'aide d'un logiciel.

Remarque : sur les systèmes d'exploitation et les cartes réseau des ordinateurs actuels, il est possible de modifier l'adresse MAC dans le logiciel. Cela peut s'avérer utile lorsque l'utilisateur tente d'accéder à un réseau qui base son filtre sur l'adresse rémanente, ce qui signifie que le contrôle du trafic en fonction de l'adresse MAC n'est plus aussi sécurisé.

Les adresses MAC sont attribuées à tous les périphériques susceptibles de devoir envoyer et/ou recevoir des données sur le réseau : postes de travail, serveurs, imprimantes, routeurs, etc. Tous les périphériques connectés à un réseau local Ethernet ont des interfaces dotées d'une adresse MAC. Les fabricants de matériel et de logiciels peuvent représenter l'adresse MAC dans des formats hexadécimaux différents. Les formats d'adresse peuvent être les suivants :

- 00-05-9A-3C-78-00
- 00:05:9A:3C:78:00
- 0005.9A3C.7800

Lorsque l'ordinateur démarre, la carte réseau commence par copier l'adresse MAC de la mémoire morte à la mémoire vive. Lorsqu'un périphérique transmet un message à un réseau Ethernet, il intègre des informations d'en-tête au paquet. Les informations d'en-tête contiennent l'adresse MAC source et de destination. Le périphérique source envoie les données sur le réseau.

Chaque carte réseau du réseau examine les informations au niveau de la sous-couche MAC pour voir si l'adresse MAC de destination indiquée dans la trame correspond à l'adresse MAC physique stockée dans la mémoire vive du périphérique. En l'absence de correspondance, la carte réseau ignore la trame. Lorsque la trame atteint la destination à laquelle l'adresse MAC de la carte réseau correspond à l'adresse MAC de destination de la trame, la carte réseau fait passer la trame à travers les couches OSI, où la désencapsulation a lieu.

5.1.2 Attributs de trame Ethernet

5.1.2.1 Encapsulation Ethernet

Depuis la création d'Ethernet en 1973, les normes se sont développées et spécifient désormais des versions plus rapides et plus flexibles. Cette capacité d'Ethernet de s'améliorer au fil du temps est l'une des raisons pour lesquelles il est devenu si populaire. Les versions précédentes d'Ethernet étaient relativement lentes, de l'ordre de 10 Mbit/s. Les versions d'Ethernet les plus récentes fonctionnent à 10 gigabits par seconde au minimum. La Figure 1 illustre l'évolution d'Ethernet au fil des versions.

Au niveau de la couche liaison de données, la structure de trame est presque la même pour tous les débits Ethernet. La structure de trame Ethernet ajoute des en-têtes et des codes de fin à l'unité de données de protocole de la couche 3 pour encapsuler le message envoyé.

L'en-tête et le code de fin Ethernet disposent tous les deux de plusieurs sections (ou champs) d'informations que le protocole Ethernet exploite. Chaque section de la trame est appelée un champ. Comme l'illustre la Figure 2, il existe deux types de tramage Ethernet :

- La norme Ethernet IEEE 802.3, qui a été mise à jour plusieurs fois pour inclure de nouvelles technologies

- La norme Ethernet créée par DIX qui est maintenant appelée Ethernet II

Les différences entre les deux types de tramage sont minimes. La différence principale entre les deux normes est l'ajout d'un délimiteur de début de trame (SFD) et le remplacement du champ Type en un champ Longueur pour la norme 802.3.

Ethernet II est le format de trame Ethernet utilisé par les réseaux TCP/IP.

5.1.2.2 Taille d'une trame Ethernet

Attributs de trame Ethernet

Les normes Ethernet II et IEEE 802.3 définissent une taille de trame minimale de 64 octets et maximale de 1 518 octets. Cela comprenait tous les octets du champ Adresse MAC de destination jusqu'au champ Séquence de contrôle de trame. Les champs Préambule et Délimiteur de début de trame n'étaient pas inclus dans la description de la taille d'une trame.

Toute trame inférieure à cette valeur est interprétée comme un fragment de collision ou une trame incomplète et est automatiquement rejetée par les périphériques récepteurs.

La norme IEEE 802.3ac, publiée en 1998, a fixé la taille de trame maximale autorisée à 1 522 octets. La taille de trame a évolué de manière à prendre en charge une technologie appelée réseau local virtuel (VLAN). Ces réseaux virtuels, créés dans un réseau commuté, font l'objet d'un autre chapitre du cours. En outre, de nombreuses technologies de qualité de service (QoS) utilisent le champ Priorité utilisateur pour mettre en œuvre différents niveaux de services, notamment la priorité au trafic voix. La figure illustre les champs contenus dans la balise VLAN 802.1Q.

Si la taille d'une trame transmise est inférieure à la taille minimale ou supérieure à la taille maximale, le périphérique récepteur abandonne la trame. Les trames abandonnées sont souvent le résultat de collisions ou d'autres signaux rejetés et donc considérées comme non valides.

Au niveau de la couche liaison de données, la structure de trame est presque identique. Au niveau de la couche physique, les différentes versions d'Ethernet proposent des méthodes différentes de détection et de placement des données sur les supports.

5.1.2.3 Initiation à la trame Ethernet

Les principaux champs de la trame Ethernet sont les suivants :

- **Champs Préambule et Délimiteur de début de trame** : les champs Préambule (7 octets) et Délimiteur de début de trame (SFD, également appelé le début de trame (1 octet)) servent à synchroniser les périphériques émetteurs et destinataires. Les huit premiers octets de la trame préparent les noeuds de réception à recevoir. Les quelques premiers octets indiquent essentiellement aux récepteurs de se préparer à recevoir une nouvelle trame.
- **Champ Adresse MAC de destination** : ce champ de 6 octets est l'identifiant du destinataire. Comme nous l'avons vu précédemment, cette adresse est utilisée par la couche 2 pour aider les périphériques à déterminer si une trame leur est adressée. L'adresse de la trame est comparée à l'adresse MAC du périphérique. Si les deux correspondent, le périphérique accepte la trame.

- **Champ Adresse MAC source** : ce champ de 6 octets identifie la carte réseau ou l'interface d'origine de la trame.
- **Champ Longueur** : pour les normes IEEE 802.3 antérieures à 1997, le champ Longueur définit la longueur exacte du champ de données de la trame. Cette longueur est ensuite utilisée dans la séquence de contrôle de trame, pour garantir la réception du message. Sinon, le rôle de ce champ est d'indiquer le protocole de couche supérieure présent. Si la valeur de deux octets est supérieure ou égale à l'hexadécimal 0x0600 ou au décimal 1 536, le contenu du champ Données est décodé selon le protocole EtherType indiqué. Par contre, si la valeur est égale ou inférieure à la valeur hexadécimale 0x05DC ou à 1 500, le champ Longueur est utilisé pour indiquer l'utilisation du format de trame IEEE 802.3. C'est ainsi que l'on distingue les trames Ethernet II et 802.3.
- **Champ Données** : ce champ de 46 à 1 500 octets contient les données encapsulées d'une couche supérieure, ce qui correspond à une unité de données de protocole générique de la couche 3 ou à un paquet IPv4 pour employer un terme plus courant. La longueur minimale de la trame est fixée à 64 octets. Si un paquet de petite taille est encapsulé, d'autres bits sont utilisés pour augmenter la trame et la ramener à sa taille minimale. Ces bits sont appelés champs de remplissage.
- **Champ Séquence de contrôle de trame** : le champ FCS (4 octets) permet de détecter les erreurs d'une trame. Il fait appel à un contrôle par redondance cyclique (CRC). Le périphérique d'envoi inclut les résultats d'un CRC dans le champ FCS de la trame. Le périphérique de réception reçoit la trame et génère un CRC pour détecter les erreurs. Si les calculs correspondent, aucune erreur ne se produit. Les calculs non rapprochés indiquent que les données ont changé et que la trame est abandonnée. Si les données sont modifiées, cela peut perturber les signaux électriques qui représentent les bits.

5.1.3 Fonctions MAC Ethernet

5.1.3.1 Adresses MAC et format hexadécimal

Fonctions MAC Ethernet

L'utilisation de l'adresse MAC est l'un des aspects les plus importants de la technologie de réseau local Ethernet. Les adresses MAC utilisent la numération hexadécimale.

Le mot hexadécimal est un adjectif parfois utilisé en tant que nom. Lorsqu'il est utilisé comme nom, il fait référence au système de numération hexadécimale. Ce type de numération permet de représenter facilement des valeurs binaires. Le système de numération décimale est en base dix, le système binaire en base deux et le système hexadécimal est en base seize.

Le système de numération en base seize utilise les chiffres 0 à 9 et les lettres A à F. La Figure 1 indique les équivalents décimaux et hexadécimaux des valeurs binaires de 0000 à 1111. Il est plus facile pour nous de représenter une valeur à l'aide d'un seul chiffre hexadécimal que de quatre bits binaires.

Sachant que 8 bits (un octet) est un regroupement binaire courant, la plage binaire de 00000000 à 11111111 correspond, dans le format hexadécimal, à la plage de 00 à FF. Les zéros de gauche sont toujours affichés pour compléter la représentation de 8 bits. Par exemple, la valeur binaire 0000 1010 correspond à 0A au format hexadécimal.

Remarque : il est important de distinguer les valeurs hexadécimales des valeurs décimales en ce qui concerne les caractères 0 à 9, comme l'indique la figure 1.

Représentation de valeurs hexadécimales

Le système hexadécimal est généralement représenté à l'écrit par la valeur concernée précédée par 0x (par exemple, 0x73) ou suivie de l'indice 16. Moins souvent, une valeur peut être suivie d'un H, par exemple 73H. Toutefois, dans la mesure où le texte sous forme d'exposant n'est pas reconnu dans les environnements de ligne de commande ou de programmation, la représentation technique hexadécimale est précédée d'un 0x. Par conséquent, les exemples ci-dessus doivent correspondre respectivement à 0x0A et 0x73.

Le format hexadécimal permet de représenter les adresses MAC Ethernet et les adresses IPv6.

Conversions hexadécimales

Les conversions numériques entre des valeurs décimales et hexadécimales sont très simples, bien que la division ou la multiplication par 16 ne soit pas toujours très commode. Lorsque de telles conversions sont nécessaires, il est habituellement plus simple de convertir la valeur décimale ou hexadécimale en valeur binaire, puis de convertir cette dernière en valeur décimale ou hexadécimale, selon le cas.

Avec un peu de pratique, il est possible de reconnaître les configurations binaires qui correspondent aux valeurs décimales et hexadécimales. La figure 2 illustre ces configurations pour des valeurs de 8 bits données.

5.1.3.2 Représentations des adresses MAC

Sur un hôte Windows, la commande **ipconfig /all** permet d'identifier l'adresse MAC d'un adaptateur Ethernet. Sur la Figure 1, notez que l'écran indique que l'adresse physique (MAC) de l'ordinateur est 00-18-DE-C7-F3-FB. Si vous avez accès à la ligne de commande, vous pouvez déterminer celle de votre propre ordinateur.

Selon le périphérique et le système d'exploitation, différentes représentations des adresses MAC s'afficheront, comme le montre la Figure 2. Les routeurs et les commutateurs Cisco utilisent la forme XXXX.XXXX.XXXX où X est un caractère hexadécimal.

5.1.3.3 Adresse MAC de monodiffusion

Avec Ethernet, des adresses MAC différentes sont utilisées pour la monodiffusion (unicast), la multidiffusion (multicast) et la diffusion (broadcast) sur la couche 2.

L'adresse MAC de monodiffusion est l'adresse unique utilisée lorsqu'une trame est envoyée à partir d'un seul périphérique émetteur, à un seul périphérique destinataire.

Dans l'exemple de la figure, un hôte avec l'adresse IP 192.168.1.5 (source) demande une page Web au serveur dont l'adresse IP est 192.168.1.200. Pour qu'un paquet de monodiffusion soit envoyé et reçu, une adresse IP de destination doit figurer dans l'en-tête du paquet IP. Une adresse MAC de destination correspondante doit également être présente dans l'en-tête de la trame Ethernet. Les adresses IP et MAC se combinent pour transmettre les données à un hôte de destination spécifique.

5.1.3.4 Adresse MAC de diffusion

Un paquet de diffusion contient une adresse IP de destination qui ne comporte que des uns (1) dans la partie hôte. Cette numérotation implique que tous les hôtes sur le réseau local (domaine de diffusion) recevront le paquet et le traiteront. De nombreux protocoles réseau, notamment DHCP et ARP utilisent des diffusions. La façon dont le protocole ARP utilise les diffusions pour mapper les adresses de la couche 2 et de la couche 3 est décrite plus loin dans ce chapitre.

Comme le montre la figure, l'adresse IP de diffusion d'un réseau requiert une adresse MAC de diffusion correspondante dans la trame Ethernet. Sur les réseaux Ethernet, l'adresse MAC de diffusion comporte 48 uns (1), représentés au format hexadécimal FF-FF-FF-FF-FF-FF.

5.1.3.5 Adresse MAC de multidiffusion

Les adresses de multidiffusion permettent à un périphérique source d'envoyer un paquet à un groupe de périphériques. Les périphériques qui font partie d'un groupe de multidiffusion se voient affecter une adresse IP de groupe de multidiffusion. La plage d'adresses de multidiffusion IPv4 s'étend de 224.0.0.0 à 239.255.255.255. Dans la mesure où les adresses de multidiffusion représentent un groupe d'adresses (parfois appelé groupe d'hôtes), elles ne peuvent s'utiliser que comme destination d'un paquet. La source doit toujours avoir une adresse monodiffusion.

Les adresses de multidiffusion sont notamment utilisées dans les jeux en ligne, où plusieurs joueurs sont connectés à distance au même jeu. L'enseignement à distance par visioconférence fait également appel aux adresses de multidiffusion. Plusieurs étudiants sont ainsi connectés au même cours.

Comme avec les adresses de monodiffusion et de diffusion, l'adresse IP multidiffusion nécessite une adresse MAC de multidiffusion correspondante pour remettre les trames sur un réseau local. L'adresse MAC de multidiffusion (utilisée conjointement avec le protocole IP) est une valeur spécifique qui commence par 01-00-5E au format hexadécimal. L'autre partie de l'adresse MAC de multidiffusion provient de la conversion des 23 bits inférieurs de l'adresse IP du groupe de multidiffusion en 6 caractères hexadécimaux.

L'adresse de multidiffusion en hexadécimal 01-00-5E-00-00-C8 représentée dans l'animation en est un exemple.

5.1.3.6 Travaux pratiques - Affichage des adresses MAC des périphériques réseau

Au cours de ce TP, vous aborderez les points suivants :

- Partie 1 : configuration de la topologie et initialisation des périphériques
- 2e partie : Configurer les périphériques et vérifier la connectivité
- 3e partie : Afficher, décrire et analyser les adresses MAC Ethernet

5.1.4 Adresses MAC et IP

5.1.4.1 Adresses MAC et IP

Adresses MAC et IP

Chaque périphérique hôte possède deux adresses principales :

- L'adresse physique (adresse MAC)
- L'adresse logique (adresse IP)

L'adresse MAC et l'adresse IP fonctionnent ensemble pour identifier un périphérique sur le réseau. L'utilisation de l'adresse MAC et de l'adresse IP pour localiser un ordinateur revient à utiliser le nom et l'adresse d'une personne pour lui envoyer une lettre.

En règle générale, une personne ne change pas de nom. En revanche, son adresse postale peut changer.

Comme le nom d'une personne, l'adresse MAC d'un hôte ne change pas ; elle est physiquement attribuée à la carte réseau de l'hôte et est appelée adresse physique. L'adresse physique reste la même, quel que soit l'emplacement de l'hôte.

L'adresse IP est similaire à l'adresse d'une personne. Cette adresse correspond à l'emplacement réel de l'hôte. Elle permet à une trame de déterminer sa destination. L'adresse IP, ou adresse réseau, est appelée adresse logique, car elle est attribuée de manière logique par un administrateur réseau en fonction du réseau local auquel l'hôte est connecté. La figure montre que la localisation d'une personne en fonction de son adresse « logique » suit une hiérarchie. Cliquez sur chaque groupe pour voir le filtrage de l'adresse.

L'adresse MAC physique et l'adresse IP logique sont toutes deux requises pour que l'ordinateur communique sur un réseau hiérarchique, tout comme le nom et l'adresse d'une personne le sont pour envoyer une lettre.

5.1.4.2 Connectivité de bout en bout, MAC et IP

Un périphérique source envoie un paquet en fonction d'une adresse IP. Les périphériques source se servent souvent du système de noms de domaine (DNS) pour déterminer l'adresse IP du périphérique de destination. Celui-ci associe l'adresse IP à un nom de domaine. Par exemple, www.cisco.com correspond à 209.165.200.225. Cette adresse IP permet d'envoyer le paquet vers l'emplacement réseau du périphérique de destination. C'est cette adresse IP que les routeurs utilisent pour déterminer le meilleur chemin vers la destination. Donc, pour résumer, l'adressage IP détermine le comportement de bout en bout d'un paquet IP.

Cependant, le long de chaque liaison d'un chemin, le paquet IP est encapsulé dans une trame propre à la technologie de liaison de données associée à cette liaison, par exemple Ethernet. Les périphériques finaux d'un réseau Ethernet ne se basent pas sur les adresses IP, mais sur les adresses MAC pour accepter et traiter les trames.

Sur les réseaux Ethernet, les adresses MAC servent à identifier, à un niveau inférieur, les hôtes source et de destination. Lorsqu'un hôte d'un réseau Ethernet communique, il envoie des

trames contenant sa propre adresse MAC comme source, et l'adresse MAC du destinataire comme destination. Tous les hôtes qui reçoivent la trame lisent l'adresse MAC de destination. Si et seulement si celle-ci correspond à l'adresse MAC configurée sur la carte réseau de l'hôte, celui-ci traite le message.

La Figure 1 montre comment un paquet de données contenant des informations d'adresse IP est encapsulé selon le tramage de couche liaison de données intégrant les adresses MAC.

La Figure 2 montre comment les trames sont encapsulées en fonction de la technologie de la liaison.

Comment les adresses IP des paquets IP d'un flux de données sont-elles associées aux adresses MAC de chaque liaison le long du chemin vers la destination ? Cette opération est effectuée selon un processus appelé protocole ARP.

5.1.4.3 Travaux pratiques – Utilisation de Wireshark pour examiner les trames Ethernet

Au cours de ce TP, vous aborderez les points suivants :

- 1re partie : Examiner les champs d'en-tête dans une trame Ethernet II
- 2e partie : Utiliser Wireshark pour capturer et analyser les trames Ethernet

5.1.4.4 Packet Tracer : identification des adresses MAC et IP

Cet exercice est optimisé pour l'affichage des PDU. Les périphériques sont déjà configurés. Vous recueillerez les informations sur les PDU en mode Simulation et répondrez à une série de questions sur les données recueillies.

5.2 Protocole ARP (Address Resolution Protocol)

5.2.1 ARP

5.2.1.1 Présentation du protocole ARP

Souvenez-vous que chaque nœud sur un réseau IP possède une adresse MAC et une adresse IP. Pour envoyer des données, le nœud doit utiliser ces deux adresses. Le nœud doit utiliser ses propres adresses MAC et IP dans les champs sources et doit fournir une adresse MAC et une adresse IP de destination. Bien que l'adresse IP de la destination soit fournie par une couche OSI supérieure, le nœud émetteur doit trouver un moyen d'obtenir l'adresse MAC de destination de la liaison Ethernet. Quel est l'objectif d'ARP ?

Le protocole ARP repose sur certains types de message de diffusion Ethernet et de message monodiffusion Ethernet, appelés requêtes ARP et réponses ARP.

Le protocole ARP assure deux fonctions de base :

- La résolution des adresses IPv4 en adresses MAC
- La tenue d'une table des mappages

Résolution des adresses IPv4 en adresses MAC

À chaque trame placée sur un support LAN doit correspondre une adresse MAC de destination. Quand un paquet est envoyé à la couche liaison de données pour être encapsulé dans une trame, le nœud consulte une table stockée dans sa mémoire pour connaître l'adresse de couche liaison de données qui est mappée à l'adresse IPv4 de destination. Cette table est appelée table ARP ou cache ARP. La table ARP est stockée dans la mémoire vive (RAM) du périphérique.

Chaque entrée, ou ligne, de la table ARP relie une adresse IP à une adresse MAC. La relation entre les deux valeurs s'appelle un mappage. Autrement dit, si vous choisissez une adresse IP dans la table, vous trouverez l'adresse MAC correspondante. La table ARP stocke temporairement (dans la mémoire cache) le mappage des périphériques du réseau local.

Pour lancer la procédure, un nœud émetteur tente de trouver l'adresse MAC associée à une adresse IPv4 de destination. Si ce mappage se trouve dans la table, le nœud utilise l'adresse MAC comme destination MAC dans la trame qui encapsule le paquet IPv4. La trame est ensuite codée sur le support réseau.

5.2.1.2 Fonctions ARP

Mise à jour de la table ARP

La table ARP est mise à jour de manière dynamique. Un périphérique dispose de deux méthodes pour obtenir des adresses MAC. La première consiste à surveiller le trafic sur le segment du réseau local. Quand un noeud reçoit des trames en provenance du support, il enregistre les adresses IP source et MAC dans la table ARP sous forme de mappage. Au fur et à mesure que les trames sont transmises sur le réseau, le périphérique remplit la table ARP de paires d'adresses.

L'envoi d'une requête ARP permet également d'obtenir une paire d'adresses, comme illustré sur la figure. Une requête ARP est une diffusion de couche 2 à tous les périphériques du réseau local Ethernet. La requête ARP contient l'adresse IP de l'hôte de destination et l'adresse MAC de diffusion, FFFF.FFFF.FFFF. Comme il s'agit d'une diffusion, tous les nœuds sur le réseau local Ethernet le reçoivent et regardent le contenu. Le nœud dont l'adresse IP correspond à l'adresse IP de la requête ARP répond. La réponse est une trame de monodiffusion contenant l'adresse MAC qui correspond à l'adresse IP de la requête. Cette réponse permet de créer une nouvelle entrée dans la table ARP du nœud émetteur.

Les entrées de la table MAC sont horodatées de la même façon que les entrées de la table MAC sur les commutateurs. Si le périphérique ne reçoit pas de trame d'un périphérique précis avant expiration de l'horodatage, l'entrée correspondant à ce périphérique précis est supprimée de la table ARP.

Des entrées statiques de mappage peuvent également être ajoutées dans une table ARP, mais ceci ne se produit que rarement. Les entrées statiques de la table ARP n'expirent pas avec le temps et elles doivent être supprimées manuellement.

5.2.1.3 Fonctionnement d'ARP

Création de la trame

Que fait un noeud lorsqu'il doit créer une trame et que le cache ARP ne contient pas la correspondance entre une adresse IP et l'adresse MAC de destination ? Il génère une requête ARP !

Quand le protocole ARP reçoit une requête de mappage entre une adresse IPv4 et une adresse MAC, il recherche le mappage stocké en mémoire cache dans sa table ARP. S'il ne trouve pas d'entrée, l'encapsulation du paquet IPv4 échoue, et les processus de la couche 2 informent le protocole ARP qu'un mappage est nécessaire. Les processus ARP envoient alors un paquet de requête ARP pour trouver l'adresse MAC du périphérique de destination sur le réseau local. Si le périphérique qui reçoit la requête possède l'adresse IP de destination, il répond à l'aide d'une réponse ARP. Une entrée est créée dans la table ARP. Les paquets à destination de cette adresse IPv4 peuvent à présent être encapsulés dans des trames.

Si aucun périphérique ne répond à la requête ARP, le paquet est abandonné car il est impossible de créer une trame. L'échec de l'encapsulation est signalé aux couches supérieures du périphérique. Dans le cas d'un périphérique intermédiaire, comme un routeur, les couches supérieures peuvent choisir de répondre à l'hôte source en générant une erreur dans un paquet ICMPv4.

Reportez-vous aux Figures 1 à 5 pour visualiser le processus utilisé pour obtenir l'adresse MAC du nœud sur le réseau local physique.

5.2.1.4 Rôle d'ARP dans les communications à distance

Toutes les trames doivent être remises à un noeud sur un segment du réseau local. Si l'hôte IPv4 de destination se trouve sur le réseau local, la trame utilise l'adresse MAC de ce périphérique comme adresse MAC de destination.

Si l'hôte IPv4 de destination ne se trouve pas sur le réseau local, le noeud source doit livrer la trame à l'interface du routeur qui sert de passerelle ou de tronçon suivant pour atteindre cette destination. Le noeud source utilise l'adresse MAC de la passerelle comme adresse de destination, pour les trames contenant un paquet IPv4 adressé à des hôtes situés sur d'autres réseaux.

L'adresse de passerelle de l'interface du routeur est stockée dans la configuration IPv4 des hôtes. Lorsqu'un hôte crée un paquet pour une destination, il compare l'adresse IP de destination à sa propre adresse IP pour déterminer si celles-ci se situent sur le même réseau de couche 3. Si l'hôte destinataire ne se situe pas sur le même réseau, l'hôte source fait appel au processus ARP pour déterminer l'adresse MAC de l'interface du routeur qui sert de passerelle.

Si l'entrée de la passerelle n'est pas dans la table, le processus ARP normal envoie une requête ARP pour retrouver l'adresse MAC associée à l'adresse IP de l'interface du routeur.

Reportez-vous aux Figures 1 à 5 pour visualiser le processus utilisé pour obtenir l'adresse MAC de la passerelle.

5.2.1.5 Suppression des entrées d'une table ARP

Pour chaque périphérique, un compteur de cache ARP supprime les entrées ARP qui n'ont pas été utilisées pendant un certain temps. Cette période varie en fonction des périphériques et des systèmes d'exploitation. Par exemple, certains systèmes d'exploitation Windows stockent les entrées de cache ARP pendant 2 minutes. Si l'entrée est de nouveau utilisée pendant ce temps, le compteur ARP de cette entrée est prolongé de 10 minutes.

Des commandes permettent aussi de supprimer manuellement les entrées de la table ARP totalement ou partiellement. Lorsqu'une entrée est supprimée, le processus d'envoi d'une requête ARP et de réception d'une réponse ARP doit être répété pour entrer le mappage dans la table ARP.

Chaque périphérique possède une commande propre au système d'exploitation permettant de supprimer le contenu du cache ARP. Ces commandes n'impliquent aucunement l'exécution du protocole ARP. Ils suppriment simplement les entrées de la table ARP. Le service ARP est intégré au protocole IPv4 et mis en oeuvre par le périphérique. Cette opération est transparente pour les utilisateurs et les applications des couches supérieures.

Comme l'illustre la figure, il est parfois nécessaire de supprimer une entrée de la table ARP.

5.2.1.6 Tables ARP sur les périphériques réseau

Sur un routeur Cisco, la commande **show ip arp** permet d'afficher la table ARP, comme illustré à la Figure 1.

Sur les ordinateurs exécutant Windows 7, c'est la commande **arp –a** qui affiche la table ARP, comme illustré à la Figure 2

5.2.1.7 Packet Tracer : examen de la table ARP

Cet exercice est optimisé pour l'affichage des PDU. Les périphériques sont déjà configurés. Vous recueillerez les informations sur les PDU en mode Simulation et répondrez à une série de questions sur les données recueillies.

Instructions de Packet Tracer - Analyse d'une table ARP

PKA de Packet Tracer - Analyse d'une table ARP

5.2.1.8 Travaux pratiques - Analyse d'ARP avec la CLI de Windows, la CLI d'IOS et Wireshark

Au cours de ce TP, vous aborderez les points suivants :

- 1re partie : Concevoir et configurer le réseau
- 2e partie : Utiliser la commande ARP de Windows
- 3e partie : Utiliser la commande show ARP d'IOS

- 4e partie : Utiliser Wireshark pour examiner les échanges ARP

Travaux pratiques - Analyse d'ARP avec la CLI de Windows, la CLI d'IOS et Wireshark

5.2.2 Problèmes liés au protocole ARP

5.2.2.1 Problèmes potentiels engendrés par ARP

a figure présente deux problèmes potentiels liés au protocole ARP.

Surcharge des supports

Comme les trames de diffusion, les requêtes ARP sont reçues et traitées par chaque périphérique du réseau local. Sur un réseau d'entreprise classique, ces diffusions auraient probablement une incidence minime sur les performances du réseau. Toutefois, si un grand nombre de périphériques sont mis sous tension et accèdent aux services du réseau au même moment, les performances du réseau peuvent s'en trouver momentanément réduites. Par exemple, si tous les participants d'une salle de travaux pratiques se connectent sur les ordinateurs et tentent d'accéder à Internet en même temps, cela peut engendrer des délais d'attente. En revanche, si les périphériques envoient les messages de diffusion ARP initiaux et disposent des adresses MAC nécessaires, l'impact sur le réseau sera minime.

Sécurité

Dans certains cas, l'utilisation du protocole ARP peut porter atteinte à la sécurité du réseau L'usurpation ARP, ou empoisonnement ARP, est une technique de piratage qui consiste à injecter un faux mappage d'adresse MAC dans un réseau en émettant de fausses réponses ARP. Si un pirate informatique usurpe l'adresse MAC d'un périphérique, les trames risquent d'être envoyées à la mauvaise destination.

La configuration manuelle d'associations ARP statiques est un moyen d'éviter l'usurpation ARP. Les adresses MAC autorisées peuvent être configurées sur certains périphériques du réseau pour limiter l'accès réseau aux seuls périphériques listés.

5.2.2.2 Limitation des problèmes engendrés par ARP

Les commutateurs récents permettent de limiter les problèmes de sécurité et de diffusion liés au protocole ARP. Les commutateurs Cisco prennent en charge plusieurs technologies de sécurité spécialement conçues pour réduire les problèmes Ethernet liés aux diffusions en général et à ARP en particulier.

Les commutateurs assurent la segmentation d'un réseau local et le divisent ainsi en domaines de collision distincts. Chaque port d'un commutateur représente un domaine de collision à part et fournit la bande passante totale du support jusqu'aux nœuds connectés sur ce port. Les commutateurs n'empêchent pas, par défaut, la propagation des diffusions aux périphériques connectés, mais ils isolent les communications Ethernet de monodiffusion de sorte qu'elles soient uniquement « entendues » par les périphériques source et de destination. Par conséquent, s'il existe de nombreuses requêtes ARP, chaque réponse ARP se fera uniquement entre deux périphériques.

Concernant les attaques de diffusion de différents types, auxquelles les réseaux Ethernet sont soumis, les ingénieurs réseau mettent en œuvre des technologies Cisco de sécurité des commutateurs, notamment des listes d'accès et des dispositifs de sécurité des ports spécialisés.

5.3 Commutateurs LAN

5.3.1 Commutation

5.3.1.1 Principes fondamentaux des ports de commutateur

Souvenez-vous que la topologie logique d'un réseau Ethernet est un bus à accès multiple dont les périphériques partagent tous l'accès au même support. Cette topologie logique détermine la manière dont les hôtes du réseau examinent et traitent les trames envoyées et reçues sur le réseau. Toutefois, la plupart des réseaux Ethernet actuels utilisent une topologie physique en étoile ou en étoile étendue. Cela signifie que sur la plupart des réseaux Ethernet, les périphériques finaux sont généralement connectés point-à-point à un commutateur de réseau local de couche 2.

Un commutateur de réseau local de couche 2 permet d'effectuer une commutation et un filtrage en se basant uniquement sur l'adresse MAC de la couche liaison de données (couche 2) du modèle OSI. Les commutateurs sont entièrement transparents pour les protocoles réseau et les applications utilisateur. Un commutateur de couche 2 génère une table d'adresses MAC qu'il utilise pour des décisions de transmission. Les commutateurs de couche 2 dépendent des routeurs pour transmettre les données entre les sous-réseaux IP indépendants.

5.3.1.2 Table d'adresses MAC du commutateur

Les commutateurs utilisent des adresses MAC pour orienter les communications réseau via leur matrice de commutation vers le port approprié et en direction du noeud de destination. La matrice de commutation désigne les circuits intégrés et les éléments de programmation associés qui permettent de contrôler les chemins de données par le biais du commutateur. Pour qu'un commutateur puisse connaître les ports à utiliser en vue de la transmission d'une trame de monodiffusion, il doit avant tout savoir quels noeuds existent sur chacun de ses ports.

Un commutateur détermine le mode de gestion des trames de données entrantes à l'aide d'une table d'adresses MAC. Il crée sa table d'adresses MAC en enregistrant celles des noeuds connectés à chacun de ses ports. Dès que l'adresse MAC d'un noeud spécifique d'un port particulier est enregistrée dans la table d'adresses, le commutateur peut alors envoyer le trafic destiné au noeud vers le port mappé à ce dernier pour les transmissions suivantes.

Lorsqu'un commutateur reçoit une trame de données entrantes et que l'adresse MAC de destination ne se trouve pas dans la table, il transmet la trame à l'ensemble des ports, à l'exception de celui sur lequel elle a été reçue. Dès que le noeud de destination répond, le commutateur enregistre l'adresse MAC de ce dernier dans la table d'adresses à partir du champ d'adresse source de la trame. Dans le cadre de réseaux dotés de plusieurs commutateurs interconnectés, les tables d'adresses MAC enregistrent plusieurs adresses MAC pour les ports chargés de relier les commutateurs qui permettent de voir au-delà du noeud. En règle générale, les ports de commutateur utilisés pour connecter entre eux deux commutateurs disposent de plusieurs adresses MAC enregistrées dans la table d'adresses MAC.

Pour mieux comprendre le processus, observez les étapes détaillées dans les Figures 1 à 6.

Ce processus se présente comme suit :

Étape 1. Le commutateur reçoit une trame de diffusion de PC1 sur le port 1.

Étape 2. Le commutateur ajoute l'adresse MAC source et le port de commutateur ayant reçu la trame dans la table d'adresses.

Étape 3. L'adresse de destination étant une diffusion, le commutateur envoie la trame sur tous les ports, sauf celui sur lequel il l'a reçue.

Étape 4. Le périphérique de destination réagit à la diffusion en envoyant une trame de monodiffusion à PC1.

Étape 5. Le commutateur enregistre, dans la table d'adresses, l'adresse MAC source de PC2 et le numéro du port du commutateur ayant reçu la trame. L'adresse de destination de la trame et le port qui lui est associé se trouvent dans la table d'adresses MAC.

Étape 6. Le commutateur peut alors transmettre les trames entre les périphériques source et de destination sans les diffuser partout, puisqu'il dispose des entrées qui identifient les ports associés dans la table d'adresses .

Remarque : la table d'adresses MAC est parfois appelée une table de mémoire associative (CAM). Même si le terme de table CAM est également utilisé, nous parlerons de la table d'adresses MAC dans le cadre de ce cours.

5.3.1.3 Paramètres bidirectionnels

Bien qu'ils soient transparents pour les protocoles réseau et les applications utilisateur, les commutateurs peuvent fonctionner dans différents modes qui peuvent avoir des effets positifs et négatifs lors du transfert des trames Ethernet sur un réseau. L'un des paramètres de base d'un commutateur est le paramètre bidirectionnel de chaque port connecté à chaque périphérique hôte. Les ports des commutateurs doivent être configurés de sorte à correspondre aux paramètres bidirectionnels du type de support. Deux types de paramètres bidirectionnels sont employés pour les communications sur les réseaux Ethernet : le mode bidirectionnel non simultané et le mode bidirectionnel simultané.

Mode bidirectionnel non simultané

La communication bidirectionnelle non simultanée repose sur un flux de données unidirectionnel où l'envoi et la réception des données n'ont pas lieu simultanément. Ceci s'apparente à la manière dont les talkies-walkies ou les radios bidirectionnelles fonctionnent puisqu'une seule personne est autorisée à parler à la fois. Si une personne prend la parole au même moment qu'une autre, il y a collision. C'est pourquoi la communication bidirectionnelle non simultanée met en oeuvre la technologie CSMA/CD afin de mieux réduire les risques de collision et les détecter dès qu'ils surviennent. Le temps d'attente qu'exigent en permanence les communications bidirectionnelles non simultanées pose des problèmes de performance puisque les données ne peuvent circuler que dans un sens à la fois. Les connexions bidirectionnelles non simultanées se rencontrent généralement dans des équipements anciens, tels que des concentrateurs. Les noeuds reliés aux concentrateurs qui partagent leur connexion

avec le port d'un commutateur doivent fonctionner en mode bidirectionnel non simultané, car les ordinateurs finaux doivent être capables de détecter des collisions. Les noeuds doivent opérer en mode bidirectionnel non simultané si la carte réseau ne peut être configurée pour des opérations bidirectionnelles simultanées. Dans ce cas, le port du commutateur fonctionne également par défaut en mode bidirectionnel non simultané. Du fait de ces restrictions, la communication bidirectionnelle simultanée a remplacé la communication bidirectionnelle non simultanée dans la plupart des équipements.

Mode bidirectionnel simultané

Dans le cadre de la communication bidirectionnelle simultanée, le flux de données est bidirectionnel, de sorte que les données peuvent être envoyées et reçues de manière simultanée. La prise en charge bidirectionnelle améliore les performances en réduisant le temps d'attente entre les transmissions. La majorité des cartes réseau Ethernet, Fast Ethernet et Gigabit Ethernet vendues à l'heure actuelle offrent des fonctions bidirectionnelles simultanées. En mode bidirectionnel simultané, le circuit de détection de collision est désactivé. Les trames transmises par les deux noeuds finaux connectés ne peuvent entrer en collision puisque ces derniers utilisent deux circuits distincts sur le câble réseau. Chaque connexion bidirectionnelle simultanée utilise un seul port. Les connexions bidirectionnelles simultanées nécessitent un commutateur qui prend en charge une connexion bidirectionnelle simultanée ou directe entre les deux noeuds qui eux-mêmes prennent individuellement en charge le mode bidirectionnel simultané. Les noeuds reliés directement à un port de commutateur dédié par l'entremise de cartes réseau prenant en charge le mode bidirectionnel simultané doivent être connectés à des ports de commutateur configurés pour fonctionner en mode bidirectionnel simultané.

La figure illustre les deux paramètres bidirectionnels disponibles dans les équipements réseau modernes.

Un commutateur Cisco Catalyst prend en charge trois paramètres bidirectionnels :

- L'option full configure le mode bidirectionnel simultané.
- L'option half configure le mode bidirectionnel non simultané.
- L'option auto configure la négociation automatique du mode bidirectionnel simultané. Avec l'auto-négociation activée, les deux ports communiquent entre eux pour convenir du meilleur mode opératoire.

Pour les ports Fast Ethernet et 10/100/1000, la valeur par défaut est auto. Pour les ports 100BASE-FX, l'option par défaut est full. Les ports 10/100/1000 fonctionnent soit en mode bidirectionnel non simultané, soit en mode bidirectionnel simultané lorsqu'ils sont définis à 10 ou 100 Mbit/s. Par contre, à 1000 Mbit/s, ils fonctionnent en mode bidirectionnel simultané.

5.3.1.4 Auto-MDIX

Outre le paramètre bidirectionnel approprié, il est également nécessaire que le type de câble adéquat soit défini pour chaque port. Les connexions entre des périphériques spécifiques, notamment entre deux commutateurs, un commutateur et un routeur, un commutateur et un hôte, et un routeur et un périphérique d'hôte nécessitaient au départ l'utilisation de types de câble spécifiques (croisés ou droits). Désormais, la plupart des commutateurs prennent en

charge la commande de configuration d'interface **mdix auto** dans l'interface de ligne de commande, qui active la fonction auto-MDIX.

Lorsque vous activez cette fonction, le commutateur détecte le type de câble requis pour les connexions Ethernet cuivre, puis configure les interfaces en conséquence. Vous devez donc opter pour un câble croisé ou un câble droit pour les connexions sur un port 10/100/1000 cuivre sur le commutateur, quel que soit le type de périphérique à l'autre extrémité de la connexion.

Par défaut, la fonction auto-MDIX est activée sur des commutateurs dotés de la version 12.2(18)SE (ou ultérieure) du logiciel Cisco IOS. Pour les versions comprises entre 12.1(14)EA1 et 12.2(18)SE de ce même logiciel, la fonction auto-MDIX est désactivée par défaut.

5.3.1.5 Méthodes de transmission de trames sur les commutateurs Cisco

Auparavant, les commutateurs faisaient appel aux méthodes de transmission pour la commutation des données entre des ports réseau :

- Stockage et retransmission (Store-and-Forward)
- Commutation Cut-through

La Figure 1 indique les différences entre ces deux méthodes.

Dans le cas de la commutation Store and Forward, lorsque le commutateur reçoit la trame, il stocke les données dans des mémoires tampons jusqu'à ce qu'il ait reçu l'intégralité de la trame. Au cours de ce processus de stockage, le commutateur recherche dans la trame des informations concernant sa destination. Dans le cadre de ce même processus, le commutateur procède à un contrôle d'erreur à l'aide du contrôle par redondance cyclique (CRC) du code de fin de la trame Ethernet.

Le contrôle par redondance cyclique (CRC) a recours à une formule mathématique fondée sur le nombre de bits (de uns) dans la trame afin de déterminer si la trame reçue possède une erreur. Une fois l'intégrité de la trame confirmée, celle-ci est transférée via le port approprié vers la destination. En cas d'erreur détectée au sein de la trame, le commutateur ignore la trame. L'abandon des trames avec erreurs réduit le volume de bande passante consommé par les données altérées. La commutation Store and Forward est nécessaire pour l'analyse de la qualité de service (QS) sur des réseaux convergés où la classification des trames pour la priorité du trafic est indispensable. Par exemple, les flux de données de voix sur IP doivent être prioritaires sur le trafic Web.

Sur la Figure 2, lancez l'animation pour afficher une démonstration du processus de stockage et retransmission. Cette méthode est actuellement la seule employée sur les modèles actuels de commutateurs Cisco Catalyst.

5.3.1.6 Commutation cut-through

Dans le cas de la commutation cut-through, le commutateur agit sur les données à mesure qu'il les reçoit, même si la transmission n'est pas terminée. Le commutateur met une quantité

juste suffisante de la trame en tampon afin de lire l'adresse MAC de destination et déterminer ainsi le port auquel les données sont à transmettre. L'adresse MAC de destination est située dans les six premiers octets de la trame à la suite du préambule. Le commutateur recherche l'adresse MAC de destination dans sa table de commutation, détermine le port d'interface de sortie et transmet la trame vers sa destination via le port de commutateur désigné. Le commutateur ne procède à aucun contrôle d'erreur dans la trame. La commutation cut-through est bien plus rapide que la commutation Store and Forward, puisque le commutateur n'a ni à attendre que la trame soit entièrement mise en mémoire tampon, ni besoin de réaliser un contrôle d'erreur. En revanche, du fait de l'absence d'un contrôle d'erreur, elle transmet les trames endommagées sur le réseau. Les trames qui ont été altérées consomment de la bande passante au cours de leur transmission. La carte de réseau de destination ignore ces trames au bout du compte.

Lancez l'animation pour afficher une démonstration du processus de commutation Cut-through.

Il existe deux variantes de la commutation cut-through :

- **Commutation Fast-Forward** : ce mode de commutation offre le niveau de latence le plus faible. La commutation Fast-Forward transmet un paquet immédiatement après la lecture de l'adresse de destination. Du fait que le mode de commutation Fast-Forward entame la transmission avant la réception du paquet tout entier, il peut arriver que des paquets relayés comportent des erreurs. Cette situation est occasionnelle et la carte réseau de destination ignore le paquet défectueux lors de sa réception. En mode Fast-Forward, la latence est mesurée à partir du premier bit reçu jusqu'au premier bit transmis. La commutation Fast-Forward est la méthode de commutation cut-through classique.

- **Commutation Fragment-Free** : dans ce mode de commutation, le commutateur stocke les 64 premiers octets de la trame avant la transmission. La commutation Fragment-Free peut être considérée comme un compromis entre la commutation Stockage et retransmission et la commutation Fast-Forward. La raison pour laquelle la commutation Fragment-Free stocke uniquement les 64 premiers octets de la trame est que la plupart des erreurs et des collisions sur le réseau surviennent pendant ces 64 premiers octets. La commutation Fragment-Free tente d'améliorer la commutation Cut-through en procédant à un contrôle d'erreur partiel sur les 64 premiers octets de la trame afin de s'assurer qu'aucune collision ne s'est produite lors de la transmission de la trame. La commutation Fragment-Free offre un compromis entre la latence élevée et la forte intégrité de la commutation Stockage et retransmission d'une part, et la faible latence et l'intégrité réduite de la commutation Cut-through d'autre part.

La figure présente un exemple de commutation Cut-through.

Certains commutateurs sont configurés pour une commutation cut-through par port. Une fois le seuil d'erreurs défini par l'utilisateur atteint, ils passent automatiquement en mode Store and Forward. Lorsque le nombre d'erreurs est inférieur au seuil défini, le port revient automatiquement en mode de commutation cut-through.

5.3.1.7 Exercice : méthodes de transferts de trames

Exercice

5.3.1.8 Mise en mémoire tampon sur les commutateurs

Comme expliqué ci-dessus, le commutateur analyse une partie ou l'intégralité de chaque paquet avant de le transmettre à l'hôte de destination. Un commutateur Ethernet peut utiliser une technique de mise en mémoire tampon pour stocker des trames avant de les transmettre. La mise en mémoire tampon peut également être une solution lorsque le port de destination est saturé suite à un encombrement et que le commutateur stocke la trame jusqu'à ce qu'il puisse la transmettre.

Comme l'illustre la figure, il existe deux méthodes de mise en mémoire tampon : la mise en mémoire tampon axée sur les ports et la mise en mémoire tampon partagée.

Mise en mémoire tampon axée sur les ports

Dans le cas de la mise en mémoire tampon axée sur les ports, les trames sont stockées dans des files d'attente liées à des ports entrants et sortants spécifiques. Une trame est transmise au port sortant uniquement si toutes les trames qui la précèdent dans la file d'attente ont été correctement transmises. Une seule trame peut retarder la transmission de toutes les trames en mémoire si un port de destination est saturé. Ce retard se produit, même si les autres trames peuvent être transmises à des ports de destination libres.

Mise en mémoire tampon partagée

La mise en mémoire tampon partagée stocke toutes les trames dans une mémoire tampon commune à tous les ports du commutateur. La capacité de mémoire tampon nécessaire à un port est allouée dynamiquement. Les trames de la mémoire tampon sont liées de manière dynamique au port de destination, ce qui permet de recevoir le paquet sur un port et de le transmettre sur un autre, sans avoir à le déplacer vers une autre file d'attente.

Le commutateur tient à jour une carte de liaisons entre une trame et un port, indiquant l'emplacement vers lequel un paquet doit être acheminé. Cette carte est effacée dès que la trame a été transmise correctement. Le nombre de trames stockées dans la mémoire tampon est limité par la taille totale de cette dernière, mais ne se limite pas à un seul tampon du port, ce qui permet de transmettre de plus grandes trames en en supprimant un minimum. Cela est particulièrement important pour la commutation asymétrique. La commutation asymétrique permet l'utilisation de différents débits de données sur différents ports. Il est ainsi possible d'attribuer davantage de bande passante à certains ports, tels qu'un port connecté à un serveur.

5.3.1.9 Exercice : commutation

Exercice

5.3.1.10 Travaux pratiques - Affichage de la table d'adresses MAC du commutateur

Au cours de ce TP, vous aborderez les points suivants :

- 1re partie : Concevoir et configurer le réseau
- 2e partie : Analyser la table d'adresses MAC du commutateur

Travaux pratiques - Utiliser l'interface en ligne de commande d'IOS avec les tables d'adresses MAC du commutateur

5.3.2 Fixe ou modulaire

5.3.2.1 Configuration fixe et configuration modulaire

Lors de la sélection d'un commutateur, il est important de comprendre les caractéristiques essentielles des options de commutation disponibles. Il est notamment nécessaire de déterminer si des fonctionnalités telles que PoE (Power over Ethernet) sont nécessaires et de définir le débit de transfert préféré.

Comme l'illustre la Figure 1, la technologie PoE permet à un commutateur de fournir une alimentation à des périphériques tels que des téléphones IP et certains points d'accès sans fil, par le biais du câblage Ethernet existant. Cela augmente la flexibilité d'installation.

Le débit de transfert définit les capacités de traitement d'un commutateur en mesurant la quantité de données pouvant être traitées chaque seconde par le commutateur. Les gammes de produits de commutateur sont classées par débits de transfert. Les commutateurs de couche d'entrée fournissent des débits de transfert inférieurs à ceux des couches d'entreprise. Il existe d'autres critères tels que la capacité d'empilage du périphérique, l'épaisseur du commutateur (exprimée en unités de rack) et la densité des ports, c'est-à-dire le nombre de ports disponibles sur un seul commutateur. La densité des ports d'un appareil peut varier selon qu'il présente une configuration fixe ou modulaire.

Ces options caractérisent parfois le type de commutateur.

Commutateurs de configuration fixe

Les commutateurs de configuration fixe disposent, comme leur nom l'indique, d'une configuration fixe. Cela signifie que vous ne pouvez pas ajouter de fonctionnalités ni d'options supplémentaires au commutateur par rapport à celles d'origine. Le modèle spécifique que vous achetez détermine les fonctionnalités et les options disponibles. Si vous achetez un commutateur fixe gigabit à 24 ports, vous ne pouvez pas rajouter des ports en cas de besoin. En général, il existe différents choix de configuration qui varient selon le nombre et les types de ports inclus.

Commutateurs modulaires

Les commutateurs modulaires offrent davantage de souplesse dans leur configuration. Les commutateurs modulaires sont en principe livrés avec des châssis de différentes tailles, ce qui permet d'installer plusieurs cartes d'interface modulaires. Ces cartes d'interface contiennent les ports. La carte d'interface s'insère dans le châssis du commutateur, comme les cartes d'extension dans un ordinateur. Plus le châssis est grand, plus il peut contenir de modules. Comme la figure l'indique, vous avez le choix entre plusieurs tailles de châssis. Si vous avez acheté un commutateur modulaire avec une carte d'interface à 24 ports, vous pouvez aisément ajouter une carte d'interface à 24 ports supplémentaire, afin d'obtenir un nombre total de 48 ports.

La Figure 2 présente des exemples de commutateurs à configuration fixe, modulaire et empilable

5.3.2.2 Modules destinés aux logements des commutateurs Cisco

Les gammes de commutateurs Cisco sont fréquemment déployées dans le monde entier en raison des options supplémentaires flexibles qu'elles offrent. Cisco IOS propose non seulement l'ensemble de fonctionnalités le plus complet par rapport à tous les autres systèmes d'exploitation réseau, mais il est également adapté aux besoins de chaque périphérique réseau Cisco, en particulier aux commutateurs.

Pour illustrer les options disponibles, qui sont bien trop nombreuses pour être répertoriées ici, nous allons nous contenter de celles des commutateurs Catalyst 3560. Les commutateurs Catalyst 3560 sont équipés de ports SFP (Small Form-Factor Pluggable) qui prennent en charge différents modules émetteurs-récepteurs SFP. Voici la liste des modules SFP pris en charge sur un ou plusieurs types de commutateurs 3560 :

Modules SFP FastEthernet

- 100BASE-FX (fibre optique multimode (MMF)) pour 2 kilomètres (km)
- 100BASE-LX10 (fibre optique monomode (SMF)) pour 2 km
- 100BASE-BX10 (SMF) pour 10 km
- 100BASE-EX (SMF) pour 40 km
- 100BASE-ZX (SMF) pour 80 km

Modules SFP Gigabit Ethernet

- 1000BASE-SX 50/62,5 µm (MMF) jusqu'à 550/220 m
- 1000BASE-LX/LH (SMF/MMF) jusqu'à 10/0,550 km
- 1000BASE-ZX (SMF) jusqu'à 70 km
- 1000BASE-BX10-D & 1000BASE-BX10-U (SMF) jusqu'à 10 km
- 1000BASE-T (émetteur-récepteur en fil de cuivre)

Modules SFP 10 Gigabit Ethernet

- 10G-SR (MMF) jusqu'à 400 m
- 10G-SR-X (MMF) jusqu'à 400 m (prise en charge d'une plage de températures étendue)
- 10G-LRM (MMF) jusqu'à 220 m
- FET-10G (MMF) jusqu'à 100 m (pour les liaisons montantes de matrice Nexus)
- 10G-LR (SMF) jusqu'à 10 km
- 10G-LR-X (SMF) jusqu'à 10 km (prise en charge d'une plage de températures étendue)
- 10G-ER (SMF) jusqu'à 40 km
- 10G-ZR (SMF) jusqu'à 80 km
- Twinax (émetteur-récepteur en fil de cuivre) jusqu'à 10 m
- Fibre optique active jusqu'à 10 m (pour les connexions intra/interrack)

Les modules 40 Gigabit Ethernet et 100 Gigabit Ethernet sont pris en charge sur les périphériques Cisco haut de gamme, tels que le commutateur Catalyst 6500, les routeurs CRS et ASR 9000 et les commutateurs Nexus 7000

5.3.3 Commutation de couche 3

5.3.3.1 Commutation de couche 2 et commutation de couche 3

En plus de déterminer le format de commutateur adéquat, il peut également s'avérer nécessaire de faire un choix entre un commutateur LAN de couche 2 ou de couche 3.

Souvenez-vous qu'un commutateur LAN de couche 2 effectue la commutation et le filtrage uniquement en fonction de l'adresse MAC de la couche liaison de données OSI (couche 2) et dépend des routeurs pour transférer les données entre les sous-réseaux IP distincts (voir Figure 1).

Comme l'illustre la Figure 2, un commutateur de couche 3 tel que le commutateur Catalyst 3560 fonctionne de manière similaire à un commutateur de couche 2 (par exemple, le commutateur Catalyst 2960) mais, à défaut d'exploiter les informations d'adresses MAC de couche 2 pour décider des opérations de transmission, le commutateur de couche 3 peut également exploiter celles des adresses IP. Un commutateur de couche 3 ne cherche pas uniquement à savoir quelles adresses MAC sont associées à chacun des ports ; il peut également identifier les adresses IP associées à ses interfaces. Il peut alors orienter le trafic sur le réseau également sur la base des informations recueillies sur les adresses IP.

Les commutateurs de couche 3 peuvent également exécuter des fonctions de routage de la couche 3, ce qui réduit le besoin de routeurs dédiés sur un réseau local. Parce que les commutateurs de couche 3 disposent d'un matériel de commutation spécifique, l'acheminement des données est généralement aussi rapide que la commutation.

5.3.3.2 Cisco Express Forwarding

Les périphériques Cisco prenant en charge la commutation de couche 3 utilisent Cisco Express Forwarding (CEF). Cette méthode de transmission est assez complexe, mais heureusement, comme toutes les bonnes technologies, elle opère principalement « en coulisse ». CEF nécessite en principe peu de configuration sur un appareil Cisco.

Grosso modo, CEF met fin à l'interdépendance stricte habituelle entre les prises de décision de couche 2 et de couche 3. En réalité, les allers-retours constants entre les structures de couche 2 et de couche 3 au sein d'un périphérique réseau ralentissent la transmission des paquets IP. Ainsi, dans la mesure où les structures de données de couche 2 et de couche 3 peuvent être dissociées, la transmission est accélérée.

Les deux principaux composants de l'opération CEF sont les suivants :

- Base d'informations de transfert (FIB)
- Tables de contiguïté

Le principe de la FIB est très similaire à celui d'une table de routage. Un routeur utilise la table de routage pour déterminer le meilleur chemin vers une destination en fonction de la partie réseau de l'adresse IP de destination. Avec CEF, les informations qui étaient stockées dans le cache du routeur sont en fait stockées dans plusieurs structures de données pour la commutation CEF. Les structures de données optimisent la recherche, ce qui permet une

transmission efficace des paquets. Un périphérique réseau utilise la table de recherche FIB pour prendre des décisions de commutation en fonction de la destination sans avoir à accéder au cache du routeur.

Cette table est mise à jour lorsque des modifications surviennent sur le réseau, et contient toutes les routes connues à chaque instant.

Les tables de contiguïté gèrent les adresses du tronçon suivant de couche 2 pour toutes les entrées de la FIB.

La séparation des informations d'accessibilité (dans la table FIB) et des informations de transmission (dans la table de contiguïté) offre un certain nombre d'avantages :

- La table de contiguïté peut être élaborée séparément de la table FIB, ce qui permet aux deux tables de se former sans nécessiter la commutation d'aucun paquet.

- La réécriture d'en-tête MAC utilisée pour transmettre un paquet n'est pas stockée dans les entrées de la mémoire cache. Par conséquent, les modifications d'une chaîne de réécriture d'en-tête MAC ne nécessitent pas la suppression des entrées du cache.

CEF est activé par défaut sur la plupart des périphériques Cisco qui effectuent la commutation de couche 3.

5.3.3.3 Types d'interface de couche 3

Les périphériques réseau Cisco prennent en charge différents types d'interface de couche 3. L'interface de couche 3 prend en charge la transmission des paquets IP vers une destination finale en fonction de l'adresse IP.

Les principaux types d'interface de couche 3 sont les suivants :

- **SVI (interface virtuelle du commutateur)** : interface logique d'un commutateur associé à un réseau local virtuel (VLAN).

- **Port routé** : port physique sur un commutateur de couche 3 configuré pour servir de port du routeur.

- **EtherChannel de couche 3** : interface logique d'un périphérique Cisco associé à un ensemble de ports routés.

Comme nous l'avons montré précédemment, une interface SVI du réseau VLAN par défaut (VLAN1) doit être activée pour que l'hôte IP soit connecté au commutateur et pour permettre la gestion à distance du commutateur. Les interfaces SVI doivent également être configurées de sorte à permettre le routage entre les réseaux VLAN. Comme indiqué, les interfaces SVI sont des interfaces logiques configurées pour des réseaux VLAN spécifiques. Pour permettre le routage entre deux ou plusieurs réseaux VLAN, chacun d'entre eux doit disposer d'une interface SVI distincte activée.

Les ports routés permettent aux commutateurs Cisco (de couche 3) de servir véritablement de routeurs. Chaque port d'un commutateur de ce type peut être configuré comme un port sur un réseau IP indépendant.

Les interfaces EtherChannel de couche 3 permettent de regrouper les liaisons Ethernet de couche 3 entre les périphériques Cisco dans le but d'agréger la bande passante, généralement sur les liaisons montantes.

Remarque : outre les interfaces SVI et EtherChannel de couche 3, il existe d'autres interfaces logiques sur les périphériques Cisco, notamment les interfaces de bouclage et les interfaces de tunnel.

5.3.3.4 Configuration d'un port routé sur un commutateur de couche 3

Un port de commutateur peut être configuré en tant que port routé de couche 3 et se comporter comme une interface de routeur classique. Les caractéristiques des ports routés sont les suivantes :

- Ils ne sont associés à aucun réseau local virtuel spécifique.
- Ils peuvent être configurés avec un protocole de routage de couche 3.
- Ils constituent des interfaces de couche 3 uniquement et ne prennent pas en charge les protocoles de couche 2.

Il suffit de configurer les ports routés en faisant passer l'interface en mode de couche 3 à l'aide de la commande de configuration d'interface **no switchport**. Il faut ensuite attribuer une adresse IP au port. La configuration est terminée !

Les fonctions de routage sont approfondies dans le chapitre suivant.

5.3.3.5 Packet Tracer : configuration des commutateurs de couche 3

L'administrateur réseau remplace le routeur et le commutateur existants par un nouveau commutateur de couche 3. En tant que technicien réseau, vous devez configurer le commutateur et le mettre en service. Vous allez travailler en dehors des heures de bureau normales afin de réduire l'impact sur l'activité.

Instructions de Packet Tracer - Configuration des commutateurs de couche 3

PKA de Packet Tracer - Configuration des commutateurs de couche 3

5.4 Résumé

5.4.1 Résumé

5.4.1.1 Exercice - Sélection MAC

Sélection MAC

Remarque : cet exercice peut être effectué individuellement, en petits groupes ou en classe entière.

Regardez la vidéo accessible depuis le lien suivant :

http://www.netevents.tv/video/bob-metcalfe-the-history-of-ethernet

Les thèmes abordés ne concernent pas uniquement l'historique du développement d'Ethernet, mais également de l'évolution actuelle de la technologie Ethernet (approche futuriste).

Lorsque vous aurez regardé la vidéo et que vous aurez comparé son contenu à celui du chapitre 5, naviguez sur le Web pour rechercher des informations sur Ethernet. Adoptez une approche comparative :

- Quelles étaient les caractéristiques d'Ethernet lors de sa création ?
- Quelles caractéristiques sont restées identiques au cours des 25 dernières années et quelles modifications sont apportées pour le rendre plus utile/applicable aux méthodes de transmission de données actuelles ?

Choisissez trois photos de périphériques et supports physiques Ethernet anciens, actuels et futurs (concentrez-vous sur les commutateurs). Partagez ces photos avec la classe et répondez aux questions suivantes :

- Comment ont évolué les supports physiques Ethernet et les périphériques intermédiaires ?
- Quels sont les aspects des supports physiques Ethernet et des périphériques intermédiaires qui sont restés les mêmes ?
- Quelle va être l'évolution d'Ethernet ?

Instructions de l'exercice en classe - Sélection MAC

5.4.1.2 Résumé

Ethernet est la technologie LAN la plus répandue aujourd'hui. Ethernet est une famille de technologies réseau définies par les normes IEEE 802.2 et 802.3. Les normes Ethernet définissent à la fois les protocoles de la couche 2 et les technologies de la couche 1. Pour les protocoles de couche 2, tout comme pour chacune des normes IEEE 802, Ethernet s'appuie sur les deux sous-couches distinctes de la couche liaison de données pour fonctionner : les sous-couches LLC et MAC.

Au niveau de la couche liaison de données, la structure de trame est presque la même pour tous les débits Ethernet. La structure de trame Ethernet ajoute des en-têtes et des codes de fin à l'unité de données de protocole de la couche 3 pour encapsuler le message envoyé.

On distingue deux types de tramage Ethernet : la norme Ethernet IEEE 802.3 et la norme Ethernet DIX, maintenant appelée Ethernet II. La différence principale entre les deux normes est l'ajout d'un délimiteur de début de trame (SFD) et le remplacement du champ Type en un champ Longueur pour la norme 802.3. Ethernet II est le format de trame Ethernet utilisé par les réseaux TCP/IP. Conformément aux spécifications des normes IEEE 802.2/3, la trame Ethernet fournit un adressage MAC et un contrôle des erreurs.

L'adressage de la couche 2 fourni par Ethernet prend en charge les différents types de communications : monodiffusion, diffusion et multidiffusion. Ethernet utilise le protocole ARP pour déterminer les adresses MAC de destination et les mapper à des adresses de couche réseau connues.

Chaque nœud sur un réseau IP possède une adresse MAC et une adresse IP. Le nœud doit utiliser ses propres adresses MAC et IP dans les champs sources et doit fournir une adresse MAC et une adresse IP de destination. Bien que l'adresse IP de la destination soit fournie par une couche OSI supérieure, le nœud émetteur doit obtenir l'adresse MAC de destination de la liaison Ethernet. Quel est l'objectif d'ARP ?

Le protocole ARP repose sur certains types de message de diffusion Ethernet et de message monodiffusion Ethernet, appelés requêtes ARP et réponses ARP. Le protocole ARP résout les adresses IPv4 en adresses MAC et met à jour une table des mappages.

Sur la plupart des réseaux Ethernet, les périphériques finaux sont généralement connectés point-à-point à un commutateur de réseau local de couche 2. Un commutateur de réseau local de couche 2 permet d'effectuer une commutation et un filtrage en se basant uniquement sur l'adresse MAC de la couche liaison de données (couche 2) du modèle OSI. Un commutateur de couche 2 génère une table d'adresses MAC qu'il utilise pour des décisions de transmission. Les commutateurs de couche 2 dépendent des routeurs pour transmettre les données entre les sous-réseaux IP indépendants.

Les commutateurs de couche 3 peuvent également exécuter des fonctions de routage de la couche 3, ce qui réduit le besoin de routeurs dédiés sur un réseau local. Parce que les commutateurs de couche 3 disposent d'un matériel de commutation spécifique, l'acheminement des données est généralement aussi rapide que la commutation

Chapitre 6: Couche réseau

6.0 Couche réseau

6.0.1 Introduction

6.0.1.1 Introduction

Les services et applications réseau d'un périphérique final peuvent communiquer avec des services et applications exécutés sur un autre périphérique final. Comment ces données peuvent-elles transiter efficacement sur tout le réseau ?

Les protocoles de la couche réseau du modèle OSI spécifient l'adressage et les processus qui permettent aux données de la couche transport d'être encapsulées et transportées. L'encapsulation de couche réseau permet aux données d'être transférées vers une destination au sein d'un réseau (ou sur un autre réseau) avec une surcharge minimale.

Ce chapitre porte sur le rôle de la couche réseau. Il examine comment cette dernière divise les réseaux en groupes d'hôtes pour gérer le flux de paquets de données dans un réseau. Ce chapitre aborde également la communication entre les réseaux. Cette communication entre réseaux est appelée routage.

6.0.1.2 Exercice – Le chemin le moins emprunté

Le chemin le moins emprunté ?

Vous avez décidé de rendre visite le weekend à un collègue qui est malade. Vous connaissez son adresse mais vous ne vous êtes jamais rendu dans cette ville auparavant. Au lieu de rechercher l'adresse sur une carte, vous décidez de demander aux résidents de la ville votre chemin après avoir pris le train. Les habitants à qui vous demandez votre route sont très aimables. Cependant, ils ont une particularité. Au lieu de vous indiquer le chemin complet jusqu'à votre destination, ils vous disent « prenez cette route et dès que vous arrivez au prochain carrefour, demandez votre chemin à quelqu'un d'autre. »

Intrigué par ces indications, vous suivez ces instructions et arrivez enfin, carrefour après carrefour, route après route, chez votre ami.

Répondez aux questions suivantes :

- Le fait d'obtenir des instructions sur le chemin complet aurait-il eu un impact significatif sur votre recherche ?

- Aurait-il été plus utile de se renseigner sur l'adresse postale complète ou simplement sur le nom de la rue ? Que se passerait-il si la personne qui vous renseigne ne connaissait pas la rue de destination ou vous indiquait la mauvaise direction ?

- Supposons qu'en rentrant chez vous, vous demandiez à nouveau aux habitants la route à emprunter. Avez-vous la certitude que le même chemin vous sera indiqué chaque fois que vous souhaitez vous rendre chez votre ami ? Expliquez votre réponse.

- Est-il nécessaire d'expliquer l'endroit d'où vous partez lorsque vous demandez des informations sur un chemin à emprunter ?

Exercice – Le chemin le moins emprunté ? Instructions

6.1 Protocoles de couche réseau

6.1.1 Couche réseau de la communication

6.1.1.1 Couche réseau

La couche réseau, ou couche 3 du modèle OSI, fournit des services permettant aux périphériques finaux d'échanger des données sur le réseau. Pour effectuer ce transport de bout en bout, la couche réseau utilise quatre processus de base :

- **Adressage des périphériques finaux** – de la même manière qu'un téléphone a un numéro unique, les périphériques finaux doivent être configurés avec une adresse IP unique pour être identifiés sur le réseau. Un périphérique final disposant d'une adresse IP est qualifié d'hôte.

- **Encapsulation** – la couche réseau reçoit une unité de données de protocole (PDU) de la couche transport. Dans le cadre d'un processus appelé l'encapsulation, la couche réseau ajoute des informations d'en-tête IP, telles que l'adresse IP des hôtes source (expéditeur) et de destination (destinataire). Une fois les informations d'en-tête ajoutées à la PDU, celle-ci est appelée paquet.

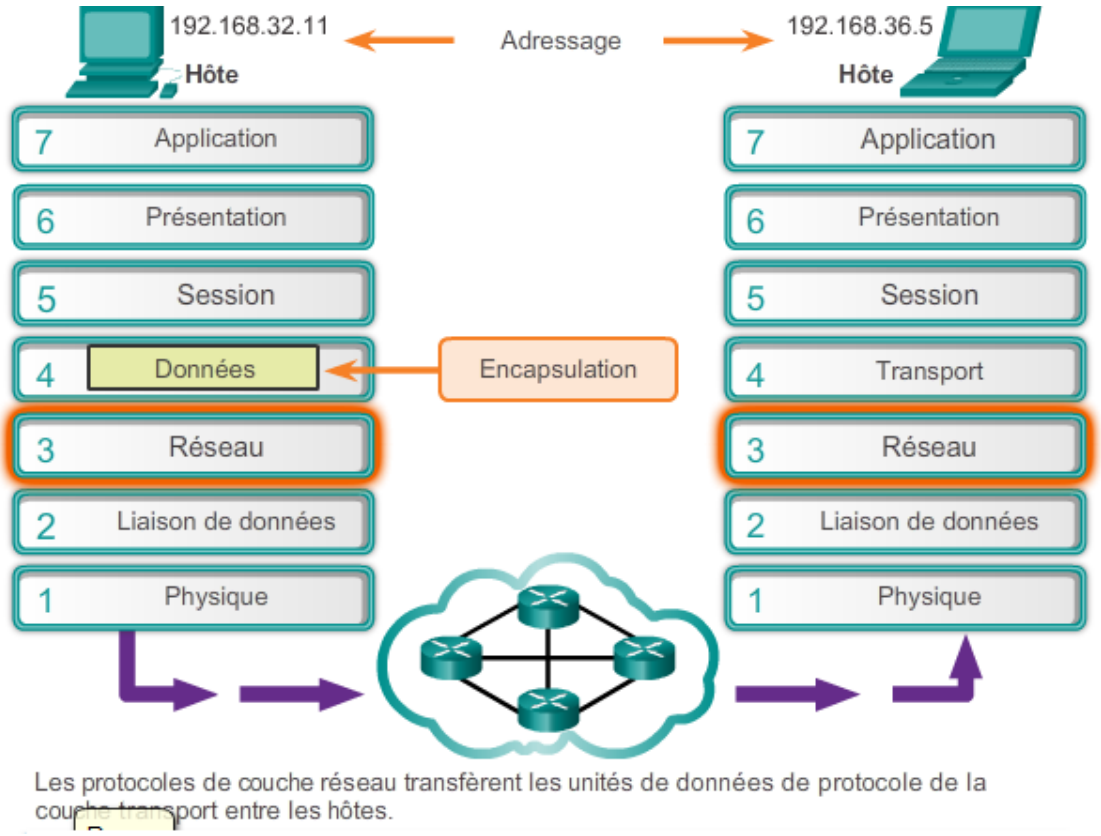
- **Routage** – la couche réseau fournit des services permettant de diriger les paquets vers un hôte de destination sur un autre réseau. Pour voyager vers d'autres réseaux, le paquet doit être traité par un routeur. Le rôle du routeur est de sélectionner les chemins afin de diriger les paquets vers l'hôte de destination. Ce processus est appelé le routage. Un paquet peut passer par de nombreux périphériques intermédiaires avant d'atteindre l'hôte de destination. Chaque route que le paquet emprunte pour atteindre l'hôte de destination est appelée un saut.

- **Désencapsulation** – lorsque le paquet arrive au niveau de la couche réseau de l'hôte de destination, l'hôte vérifie l'en-tête du paquet IP. Si l'adresse IP de destination dans l'en-tête correspond à l'adresse IP de l'hôte qui effectue la vérification, l'en-tête IP est supprimé du paquet. Ce processus de suppression des en-têtes des couches inférieures est appelé la désencapsulation. Une fois la désencapsulation effectuée par la couche

réseau, la PDU de couche 4 est transmise au service approprié au niveau de la couche transport.

Contrairement à la couche transport (couche 4 OSI), qui gère le transport des données entre les processus s'exécutant sur chaque hôte, les protocoles de couche réseau spécifient la structure et le traitement des paquets utilisés pour transporter les données d'un hôte à un autre. Un fonctionnement indépendant des données transportées dans chaque paquet permet à la couche réseau d'acheminer des paquets pour plusieurs types de communication entre plusieurs hôtes.

L'animation de la figure illustre l'échange des données.



6.1.1.2 Protocoles de couche réseau

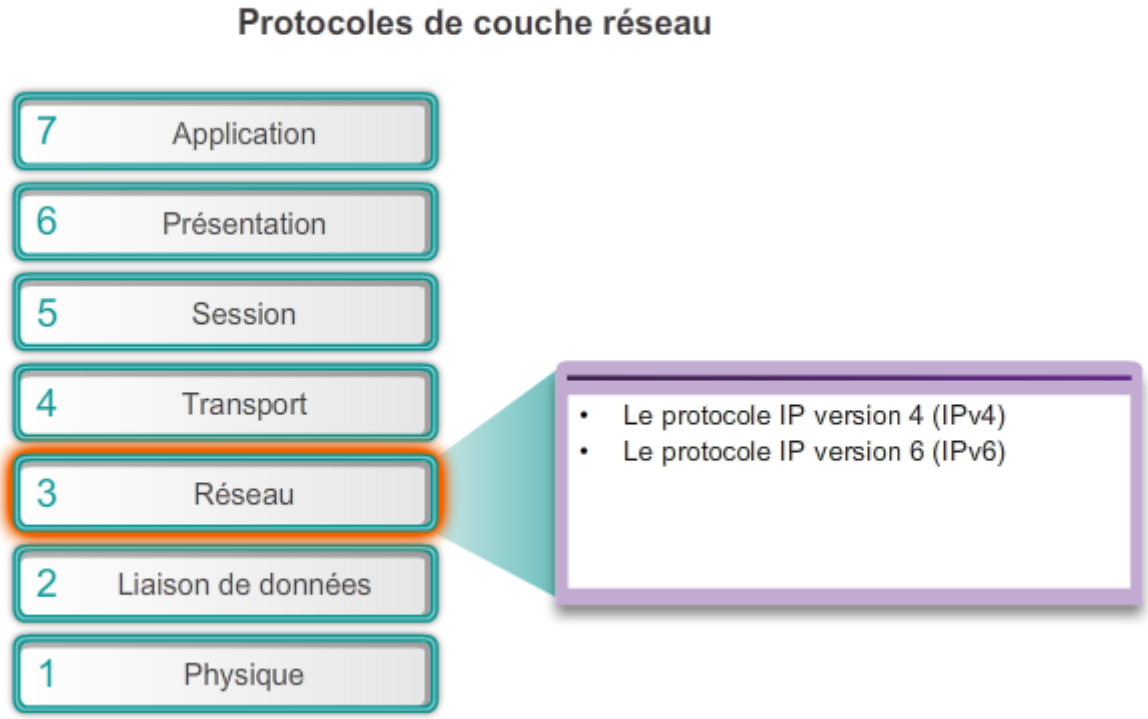
Il existe plusieurs protocoles de couche réseau. Cependant, seuls les deux protocoles suivants sont généralement mis en œuvre, comme l'illustre la figure :

- Le protocole IP version 4 (IPv4)
- Le protocole IP version 6 (IPv6)

Il existe également des protocoles de couche réseau peu utilisés :

- Novell Internetwork Packet Exchange (IPX)
- AppleTalk
- Connectionless Network Service (CLNS/DECNet)

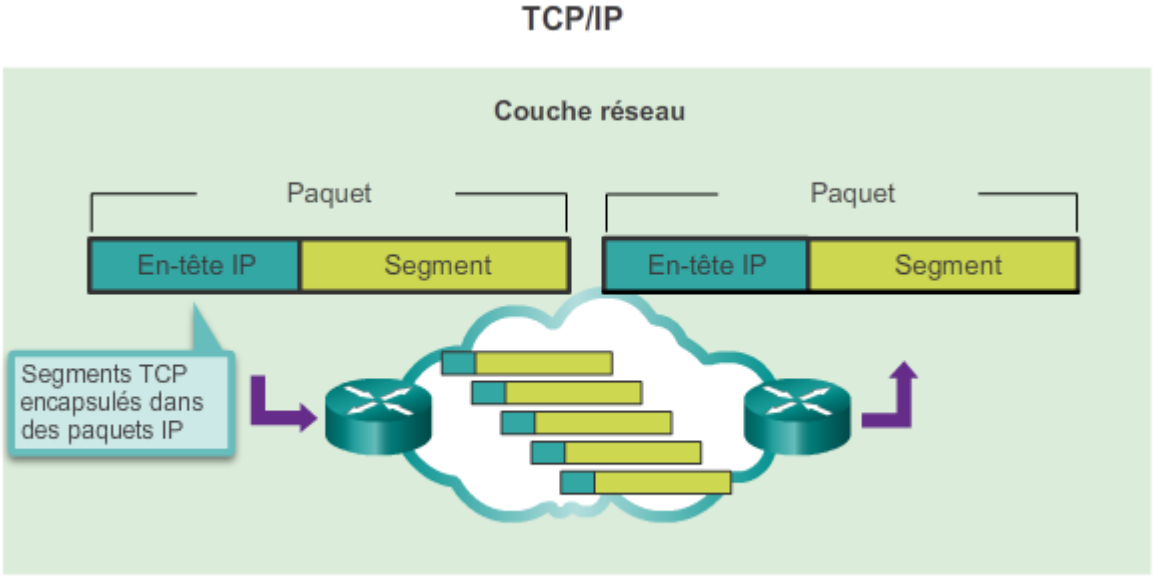
Ces protocoles ne seront que peu abordés dans ce cours.



6.1.2 Caractéristiques du protocole IP

6.1.2.1 Caractéristiques du protocole IP

Caractéristiques du protocole IP



Les paquets IP circulent dans l'interréseau.

Le protocole IP est le service de couche réseau mis en œuvre par la suite de protocoles TCP/IP.

Il a été conçu pour ne pas surcharger les réseaux. Il fournit uniquement les fonctions requises pour transférer un paquet d'une source à une destination en passant par un système interconnecté de réseaux. Ce protocole n'est pas destiné au suivi et à la gestion du flux de paquets. Ces fonctions sont effectuées par d'autres protocoles d'autres couches, si nécessaire.

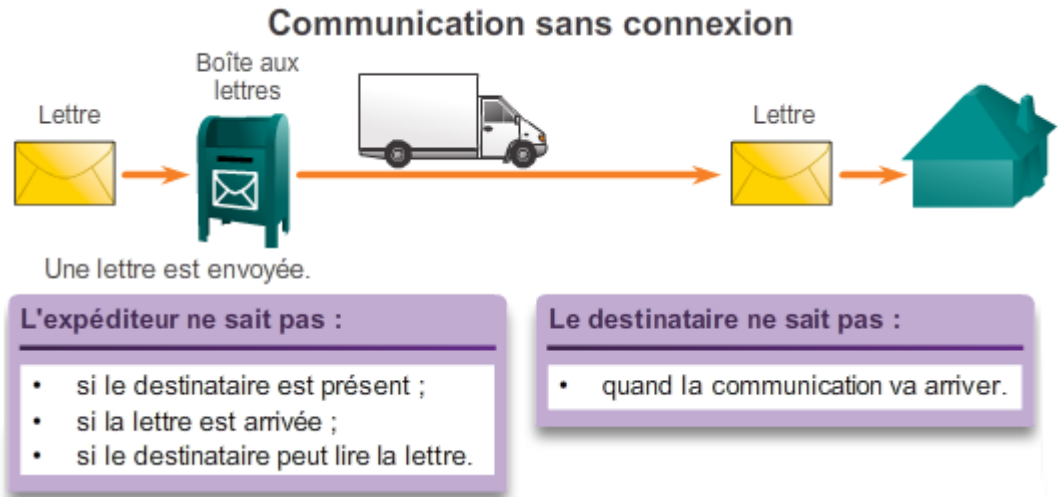
Les principales caractéristiques du protocole IP sont les suivantes :

- **Sans connexion** – aucune connexion avec la destination n'est établie avant d'envoyer des paquets de données.
- **Acheminement au mieux (peu fiable)** – la livraison des paquets n'est pas garantie.
- **Indépendant du support** – le fonctionnement est indépendant du support transportant les données.

6.1.2.2 IP – Sans connexion

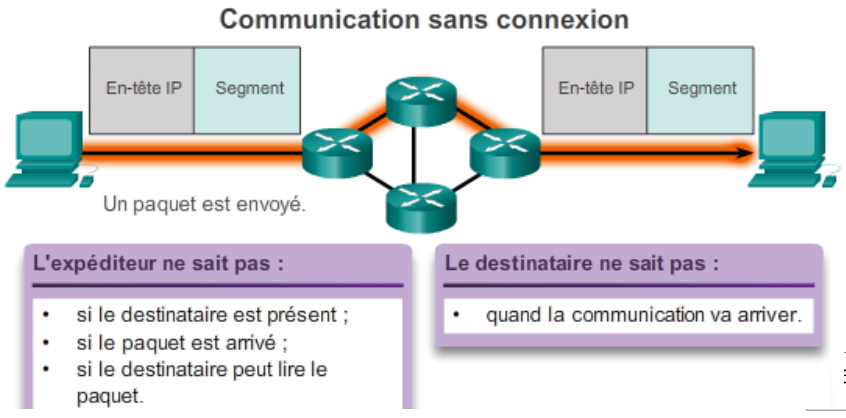
Le rôle de la couche réseau est de transporter les paquets entre les hôtes, tout en imposant le moins de charge possible au réseau. La couche réseau n'est pas concernée par le type de communication présent dans un paquet et l'ignore. Le protocole IP est sans connexion, ce qui signifie que la connexion de bout en bout dédiée est créée avant que les données soient envoyées. L'envoi d'une lettre sans en avertir le destinataire illustre bien la communication sans connexion.

Comme l'illustre la Figure 1, le service postal utilise les informations inscrites sur les lettres pour acheminer les lettres à leur destinataire. L'adresse inscrite sur une enveloppe n'indique pas si le destinataire sera présent, si la lettre va arriver ou si le destinataire pourra lire la lettre. En fait, le service postal n'a aucune information sur le contenu du paquet qu'il achemine et ne peut donc fournir aucun mécanisme de correction des erreurs.



Les communications de données sans connexion fonctionnent sur le même principe.

Le protocole IP est sans connexion et ne requiert, par conséquent, aucun échange initial d'informations de contrôle pour établir une connexion de bout en bout avant que les paquets soient transférés. Le protocole IP ne nécessite pas non plus de champs supplémentaires dans l'en-tête de PDU pour maintenir une connexion établie. Ce processus réduit sensiblement la surcharge du protocole IP. Cependant, sans connexion de bout en bout préétablie, les expéditeurs ne savent pas si les périphériques de destination sont présents et fonctionnels lors de l'envoi des paquets. Ils ne savent pas non plus si le destinataire reçoit le paquet ou s'il peut accéder et lire le paquet. La Figure 2 présente un exemple de communication sans connexion.

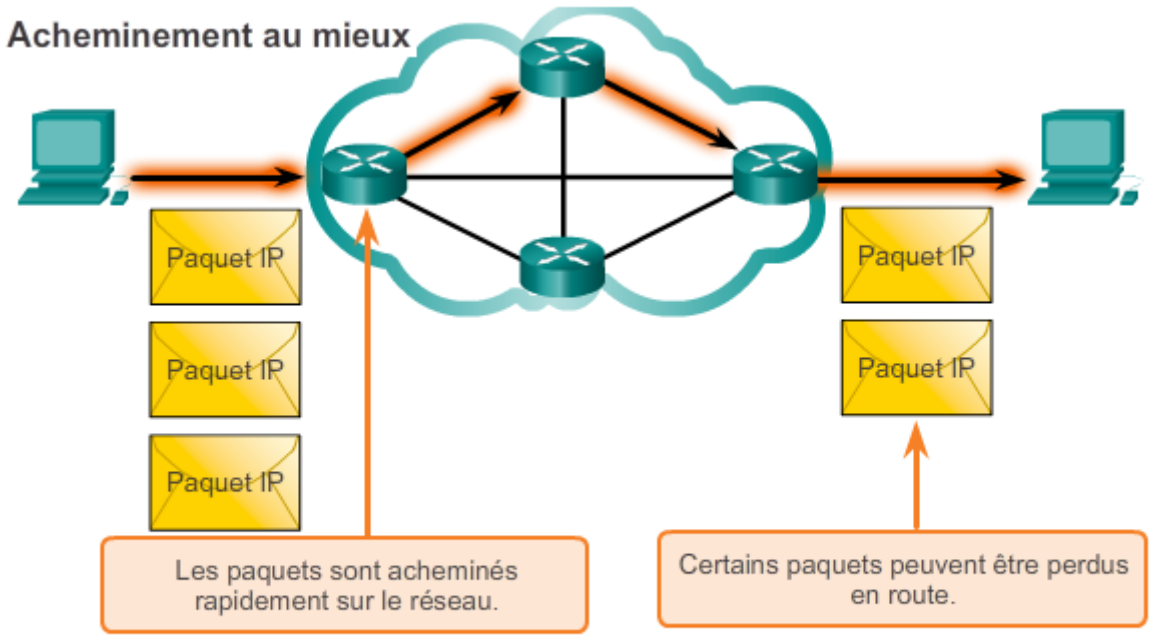


6.1.2.3 IP – Acheminement au mieux

Le protocole IP est souvent qualifié de protocole non fiable ou de protocole d'acheminement au mieux. Cela ne signifie pas que le protocole IP ne fonctionne que par intermittence, ni que ce protocole de communication de données n'est pas efficace. Le terme « non fiable » signifie simplement que le protocole IP n'a pas la capacité de gérer (ni de récupérer) les paquets endommagés ou non remis. En effet, alors que les paquets IP sont envoyés avec des informations sur l'emplacement de la destination, ils ne contiennent aucune information pouvant être traitée pour informer l'expéditeur que les paquets ont bien été reçus. Aucune donnée de synchronisation n'est comprise dans l'en-tête du paquet pour suivre l'ordre de livraison de paquets. De plus, aucun accusé de réception de la transmission de paquets n'existe dans le protocole IP et aucune donnée de contrôle des erreurs ne permet de savoir si les paquets ont été acheminés sans être modifiés. Les paquets peuvent arriver à destination endommagés, dans le désordre, ou même ne pas arriver du tout. Avec les informations de l'en-tête IP, il est impossible de retransmettre des paquets en cas d'erreur.

Si des paquets dans le désordre ou manquants génèrent des problèmes pour l'application utilisant les données, des services de couche supérieure (par exemple, TCP) devront résoudre ces incidents. Cela permet au protocole IP d'être très efficace. Si des données supplémentaires relatives à la fiabilité étaient incluses au protocole IP, les communications n'exigeant pas de connexions ou de fiabilité augmenteraient pour rien la consommation de bande passante et les délais. Dans la suite de protocoles TCP/IP, la couche transport peut utiliser le protocole TCP ou UDP en fonction du besoin de fiabilité de la transmission. Laisser la décision de fiabilité à la couche transport permet au protocole IP d'être plus adaptable et approprié à différents types de communication.

La figure montre un exemple de communications IP. Les protocoles orientés connexion, tels que TCP, exigent que des données de contrôle soient échangées pour établir la connexion. Pour mettre à jour des informations sur la connexion, le protocole TCP nécessite également des champs supplémentaires dans l'en-tête PDU.



En tant que protocole de couche réseau peu fiable, le protocole IP ne garantit pas que tous les paquets envoyés seront reçus. D'autres protocoles gèrent le processus de suivi des paquets et garantissent leur livraison.

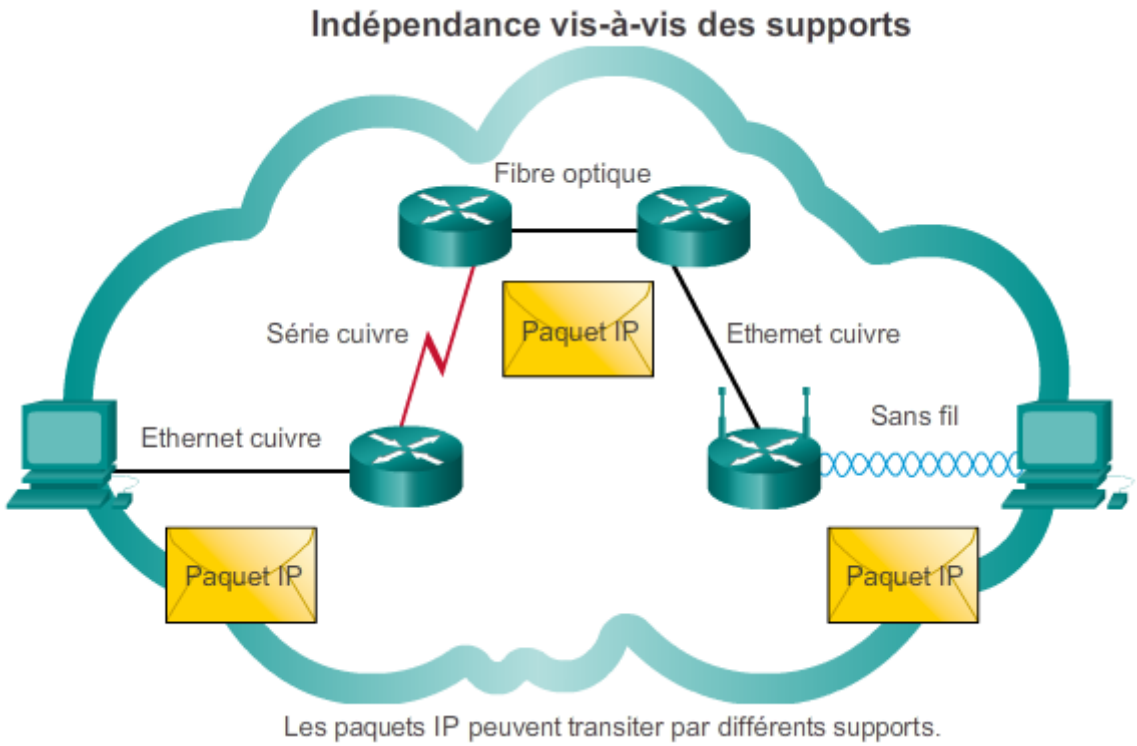
6.1.2.4 Indépendance vis-à-vis des supports

La couche réseau n'est pas non plus pénalisée par les caractéristiques du support transportant les paquets. Le protocole IP fonctionne indépendamment des supports acheminant les données dans les couches inférieures de la pile de protocoles. Comme l'illustre la figure, tout paquet IP peut être communiqué électriquement par voie filaire (en tant que signaux optiques sur de la fibre) ou sans fil (sous la forme de signaux radio).

Il incombe à la couche liaison de données OSI de prendre un paquet IP et de le préparer en vue de sa transmission sur le support de communication. Cela signifie que le transport des paquets IP ne se limite pas à un support particulier.

Il existe, toutefois, une caractéristique majeure du support que la couche réseau prend en compte : la taille maximale de la PDU que chaque support peut transporter. Cette caractéristique est appelée unité de transmission maximale (MTU). Une partie de la communication de contrôle entre la couche liaison de données et la couche réseau est l'établissement d'une taille maximale pour le paquet. La couche liaison de données transmet la MTU à la couche réseau. La couche réseau détermine ensuite la taille maximale des paquets.

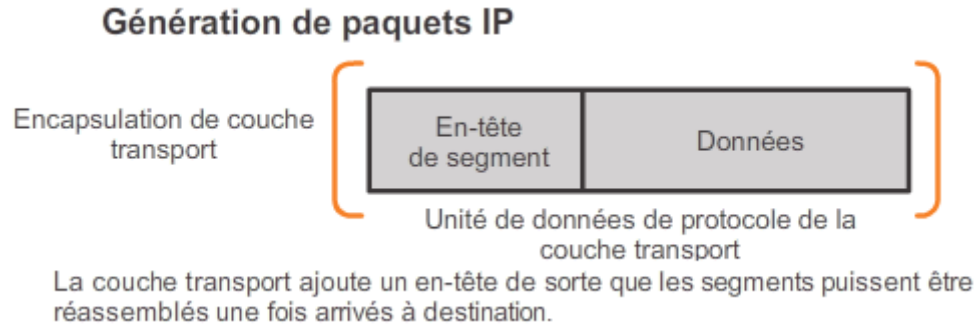
Dans certains cas, un périphérique intermédiaire, généralement un routeur, doit scinder un paquet lors de la transmission dudit paquet d'un support à un autre support de MTU inférieure. Ce processus porte le nom de fragmentation du paquet ou simplement fragmentation.



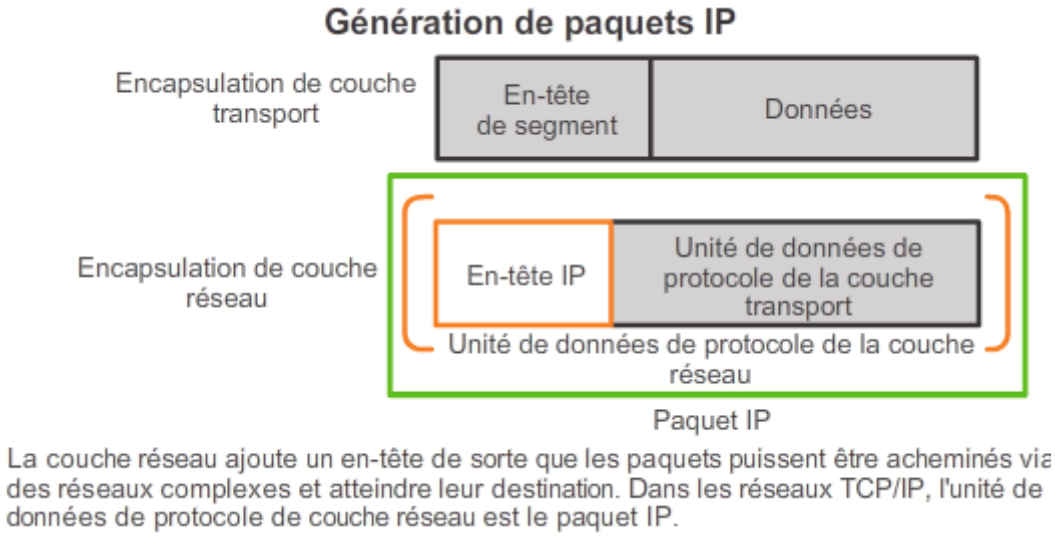
6.1.2.5 Encapsulation IP

Le protocole IP encapsule le segment de couche transport en ajoutant un en-tête IP. Cet en-tête est utilisé pour acheminer le paquet vers l'hôte de destination. L'en-tête IP reste en place du moment où le paquet quitte la couche réseau de l'hôte source jusqu'à son arrivée dans la couche réseau de l'hôte de destination.

La Figure 1 illustre le processus de création de la PDU de couche transport.



La Figure 2 illustre le processus consécutif de création de la PDU de couche réseau.



Ce processus d'encapsulation des données couche par couche permet aux services des différentes couches de se développer et d'évoluer sans affecter les autres couches. Cela signifie que les segments de couche transport peuvent être facilement encapsulés par les protocoles IPv4 et IPv6, ou par tout nouveau protocole pouvant être mis au point dans le futur.

Les routeurs peuvent mettre en œuvre ces différents protocoles de couche réseau pour fonctionner simultanément sur un réseau vers et depuis les mêmes hôtes ou des hôtes différents. Le routage effectué par ces périphériques intermédiaires tient compte uniquement du contenu de l'en-tête de paquet qui encapsule le segment. Dans tous les cas, la partie données du paquet (à savoir l'unité de données de protocole de couche transport encapsulée) reste inchangée durant les processus de couche réseau.

6.1.2.6 Exercice – Caractéristiques du protocole IP

Exercice

6.1.3 Paquet IPv4

6.1.3.1 En-tête de paquet IPv4

L'IPv4 est en service depuis 1983, date à laquelle le protocole a été mis en place sur le réseau ARPANET (Advanced Research Projects Agency Network), l'ancêtre d'Internet. Internet repose essentiellement sur l'IPv4, qui est toujours le protocole de couche réseau le plus répandu.

Un paquet IPv4 comporte deux parties :

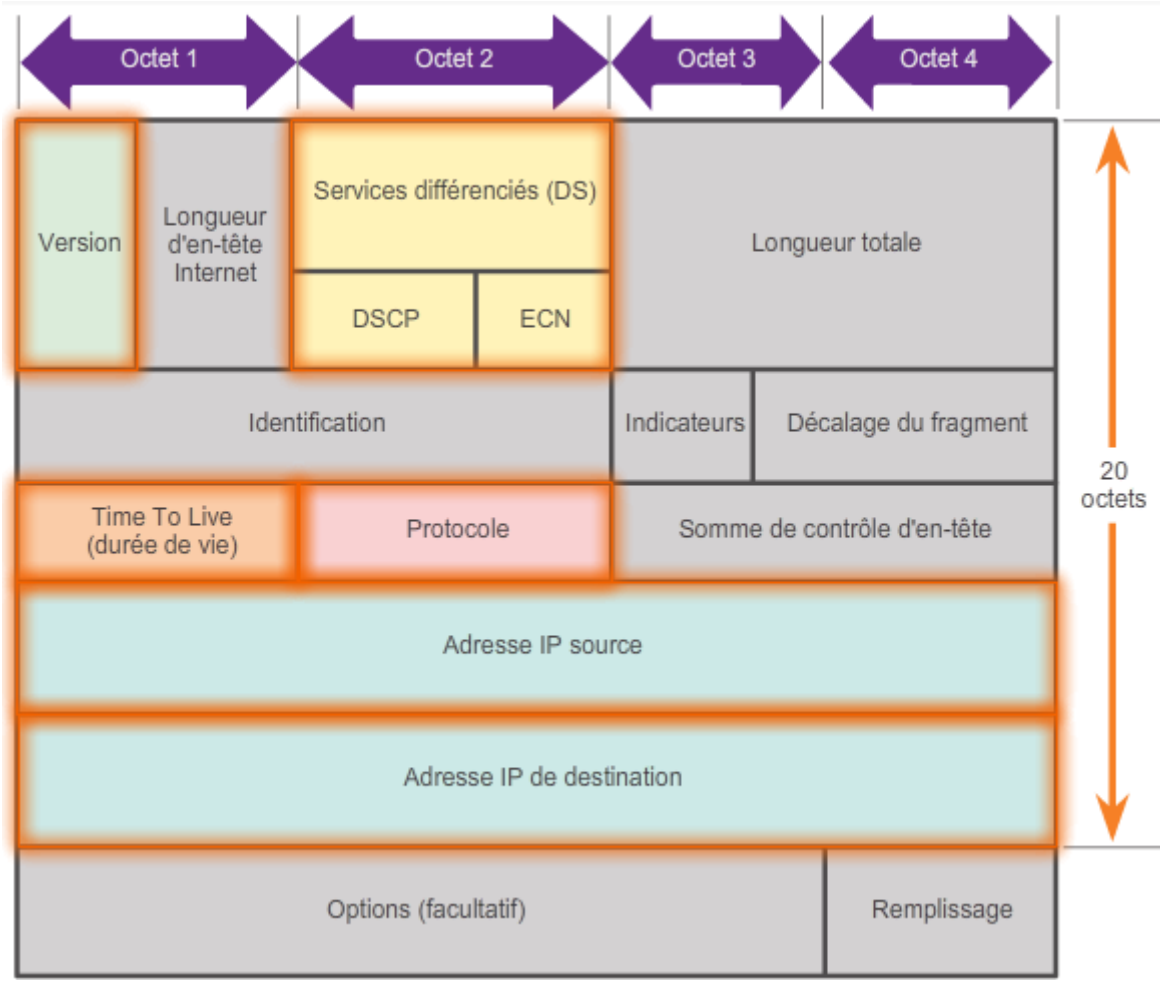
- **En-tête IP** – indique les caractéristiques du paquet.
- **Données utiles** – contient les informations du segment de couche 4 et les données en elles-mêmes.

Comme le montre la figure, un en-tête de paquet IPv4 comporte des champs contenant des informations importantes sur le paquet. Ces champs contiennent des nombres binaires, examinés par le processus de couche 3. Les valeurs binaires de chaque champ indiquent divers paramètres du paquet IP.

Les champs importants de l'en-tête IPv4 sont les suivants :

- **Version** – contient une valeur binaire de 4 bits indiquant la version du paquet IP. Pour les paquets IPv4, ce champ est toujours 0100.
- **Services différenciés** – anciennement appelé champ de type de service, le champ Services différenciés est un champ de 8 bits utilisé pour définir la priorité de chaque paquet. Les 6 premiers bits définissent la valeur DCSP (Differentiated Services Code Point) qui est utilisée par un mécanisme de qualité de service. Les 2 derniers bits identifient la valeur de notification explicite de congestion qui peut être utilisée pour empêcher l'abandon de paquets pendant les périodes d'encombrement du réseau.
- **Time-to-live (durée de vie, TTL)** – contient une valeur binaire de 8 bits utilisée pour limiter la durée de vie d'un paquet. Cette durée est indiquée en secondes mais est généralement appelée « nombre de sauts ». L'expéditeur du paquet définit la valeur de durée de vie initiale et celle-ci diminue de un chaque fois que le paquet est traité par un routeur, ou effectue un saut. Si la valeur du champ TTL (durée de vie) arrive à zéro, le routeur rejette le paquet et envoie un message de dépassement de délai ICMP à l'adresse IP source. La commande **traceroute** utilise ce champ pour identifier les routeurs utilisés entre la source et la destination.
- **Protocole** – cette valeur binaire de 8 bits indique le type de données utiles transportées par le paquet, ce qui permet à la couche réseau de transmettre les données au protocole de couche supérieure approprié. Les valeurs habituelles sont notamment ICMP (1), TCP (6) et UDP (17).
- **Adresse IP source** – contient une valeur binaire de 32 bits qui représente l'adresse IP source du paquet.
- **Adresse IP de destination** – contient une valeur binaire de 32 bits qui représente l'adresse IP de destination du paquet.

Les deux champs les plus souvent utilisés sont les adresses IP source et de destination. Ces champs indiquent d'où vient et où va le paquet. Généralement, ces adresses ne changent pas lors du déplacement de la source vers la destination



Figure

6.1.3.2 Champs d'en-tête IPv4

Les champs restants sont utilisés pour identifier et valider le paquet, ou pour réassembler un paquet fragmenté.

Les champs utilisés pour identifier et valider le paquet incluent :

- **Longueur d'en-tête Internet** – contient une valeur binaire de 4 bits indiquant le nombre de mots de 32 bits contenus dans l'en-tête. Cette valeur varie en fonction des champs d'options et de remplissage. La valeur minimale de ce champ est 5 (c.-à-d., 5 x 32 = 160 bits = 20 octets) et la valeur maximale 15 (c.-à-d., 15 x 32 = 480 bits = 60 octets).

- **Longueur totale** – parfois appelé longueur de paquet, ce champ de 16 bits indique la taille globale du paquet (fragment), y compris l'en-tête et les données, en octets. Sa valeur minimale est de 20 octets (un en-tête de 20 octets + 0 octet de données) et sa valeur maximale est de 65 535 octets.

- **Somme de contrôle de l'en-tête** – champ de 16 bits utilisé pour le contrôle des erreurs sur l'en-tête IP. La somme de contrôle de l'en-tête est recalculée et comparée à la valeur contenue dans le champ de somme de contrôle. Si les valeurs ne correspondent pas, le paquet est rejeté.

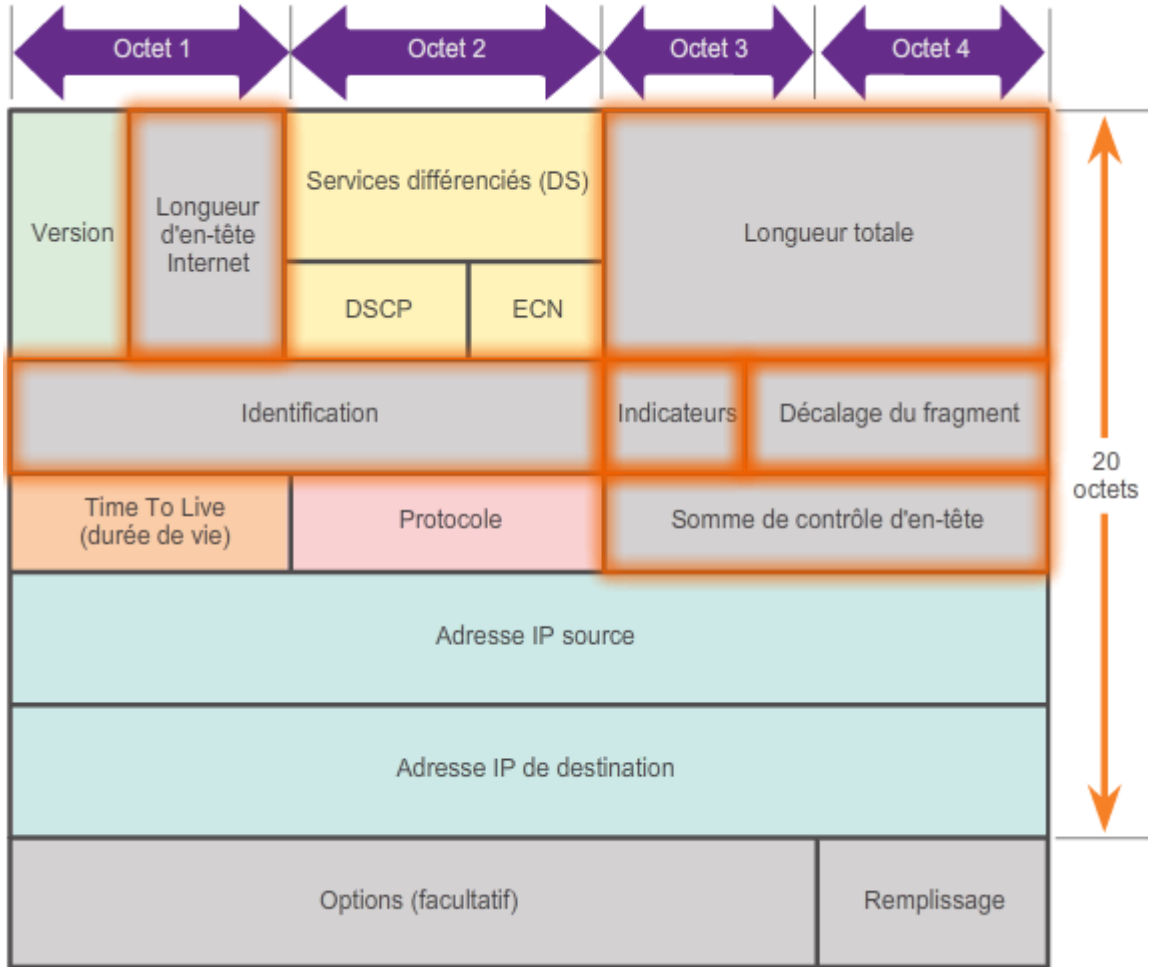
Un routeur peut devoir fragmenter un paquet lors de la transmission dudit paquet d'un support à un autre de MTU inférieure. Dans ce cas, la fragmentation se produit et le paquet IPv4 utilise les champs suivants pour suivre les fragments :

- **Identification** – ce champ de 16 bits identifie de manière unique le fragment d'un paquet IP d'origine.

- **Indicateurs** – ce champ de 3 bits indique la façon dont le paquet est fragmenté. Il est utilisé avec les champs de décalage du fragment et d'identification pour reconstituer le paquet d'origine.

- **Décalage du fragment** – ce champ de 13 bits indique la position dans laquelle placer le fragment de paquet pour reconstituer le paquet d'origine.

Remarque : les champs d'options et de remplissage sont rarement utilisés et ne sont pas abordés dans ce chapitre.

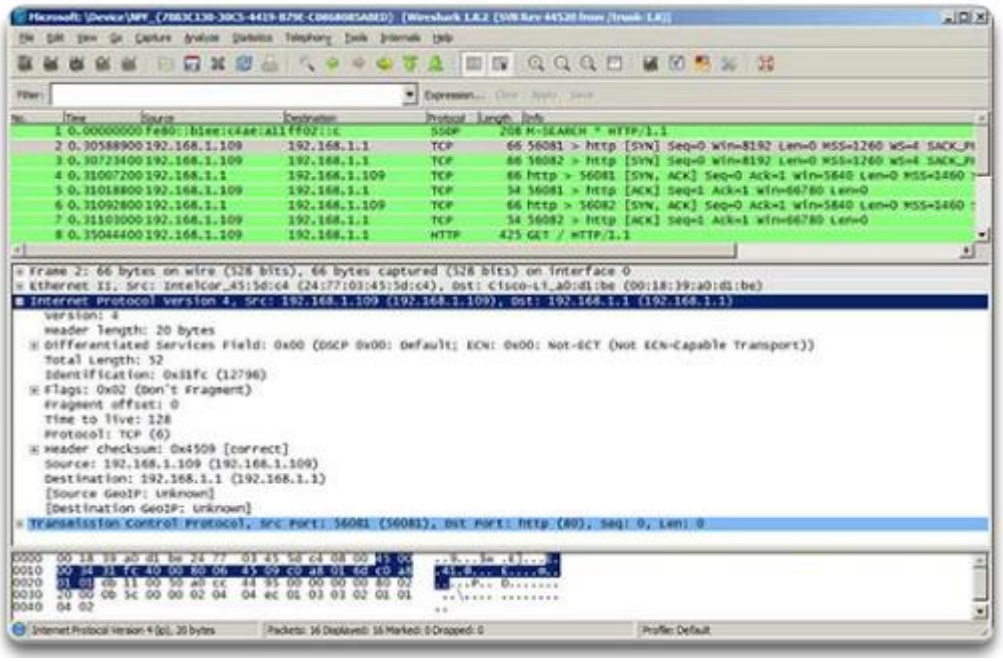


6.1.3.3 Exemples d'en-tête IPv4

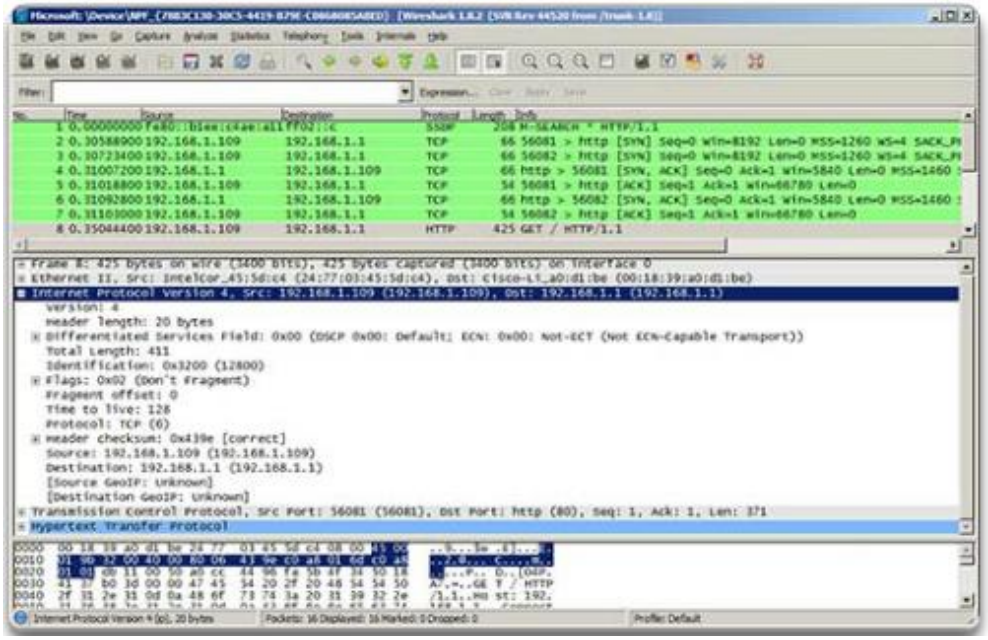
Wireshark est un outil de contrôle de réseau utile pour toute personne qui travaille sur les réseaux. Il peut être utilisé avec la plupart des travaux pratiques des cours CCNA pour l'analyse de données et le dépannage. Cet outil permet également d'afficher des exemples de valeurs contenues dans des champs d'en-tête IP.

Les trois figures ci-contre contiennent des exemples de capture de différents paquets IP :

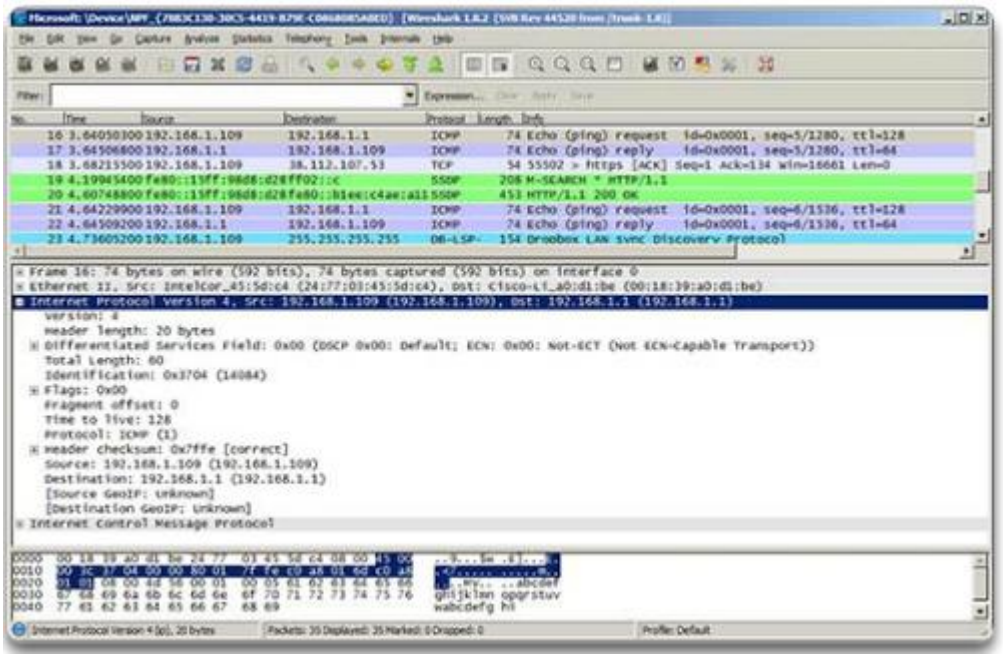
- La Figure 1 affiche le contenu du paquet numéro 2 de cet exemple de capture. Notez que la source est 192.168.1.109 et que la destination est 192.168.1.1. La fenêtre du milieu contient des informations sur l'en-tête IPv4 telles que la taille d'en-tête, la longueur totale, et tous les indicateurs définis.



- La Figure 2 affiche le contenu du paquet numéro 8 de cet exemple de capture. Il s'agit d'un paquet HTTP. Remarquez la présence d'informations au-delà de la section TCP.



- Enfin, la Figure 3 illustre le contenu du paquet numéro 16 de cet exemple de capture. L'exemple de paquet est une requête ping envoyée par l'hôte 192.168.1.109 à l'hôte 192.168.1.1. Remarquez qu'aucune information TCP ou UDP n'est présente, car il s'agit d'un paquet ICMP.



6.1.3.4 Exercice – Champs d'en-tête IPv4

Champs d'en-tête IPv4

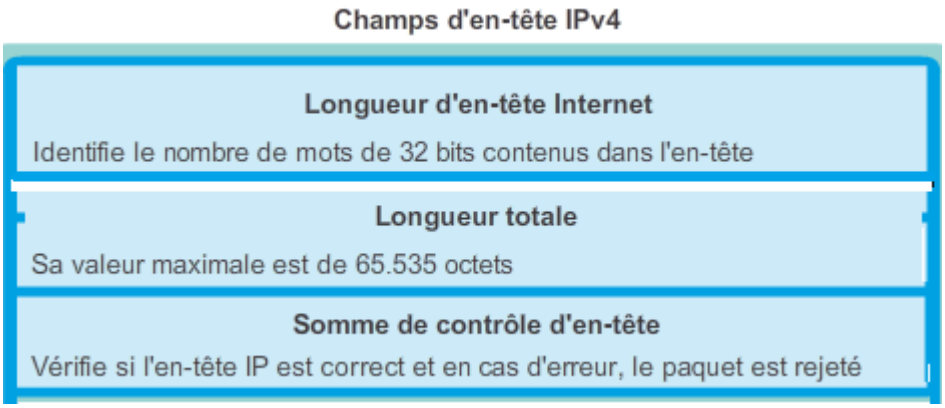
Version Toujours défini sur 0100 pour l'IPv4	**Services différenciés** Définit la priorité de chaque paquet
Time To Live (durée de vie) Généralement appelé « nombre de sauts »	**Protocole** Indique le prochain protocole de couche supérieure à utiliser
Adresse IP source Identifie l'adresse IP de l'hôte d'expédition	**Adresse IP de destination** Identifie l'adresse IP de l'hôte destinataire

Exercice – Partie 1 : Champs d'en-tête IPv4

Lisez les fonctions d'en-tête IPv4, puis cliquez sur les champs d'en-tête IPv4 correspondants.

Exercice – Partie 2 : Champs d'en-tête IPv4

Lisez les descriptions d'en-tête IPv4 de validation et d'identification, puis cliquez sur les champs d'en-tête IPv4 correspondants.



6.1.4 Paquet IPv6

6.1.4.1 Limites du protocole IPv4

Au fil des années, l'IPv4 a été mis à jour afin de relever de nouveaux défis. Cependant, même avec des modifications, l'IPv4 a toujours trois problèmes majeurs :

- **Manque d'adresses IP** – l'IPv4 a un nombre limité d'adresses IP publiques disponibles. Bien qu'il existe environ 4 milliards d'adresses IPv4, le nombre croissant de périphériques IP, les connexions permanentes et la croissance potentielle des pays en voie de développement entraînent une hausse du nombre d'adresses devant être disponibles.

- **Croissance de la table de routage Internet** – une table de routage est utilisée par les routeurs pour déterminer les meilleurs chemins disponibles. À mesure que le nombre de serveurs (nœuds) connectés à Internet augmente, il en va de même pour le nombre de routes réseau. Ces routes IPv4 consomment beaucoup de mémoire et de ressources processeur sur les routeurs Internet.

- **Manque de connectivité de bout en bout** – la technologie de traduction d'adresses réseau (NAT) est généralement implémentée dans les réseaux IPv4. Cette technologie permet à plusieurs périphériques de partager une adresse IP publique unique. Cependant, étant donné que l'adresse IP publique est partagée, l'adresse IP d'un hôte interne du réseau est masquée. Cela peut être problématique pour les technologies nécessitant une connectivité de bout en bout.

6.1.4.2 Présentation de l'IPv6

Au début des années 90, l'Internet Engineering Task Force (IETF) a commencé à se soucier de ces problèmes liés à l'IPv4 et a commencé à chercher une alternative. Cela a conduit au développement de la version 6 du protocole IP (IPv6). L'IPv6 supprime les limites de l'IPv4 et améliore de façon efficace le protocole, grâce à des fonctionnalités qui correspondent mieux aux exigences actuelles et futures des réseaux.

Voici les améliorations apportées par l'IPv6 :

- **Espace d'adressage plus important** – les adresses IPv6 sont basées sur un adressage hiérarchique 128 bits (32 bits pour l'IPv4). Cela augmente considérablement le nombre d'adresses IP disponibles.

- **Traitement des paquets plus efficace** – l'en-tête IPv6 a été simplifié et comporte moins de champs. Cela améliore le traitement des paquets par les routeurs intermédiaires et permet également la prise en charge d'extensions et d'options pour plus d'évolutivité et de longévité.

- **Traduction d'adresses réseau non nécessaire** – grâce au grand nombre d'adresses publiques IPv6, la technologie NAT n'est plus nécessaire. Les sites clients, des plus grandes entreprises aux sites de particuliers, peuvent obtenir une adresse réseau publique IPv6. Cela évite certains des problèmes d'application causés par la technologie NAT, qui sont rencontrés par des applications nécessitant une connectivité de bout en bout.

- **Sécurité intégrée** – l'IPv6 prend nativement en charge les fonctions d'authentification et de confidentialité. Avec l'IPv4, d'autres fonctions devaient être mises en œuvre pour bénéficier de ces fonctionnalités.

L'espace d'adressage IPv4 de 32 bits fournit environ 4 294 967 296 adresses uniques. Parmi ces adresses, seules 3,7 milliards peuvent être attribuées car le système d'adressage IPv4 sépare les adresses en classes et réserve des adresses pour la multidiffusion, les tests et d'autres usages spécifiques.

Comme l'illustre la figure, l'espace d'adressage IPv6 fournit 340 282 366 920 938 463 463 374 607 431 768 211 456 adresses, soit 340 un décillions d'adresses, nombre presque équivalent au nombre de grains de sable sur Terre.

Appellation du nombre	Notation scientifique	Nombre de zéros
Mille	10^3	1,000
1million	10^6	1,000,000
1milliard	10^9	1,000,000,000
1trillion	10^12	1,000,000,000,000
1quadrillion	10^15	1,000,000,000,000,000
1quintillion	10^18	1,000,000,000,000,000,000
1sextillion	10^21	1,000,000,000,000,000,000,000
1septillion	10^24	1,000,000,000,000,000,000,000,000
1octillion	10^27	1,000,000,000,000,000,000,000,000,000
1nonillion	10^30	1,000,000,000,000,000,000,000,000,000,000
1décillion	10^33	1,000,000,000,000,000,000,000,000,000,000,000
1undécillion	10^36	1,000,000,000,000,000,000,000,000,000,000,000,000

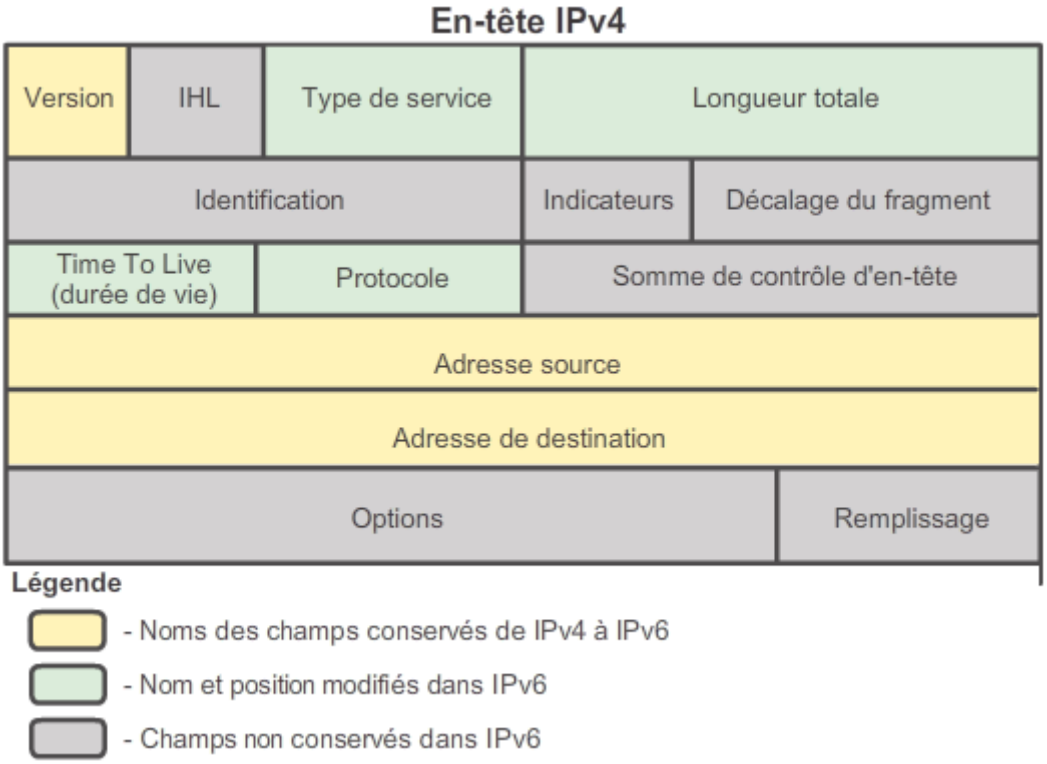
6.1.4.3 Encapsulation IPv6

L'une des principales améliorations de conception de l'IPv6 par rapport à l'IPv4 est l'en-tête simplifié.

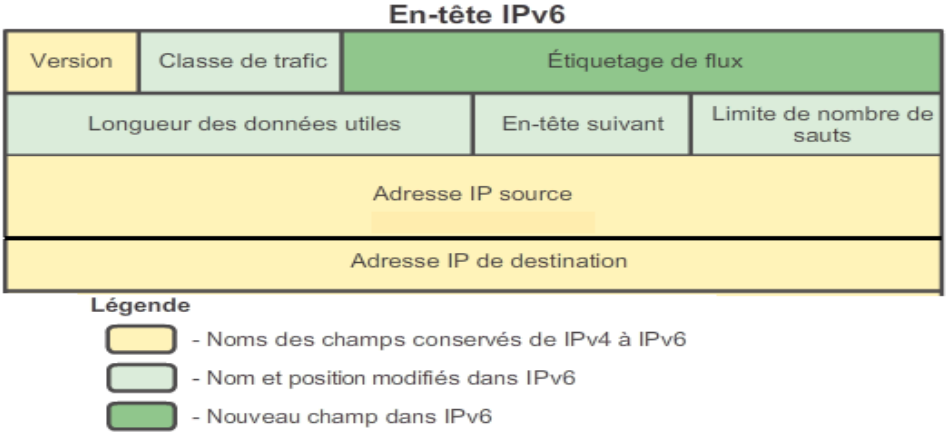
L'en-tête IPv4 contient 20 octets (jusqu'à 60 octets si le champ des options est utilisé) et 12 champs d'en-tête de base, sans compter le champ des options et le champ de remplissage.

L'en-tête IPv6 est constitué de 40 octets (principalement en raison de la longueur des adresses IPv6 source et de destination) et de 8 champs d'en-tête (3 champs d'en-tête IPv4 de base et 5 champs d'en-tête supplémentaires).

La Figure 1 illustre la structure de l'en-tête IPv4.



Comme l'illustre la figure, pour l'IPv6, certains champs ont été conservés, certains champs de l'en-tête IPv4 ne sont pas utilisés et les noms et positions de certains champs ont été modifiés. En outre, un nouveau champ a été ajouté. L'en-tête IPv6 simplifié est présenté à la Figure 2.



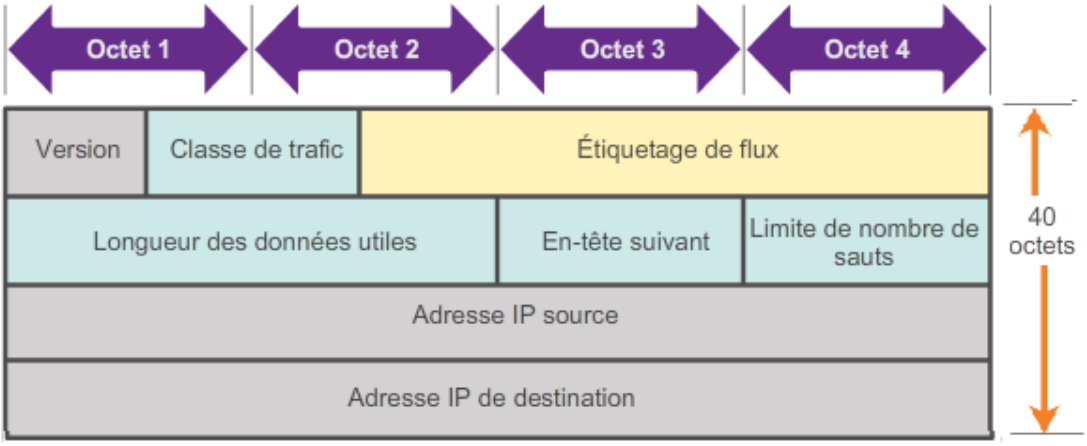
L'en-tête IPv6 offre plusieurs avantages par rapport à l'en-tête IPv4 :

- Une plus grande efficacité du routage pour des performances et évolutivité du débit de transmission.
- Aucune exigence pour le traitement des sommes de contrôle.
- Des mécanismes d'en-tête d'extension simplifiés (par rapport au champ d'options IPv4).
- Un champ d'étiquetage de flux pour le traitement par flux sans avoir besoin d'ouvrir le paquet interne de transport pour identifier les différents flux de trafic

6.1.4.4 En-tête de paquet IPv6

Les champs d'en-tête de paquet IPv6 incluent :

- **Version** – contient une valeur binaire de 4 bits indiquant la version du paquet IP. Pour les paquets IPv6, ce champ est toujours 0110.
- **Classe de trafic** – ce champ de 8 bits est équivalent au champ de services différenciés pour l'IPv4. Il contient également une valeur DSCP de 6 bits utilisée pour classer les paquets et une valeur de notification explicite de congestion de 2 bits utilisée pour contrôler l'encombrement.
- **Étiquetage de flux** – ce champ de 20 bits fournit un service spécifique pour les applications en temps réel. Ce champ peut être utilisé pour indiquer aux routeurs et aux commutateurs de conserver le même chemin pour le flux de paquets, de telle sorte que l'ordre des paquets ne soit pas modifié.
- **Longueur des données utiles** – ce champ de 16 bits est équivalent au champ de longueur totale de l'en-tête IPv4. Il définit la taille globale du paquet (fragment), y compris l'en-tête et les extensions facultatives.
- **En-tête suivant** – ce champ de 8 bits est équivalent au champ de protocole de l'IPv4. Il indique le type de données utiles transportées par le paquet, permettant ainsi à la couche réseau de transmettre les données au protocole de couche supérieure approprié. Ce champ est également utilisé s'il existe des en-têtes d'extension ajoutés au paquet IPv6.
- **Limite de nombre de sauts** – ce champ de 8 bits remplace le champ de durée de vie (TTL) de l'IPv4. Cette valeur est réduite de un chaque fois qu'un routeur transmet le paquet. Lorsque le compteur atteint 0, le paquet est rejeté et un message ICMPv6 est transféré à l'hôte émetteur, indiquant que le paquet n'a pas atteint sa destination.
- **Adresse source** – ce champ de 128 bits identifie l'adresse IPv6 de l'hôte émetteur.
- **Adresse de destination** – ce champ de 128 bits indique l'adresse IPv6 de l'hôte récepteur.



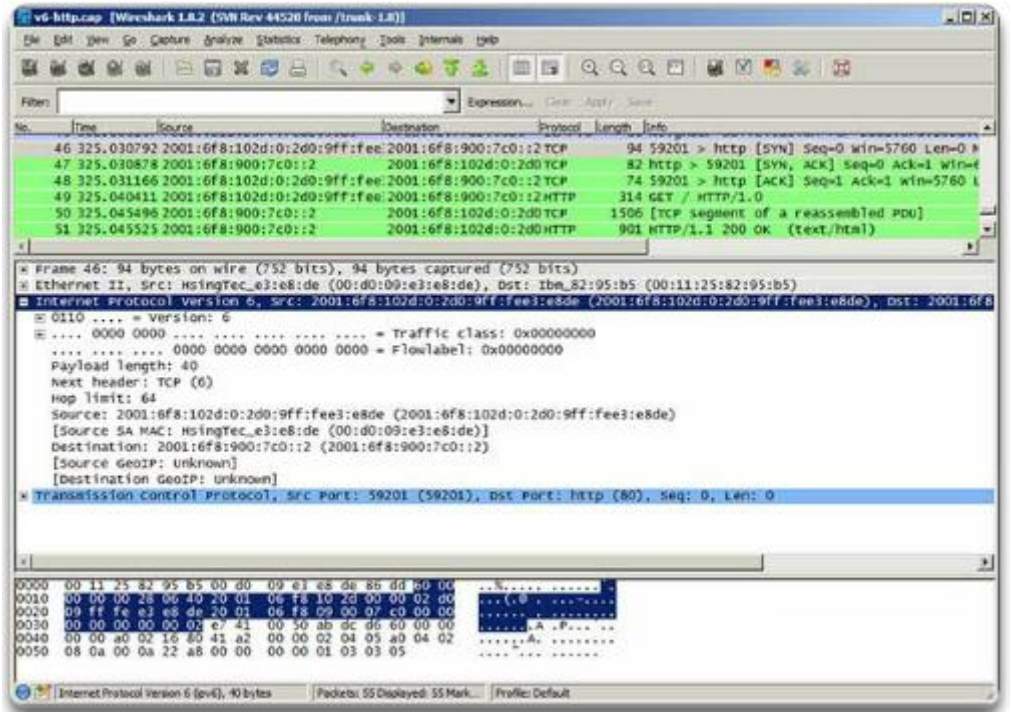
Un paquet IPv6 peut également contenir des en-têtes d'extension qui fournissent des informations facultatives de couche réseau. Les en-têtes d'extension sont facultatifs et sont placés entre l'en-tête IPv6 et les données utiles. Ces en-têtes sont utilisés pour la fragmentation, la sécurité, la prise en charge de la mobilité, etc.

6.1.4.5 Exemples d'en-tête IPv6

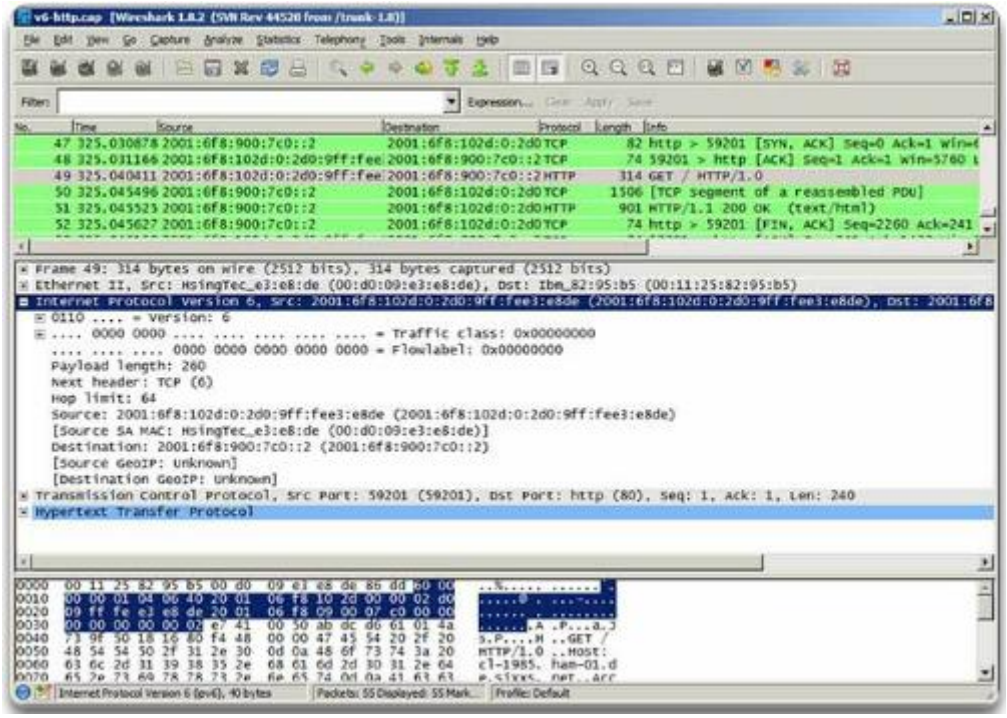
Sur les captures Wireshark IPv6, notez que l'en-tête IPv6 a nettement moins de champs qu'un en-tête IPv4. Cela simplifie l'en-tête IPv6, qui est ainsi plus rapidement traité par les routeurs.

L'adresse IPv6 a elle-même l'air très différente. En raison des adresses IPv6 plus longues (128 bits), le système de notation hexadécimal est utilisé pour simplifier la représentation de l'adresse. Les adresses IPv6 utilisent donc des signes deux-points (:) pour diviser les adresses en groupes de 16 bits.

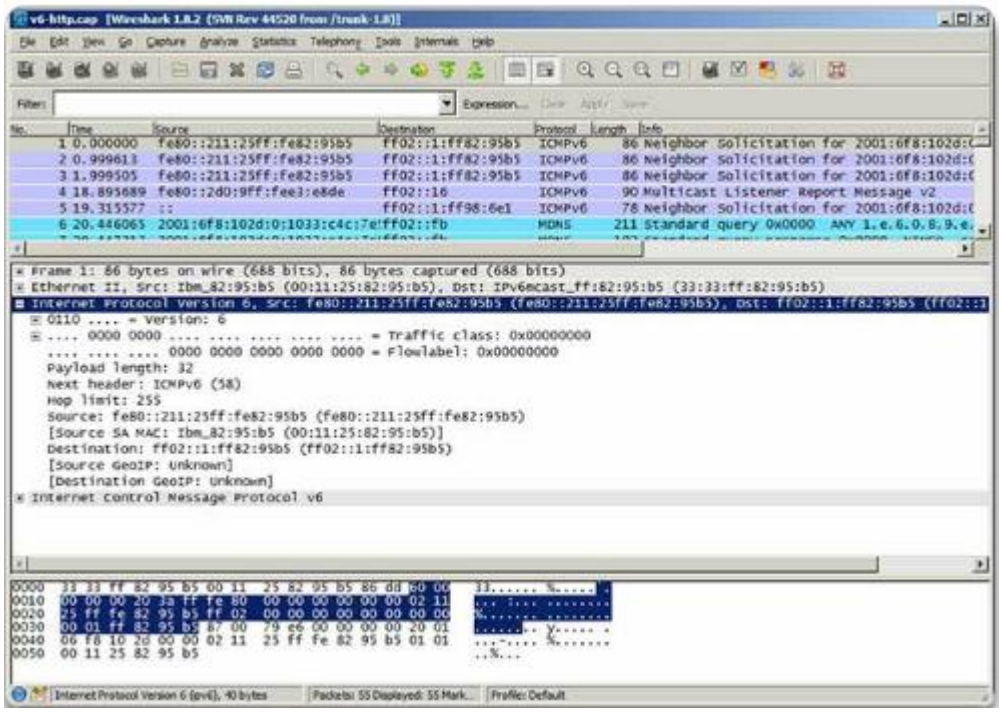
La Figure 1 affiche le contenu du paquet numéro 46 de cet exemple de capture. Le paquet contient le message initial de connexion en trois étapes du protocole TCP entre un hôte IPv6 et un serveur IPv6. Notez les valeurs de la section d'en-tête IPv6 étendue. Notez également qu'il s'agit d'un paquet TCP et qu'il ne contient aucune autre information au-delà de la section TCP.



La Figure 2 affiche le contenu du paquet numéro 49 de cet exemple de capture. Le paquet contient le message HTTP GET destiné au serveur. Notez qu'il s'agit d'un paquet HTTP et qu'il contient désormais des informations au-delà de la section TCP.



Enfin, la Figure 3 illustre le contenu du paquet numéro 1 de cet exemple de capture. Ce paquet est un message de sollicitation de voisin ICMPv6. Notez qu'aucune information TCP ou UDP n'est présente.



6.1.4.6 Exercice - Champs d'en-tête IPv6

Exercice – Champs d'en-tête IPv6

Lisez les descriptions d'en-tête IPv6, puis cliquez sur les champs d'en-tête IPv6 auxquels elles correspondent.

Champs d'en-tête IPv6

Version Est toujours défini sur 0110	**Longueur des données utiles** Indique la taille du fragment de paquet
Classe de trafic Classe les paquets pour le contrôle d'encombrement	**En-tête suivant** Indique le type d'application au protocole de couche supérieure
Étiquetage de flux Peut être configuré pour utiliser le même chemin, de sorte que les paquets ne soient pas réorganisés à la livraison	**Limite de nombre de sauts** Lorsque cette valeur atteint 0, l'expéditeur est averti que le paquet n'a pas été livré

6.2 Routage

6.2.1 Méthode de routage des hôtes

6.2.1.1 Décisions relatives aux transmissions

Méthode de routage des hôtes

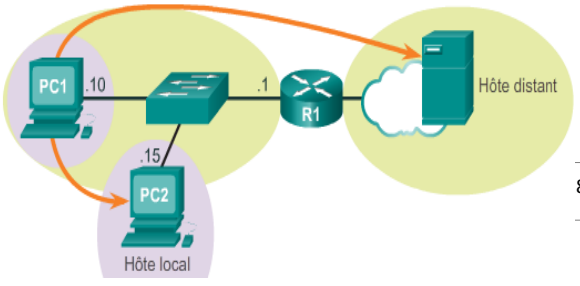
Un autre rôle de la couche réseau est de diriger les paquets entre les hôtes. Un hôte peut envoyer un paquet à :

- **Lui-même** – il s'agit d'une adresse IP spécifique, 127.0.0.1, appelée interface de bouclage. Cette adresse de bouclage est automatiquement attribuée à un hôte lorsque la suite de protocoles TCP/IP s'exécute. La capacité d'un hôte à envoyer un paquet à lui-même grâce à la fonctionnalité réseau est utile à des fins de test. Toute adresse IP appartenant au réseau 127.0.0.0/8 se rapporte à l'hôte local.
- **Un hôte local** – il s'agit d'un hôte sur le même réseau que l'hôte émetteur. Les hôtes partagent la même adresse réseau.
- **Un hôte distant** – il s'agit d'un hôte sur un réseau distant. Les hôtes ne partagent pas la même adresse réseau.

Le fait que le paquet soit destiné à un hôte local ou à un hôte distant est déterminé par la comparaison de la combinaison adresse IP/masque de sous-réseau du périphérique source (expéditeur) à la combinaison adresse IP/masque de sous-réseau du périphérique de destination.

Dans un réseau domestique ou d'entreprise, il peut y avoir plusieurs périphériques filaires et sans fil interconnectés par le biais d'un périphérique intermédiaire tel qu'un commutateur LAN et/ou un point d'accès sans fil (WAP). Ce périphérique intermédiaire permet l'interconnexion entre les hôtes locaux sur le réseau local. Les hôtes locaux peuvent se joindre et partager des informations sans nécessiter de périphériques supplémentaires. Si un hôte envoie un paquet à un périphérique appartenant au même réseau IP, le paquet est simplement transféré à l'interface hôte, par le biais du périphérique intermédiaire, directement au périphérique de destination.

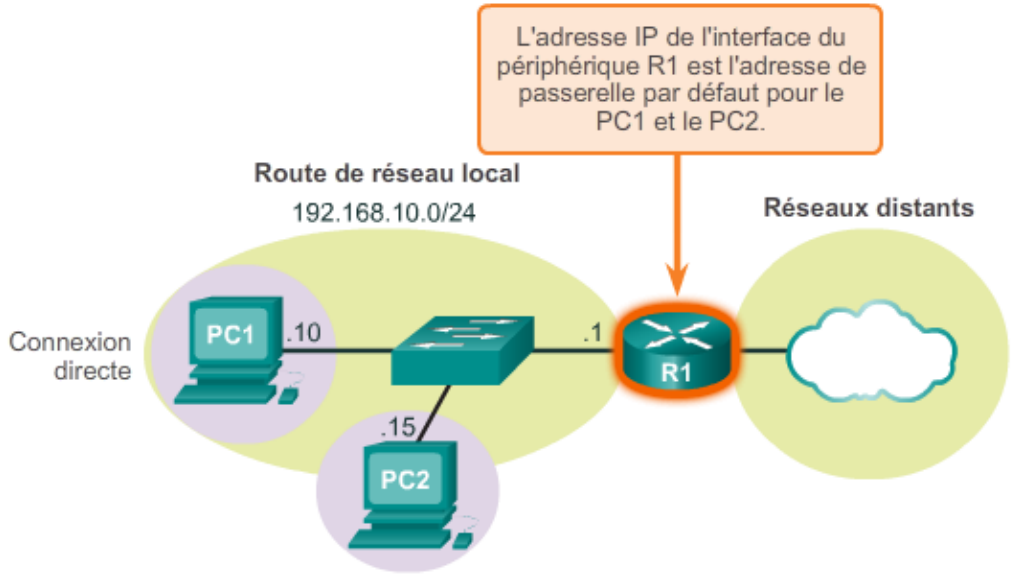
Naturellement, dans la plupart des situations, nous voulons que nos périphériques soient connectés au-delà du segment de réseau local, à d'autres maisons, à d'autres entreprises et à Internet. Les périphériques se trouvant au-delà du segment de réseau local sont appelés hôtes distants. Lorsqu'un périphérique source envoie un paquet à un périphérique de destination distant, alors l'aide des routeurs et le routage sont nécessaires. Le routage est le processus de détermination du meilleur chemin vers une



destination. Le routeur connecté au segment de réseau local est appelé la **passerelle par défaut.**

6.2.1.2 Passerelle par défaut

La passerelle par défaut est le périphérique qui achemine le trafic du réseau local vers des périphériques sur des réseaux distants. Dans un environnement domestique ou de petite entreprise, la passerelle par défaut est souvent utilisée pour connecter le réseau local à Internet.



Si l'hôte envoie un paquet à un périphérique sur un réseau IP différent, il doit faire passer le paquet par le périphérique intermédiaire pour atteindre la passerelle par défaut. Cela est dû au fait qu'un périphérique hôte ne contient pas d'informations de routage concernant les communications destinées aux destinations distantes, situées au-delà du réseau local. La passerelle par défaut, quant à elle, contient ces informations. La passerelle par défaut, qui est le plus souvent un routeur, gère une table de routage. Une table de routage est un fichier de données stocké dans la mémoire vive qui contient des informations de route sur le réseau connecté directement, ainsi que les entrées de réseaux distants que le périphérique a découvertes. Un routeur utilise les informations de la table de routage pour déterminer le meilleur chemin pour atteindre ces destinations.

Comment un hôte peut-il savoir si les paquets doivent être transmis à la passerelle par défaut ? Les hôtes ont également besoin d'une table de routage locale pour s'assurer que les paquets de couche réseau sont dirigés vers le réseau de destination correct. La table locale de l'hôte contient généralement :

- **Connexion directe** – route vers l'interface de bouclage (127.0.0.1).
- **Route de réseau local** – le réseau auquel l'hôte est connecté est automatiquement indiqué dans la table de routage d'hôte.
- **Route locale par défaut** – la route par défaut est la route que les paquets doivent emprunter pour atteindre toutes les adresses sur des réseaux distants. La route par défaut est créée lorsqu'une adresse de passerelle par défaut est présente sur l'hôte. L'adresse de passerelle par défaut est l'adresse IP de l'interface réseau du routeur connecté au réseau local. L'adresse de la passerelle par défaut peut être configurée sur l'hôte manuellement ou de manière dynamique.

Il est important de noter que la route par défaut et, par conséquent, la passerelle par défaut, sont utilisées uniquement lorsqu'un hôte doit transmettre des paquets à un réseau distant. Elles ne sont pas obligatoires, ni même configurées, si les paquets sont uniquement destinés aux périphériques du réseau local.

Prenons l'exemple d'une imprimante multifonction. Si l'imprimante réseau a une adresse IP et un masque de sous-réseau configurés, les hôtes locaux peuvent envoyer des documents à l'imprimante. En outre, l'imprimante peut transférer les documents scannés à tous les hôtes locaux. Tant que l'imprimante n'est utilisée que localement, une adresse de passerelle par défaut n'est pas obligatoire. En fait, si aucune adresse de passerelle par défaut n'est attribuée à l'imprimante, vous bloquez efficacement l'accès à Internet, ce qui peut être un choix judicieux en matière de sécurité. Aucun accès à Internet signifie aucun risque de sécurité. Bien que les périphériques tels que les imprimantes peuvent se mettre à jour automatiquement via Internet, il est généralement plus facile et plus sécurisé d'obtenir les mêmes mises à jour via un téléchargement local (upload) à partir d'un hôte local sécurisé tel qu'un PC.

6.2.1.3 Table de routage d'hôte IPv4

Sur un hôte Windows, les commandes **route print** ou **netstat -r** permettent d'afficher la table de routage d'hôte. Ces deux commandes génèrent le même résultat. Le résultat peut sembler déroutant au début, mais est relativement simple à comprendre.

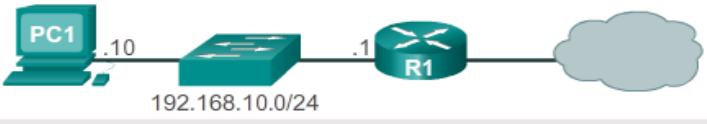
Si vous saisissez la commande **netstat -r** ou la commande **route print** équivalente, trois sections liées aux connexions réseau TCP/IP actuelles s'affichent :

- **Liste des interfaces** – répertorie l'adresse MAC et le numéro d'interface attribués à chaque interface réseau de l'hôte, notamment les adaptateurs Ethernet, Wi-Fi et Bluetooth.

- **Table de route IPv4** – répertorie toutes les routes IPv4 connues, y compris les connexions directes, le réseau local et les routes locales par défaut.

- **Table de route IPv6** – répertorie toutes les routes IPv6 connues, y compris les connexions directes, le réseau local et les routes locales par défaut.

Remarque : les informations affichées varient en fonction de la façon dont l'hôte est configuré et des interfaces de l'hôte.




```
C:\Users\PC1>netstat -r

<Résultat omis>
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.10.1   192.168.10.10     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
     192.168.10.0    255.255.255.0         On-link    192.168.10.10    281
    192.168.10.10  255.255.255.255         On-link    192.168.10.10    281
   192.168.10.255  255.255.255.255         On-link    192.168.10.10    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10    281
===========================================================================
<Résultat omis>
```

La figure ci-contre illustre la section de table de route IPv4. Notez que le résultat est divisé en cinq colonnes :

- **Destination réseau -** affiche la liste des réseaux accessibles.
- **Masque de sous-réseau** – indique un masque de sous-réseau qui indique à l'hôte comment déterminer les parties réseau et hôte de l'adresse IP.
- **Passerelle** – répertorie l'adresse utilisée par l'ordinateur local pour accéder à une destination sur un réseau distant. Si une destination est accessible directement, elle s'affiche comme « on-link » dans cette colonne.
- **Interface** – répertorie l'adresse de l'interface physique utilisée pour envoyer le paquet à la passerelle utilisée pour atteindre la destination réseau.
- **Métrique** – liste le coût de chaque route et est utilisée pour déterminer la meilleure route vers une destination.

6.2.1.4 Entrées de routage d'hôte IPv4

Afin de simplifier les résultats, les réseaux de destination peuvent être regroupés dans cinq sections,


```
C:\Users\PC1> netstat -r

<Résultat omis>

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10      25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1     306
      192.168.10.0    255.255.255.0         On-link    192.168.10.10     281
    192.168.10.10  255.255.255.255         On-link    192.168.10.10     281
    192.168.10.255  255.255.255.255         On-link    192.168.10.10     281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1     306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10     281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1     306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10     281
===========================================================================
<Résultat omis>
```

comme illustré par les zones mises en évidence dans la figure :
0.0.0.0

La route locale par défaut : tous les paquets dont les destinations ne correspondent pas aux autres adresses indiquées dans la table de routage sont transférés vers la passerelle. Par conséquent, toutes les routes de destination ne correspondant pas sont envoyées à la passerelle par le biais de l'adresse IP 192.168.10.1 (R1) et sortent de l'interface avec l'adresse IP 192.168.10.10. Notez que l'adresse de destination finale indiquée dans le paquet reste inchangée. En revanche, l'hôte sait transférer le paquet à la passerelle pour poursuivre le traitement.

127.0.0.0 – 127.255.255.255

Ces adresses de bouclage correspondent toutes à la connexion directe et fournissent des services à l'hôte local.

192.168.10.0 - 192.168.10.255

Ces adresses correspondent toutes à l'hôte et au réseau local. Tous les paquets dont l'adresse de destination appartient à cette catégorie quitteront l'interface 192.168.10.10.

- **192.168.10.0** – adresse de route du réseau local. Représente tous les ordinateurs du réseau 192.168.10.x.
- **192.168.10.10** – adresse de l'hôte local.
- **192.168.10.255** – adresse de diffusion du réseau. Envoie des messages à tous les hôtes sur la route de réseau local.

224.0.0.0

Ces adresses spéciales de multidiffusion (classe D) sont réservées à une utilisation dans l'interface de bouclage (127.0.0.1) ou l'adresse IP d'hôte (192.168.10.10).

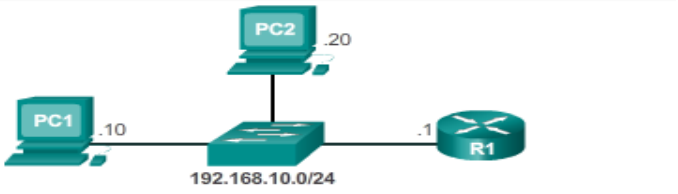
255.255.255.255

Les deux dernières adresses représentent les valeurs de l'adresse IP de diffusion limitée pour une utilisation dans l'interface de bouclage (127.0.0.1) ou l'adresse IP d'hôte (192.168.10.10). Ces adresses peuvent être utilisées pour trouver un serveur DHCP avant que l'adresse IP locale ne soit déterminée.

6.2.1.5 Exemples de table de routage d'hôte IPv4

Par exemple, si le PC1 veut envoyer un paquet à 192.168.10.20, il :

1. Consulte la table de route IPv4.
2. Fait correspondre l'adresse IP de destination avec l'entrée de destination réseau 192.168.10.0 pour indiquer que l'hôte se trouve sur le même réseau (on-link).
3. Le PC1 envoie ensuite le paquet vers la destination finale via son interface locale (192.168.10.10).



La Figure 1 illustre la route correspondante.

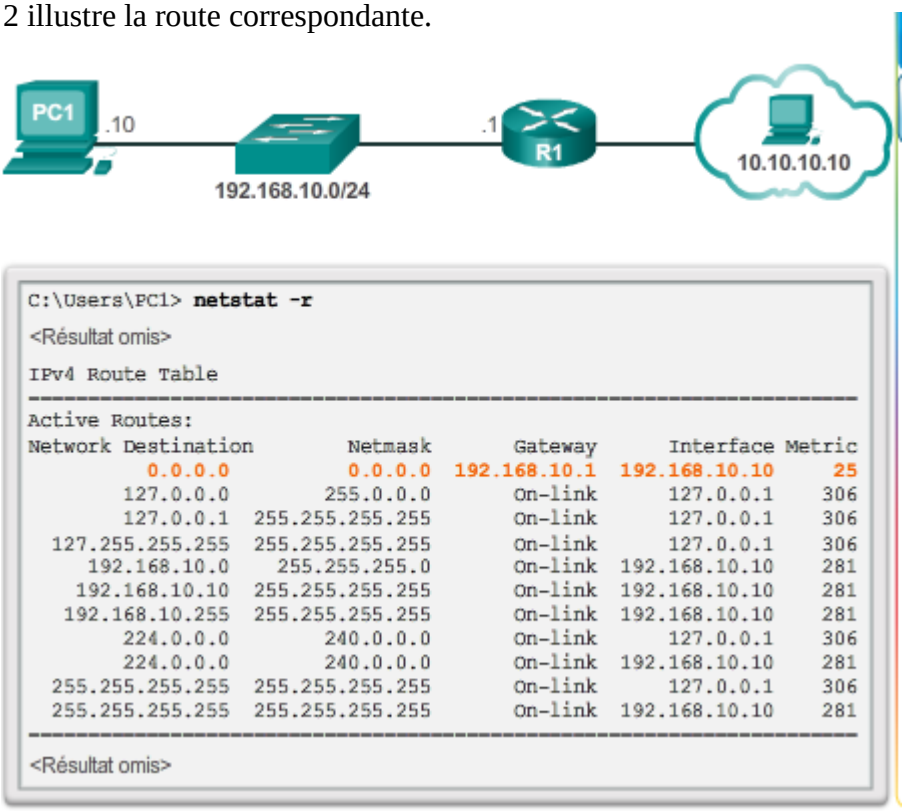
```
C:\Users\PC1> netstat -r
<Résultat omis>
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
    192.168.10.0    255.255.255.0         On-link    192.168.10.10    281
   192.168.10.10  255.255.255.255         On-link    192.168.10.10    281
  192.168.10.255  255.255.255.255         On-link    192.168.10.10    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10    281
===========================================================================
<Résultat omis>
```

Si le PC1 veut envoyer un paquet à un hôte

distant situé à l'adresse 10.10.10.10, il :

1. Consulte la table de route IPv4.
2. Découvre qu'il n'y a aucune correspondance exacte pour l'adresse IP de destination.
3. Choisit la route locale par défaut (0.0.0.0) pour indiquer qu'il doit transférer le paquet à l'adresse de passerelle 192.168.10.1.
4. Le PC1 transmet ensuite le paquet à la passerelle pour utiliser son interface locale (192.168.10.10). Le périphérique passerelle détermine alors le chemin suivant que le paquet doit emprunter pour atteindre l'adresse de destination finale 10.10.10.10.

La Figure 2 illustre la route correspondante.



6.2.1.6 Exemples de table de routage d'hôte IPv6

Le résultat de la table de route IPv6 varie en termes de titres de colonne et de format en raison de la longueur des adresses IPv6.

La section de la table de route IPv6 représente quatre colonnes, qui identifient :

- **Si** – répertorie les numéros d'interface de la section Liste des interfaces de la commande **netstat –r**. Les numéros d'interface correspondent à l'interface réseau sur l'hôte, y compris les adaptateurs Ethernet, Wi-Fi et Bluetooth.

- **Métrique** – liste le coût de chaque route vers une destination. Les numéros les plus petits indiquent les routes privilégiées.

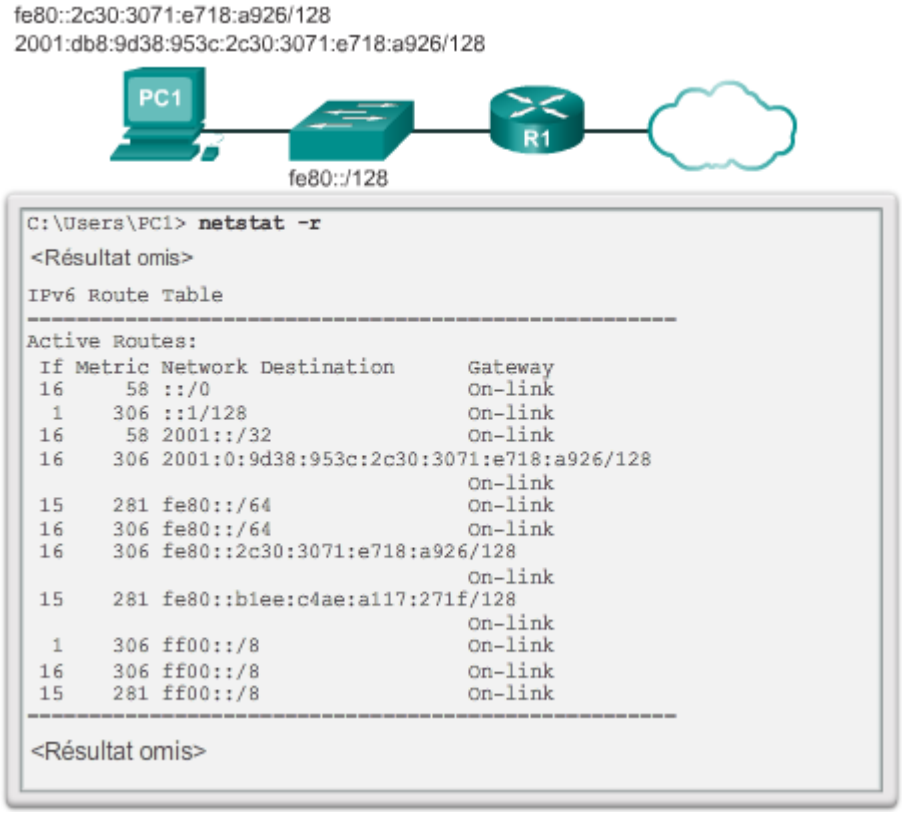
- **Destination réseau** - affiche la liste des réseaux accessibles.

- **Passerelle** – indique l'adresse utilisée par l'hôte local pour transmettre les paquets à une destination sur un réseau distant. On-link indique que l'hôte est actuellement connecté.

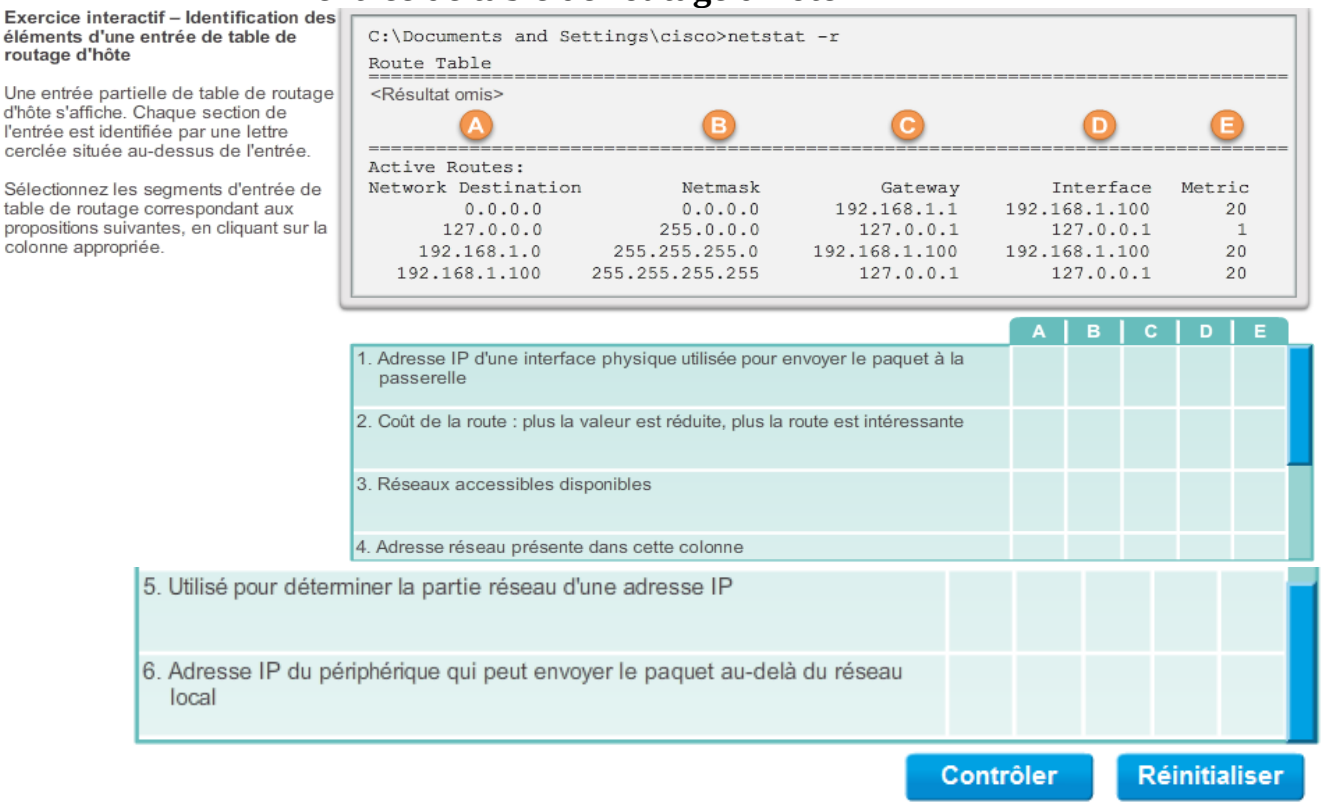
Par exemple, la figure illustre la section de route IPv6 générée par la commande **netstat –r** pour indiquer les destinations réseau suivantes :

- **::/0** – équivalent IPv6 de la route locale par défaut.
- **::1/128** – équivalent de l'adresse de bouclage IPv4. Fournit des services à l'hôte local.
- **2001::/32** – préfixe de réseau de monodiffusion globale.
- **2001:0:9d38:953c:2c30:3071:e718:a926/128** – adresse IPv6 de monodiffusion globale de l'ordinateur local.
- **fe80::/64** – adresse de route réseau de liaison locale. Représente tous les ordinateurs du réseau IPv6 de liaison locale.
- **fe80::2c30:3071:e718:a926/128** : adresse IPv6 link-local de l'ordinateur local.
- **ff00::/8** – adresses spéciales de multidiffusion (classe D) équivalant aux adresses IPv4 224.x.x.x.

Remarque : les interfaces IPv6 ont généralement deux adresses IPv6 – une adresse link-local et une adresse de monodiffusion globale. En outre, notez qu'il n'y a pas d'adresse de diffusion en IPv6. Les adresses IPv6 seront décrites plus en détail dans le chapitre suivant.



6.2.1.7 Exercice - Identification des éléments d'une entrée de table de routage d'hôte



6.2.2 Tables de routage du routeur

6.2.2.1 Décisions relatives à la transmission de paquets du routeur

Tables de routage du routeur

Lorsqu'un hôte envoie un paquet à un autre hôte, il utilise sa table de routage pour déterminer où envoyer le paquet. Si l'hôte de destination se trouve sur un réseau distant, le paquet est transmis à l'adresse d'un périphérique passerelle.

Que se passe-t-il lorsqu'un paquet arrive sur une interface de routeur ? Le routeur consulte sa table de routage pour déterminer où transmettre les paquets.

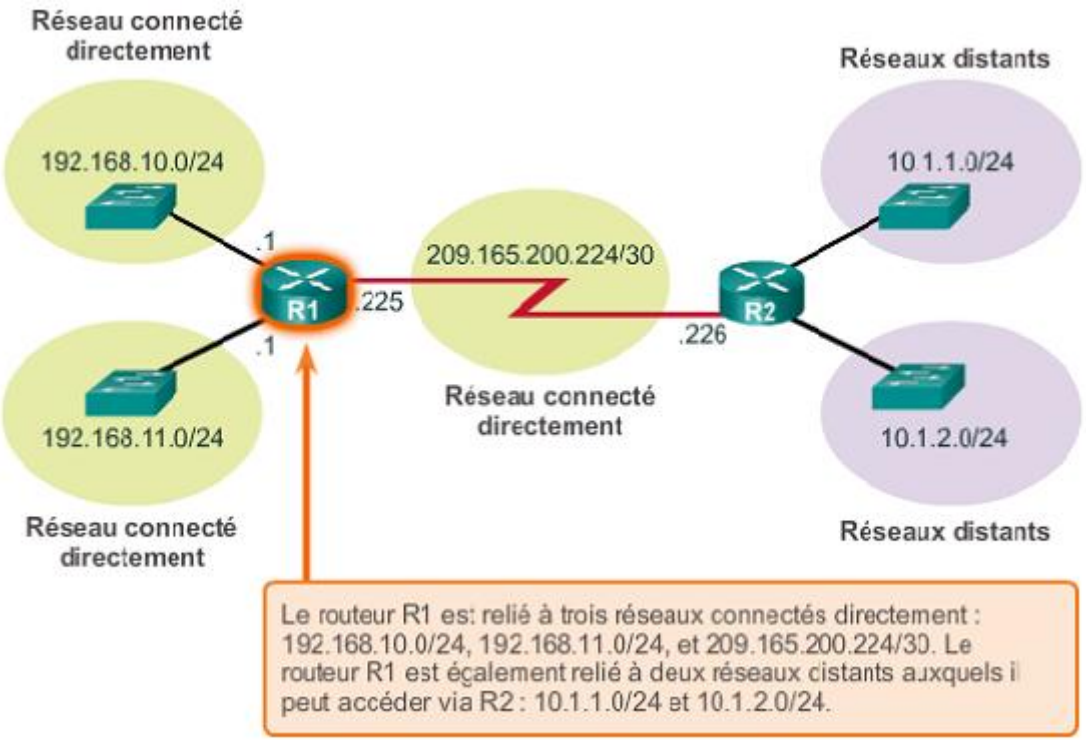
La table de routage d'un routeur stocke des informations sur :

- **Les routes directement connectées** – ces routes proviennent des interfaces actives du routeur. Les routeurs ajoutent une route connectée directement lorsqu'une interface est configurée avec une adresse IP et est activée. Chacune des interfaces du routeur est connectée à un segment de réseau différent. Les routeurs tiennent à jour des informations sur les segments réseau auxquels ils sont connectés dans la table de routage.

- **Routes distantes** – ces routes correspondent aux réseaux distants connectés à d'autres routeurs. Les routes vers ces réseaux peuvent être configurées manuellement sur le routeur local par l'administrateur réseau ou être configurées de manière dynamique en

permettant au routeur local d'échanger des informations de routage avec d'autres routeurs en utilisant des protocoles de routage dynamique.

La figure identifie les réseaux connectés directement et les réseaux distants du routeur R1.



6.2.2.2 Table de routage d'un routeur IPv4

Une table de routage d'hôte ne contient que les informations sur les réseaux directement connectés. Un hôte nécessite une passerelle par défaut pour envoyer des paquets vers une destination distante. La table de routage d'un routeur contient des informations similaires mais peut également identifier des réseaux distants spécifiques.

La table de routage d'un routeur est similaire à la table de routage d'un hôte. En effet, ces deux tables de routage indiquent :

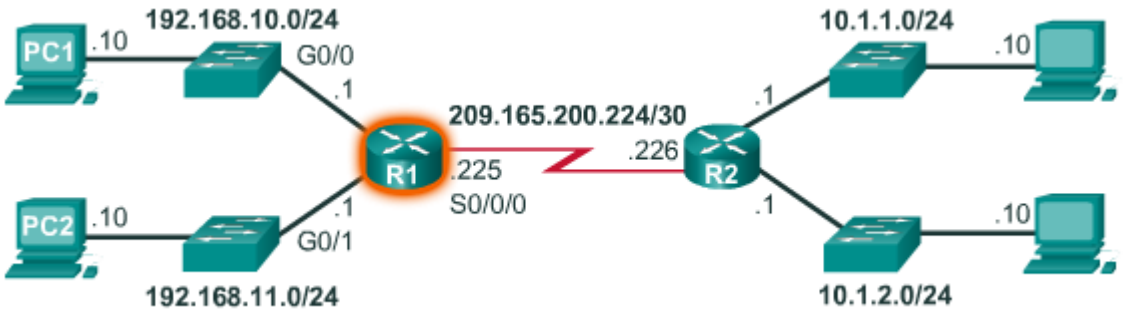
- Réseau de destination
- la métrique associée au réseau de destination ;
- la passerelle permettant d'atteindre le réseau de destination.

Sur un routeur Cisco IOS, la commande **show ip route** peut être utilisée pour afficher la table de routage de routeur. Un routeur fournit également des informations de routage supplémentaires, notamment comment la route a été découverte, la date de la dernière mise à jour et l'interface spécifique à utiliser pour atteindre une destination prédéfinie.

Lorsqu'un paquet arrive sur l'interface de routeur, le routeur examine l'en-tête du paquet pour déterminer le réseau de destination. Si le réseau de destination correspond à une route dans la table de routage, le routeur transfère le paquet en utilisant les informations indiquées dans la

table de routage. Si plusieurs routes sont possibles pour la même destination, la métrique est utilisée pour décider de la route qui apparaît dans la table de routage.

La figure ci-contre illustre la table de routage du périphérique R1 dans un réseau simple. Contrairement à la table de routage d'hôte, il n'y a pas dans cette table de titre de colonne identifiant les informations contenues dans une entrée de table de routage. Par conséquent, il est important d'apprendre la signification des différents types d'informations inclus dans chaque entrée.




```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
        Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
L       192.168.11.1/32 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

6.2.2.3 Entrées de table de routage d'un réseau connecté directement

Deux entrées de table de routage sont automatiquement créées lorsqu'une interface de routeur active comporte une adresse IP et un masque de sous-réseau. La figure affiche les entrées de

la table de routage sur R1 pour le réseau connecté directement 192.168.10.0. Ces entrées ont été automatiquement ajoutées à la table de routage lorsque l'interface GigabitEthernet 0/0 a été configurée et activée. Les rapports contiennent les informations suivantes :

Origine de la route

La source de la route est appelée « A » sur la figure. Elle indique comment la route a été découverte. Les interfaces connectées directement ont deux codes d'origine de la route.

- **C** – signale un réseau connecté directement. Les réseaux connectés directement sont automatiquement créés lorsqu'une interface est configurée avec une adresse IP et activée.
- **L** – indique qu'il s'agit d'une route link-local. Les routes link-local sont automatiquement créées lorsqu'une interface est configurée avec une adresse IP et activée.

Réseau de destination

Le réseau de destination est appelé « B » sur la figure. Il identifie l'adresse du réseau distant.

Interface de sortie :

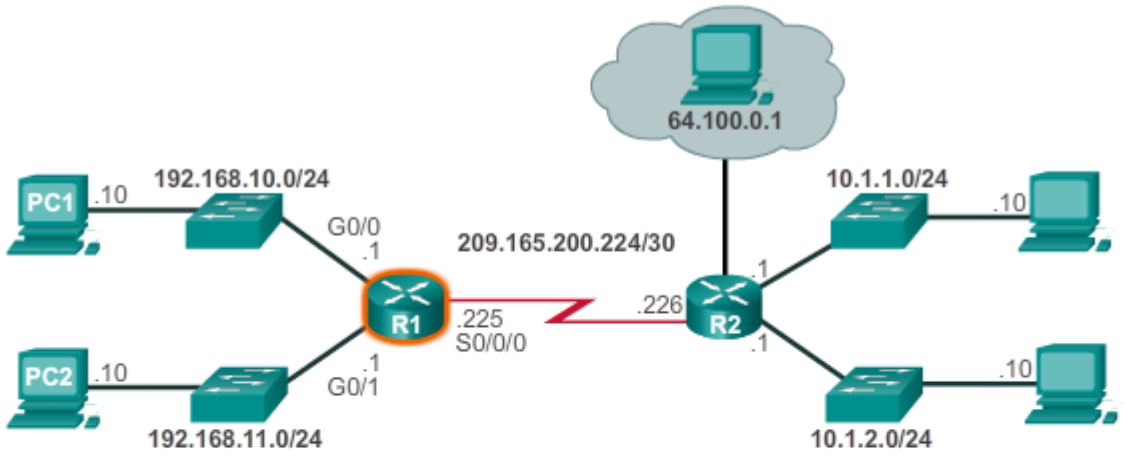
L'interface de sortie est appelée « C » sur la figure. Elle identifie l'interface de sortie à utiliser lors de la transmission des paquets au réseau de destination.

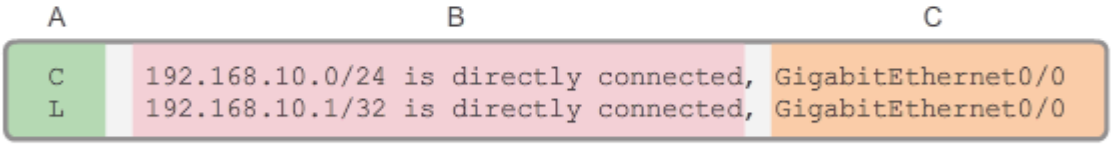
Remarque : les entrées de la table de routage link-local ne sont pas apparues dans les tables de routage avant la version 15 d'IOS.

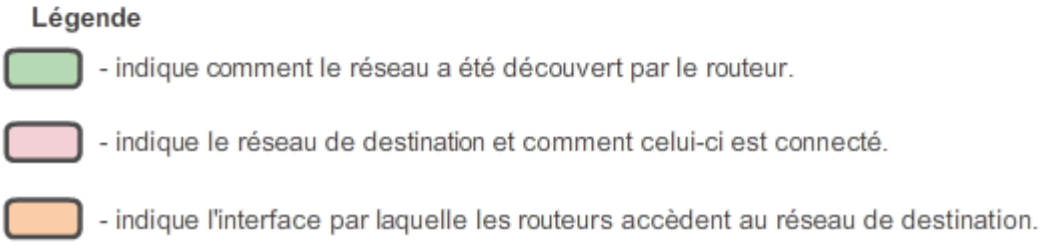
Un routeur comporte généralement plusieurs interfaces configurées. La table de routage stocke des informations sur les routes directement connectées et les routes distantes. Comme avec les réseaux connectés directement, la source de la route indique comment la route a été découverte. Par exemple, les codes courants des réseaux distants sont les suivants :

- **S** – indique que la route a été créée manuellement par un administrateur pour atteindre un réseau spécifique. Il s'agit d'une route statique.
- **D** – indique que la route a été découverte dynamiquement à partir d'un autre routeur à l'aide du protocole EIGRP (Enhanced Interior Gateway Routing Protocol).
- **O** – indique que la route a été découverte dynamiquement à partir d'un autre routeur à l'aide du protocole OSPF (Open Shortest Path First).

Remarque : certains des codes ne sont pas abordés dans ce chapitre.



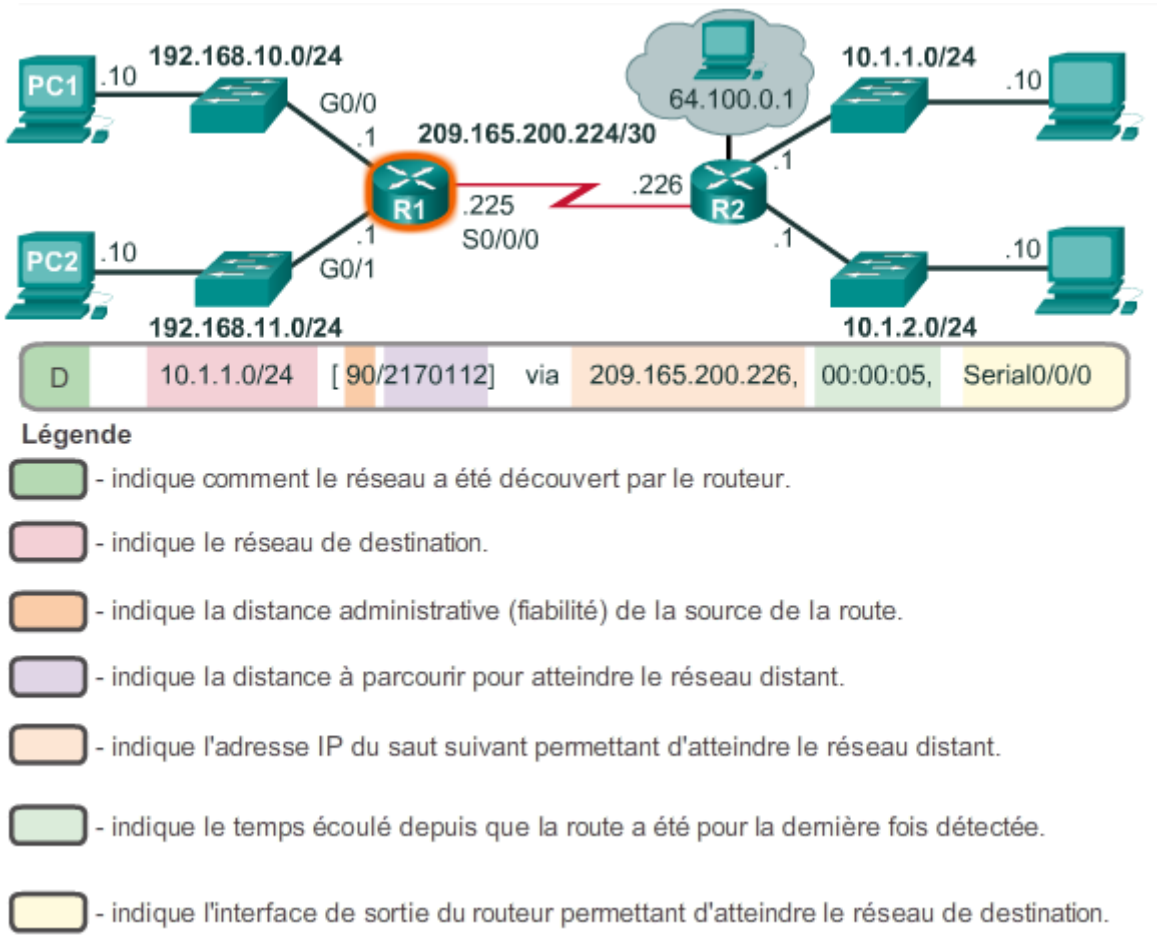




6.2.2.4 Entrées de table de routage d'un réseau distant

La figure ci-contre illustre une entrée de table de routage sur le périphérique R1, pour la route vers le réseau distant 10.1.1.0. L'entrée identifie les informations suivantes :

- **Source de la route** – indique comment la route a été découverte.
- **Réseau de destination** – indique l'adresse du réseau distant.
- **Distance administrative** – indique la fiabilité de la source de la route.
- **Métrique** – indique la valeur attribuée pour atteindre le réseau distant. Les valeurs inférieures indiquent les routes préférées.
- **Saut suivant** – indique l'adresse IP du prochain routeur à transférer le paquet.
- **Horodatage de route** – détermine à quel moment la route a été détectée pour la dernière fois.
- **Interface de sortie** – indique l'interface de sortie à utiliser pour acheminer un paquet vers la destination finale.



6.2.2.5 Adresse du tronçon suivant

Le saut suivant est l'adresse du prochain périphérique à traiter le paquet. Pour un hôte sur un réseau, l'adresse de la passerelle par défaut (interface de routeur) est le saut suivant pour tous les paquets destinés à un autre réseau. Dans la table de routage d'un routeur, chaque route vers un réseau distant indique le saut suivant.

Lorsqu'un paquet destiné à un réseau distant arrive au niveau du routeur, ce dernier compare le réseau de destination à une route de la table de routage. Si une correspondance est trouvée, le routeur transfère le paquet à l'adresse IP du routeur du saut suivant à l'aide de l'interface indiquée par l'entrée de route.

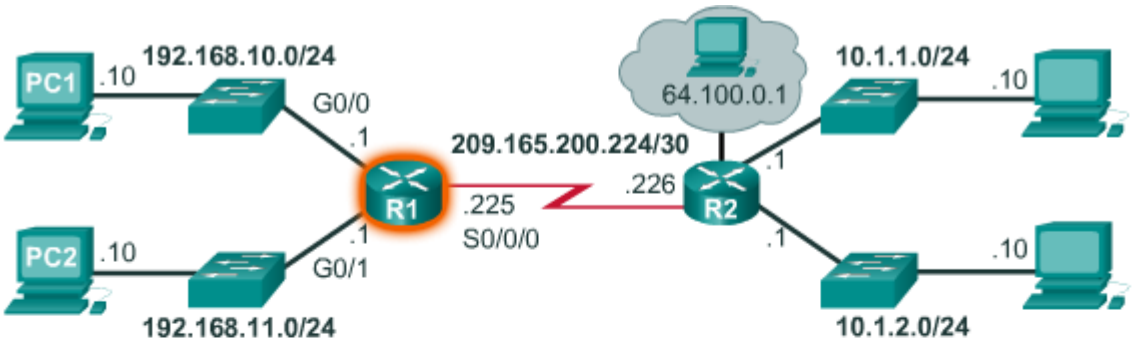
Un routeur de saut suivant est la passerelle vers les réseaux distants.

Par exemple, dans la figure, un paquet arrivant au périphérique R1 et destiné au réseau 10.1.1.0 ou 10.1.2.0 est transféré à l'adresse de saut suivant, 209.165.200.226, par le biais de l'interface série 0/0/0.

Les réseaux directement connectés à un routeur n'ont pas d'adresse de saut suivant, car un routeur peut transférer des paquets directement aux hôtes sur ces réseaux via l'interface indiquée.

Les paquets ne peuvent pas être acheminés par le routeur sans route pour le réseau de destination dans la table de routage. Si une route représentant le réseau de destination ne figure pas dans la table de routage, le paquet est abandonné (non transféré).

Toutefois, tout comme un hôte peut utiliser une passerelle par défaut pour transférer un paquet vers une destination inconnue, un routeur peut également être configuré pour utiliser une route statique par défaut pour créer une passerelle de dernier recours. La passerelle de dernier recours est traitée plus en détail dans le cours CCNA sur le routage.




```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
       B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
        Serial0/0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
        Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
L       192.168.11.1/32 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.225/32 is directly connected, Serial0/0/0
```

6.2.2.6 Exemples de table de routage d'un routeur IPv4

Supposons que le PC1 avec l'adresse IP 192.168.10.10 souhaite envoyer un paquet à un autre hôte sur le même réseau. Le PC1 vérifie la table de route IPv4 en fonction de l'adresse IP de destination. Ensuite, le PC1 détecte que l'hôte se trouve sur le même réseau et l'envoie simplement hors de son interface (on-link).

Remarque : le périphérique R1 n'est pas impliqué dans le transfert du paquet. Si le PC1 transfère un paquet à un réseau autre que son réseau local, il doit utiliser les services du routeur R1 et transférer le paquet à la route locale par défaut (192.168.10.1).

Les exemples suivants illustrent comment un hôte et un routeur prennent des décisions de routage de paquets en consultant leurs tables de routage respectives :

Exemple 1 : le PC1 souhaite vérifier la connectivité à sa passerelle locale par défaut à l'adresse 192.168.10.1 (l'interface du routeur) :

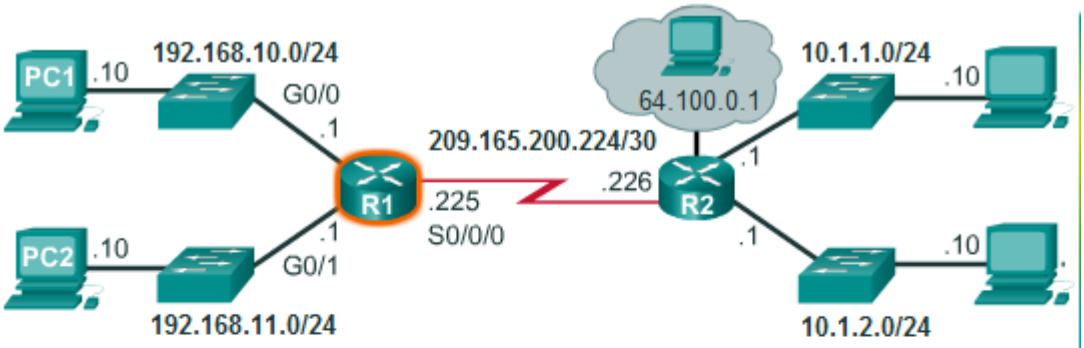
1. Le PC1 vérifie la table de route IPv4 en fonction de l'adresse IP de destination.

2. Le PC1 détecte que l'hôte se trouve sur le même réseau et envoie simplement un paquet de requête ping hors de son interface (on-link).

3. Le périphérique R1 reçoit le paquet sur son interface gigabit ethernet 0/0 (G0/0) et recherche l'adresse IP de destination.

4. Le périphérique R1 consulte sa table de routage

5. Il fait correspondre l'adresse IP de destination à l'entrée de table de routage **L 192.168.10.1/32** et découvre que cette route pointe vers sa propre interface locale, comme illustré à la Figure 1.




```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
       B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2170112] via 209.165.200.226, 01:13:55,
        Serial0/0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.226, 01:13:55,
        Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
L       192.168.11.1/32 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.225/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.200.226
```

Fg1

6. Le périphérique R1 affiche le reste du paquet IP et réagit en conséquence.

Exemple 2 : le PC1 souhaite envoyer un paquet au PC2 (192.168.11.10) :

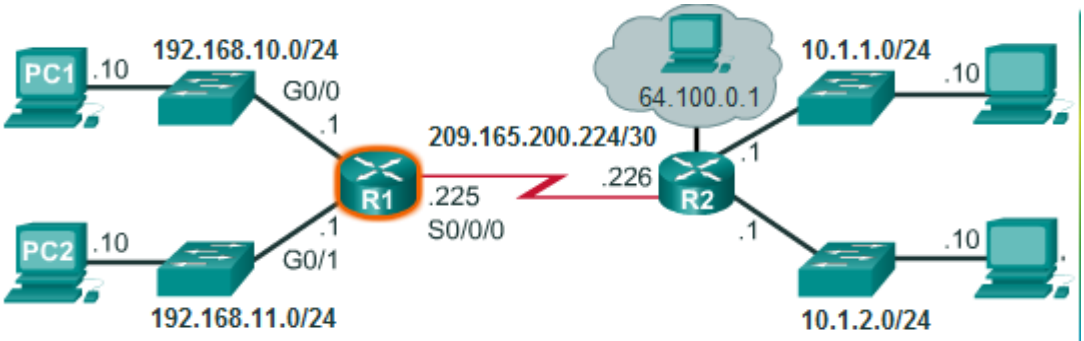
1. Le PC1 consulte la table de route IPv4 et découvre qu'il n'existe pas de correspondance exacte.

2. Le PC1 utilise par conséquent le réseau de toutes les routes (0.0.0.0) et envoie le paquet via la route locale par défaut (192.168.10.1).

3. Le périphérique R1 reçoit le paquet sur son interface gigabit ethernet 0/0 (G0/0) et recherche l'adresse IP de destination (192.168.11.10).

4. Le périphérique R1 consulte sa table de routage et fait correspondre l'adresse IP de destination à l'entrée de table de routage **C 192.168.11.0/24**,

Comme illustré à la Figure 2.




```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
       B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2170112] via 209.165.200.226, 01:13:55,
        Serial0/0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.226, 01:13:55,
        Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
L       192.168.11.1/32 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.225/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.200.226
```

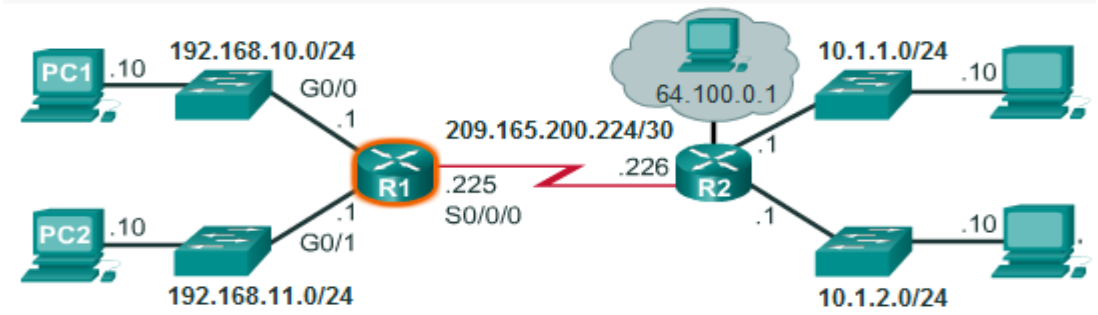
5. Le périphérique R1 transmet le paquet hors de son interface gigabit ethernet 0/1 directement connectée (G0/1).
6. Le PC2 reçoit le paquet et consulte sa table de routage d'hôte IPv4.

7. Le PC2 détecte que le paquet lui est adressé, ouvre le reste du paquet et réagit en conséquence.

Exemple 3 : le PC1 souhaite envoyer un paquet à 209.165.200.226 :

1. Le PC1 consulte la table de route IPv4 et découvre qu'il n'existe pas de correspondance exacte.
2. Le PC1 utilise par conséquent la route par défaut (0.0.0.0/0) et transfère le paquet via la passerelle par défaut (192.168.10.1).
3. Le périphérique R1 reçoit le paquet sur son interface gigabit ethernet 0/0 (G0/0) et recherche l'adresse IP de destination (209.165.200.226).
4. Le périphérique R1 consulte sa table de routage et fait correspondre l'adresse IP de destination à l'entrée de table de routage **C 209.165.200.224/30**,

Comme illustré à la Figure 3.




```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
       B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2170112] via 209.165.200.226, 01:13:55,
        Serial0/0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.226, 01:13:55,
        Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
L       192.168.11.1/32 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.225/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.200.226
```

5. Le routeur R1 transmet le paquet hors de son interface série 0/0/0 (S0/0/0) connectée directement.

Exemple 4 : le PC1 souhaite envoyer un paquet à l'hôte avec l'adresse IP 10.1.1.10 :

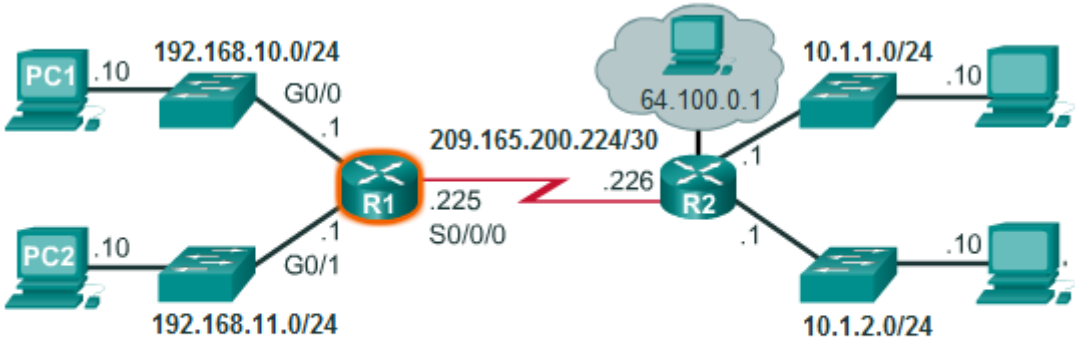
1. Le PC1 consulte la table de route IPv4 et découvre qu'il n'existe pas de correspondance exacte.

2. Le PC1 utilise par conséquent le réseau de toutes les routes (0.0.0.0) et envoie le paquet via la route locale par défaut (192.168.10.1).

3. Le périphérique R1 reçoit le paquet sur son interface gigabit ethernet 0/0 (G0/0) et recherche l'adresse IP de destination (10.1.1.10).

4. Le périphérique R1 consulte sa table de routage et fait correspondre l'adresse IP de destination à l'entrée de table de routage **D 10.1.1.0/24**,

comme illustré à la Figure 4.




```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
       B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
```

```
D       10.1.1.0/24 [90/2170112] via 209.165.200.226, 01:13:55,
        Serial0/0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.226, 01:13:55,
        Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
L       192.168.11.1/32 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.225/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.200.226
```

5. Le périphérique R1 détecte qu'il doit envoyer le paquet à l'adresse de saut suivant 209.165.200.226.

6. Le périphérique R1 consulte sa table de routage et fait correspondre l'adresse IP de destination à l'entrée de table de routage **C 209.165.200.224/30**, comme illustré à la Figure 4.

7. Le routeur R1 transmet le paquet hors de son interface série 0/0/0 (S0/0/0) connectée directement.

6.2.2.7 Exercice – Identification des éléments d'une entrée de table de routage de routeur

Exercice – Identification des éléments d'une entrée de table de routage de routeur

Une entrée partielle de la table de routage d'un **routeur** s'affiche. Chaque section de l'entrée est identifiée par une lettre cerclée située au-dessus de l'entrée.

Sélectionnez la section d'entrée de table de routage appropriée pour chaque proposition.

```
A     B                C           D                  E          F
D     192.168.1.0/24   [90/3072]   via 192.168.3.1,   00:06:03,  GigabitEthernet0/0
```

	A	B	C	D	E	F
1. Temps écoulé depuis que le réseau a été découvert						
2. Distance administrative (source) et distance à parcourir pour atteindre le réseau distant						
3. Manière dont le réseau a été découvert par le routeur						
4. Affiche le réseau de destination						
5. Adresse IP du saut suivant permettant d'atteindre le réseau distant						
6. Interface de sortie du routeur permettant d'atteindre le réseau de destination						

6.2.2.8 Travaux pratiques – Affichage des tables de routage d'hôte

Au cours de ce TP, vous aborderez les points suivants :

- 1re partie : Accéder à la table de routage d'hôte
- 2e partie : Analyser les entrées de table de routage d'hôte IPv4
- 3e partie : Analyser les entrées de table de routage d'hôte IPv6

Travaux pratiques – Affichage des tables de routage d'hôte

6.3 Routeurs

6.3.1 Composants d'un routeur

6.3.1.1 Un routeur est un ordinateur Routeurs

Il existe de nombreux types de routeur d'infrastructure. En fait, les routeurs Cisco sont conçus pour répondre aux besoins suivants :

- **Filiales –** télétravailleurs, PME et filiales de taille moyenne. Inclut les routeurs à services intégrés Cisco 800, 1900, 2900 et 3900 G2 (2e génération).
- **WAN –** grandes entreprises et organisations. Inclut les commutateurs de la gamme Cisco Catalyst 6500 et le routeur ASR (Aggregation Service Router) Cisco 1000.
- **Fournisseurs de services –** fournisseurs de services importants. Inclut les routeurs Cisco ASR 1000 et 9000, Cisco XR 12000, Cisco CRS-3 (Carrier Routing System) et les routeurs de la gamme 7600.

La certification CCNA se concentre sur les routeurs destinés aux filiales. La figure ci-contre présente la gamme G2 de routeurs à services intégrés Cisco 1900, 2900 et 3900.

Quelles que soient leur fonction, leur taille et leur complexité, tous les modèles de routeur sont en fait des ordinateurs. Tout comme les ordinateurs, les tablettes et les périphériques connectés, les routeurs nécessitent également :

- des systèmes d'exploitation ;
- des processeurs ;
- de la mémoire vive ;
- de la mémoire morte.

Un routeur dispose également d'une mémoire spécifique, qui inclut de la mémoire Flash et de la mémoire vive non volatile.

6.3.1.2 Processeur et système d'exploitation d'un routeur

Comme tous les ordinateurs, tablettes, et périphériques connectés, les périphériques Cisco nécessitent un processeur pour exécuter les instructions des systèmes d'exploitation, telles que l'initialisation du système, les fonctions de routage et les fonctions de commutation.

Le processeur nécessite un système d'exploitation pour fournir des fonctions de routage et de commutation. Cisco IOS est le logiciel système utilisé pour la plupart des périphériques Cisco, indépendamment de leur taille et de leur type. Ce logiciel est par exemple utilisé pour des routeurs, des commutateurs de réseau local, des petits points d'accès sans fil, des grands routeurs dotés de dizaines d'interfaces et bien d'autres périphériques.

Le composant en surbrillance dans la figure est le processeur d'un routeur Cisco 1941 équipé d'un dissipateur thermique.

6.3.1.3 Mémoire des routeurs

Un routeur a accès à quatre types de mémoire : vive, morte, vive non volatile et Flash.

Mémoire vive (RAM)

La mémoire vive est utilisée pour stocker divers processus et applications, notamment les suivants :

- **Cisco IOS** – l'IOS est copié dans la mémoire vive pendant le démarrage.
- **Fichier de configuration en cours** – il s'agit du fichier de configuration qui stocke les commandes de configuration actuellement utilisées par l'IOS du routeur. On parle également de « running-config ».
- **Table de routage IP** – ce fichier stocke des informations sur les réseaux directement connectés et distants. Il permet de déterminer le meilleur chemin à utiliser pour transférer des paquets.
- **Cache ARP** – ce cache contient les mappages adresses IPv4/adresses MAC, de la même manière que le cache ARP d'un PC. Le cache ARP est utilisé sur les routeurs dotés d'interfaces de réseau local telles que les interfaces Ethernet.

- **Mémoire tampon de paquets** – les paquets sont stockés temporairement dans une mémoire tampon lors de leur réception sur une interface ou avant de quitter une interface.

Tout comme des ordinateurs, les routeurs Cisco utilisent en fait de la mémoire vive dynamique (DRAM). La mémoire DRAM est un type très répandu de mémoire vive, qui stocke les instructions et les données requises par le processeur. Contrairement à la mémoire morte, la mémoire vive est une mémoire volatile et nécessite une alimentation continue pour conserver les informations qu'elle contient. Elle perd tout son contenu lorsque le routeur est mis hors tension ou redémarré.

Par défaut, les routeurs 1941 sont fournis avec 512 Mo de mémoire DRAM, soudés sur la carte système principale (intégrés) et un module DIMM pour les mises à niveau de mémoire (jusqu'à 2 Go supplémentaires). Les modèles Cisco 2901, 2911 et 2921 sont fournis avec 512 Mo de mémoire DRAM intégrés. Notez que la première génération de routeurs à services intégrés et que les routeurs Cisco plus anciens ne possèdent pas de mémoire vive intégrée.

ROM

Les routeurs Cisco utilisent la mémoire morte pour stocker :

- **les instructions de démarrage** – contiennent les instructions de démarrage.
- **le logiciel de diagnostic de base** – effectue un test POST de tous les composants.
- **un IOS limité** – version de sauvegarde limitée du système d'exploitation, au cas où le routeur ne puisse pas charger l'IOS complet.

La mémoire morte contient un firmware inclus dans un circuit intégré du routeur et ne perd pas son contenu lorsque le routeur est mis hors tension ou redémarré.

NVRAM

La mémoire vive non volatile est utilisée par Cisco IOS comme stockage permanent pour le fichier de configuration initiale (startup-config). Tout comme la mémoire morte, la mémoire vive non volatile ne perd pas son contenu lors de la mise hors tension du périphérique.

Mémoire Flash

La mémoire Flash est une mémoire non volatile utilisée comme stockage permanent pour l'IOS et d'autres fichiers associés au système. L'IOS est copié de la mémoire Flash vers la mémoire vive lors du processus de démarrage.

Les routeurs Cisco 1941 sont livrés avec deux slots CompactFlash externes. Chacun d'eux peut prendre en charge des densités de stockage haut débit pouvant être mises à niveau jusqu'à un maximum de 4 Go.

La figure ci-contre présente les quatre types de mémoire

Mémoire	Volatile/Non volatile	Données stockées
Mémoire vive (RAM)	Volatile	• Exécution de l'autotest à la mise sous tension (IOS) • Fichier de configuration en cours • TablesARP et de routageIP • Mémoire tampon de paquets
ROM	Non volatile	• Instructions de démarrage • un logiciel de diagnostic de base; • IOS limitée
NVRAM	Non volatile	• Fichier de configuration initiale
Flash	Non volatile	• IOS • Autres fichiers système

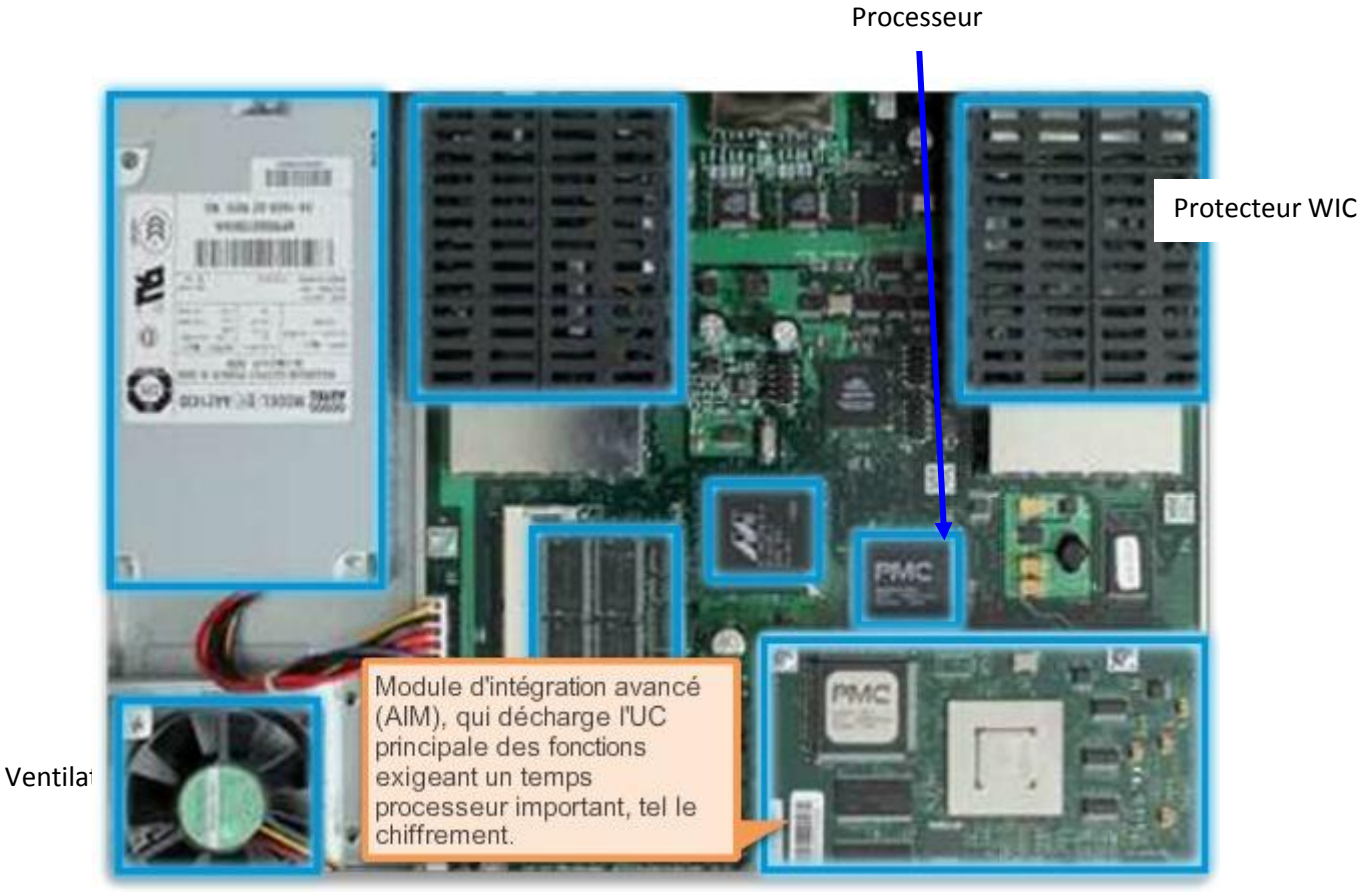
6.3.1.4 À l'intérieur d'un routeur

Bien qu'il existe plusieurs types et modèles de routeurs, chacun comporte, à la base, les mêmes composants matériels.

La figure ci-contre présente l'intérieur d'un routeur à services intégrés Cisco 1841 de première génération. Cliquez sur les composants pour afficher une brève description.

Notez que la figure illustre également les autres composants présents dans un routeur, tels que l'alimentation, le ventilateur de refroidissement, les protections thermiques et le module d'intégration avancé (AIM), qui ne sont pas abordés dans ce chapitre.

Remarque : un professionnel des réseaux doit connaître et comprendre le fonctionnement des principaux composants internes d'un routeur, plutôt que de connaître l'emplacement exact de ces composants. Selon le modèle, ces composants se trouvent à différents emplacements dans le routeur.



Ventila

6.3.1.5 Fond de panier de routeur

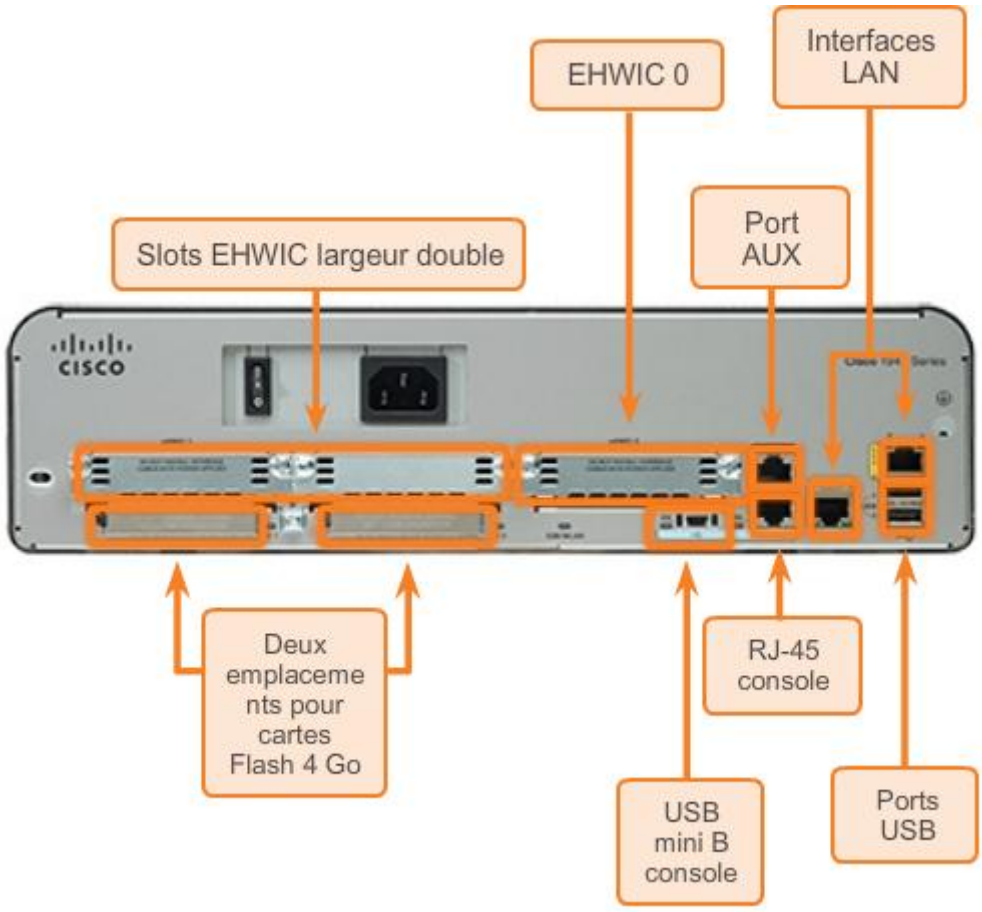
Un routeur Cisco 1941 comprend les connexions suivantes :

- **Ports de console** – deux ports de console pour la configuration initiale et l'accès à l'interface de ligne de commande (CLI) via un port RJ-45 standard et un nouveau connecteur USB de type B (USB mini B).
- **Port AUX** – un port RJ-45 pour la gestion à distance, similaire au port de console.
- **Deux interfaces LAN** – deux interfaces gigabit ethernet pour l'accès au réseau local.
- **Slots EHWIC (carte d'interface WAN haut débit avancée)** – deux slots qui fournissent modularité et flexibilité en permettant au routeur de prendre en charge différents types de module d'interface, y compris la connexion série, la DSL, le port de commutateur et le sans fil.

Le routeur à services intégrés Cisco 1941 est également équipé de slots pour que sa capacité puisse être augmentée. Les deux slots de mémoire CompactFlash sont capables de prendre en charge des cartes CompactFlash de 4 Go chacune pour augmenter l'espace de stockage. Deux ports hôtes USB sont inclus pour permettre l'augmentation de l'espace de stockage et de le sécuriser à l'aide de la fonctionnalité de jeton.

Une carte CompactFlash permet de stocker l'image du logiciel Cisco IOS, les fichiers logs, les fichiers de configuration vocale, les fichiers HTML, les sauvegardes de configuration, ou d'autres fichiers requis pour le système. Par défaut, seul le slot 0 est équipé en usine d'une carte CompactFlash et constitue l'emplacement de démarrage par défaut.

La figure ci-contre indique l'emplacement de ces connexions et slots.



6.3.1.6 Connexion à un routeur

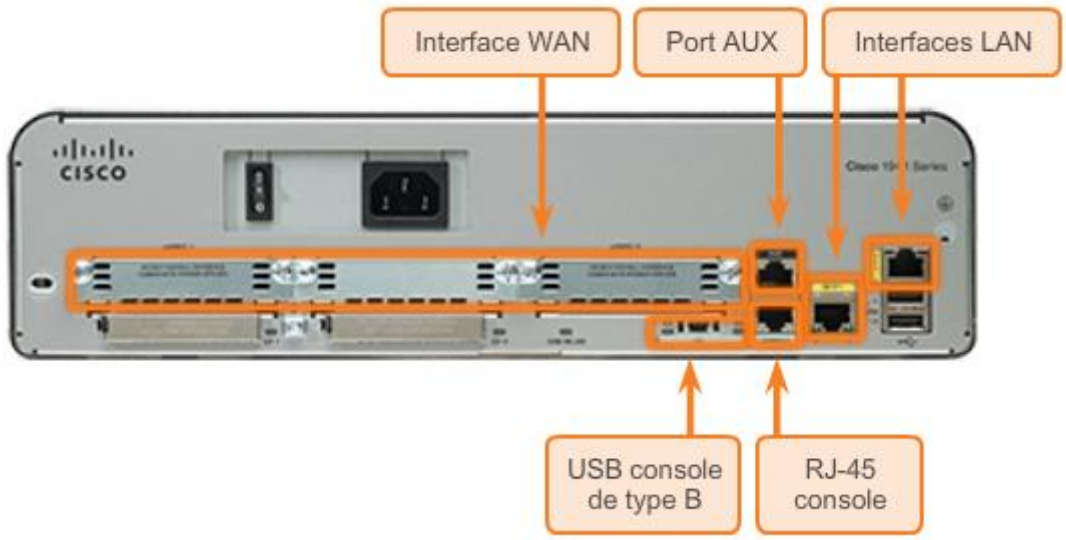
Les périphériques, routeurs et commutateurs Cisco interconnectent généralement de nombreux périphériques. Pour cette raison, ces périphériques possèdent plusieurs types de port et d'interface. Ces ports et interfaces sont utilisés pour connecter des câbles aux périphériques.

Les connexions sur un routeur Cisco peuvent être regroupées en deux catégories :

- **Ports de gestion** – ports de console et auxiliaire utilisés pour configurer, gérer et dépanner le routeur. Contrairement aux interfaces LAN et WAN, les ports de gestion ne sont pas utilisés pour le transfert de paquets.
- **Interfaces inband de routeur** – interfaces LAN et WAN configurées via l'adressage IP pour transporter le trafic. Les interfaces Ethernet sont les connexions LAN les plus courantes, tandis que les connexions WAN les plus répandues sont les interfaces série et DSL.

La figure illustre les ports et les interfaces d'un routeur à services intégrés Cisco 1941 G2.

Comme de nombreux périphériques réseau, les périphériques Cisco utilisent des LED pour fournir des informations d'état. Une LED indique l'activité de l'interface correspondante. Si une LED est éteinte alors que l'interface est active et correctement connectée, cela peut indiquer un problème avec cette interface. Si une interface est très occupée, sa LED reste toujours allumée.



6.3.1.7 Interfaces LAN et WAN

Tout comme pour un commutateur Cisco, il existe plusieurs moyens d'accéder à la CLI d'un routeur Cisco. Voici les méthodes les plus répandues :

- **Console** – utilise une connexion USB ou série à bas débit pour fournir un accès direct hors réseau pour gérer un périphérique Cisco.
- **Telnet ou SSH** – deux méthodes d'accès distant à une session CLI via une interface réseau active.
- **Port AUX** – utilisé pour la gestion à distance d'un routeur à l'aide d'une ligne téléphonique et d'un modem.

Les ports de console et auxiliaire sont situés sur le routeur.

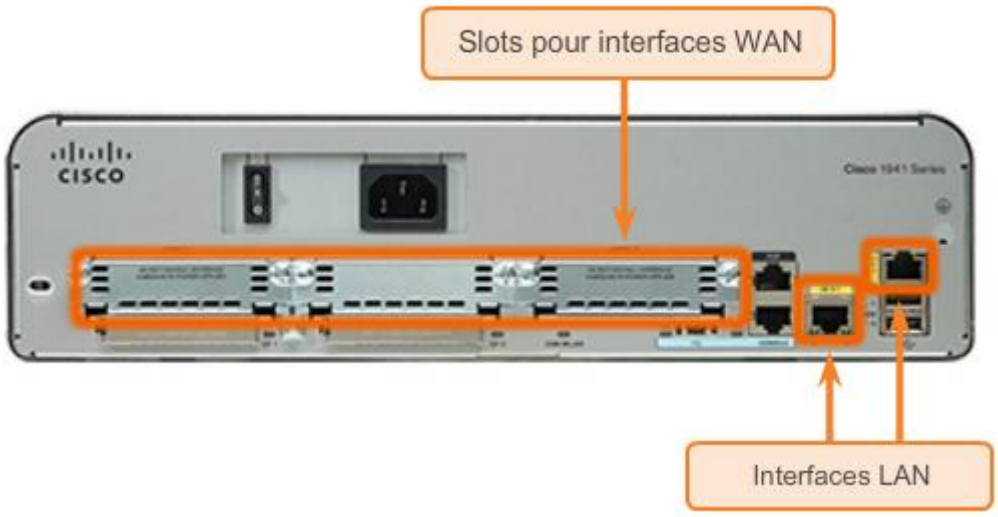
En plus de ces ports, les routeurs possèdent également des interfaces réseau permettant de recevoir et de transférer des paquets IP. Les routeurs ont plusieurs interfaces, utilisées pour se connecter à plusieurs réseaux. Généralement, les interfaces se connectent à différents types de réseau, ce qui veut dire que différents types de support et de connecteur sont nécessaires.

Chaque interface du routeur est un membre ou un hôte d'un réseau IP différent. Chaque interface doit être configurée avec l'adresse IP et le masque de sous-réseau d'un réseau différent. Avec Cisco IOS, deux interfaces actives du même routeur ne peuvent pas appartenir au même réseau.

Les interfaces de routeur peuvent être regroupées en deux catégories :

- **Interfaces LAN Ethernet** – utilisées pour connecter les câbles de connexion aux périphériques de réseau local, tels que des ordinateurs et des commutateurs. Cette interface peut également être utilisée pour connecter des routeurs entre eux. Plusieurs conventions de nommage des interfaces Ethernet sont répandues : Ethernet, FastEthernet et Gigabit Ethernet. Le nom utilisé dépend du type de périphérique et du modèle.
- **Interfaces WAN série** – utilisées pour connecter des routeurs à des réseaux externes, généralement sur une distance importante. À l'instar des interfaces LAN, chaque interface WAN a sa propre adresse IP et son propre masque de sous-réseau, lui permettant d'être identifiée comme faisant partie d'un réseau donné.

La figure montre les interfaces LAN et les interfaces série du routeur.



Exercice – Identification des composants d'un routeur

Les descriptions des fonctions du routeur et des pièces sont fournies ci-contre. Faites glisser chaque nom de composant de routeur à sa fonction/description.

- Interface WAN
- Port AUX
- Interface LAN
- Telnet ou SSH
- Port de console

Composants du routeur	Fonction/Description
	Connecte les routeurs à des réseaux externes, généralement sur une grande distance
	Moyen d'accéder à distance à la CLI via une interface réseau
	Connecte les ordinateurs, les commutateurs et les routeurs pour le réseau interne
	Port local qui utilise une connexion USB ou des connexions série bas débit pour gérer les périphériques réseau
	Port permettant de gérer les routeurs par le biais de lignes téléphoniques et de modems

6.3.1.9 Travaux pratiques – Découverte des caractéristiques physiques d'un routeur

Au cours de ce TP, vous aborderez les points suivants :

- 1re partie : Analyser les caractéristiques externes d'un routeur
- 2e partie : Analyser les caractéristiques internes d'un routeur à l'aide des commandes show

Travaux pratiques – Découverte des caractéristiques physiques d'un routeur

6.3.2 Démarrage du routeur

6.3.2.1 Cisco IOS

Les détails du fonctionnement de Cisco IOS varient d'un périphérique à l'autre selon le but et l'ensemble de fonctionnalités du périphérique. Toutefois, Cisco IOS offre les avantages suivants aux routeurs :

- Adressage
- Interfaces
- Routage
- Sécurité
- QS
- Gestion des ressources

Le fichier IOS proprement dit pèse plusieurs mégaoctets et, comme sur les commutateurs Cisco IOS, il est stocké dans la mémoire Flash. Grâce à la mémoire Flash, il est possible de mettre l'IOS à niveau en installant de nouvelles versions ou en ajoutant de nouvelles fonctionnalités. Lors du démarrage, l'IOS est copié de la mémoire Flash vers la mémoire vive. La mémoire DRAM est beaucoup plus rapide que la mémoire Flash. Par conséquent, copier l'IOS dans la mémoire vive améliore les performances du périphérique.

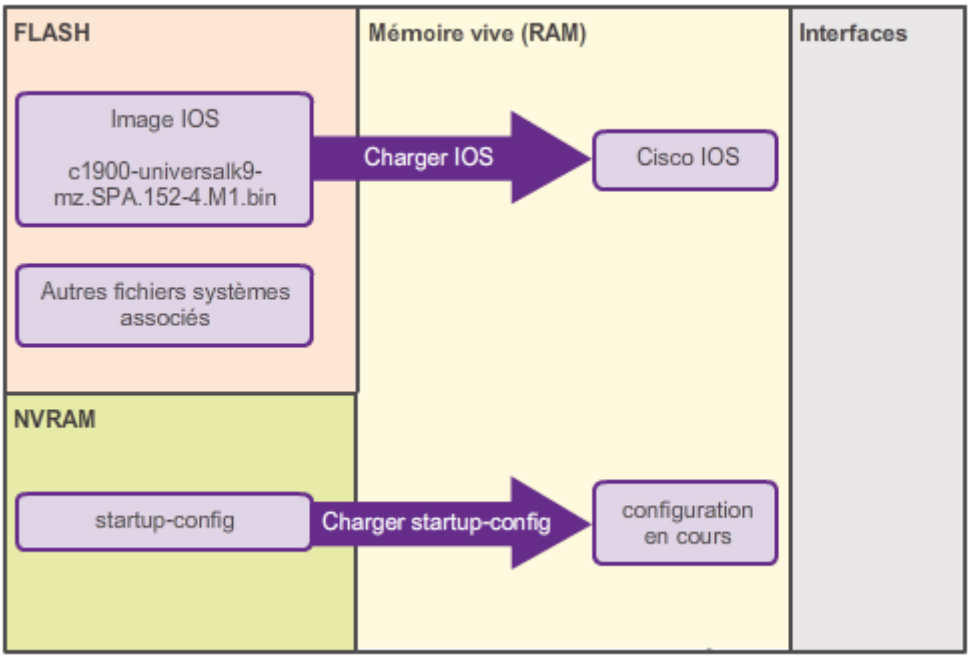
6.3.2.2 Fichiers de démarrage prédéfinis

Comme l'illustre la figure, un routeur charge les deux fichiers suivants dans la mémoire vive lorsqu'il est démarré :

- **Fichier d'image IOS** – l'IOS facilite le fonctionnement de base des composants matériels du périphérique. Le fichier d'image IOS est stocké dans la mémoire Flash.

- **Fichier de configuration initiale** – contient les commandes utilisées initialement pour configurer un routeur et créer le fichier de configuration en cours stocké dans la mémoire vive. Le fichier de configuration initiale est stocké dans la mémoire vive non volatile. Toutes les modifications de configuration sont enregistrées dans le fichier de configuration en cours et sont mises en œuvre immédiatement par l'IOS.

La configuration en cours est modifiée lorsque l'administrateur réseau configure le périphérique. Une fois les modifications apportées au fichier running-config, ce dernier doit être enregistré dans la mémoire vive non volatile en tant que fichier de configuration initiale, au cas où le routeur serait redémarré ou mis hors tension.



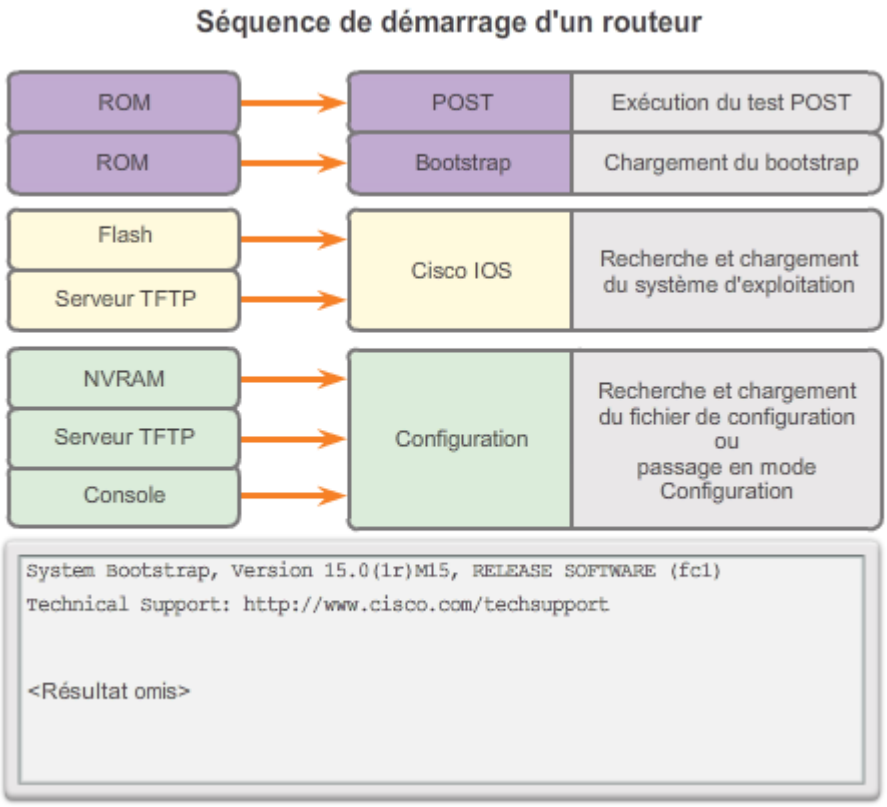
6.3.2.3 Processus de démarrage d'un routeur

Démarrage du routeur

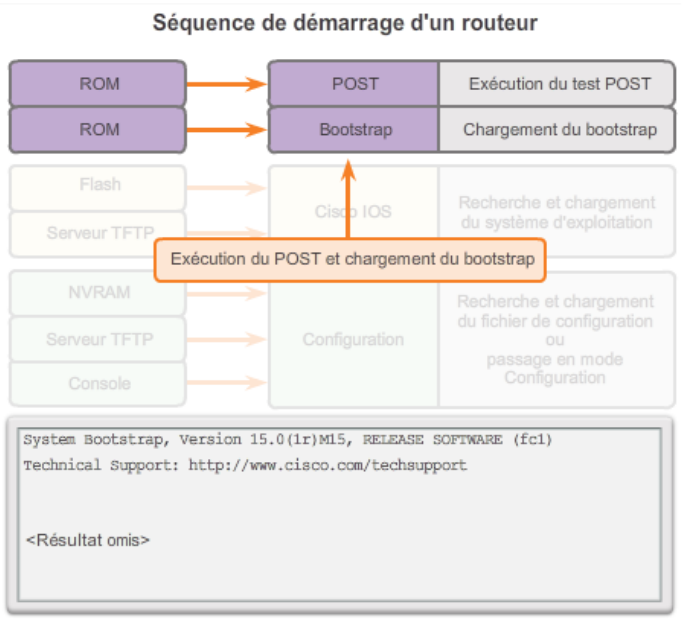
Le processus de démarrage est composé de trois phases principales, décrites à la Figure 1 :

1. Exécution du POST et chargement du bootstrap
2. Localisation et chargement du logiciel Cisco IOS

3. Localisation et chargement du fichier de configuration initiale ou passage en mode Configuration



1. Exécution du POST et chargement du bootstrap (Figure 2)



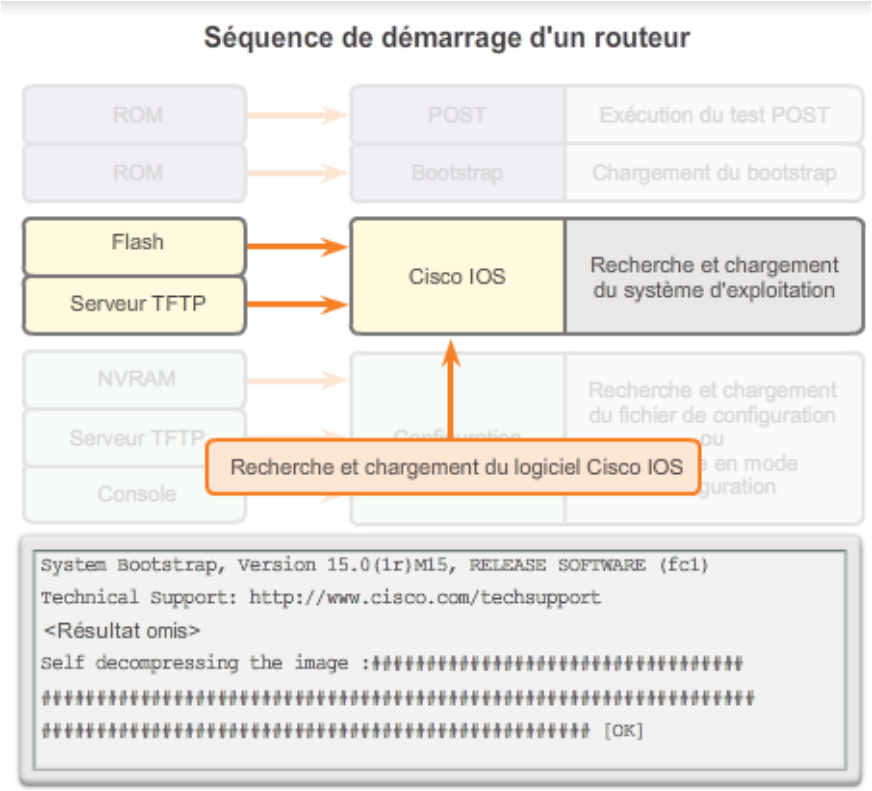
Le Power-On Self Test (POST) est un processus courant qui s'exécute au démarrage de la quasi-totalité des ordinateurs. Le processus POST est utilisé pour tester le matériel du routeur. Lorsque le routeur est mis sous tension, le logiciel présent sur la puce de mémoire morte effectue le POST. Au cours de ce test automatique, le routeur exécute des diagnostics à partir de la mémoire morte sur plusieurs composants matériels, notamment le processeur, la mémoire vive et la mémoire vive non volatile. Une fois le POST terminé, le routeur exécute le programme d'amorçage.

Après le POST, le programme d'amorçage est copié de la mémoire morte à la mémoire vive. Ensuite, le processeur exécute les instructions du programme d'amorçage. Le rôle principal du programme d'amorçage est de localiser Cisco IOS et de le charger dans la mémoire vive.

Remarque : à ce stade, si vous disposez d'une connexion console au routeur, vous commencez à voir les résultats sur l'écran.

2. Localisation et chargement de Cisco IOS (Figure 3)

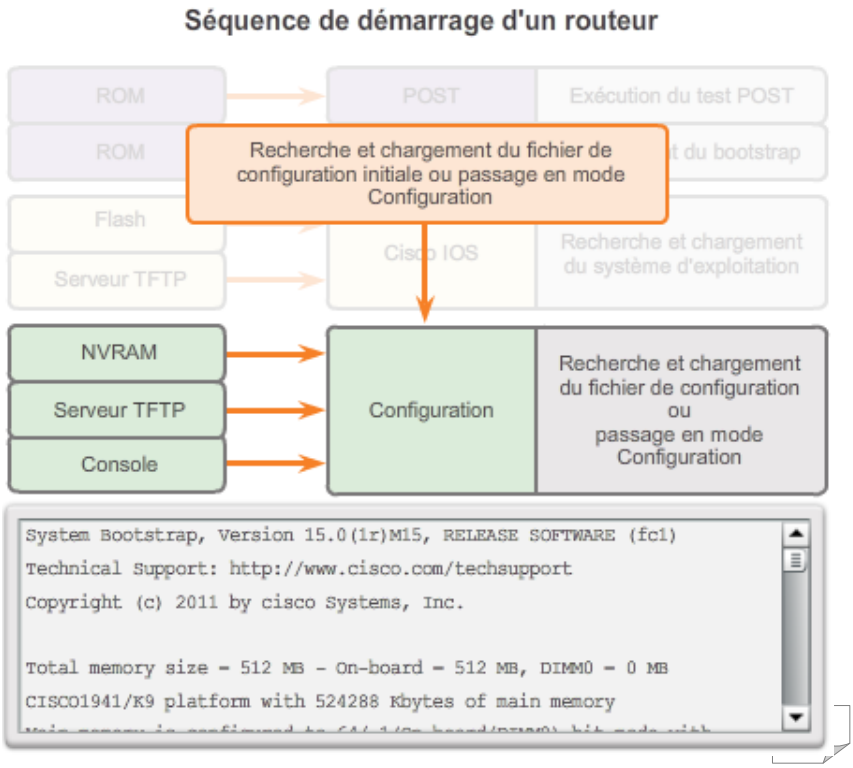
L'IOS est généralement stocké dans la mémoire Flash et est copié dans la mémoire vive par le processeur pour être exécuté. Pendant la décompression automatique du fichier d'image IOS, une suite de signes dièse **(#)** s'affiche.



Si l'image IOS ne figure pas dans la mémoire Flash, le routeur peut la rechercher à l'aide d'un serveur TFTP. S'il est impossible de localiser une image IOS entière, une version réduite de l'IOS est copiée de la mémoire morte vers la mémoire vive. Cette version de l'IOS permet de diagnostiquer les éventuels problèmes et peut servir à charger une version complète de l'IOS dans la mémoire vive.

3. Localisation et chargement du fichier de configuration (Figure 4)

Le bootstrap recherche le fichier de configuration initiale (également appelé startup-config) dans la mémoire vive non volatile. Ce fichier contient les commandes et paramètres de configuration précédemment enregistrés. S'il existe, il est copié dans la mémoire vive en tant que fichier de configuration en cours, ou running-config. Le fichier de configuration en cours contient des adresses d'interface, lance les processus de routage, configure les mots de passe du routeur et définit d'autres caractéristiques du routeur.



Si le fichier startup-config n'existe pas dans la mémoire vive non volatile, le routeur peut rechercher un serveur TFTP (Trivial File Transfer Protocol). Si le routeur détecte qu'il possède un lien actif avec un autre routeur configuré, il envoie une requête de recherche par diffusion pour trouver un fichier de configuration dans le lien actif.

Si un tel serveur est introuvable, le routeur affiche l'invite du mode Configuration. Le mode Configuration est une série de questions invitant l'utilisateur à entrer des informations de configuration de base. Ce mode n'est pas destiné à être utilisé pour effectuer des configurations de routeur complexes et n'est généralement pas utilisé par les administrateurs réseau.

Remarque : dans ce cours, le mode Configuration n'est pas utilisé pour configurer le routeur. Lorsque vous êtes invité à passer en mode Configuration, répondez toujours **no**. Si vous répondez **yes** et que vous passez en mode Configuration, vous pouvez appuyer à tout moment sur **Ctrl** + **C** pour mettre fin au processus de configuration.

6.3.2.4 Résultat de la commande show version

La commande **show version** peut être utilisée pour vérifier et dépanner certains composants matériels et logiciels de base du routeur. Cette commande affiche des informations sur la version du logiciel Cisco IOS en cours d'exécution sur le routeur, sur la version du bootstrap, ainsi que sur la configuration matérielle, en indiquant notamment la quantité de mémoire système.

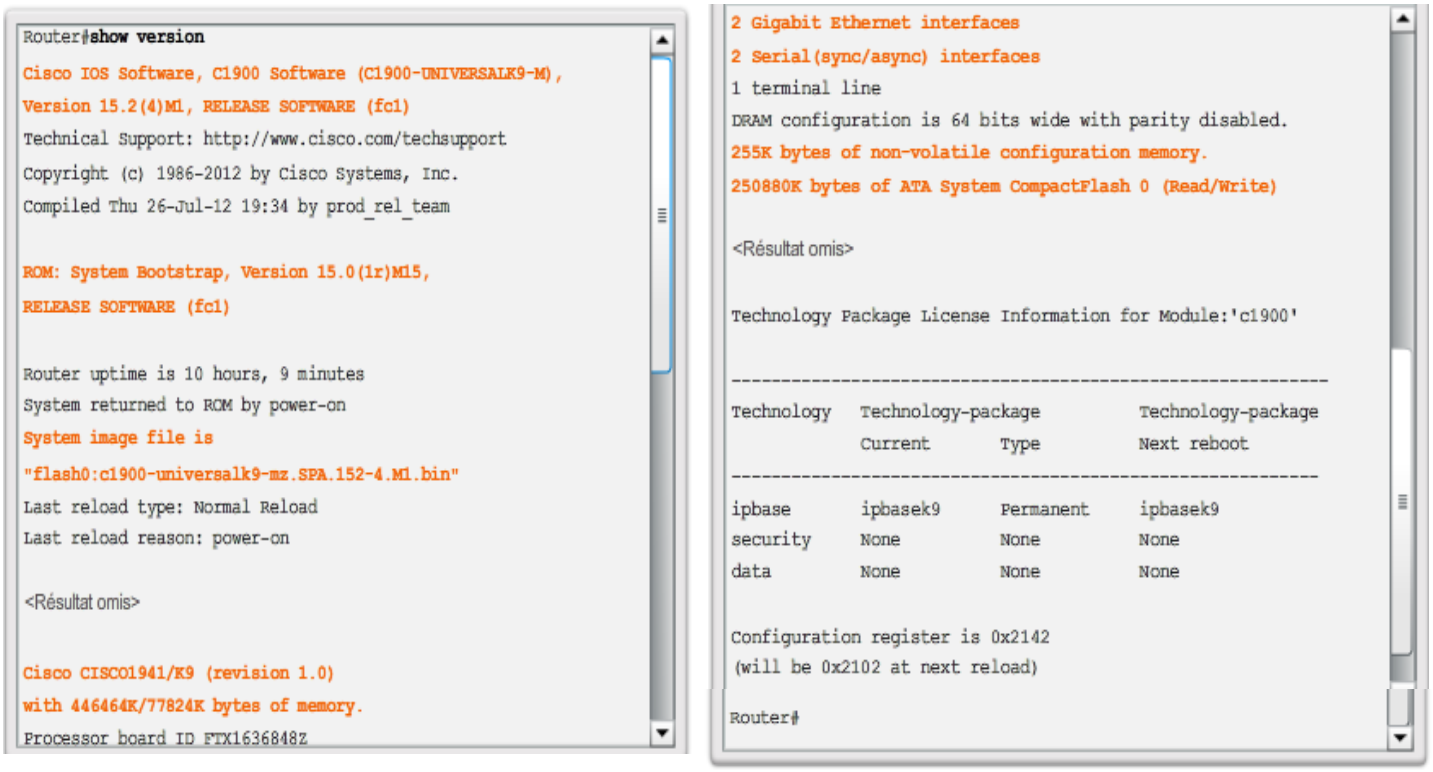
Le résultat de la commande **show version** comprend les éléments suivants :

- **Version d'IOS** – version du logiciel Cisco IOS stocké dans la mémoire vive et utilisé par le routeur.
- **Bootstrap de la mémoire morte** – version du logiciel de démarrage du système, stocké dans la mémoire morte et qui a été initialement utilisé pour démarrer le routeur.
- **Emplacement de l'IOS** – indique où se trouve le bootstrap et où ce dernier a chargé le logiciel Cisco IOS, ainsi que le nom de fichier complet de l'image IOS.
- **Processeur et quantité de mémoire vive** – la première partie de cette ligne indique le type de processeur du routeur. La dernière partie de cette ligne affiche la quantité de mémoire vive dynamique. Certains modèles de routeur, comme les routeurs à services intégrés Cisco 1941, utilisent une portion de DRAM comme mémoire de paquets. Celle-ci est utilisée pour mettre les paquets en mémoire tampon. Pour déterminer la quantité totale de mémoire vive dynamique présente sur le routeur, additionnez les deux nombres.
- **Interfaces** – affiche les interfaces physiques du routeur. Dans cet exemple, le routeur à services intégrés Cisco 1941 dispose de deux interfaces gigabit ethernet et de deux interfaces série bas débit.
- **Quantité de mémoire vive non volatile et de mémoire Flash** – il s'agit de la quantité de mémoire vive non volatile et de la quantité de mémoire Flash du routeur. La mémoire vive non volatile est utilisée pour stocker le fichier de configuration initiale et la mémoire Flash est utilisée pour stocker Cisco IOS de façon permanente.

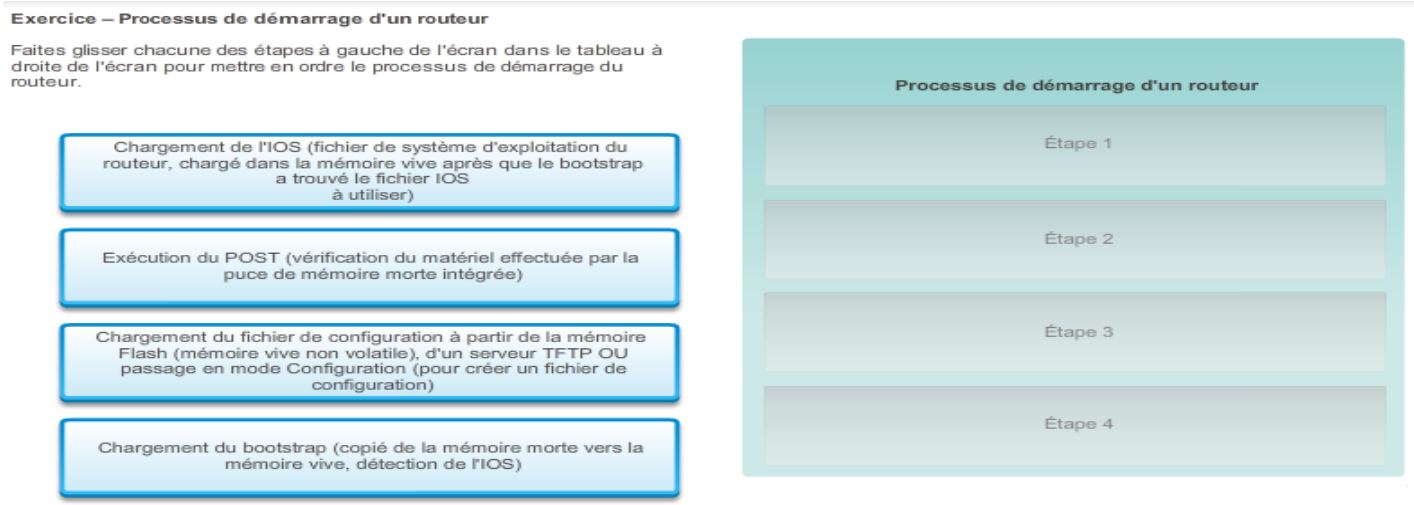
La dernière ligne de la commande **show version** affiche l'actuelle valeur configurée du registre de configuration du logiciel au format hexadécimal. Si une deuxième valeur est

affichée entre parenthèses, elle correspond à la valeur du registre de configuration qui sera utilisée lors du prochain rechargement.

Le registre de configuration a plusieurs fonctions, notamment la récupération de mot de passe. Le paramètre d'usine par défaut pour le registre de configuration est 0x2102. Cette valeur indique que le routeur tente de charger une image du logiciel Cisco IOS à partir de la mémoire Flash et de charger le fichier de configuration initiale à partir de la mémoire vive non volatile.



6.3.2.5 Démonstration vidéo – Processus de démarrage d'un routeur



6.3.2.6 Exercice – Processus de démarrage d'un routeur

6.4 Configuration d'un routeur Cisco

6.4.1 Configuration des paramètres initiaux

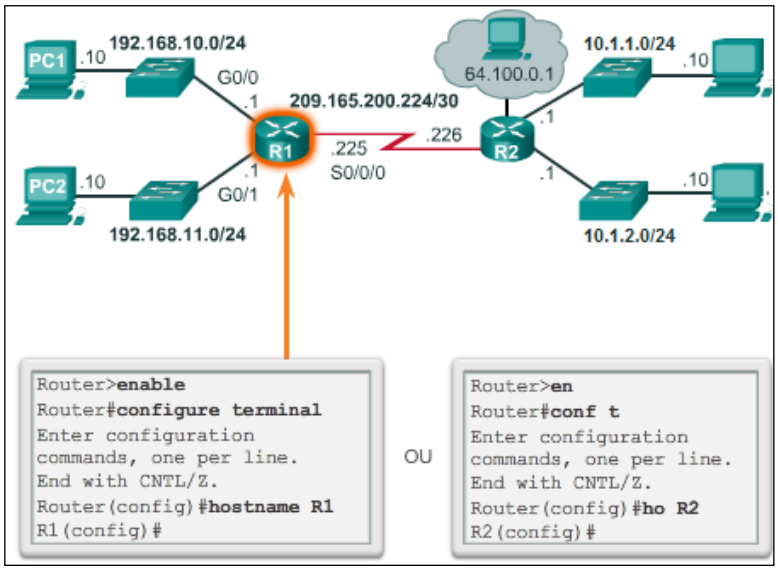
6.4.1.1 Étapes de configuration d'un routeur

Configuration des paramètres initiaux

Les routeurs Cisco et les commutateurs Cisco ont beaucoup de points communs. Ils prennent en charge le même système d'exploitation de modes, les mêmes structures de commandes et comptent de nombreuses commandes similaires. En outre, les étapes de configuration initiale sont identiques pour les deux périphériques lors de la mise en œuvre dans un réseau.

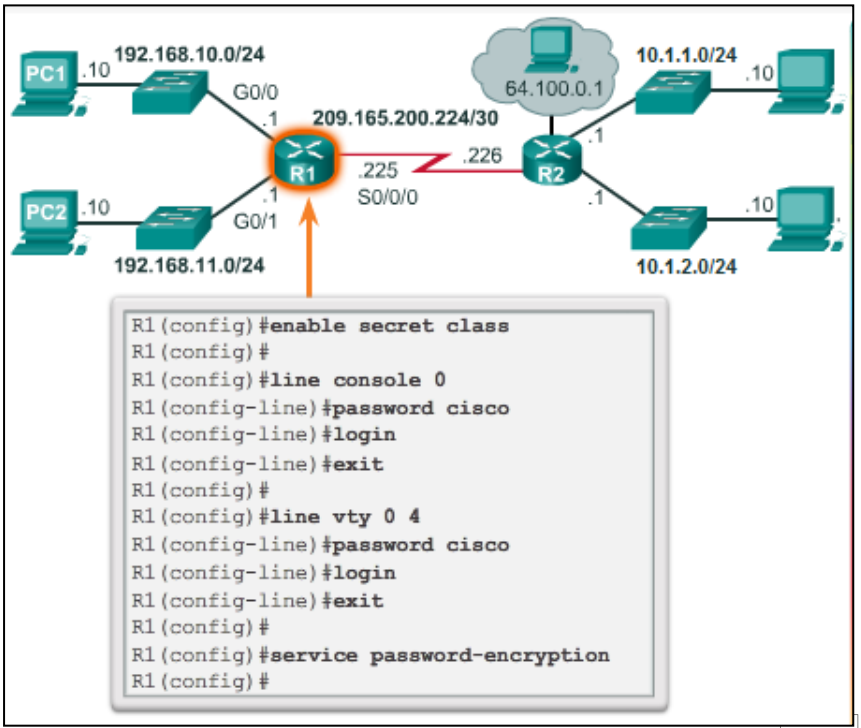
Les étapes suivantes, similaires à celles suivies pour la configuration d'un commutateur, doivent être réalisées lors de la configuration des paramètres initiaux d'un routeur :

1. Attribuez un nom de périphérique à l'aide de la commande de configuration globale **hostname**. (Figure 1)



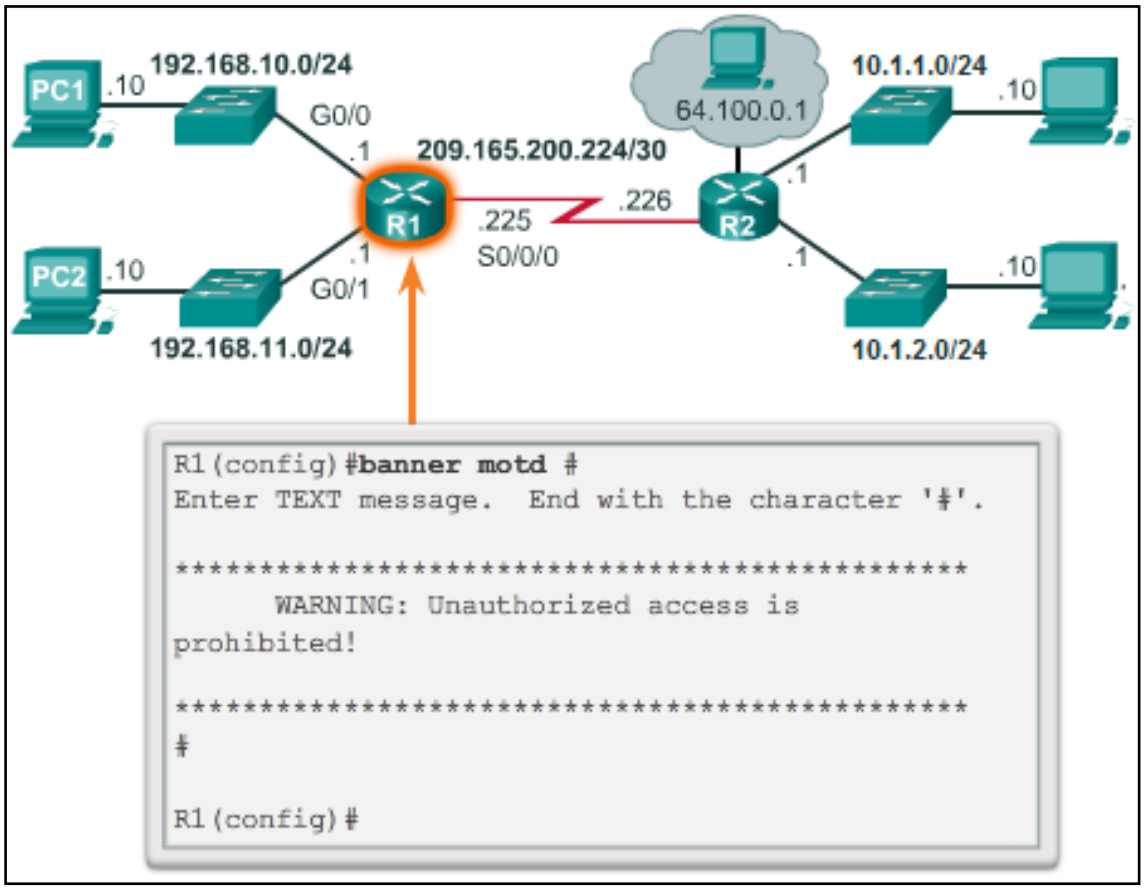
2. Définissez les mots de passe. (Figure 2)

- Sécurisez l'accès au mode d'exécution privilégié à l'aide de la commande **enable secret**.
- Sécurisez l'accès au mode d'exécution à l'aide de la commande **login** sur le port de console et de la commande **password** pour définir le mot de passe.
- Sécurisez l'accès virtuel des lignes VTY de la même manière que pour sécuriser l'accès au mode d'exécution.
- Utilisez la commande de configuration globale **service password-encryption** pour empêcher les mots de passe

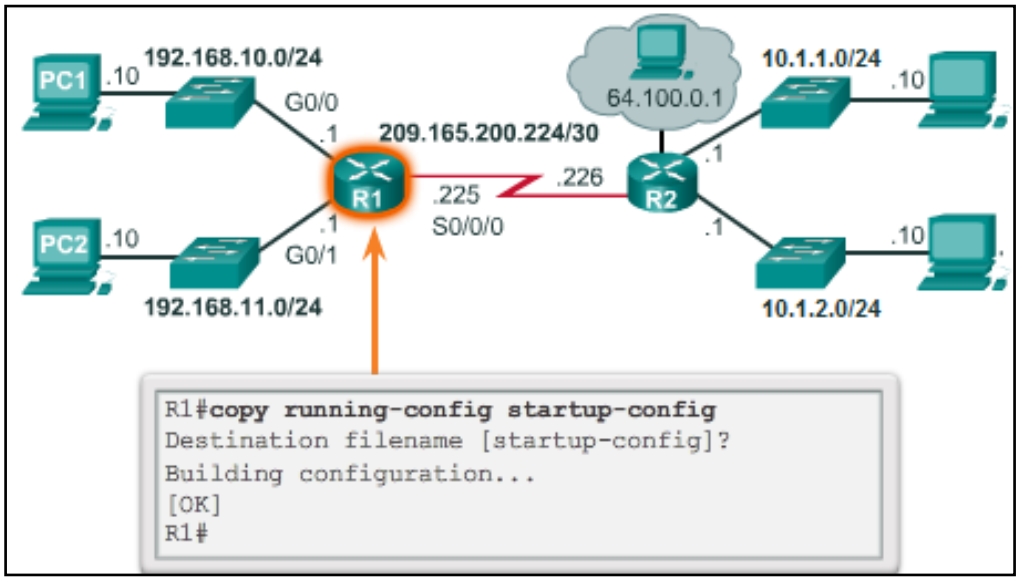


d'apparaître en clair dans le fichier de configuration.

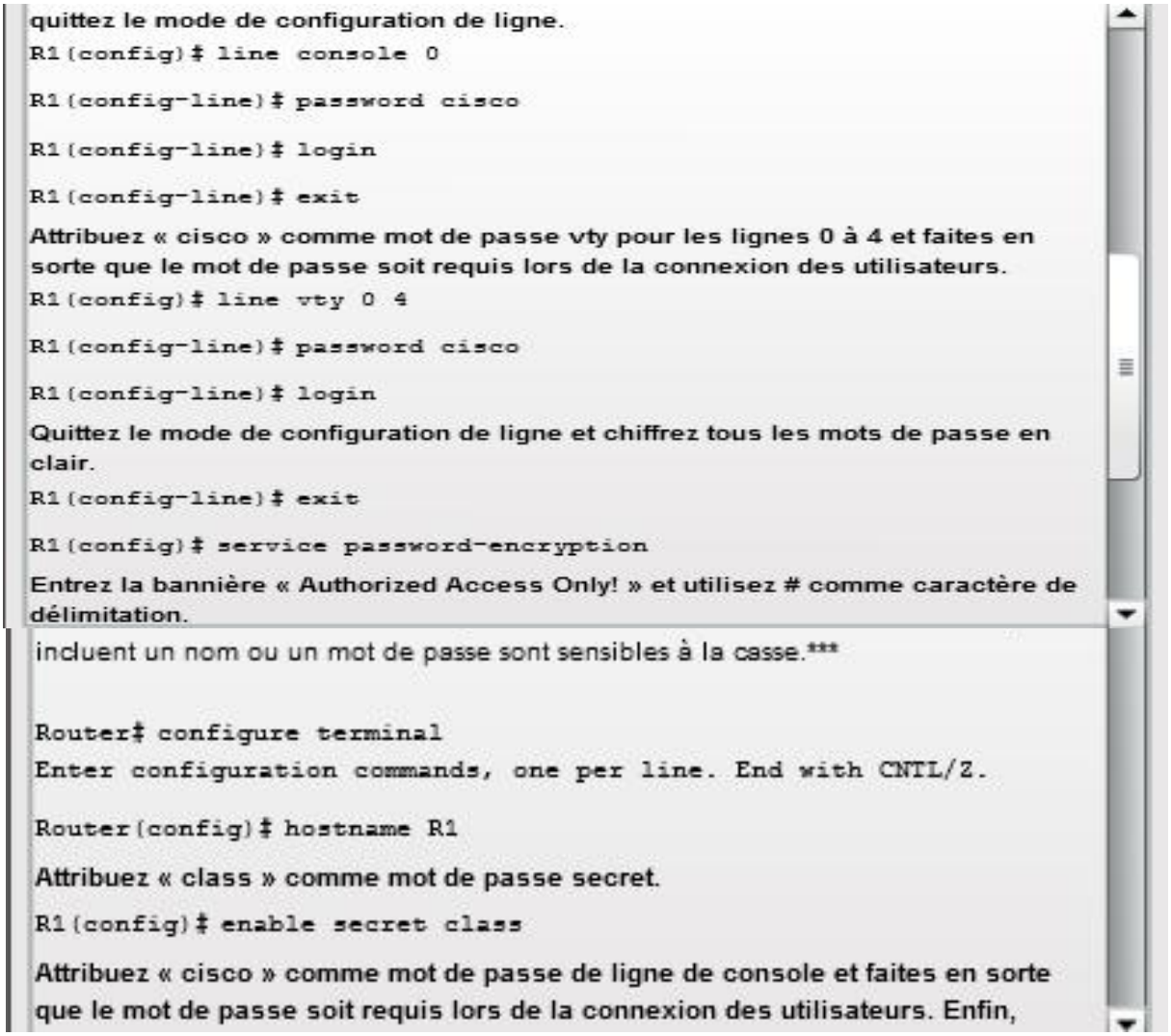
3. Rédigez les mentions légales à l'aide de la commande de configuration globale **banner motd** (message du jour, MOTD). (Figure 3)



4. Enregistrez la configuration à l'aide de la commande **copy run start**. (Figure 4)



5. Vérifiez la configuration à l'aide de la commande **show run**.

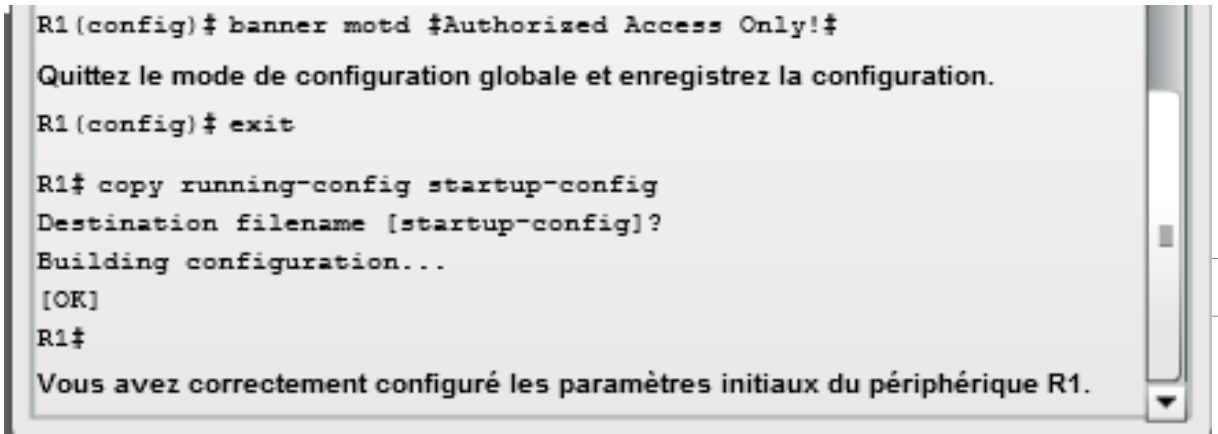


La Figure 5 est un contrôleur de syntaxe qui vous permet de mettre en pratique ces étapes de configuration

6.4.1.2 Packet Tracer : configuration des paramètres initiaux du routeur

Configuration des paramètres initiaux

Au cours de cet exercice, vous allez effectuer des configurations de base de routeurs. Vous allez sécuriser l'accès à la CLI et au port de console à l'aide de mots de passe chiffrés et en texte clair. Vous allez également configurer les messages affichés lors de la connexion des utilisateurs au routeur. Ces bannières avertissent également les utilisateurs non autorisés que l'accès est interdit. Enfin, vous allez vérifier et enregistrer votre configuration en cours.
Packet Tracer – Configuration des paramètres initiaux du routeur : instructions



6.4.2 Configurer les interfaces

6.4.2.1 Configurations des interfaces LAN

Pour que les routeurs soient accessibles, les interfaces de routeur doivent être configurées. Par conséquent, pour activer une interface spécifique, passez en mode de configuration d'interface via la commande de configuration globale **interface** *type-et-numéro*.

Il existe différents types d'interfaces disponibles sur les routeurs Cisco. Dans cet exemple, le routeur Cisco 1941 est équipé de deux interfaces gigabit ethernet et d'une carte d'interface WAN série (WIC) constituée de deux interfaces. Les interfaces sont nommées comme suit :

- Gigabit Ethernet 0/0 (G0/0)
- Gigabit Ethernet 0/1 (G0/1)
- Serial 0/0/0 (S0/0/0)
- Serial 0/0/1 (S0/0/1)

Pour activer une interface de routeur, configurez les éléments suivants :

- **Adresse IPv4 et masque de sous-réseau -** configurez l'adresse IP et le masque de sous-réseau au moyen de la commande de configuration d'interface **ip address** *address subnet-mask*.
- **Activez l'interface** – par défaut, les interfaces LAN et WAN ne sont pas activées. L'interface doit être activée à l'aide de la commande **no shutdown**. Cela revient à mettre l'interface sous tension. L'interface doit également être connectée à un autre périphérique (concentrateur, commutateur ou autre routeur) pour que la couche physique soit active.

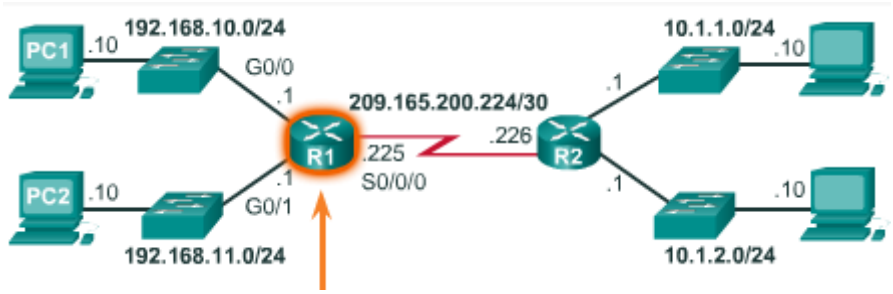
Bien que cela ne soit pas obligatoire, il est conseillé de configurer une description sur chaque interface pour mieux documenter les informations réseau. Le texte de description est limité à 240 caractères. Sur les réseaux de production, une description peut être utile pour le dépannage, puisqu'elle fournit des informations sur le type de réseau auquel l'interface se connecte et indique la présence éventuelle d'autres routeurs sur ce réseau. Si l'interface se connecte à un FAI ou à un fournisseur de services, il est utile d'entrer les informations de connexion et de contact du fournisseur.

La Figure 1 présente la configuration des interfaces LAN connectées au périphérique R1. Dans la Figure 2, entraînez-vous à configurer une interface LAN.

Remarque : les abréviations de commande sont utilisées pour la configuration de l'interface gigabitethernet 0/1.

```
R1#conf t
Enter configuration commands, one per line.
End with CNTL/Z.
R1(config)#
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#description Link to LAN-10
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0,changed state to up
```

```
R1(config-if)#exit
R1(config)#
R1(config)#int g0/1
R1(config-if)#ip add 192.168.11.1 255.255.255.0
R1(config-if)#des Link to LAN-11
R1(config-if)#no shut
%LINK-5-CHANGED: Interface GigabitEthernet0/1,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
R1(config-if)#exit
R1(config)#
```



Configuration des interfaces LAN

Configurez l'interface gigabit ethernet 0/0 avec l'adresse IP « 192.168.10.1 » et le masque de sous-réseau « 255.255.255.0 ». Attribuez la description « LAN-10 » à la liaison et activez l'interface.

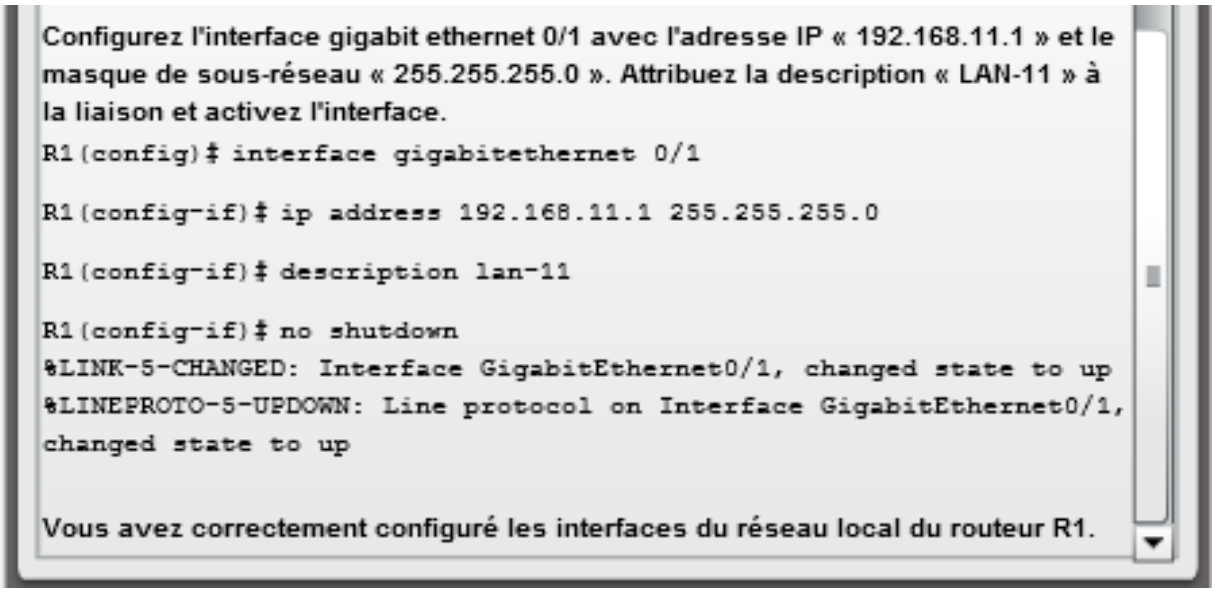
```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

R1(config)# interface gigabitethernet 0/0

R1(config-if)# ip address 192.168.10.1 255.255.255.0

R1(config-if)# description LAN-10

R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
R1(config-if)#exit
```



6.4.2.2 Vérification de la configuration d'interface

Il existe plusieurs commandes permettant de vérifier la configuration d'interface. La commande la plus utile d'entre elles est la commande **show ip interface brief**. Le résultat généré répertorie toutes les interfaces, leur adresse IP et leur état actuel. Les interfaces configurées et connectées doivent afficher l'état « up » et le protocole « up ». Tout autre état indique un problème de configuration ou de câblage.

Vous pouvez vérifier la connectivité à partir de l'interface, à l'aide de la commande **ping**. Les routeurs Cisco envoient cinq requêtes ping consécutives et mesurent les durées de transmission minimale, moyenne et maximale. Les points d'exclamation permettent de vérifier la connectivité.

La Figure 1 présente le résultat de la commande **show ip interface brief**, qui indique que toutes les interfaces LAN et que la liaison WAN sont activées et opérationnelles. Notez que la commande **ping** a généré cinq points d'exclamation pour vérifier la connectivité au périphérique R2.

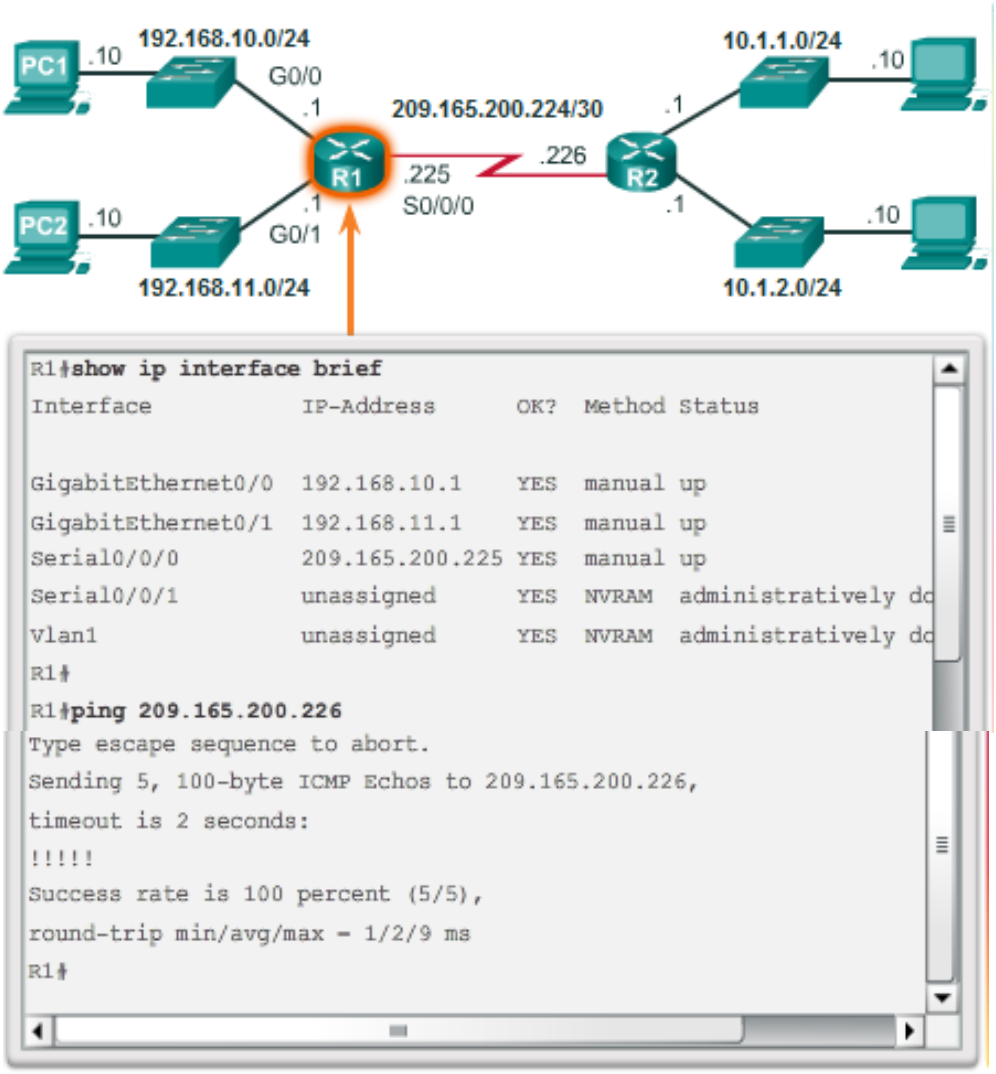
Voici d'autres commandes de vérification d'interface :

- **show ip route -** Affiche le contenu de la table de routage IPv4 stocké dans la mémoire vive.
- **show interfaces -** Affiche des statistiques relatives à toutes les interfaces du périphérique.
- **show ip interface -** Affiche des statistiques IPv4 relatives à toutes les interfaces d'un routeur.

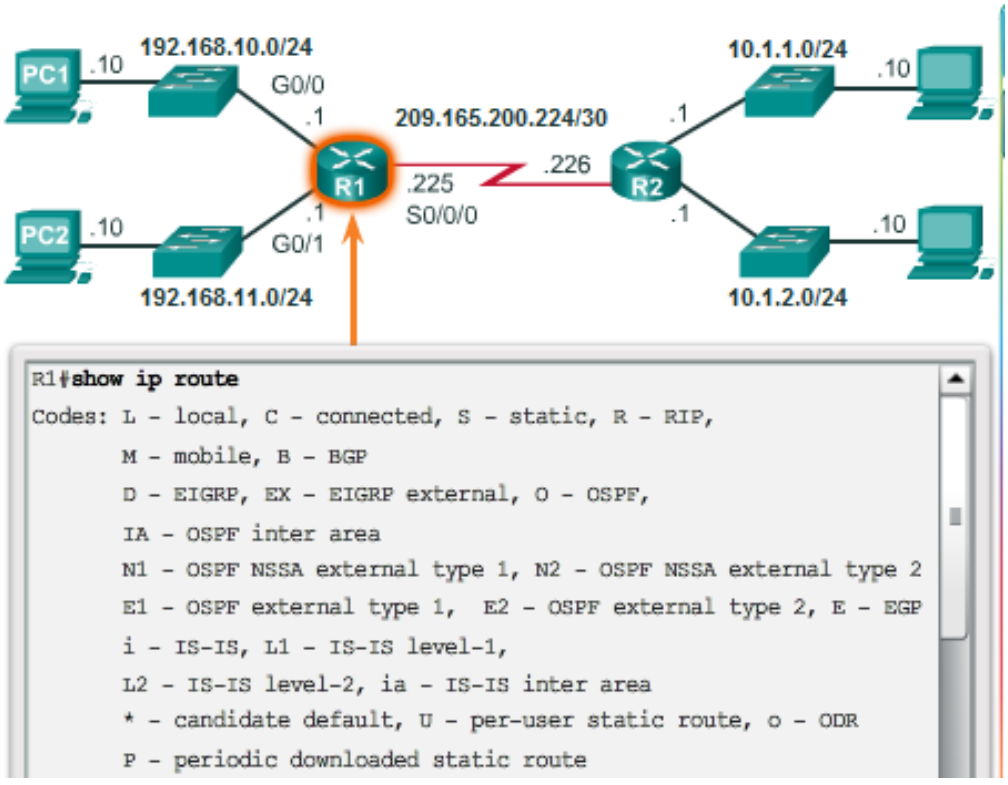
La Figure 2 illustre le résultat de la commande **show ip route**. Notez bien les trois entrées réseau directement connectées et les entrées d'interface de liaison locale.

Pensez à enregistrer la configuration à l'aide de la commande **copy running-config startup-config**.

Fg1


192.168.10.0/24
PC1
.10
G0/0
.1
209.165.200.224/30
.225
S0/0/0
.226
R1
R2
10.1.1.0/24
.10
.1
PC2
.10
G0/1
.1
192.168.11.0/24
10.1.2.0/24
.10
.1
R1#show ip interface brief
Interface IP-Address OK? Method Status
GigabitEthernet0/0 192.168.10.1 YES manual up
GigabitEthernet0/1 192.168.11.1 YES manual up
Serial0/0/0 209.165.200.225 YES manual up
Serial0/0/1 unassigned YES NVRAM administratively do
Vlan1 unassigned YES NVRAM administratively do
R1#
R1#ping 209.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max = 1/2/9 ms
R1#

Fg2


192.168.10.0/24
PC1
.10
G0/0
.1
209.165.200.224/30
.225
S0/0/0
.226
R1
R2
10.1.1.0/24
.10
.1
PC2
.10
G0/1
.1
192.168.11.0/24
10.1.2.0/24
.10
.1
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP,
M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF,
IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1,
L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

```
Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
L       192.168.11.1/32 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

6.4.3 Configuration de la passerelle par défaut

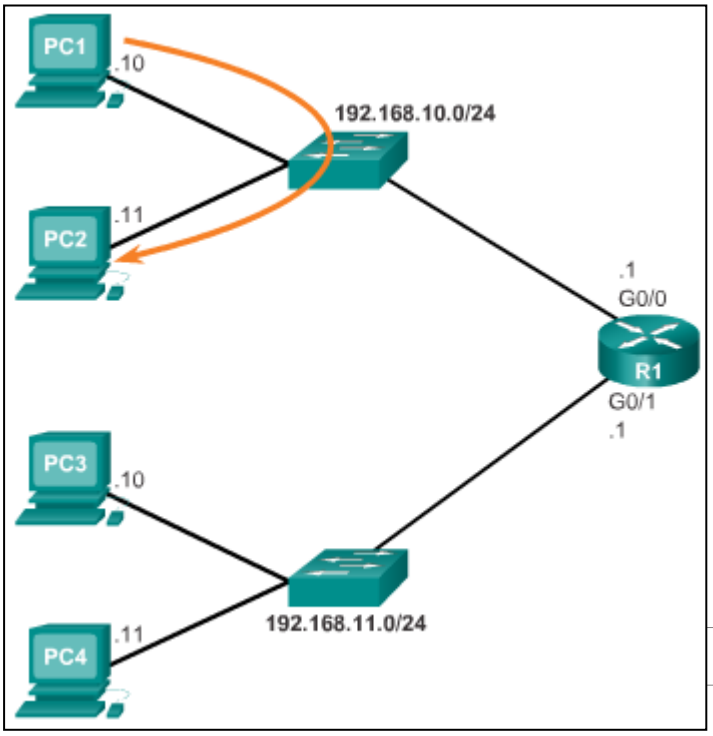
6.4.3.1 Passerelle par défaut sur un hôte

La plupart des routeurs comportent, au minimum, deux interfaces. Chaque interface comporte une adresse IP distincte dans un réseau distinct.

Pour qu'un périphérique final communique sur le réseau, il doit être configuré avec les informations correctes d'adresse IP, y compris l'adresse de la passerelle par défaut. La passerelle par défaut est utilisée uniquement lorsque l'hôte veut transmettre un paquet à un périphérique sur un autre réseau. L'adresse de la passerelle par défaut est généralement l'adresse d'interface de routeur reliée au réseau local auquel l'hôte est connecté. Alors que l'adresse configurée sur l'interface du routeur peut être n'importe quelle adresse, l'adresse IP du périphérique hôte et l'adresse de l'interface de routeur doivent se trouver sur le même réseau.

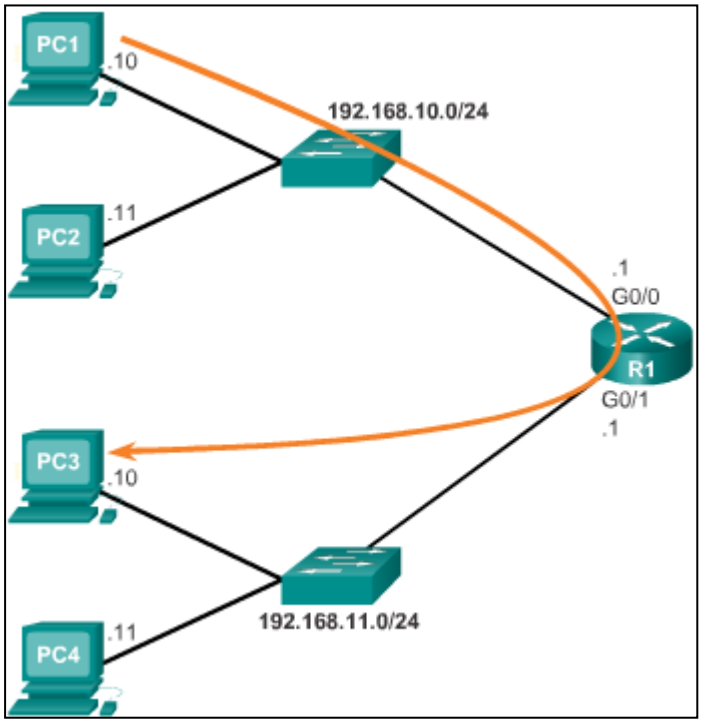
Les figures illustrent une topologie composée d'un routeur comportant deux interfaces distinctes. Chaque interface est connectée à un réseau distinct. G0/0 est connectée au réseau 192.168.10.0, alors que G0/1 est connectée au réseau 192.168.11.0. Chaque périphérique hôte est configuré avec l'adresse de la passerelle par défaut appropriée.

Dans la Figure 1, le PC1 envoie un paquet au PC2. Dans cet exemple, la passerelle par défaut n'est pas utilisée. En revanche, le PC1 envoie un paquet avec l'adresse IP du PC2 et transfère le paquet directement au PC2 par le biais du commutateur.



Fg1

Dans la Figure 2, le PC1 envoie un paquet au PC3. Dans cet exemple, le PC1 envoie un paquet avec l'adresse IP du PC3, mais transfère le paquet au routeur. Le routeur accepte le paquet, accède à sa table de route pour déterminer l'interface de sortie appropriée en fonction de l'adresse de destination, puis transmet le paquet via l'interface appropriée pour atteindre le PC3.



Fg2

6.4.3.2 Passerelle par défaut sur un commutateur

Une passerelle par défaut est utilisée par tous les périphériques qui requièrent l'utilisation d'un routeur pour déterminer le meilleur chemin vers une destination distante. Les périphériques finaux nécessitent des adresses de passerelle par défaut, tout comme les périphériques intermédiaires tels que le commutateur Cisco IOS.

Les informations d'adresse IP d'un commutateur sont uniquement nécessaires pour gérer le commutateur à distance. En d'autres termes, pour pouvoir établir une connexion Telnet au commutateur, ce dernier doit comporter une adresse IP sur laquelle il est possible d'établir une connexion Telnet. Si le commutateur est uniquement accessible depuis les périphériques du réseau local, seule une adresse IP est requise.

Pour configurer l'adresse IP sur un commutateur, il faut utiliser l'interface virtuelle de commutateur (SVI) :

S1(config)# **interface vlan1**

S1(config-vlan)# **ip address 192.168.10.50 255.255.255.0**

S1(config-vlan)# **no shut**

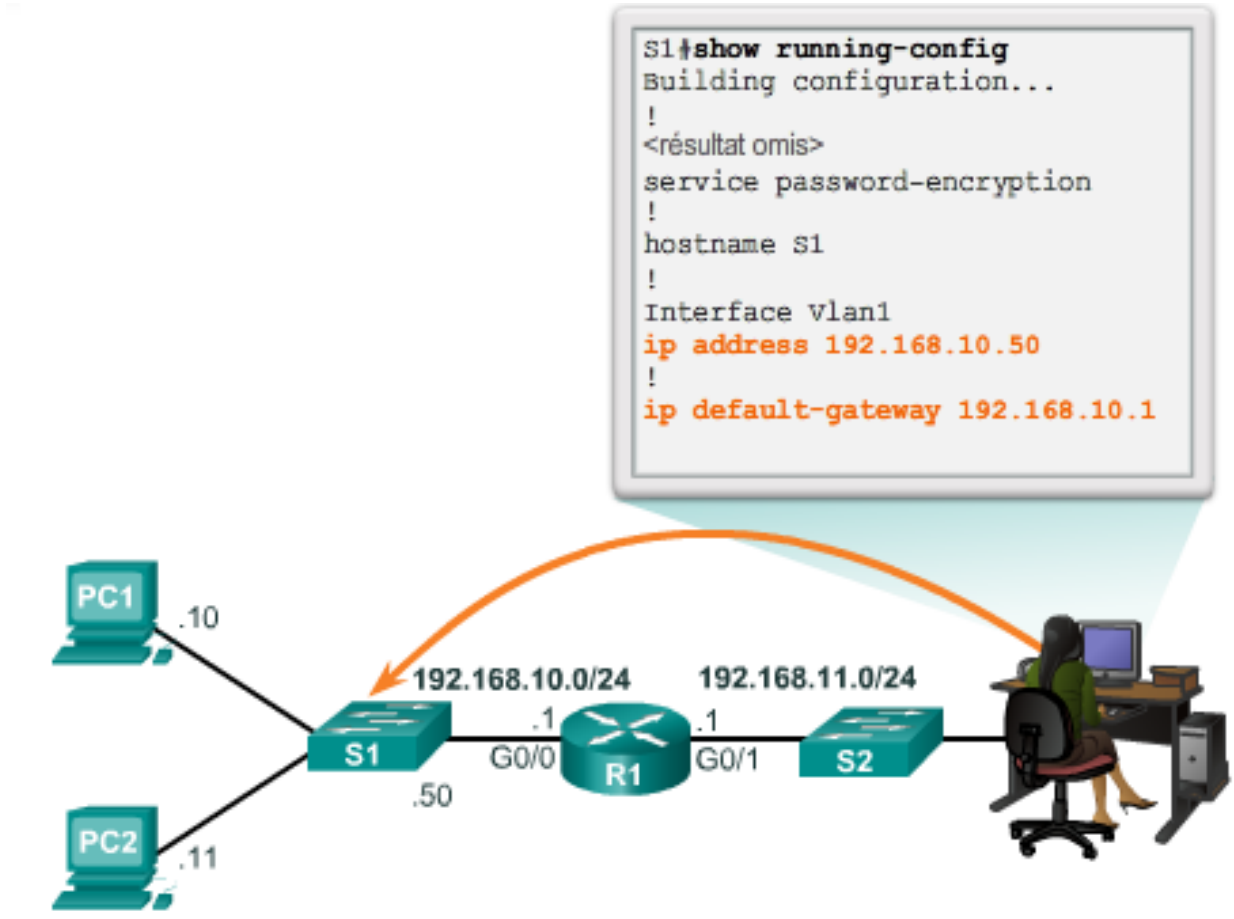
Cependant, si le commutateur doit être accessible pour les périphériques d'un autre réseau, il doit être configuré avec une adresse de passerelle par défaut, car les paquets provenant du commutateur sont pris en charge comme les paquets provenant d'un périphérique hôte. Par conséquent, les paquets provenant du commutateur et destinés à un périphérique sur le même réseau sont transmis directement au périphérique approprié. Les paquets provenant du commutateur et destinés à un périphérique sur un réseau distant doivent être transmis à la passerelle par défaut pour déterminer le chemin à emprunter.

Pour configurer une passerelle par défaut sur un commutateur, utilisez la commande de configuration globale suivante :

S1(config)# **ip default-gateway 192.168.10.1**

La Figure 1 montre un administrateur se connectant à un commutateur sur un réseau distant. Pour que le commutateur transfère les paquets de réponse à l'administrateur, la passerelle par défaut doit être configurée.

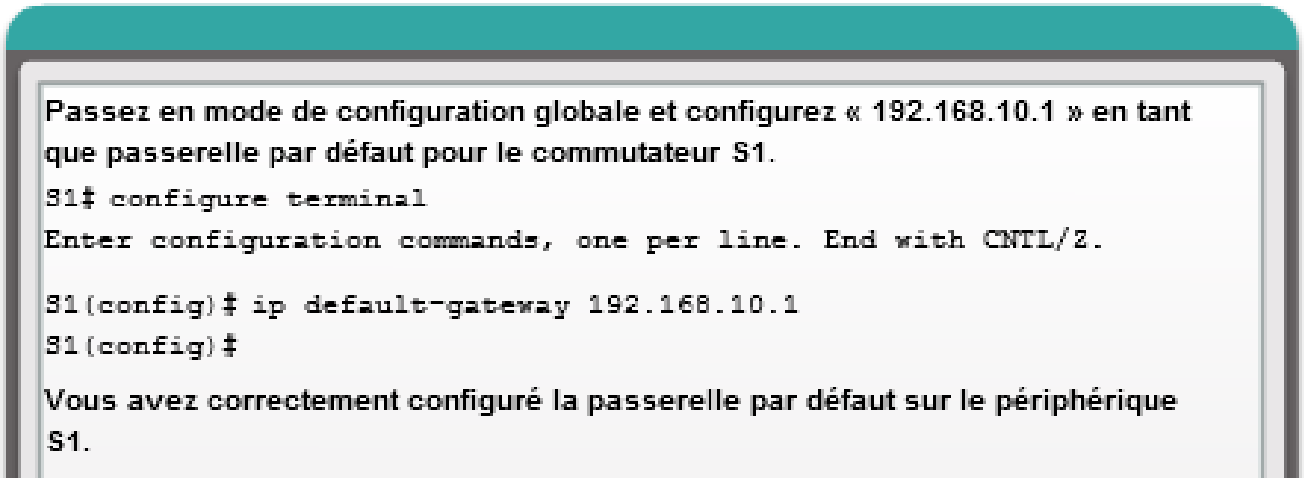
On pense souvent à tort que le commutateur utilise son adresse de passerelle par défaut pour savoir où transmettre des paquets provenant des hôtes connectés au commutateur et destinés aux hôtes sur un réseau distant. En fait, l'adresse IP et les informations relatives à la passerelle par défaut ne sont utilisées que pour les paquets provenant du commutateur. Les paquets provenant des hôtes connectés au commutateur doivent comporter des informations sur la passerelle par défaut pour communiquer sur les réseaux distants. À l'aide de la Figure 2, essayez de configurer une passerelle par défaut sur un commutateur



Si la passerelle par défaut n'était pas configurée sur le périphérique S1, les paquets de réponse de S1 ne pourraient pas contacter l'administrateur à l'adresse 192.168.11.10. L'administrateur ne pourrait pas gérer le périphérique à distance.

Fg1

Configuration de la passerelle par défaut d'un commutateur



Fg2

6.4.3.3 Packet Tracer : connexion d'un routeur à un réseau local

Dans cet exercice, vous allez utiliser différentes commandes **show** pour afficher l'état actuel du routeur. Vous utiliserez ensuite la table d'adressage pour configurer les interfaces Ethernet du routeur. Enfin, vous utiliserez des commandes pour vérifier et tester vos configurations.

Packet Tracer – Connexion d'un routeur à un réseau local : instructions
Packet Tracer – Connexion d'un routeur à un réseau local : PKA

6.4.3.4 Packet Tracer : résolution des problèmes de passerelle par défaut

Pour qu'un périphérique puisse communiquer sur plusieurs réseaux, l'adresse IP, le masque de sous-réseau et la passerelle par défaut doivent être configurés. La passerelle par défaut est utilisée lorsque l'hôte veut transmettre un paquet à un périphérique sur un autre réseau. L'adresse de la passerelle par défaut est généralement l'adresse d'interface de routeur reliée au réseau local auquel l'hôte est connecté. Dans cet exercice, vous allez terminer la documentation du réseau. Vous vérifierez ensuite la documentation du réseau en testant la connectivité de bout en bout et en résolvant les différents problèmes. La méthode de dépannage que vous utiliserez comprend les étapes suivantes :

- Consulter la documentation du réseau et mettre en place des tests pour repérer les problèmes.
- Trouver une solution appropriée pour résoudre un problème donné.
- Mettre en œuvre la solution.
- Mettre en place des tests pour vérifier que le problème est résolu.
- Documenter la solution

6.4.3.5 Travaux pratiques - Initialisation et rechargement d'un routeur et d'un commutateur

Au cours de ce TP, vous aborderez les points suivants :

- Partie 1 : configuration de la topologie et initialisation des périphériques
- 2e partie : Configurer les périphériques et vérifier la connectivité
- 3e partie : Afficher les informations sur le périphérique

Travaux pratiques - Création d'un réseau avec un routeur et un commutateur

6.5 Résumé

6.5.1 Résumé

6.5.1.1 Exercice en classe – Pouvez-vous lire cette carte ?

Pouvez-vous lire cette carte ?

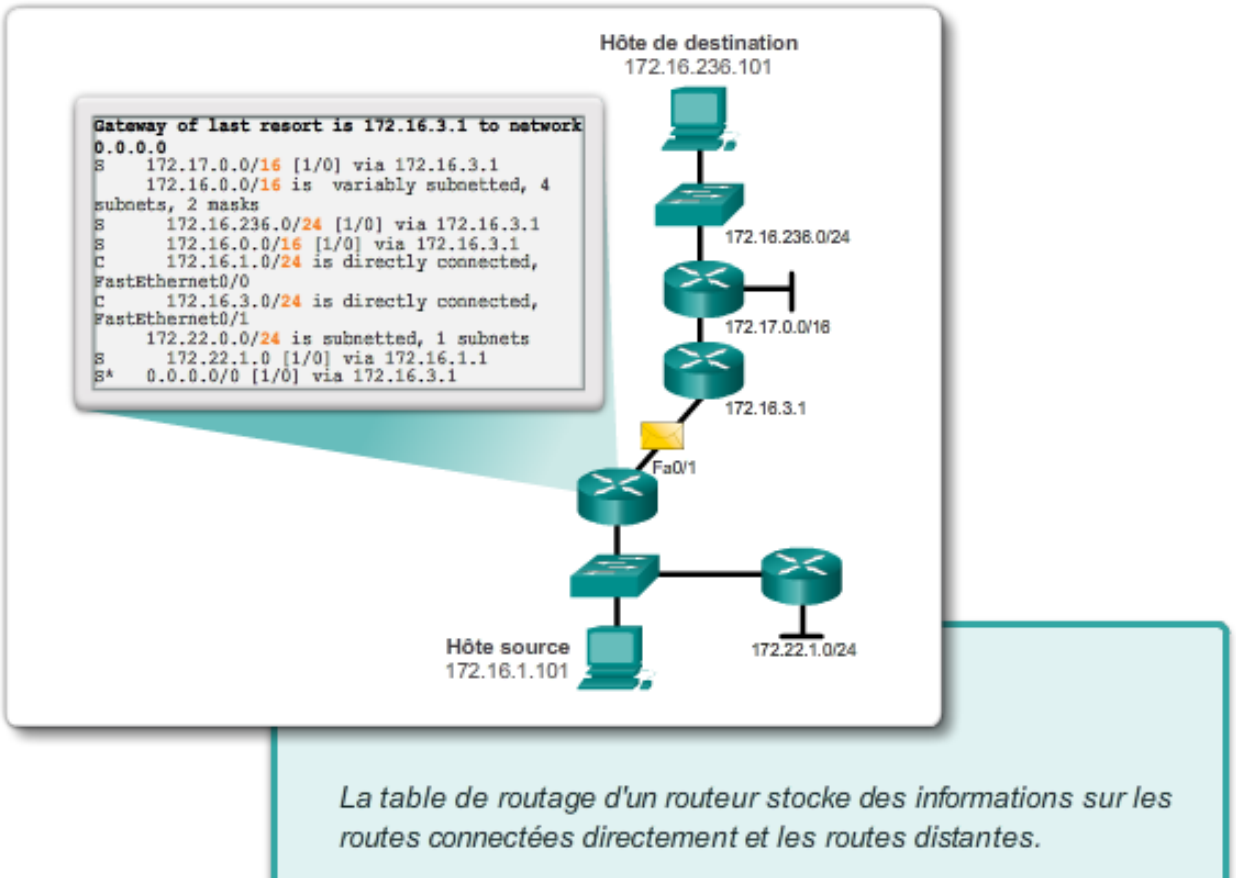
Remarque : il est conseillé de faire travailler les participants par groupes de deux. Cependant, cet exercice peut également être effectué de manière individuelle.

Votre instructeur vous fournira le résultat généré par la commande **show ip route** d'un routeur. Utilisez Packet Tracer pour créer un modèle de topologie à l'aide de ces informations de routage.

Les éléments suivants doivent absolument être utilisés dans votre modèle de topologie :

- 1 commutateur Catalyst 2960
- 1 routeur Cisco de la gamme 1941 avec une carte modulaire de port de commutation HWIC-4ESW et IOS version 15.1 ou ultérieure
- 3 PC (peuvent être des serveurs, des PC génériques, des ordinateurs portables, etc.)

Utilisez l'outil de notes dans Packet Tracer pour indiquer les adresses des interfaces de routeur et les adresses disponibles pour les périphériques finaux que vous avez choisis pour votre modèle. Donnez un nom aux périphériques finaux, aux ports et aux adresses vérifiés par l'utilisation de la commande **show ip route**/des informations de la table de routage dans votre fichier Packet Tracer. Enregistrez votre travail sous forme numérique ou imprimez-le pour le partager avec les autres participants.



6.5.1.2 Packet Tracer : projet d'intégration des compétences

L'administratrice réseau est impressionnée par vos performances en tant que technicien responsable du LAN. Elle aimerait que vous lui démontriez votre capacité à configurer un routeur reliant deux réseaux locaux. Vos tâches incluent la configuration des paramètres de base d'un routeur et d'un commutateur à l'aide de Cisco IOS. Vous vérifierez ensuite vos configurations, ainsi que les configurations sur les périphériques existants en testant la connectivité de bout en bout.

Exercice d'intégration des compétences Packet Tracer : instructions

Exercice d'intégration des compétences Packet Tracer : PKA

6.5.1.3 Résumé

La couche réseau, ou couche 3 du modèle OSI, fournit des services permettant aux périphériques finaux d'échanger des données sur le réseau. Pour effectuer ce transport de bout en bout, la couche réseau utilise quatre fonctions de base : l'adressage IP pour les périphériques finaux, l'encapsulation, le routage et la désencapsulation.

Internet repose essentiellement sur l'IPv4, qui est toujours le protocole de couche réseau le plus répandu. Un paquet IPv4 contient l'en-tête IP et les données utiles. Cependant, l'IPv4 a un nombre limité d'adresses IP publiques uniques. Cela a conduit au développement de la version 6 du protocole IP (IPv6). L'en-tête simplifié IPv6 offre plusieurs avantages par rapport à l'IPv4, y compris une meilleure efficacité du routage, des en-têtes d'extension simplifiés et le traitement par flux. En outre, les adresses IPv6 sont basées sur un adressage hiérarchique 128 bits (32 bits pour l'IPv4). Cela augmente considérablement le nombre d'adresses IP disponibles.

En plus de gérer l'adressage hiérarchique, la couche réseau est également responsable du routage.

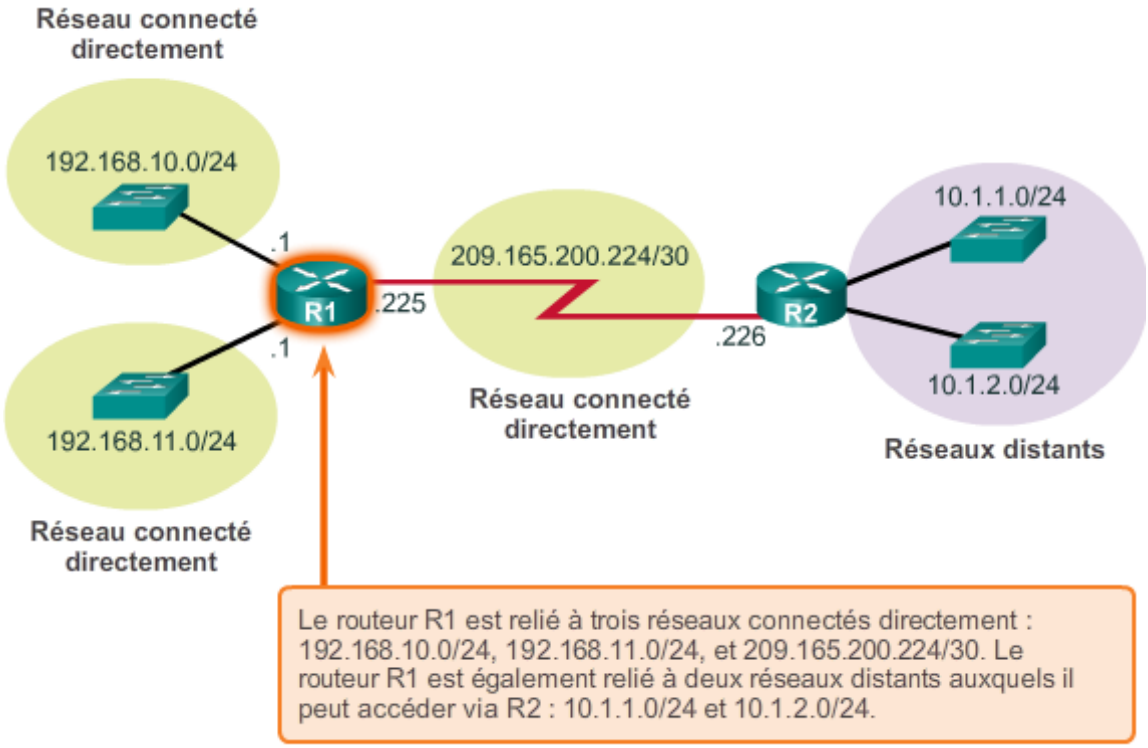
Les hôtes ont besoin d'une table de routage locale pour s'assurer que les paquets sont dirigés vers le réseau de destination correct. La table locale d'un hôte contient généralement la connexion directe, la route de réseau local et la route locale par défaut. La route locale par défaut est la route à la passerelle par défaut.

La passerelle par défaut est l'adresse IP d'une interface de routeur connectée au réseau local. Lorsqu'un hôte doit transmettre un paquet vers une adresse de destination qui n'est pas sur le même réseau que l'hôte, le paquet est envoyé à la passerelle par défaut.

Lorsqu'un routeur, tel que la passerelle par défaut, reçoit un paquet, il examine l'adresse IP de destination pour déterminer le réseau de destination. La table de routage d'un routeur stocke des informations sur les routes connectées directement et les routes distantes vers les réseaux IP. Si le routeur possède une entrée dans sa table de routage correspondant au réseau de destination, le routeur transfère le paquet. S'il n'existe aucune entrée de routage, le routeur peut transférer le paquet vers sa propre route par défaut, si elle est configurée, ou il abandonne le paquet.

Les entrées de la table de routage peuvent être configurées manuellement sur chaque routeur pour fournir le routage statique, ou les routeurs peuvent se transmettre les informations concernant les routes de manière dynamique à l'aide d'un protocole de routage.

Pour que les routeurs soient accessibles, l'interface de routeur doit être configurée. Pour activer une interface spécifique, passez en mode de configuration d'interface via la commande de configuration globale **interface** *type-et-numéro*.



Chapitre 7

7.0.1.1 Introduction

Les réseaux de données et Internet soutiennent le réseau humain en permettant une communication fiable entre les personnes. Nous pouvons, sur un même périphérique, utiliser des services aussi divers que les messageries électroniques, le Web ou les messageries instantanées pour envoyer des messages et recevoir des informations. Grâce aux applications telles que les clients de messagerie, les navigateurs Internet et les clients de messagerie instantanée, nous sommes en mesure d'envoyer et de recevoir des messages et des informations par le biais d'ordinateurs et de réseaux.

Les données envoyées par ces applications sont empaquetées, transportées et livrées à l'application voulue sur le périphérique de destination. Les processus décrits dans la couche transport OSI acceptent des données provenant de la couche application et les préparent pour les adresser à la couche réseau. La couche transport **prépare** les données à transmettre sur le réseau. Un ordinateur source communique avec un ordinateur destinataire pour décider de la méthode de division des données en **segments**, de la méthode permettant de s'assurer qu'aucun des segments n'est perdu et de la méthode de vérification permettant de savoir si tous les segments sont arrivés. Pour comprendre la couche transport, pensez à un service des expéditions qui prépare une seule commande composée de plusieurs colis à livrer.

Ce chapitre est consacré à l'étude du rôle de la couche transport dans le processus d'encapsulation des données d'application en vue de leur utilisation par la couche réseau. La couche transport remplit également les fonctions suivantes :

- Elle permet à plusieurs applications, par exemple la messagerie électronique et les réseaux sociaux, de communiquer sur le réseau simultanément, sur un seul périphérique

- Elle vérifie, si cela est nécessaire, que toutes les données sont reçues de façon fiable et dans l'ordre par l'application voulue ;

- Elle utilise des mécanismes de gestion des erreurs.

Objectifs pédagogiques

À l'issue de ce chapitre, vous serez en mesure d'effectuer les tâches suivantes :

- Expliquer l'utilité de la couche transport.

- Définir le rôle de la couche transport en matière de transfert de bout en bout des données entre applications.

- Décrire le rôle de deux protocoles de couche transport TCP/IP : TCP et UDP.

- Citer les principales fonctions de la couche transport, y compris en matière de fiabilité, d'adressage de ports et de segmentation.

- Expliquer comment les protocoles TCP et UDP gèrent, chacun, des fonctions clés

- Reconnaître les situations où l'utilisation des protocoles TCP ou UDP s'impose et fournir des exemples d'applications utilisant chacun de ces protocoles

7.1 Protocole de couche Transport

7.1.1 Transport des données

7.1.1.1 Rôle de la couche transport

La couche transport est chargée de l'établissement d'une session de communication temporaire entre deux applications et de l'acheminement des données entre ces deux applications. Une application génère les données à envoyer d'une application sur un hôte source vers une application sur un hôte de destination, quels que soient le type d'hôte de destination, le type de support sur lequel aura lieu la transmission, le chemin emprunté par les données, l'encombrement de la liaison et la taille du réseau. Comme le montre la figure, la couche transport constitue la liaison entre la couche application et les couches inférieures chargées de la transmission sur le réseau.

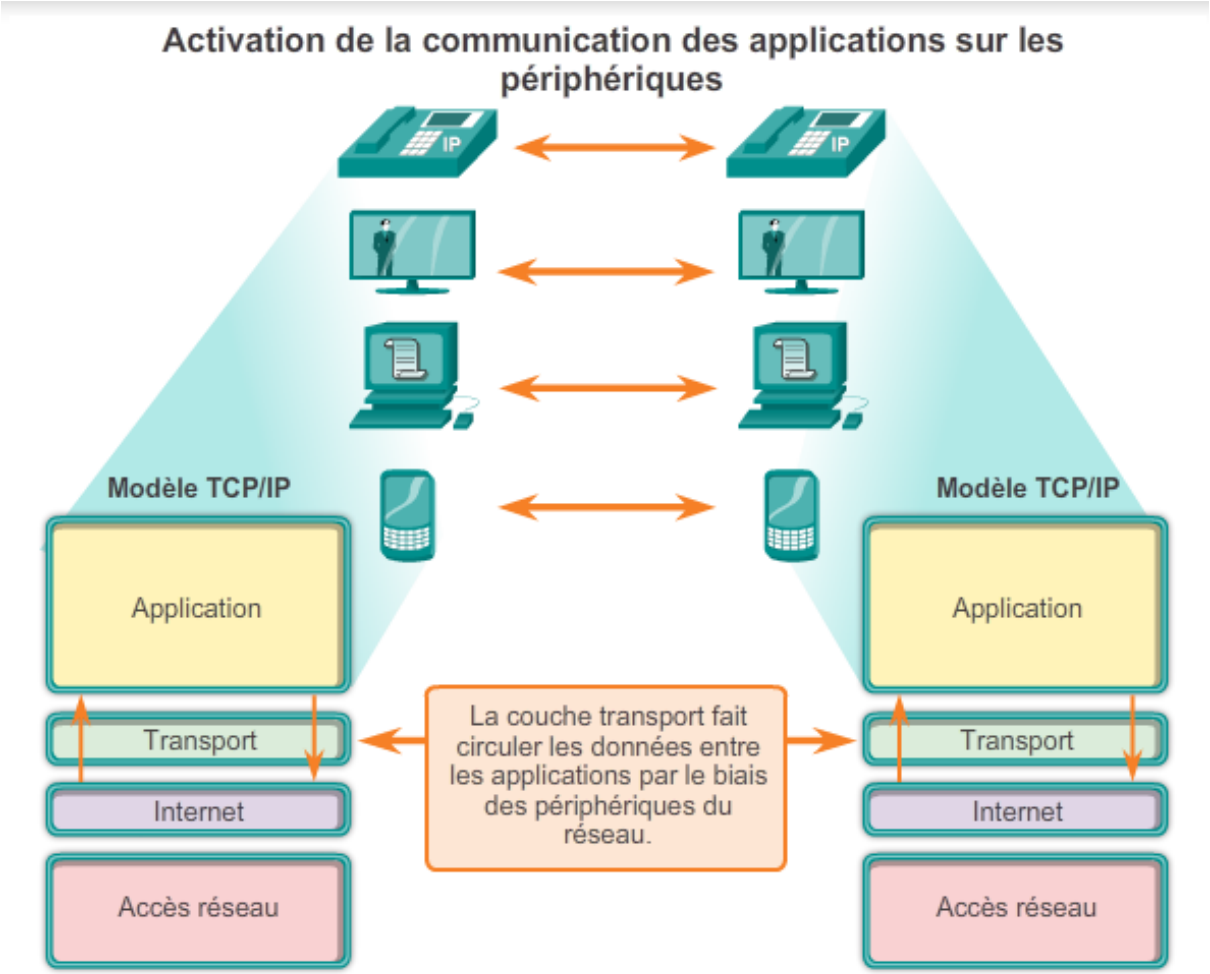
La couche transport fournit une méthode d'acheminement des informations sur l'ensemble du réseau qui garantit que les données peuvent être correctement rassemblées au niveau du destinataire. La couche transport segmente les données et se charge des contrôles nécessaires à la réorganisation de ces segments de données en différents flux de communication. Dans le cadre de la suite de protocoles TCP/IP, ces processus de segmentation et de réorganisation peuvent être réalisés à l'aide de deux protocoles de couche transport très différents : TCP (Transmission Control Protocol) et UDP (User Datagram Protocol).

Les protocoles de couche transport effectuent les tâches principales suivantes :

- Effectuer un suivi des communications individuelles entre les applications résidant sur les hôtes source et de destination ;

- Segmenter les données pour faciliter la gestion et réassembler les données segmentées en flux de données d'application vers la destination

- Identifier l'application appropriée pour chaque flux de communication



7.1.1.2 Rôle de la couche transport (suite)

Suivi des conversations individuelles

Au niveau de la couche transport, chaque ensemble de données transitant entre une application source et une application de destination est appelé une conversation (Figure 1). Un hôte peut héberger plusieurs applications qui communiquent sur le réseau simultanément. Chacune de ces applications communique avec une ou plusieurs applications sur un ou plusieurs hôtes distants. La couche transport est chargée de garantir ces multiples conversations et d'en effectuer le suivi.

Segmentation des données et reconstitution des segments

Les données doivent être préparées à être envoyées sur le support sous forme de blocs faciles à gérer. La plupart des réseaux limitent la quantité de données pouvant être incluses dans un paquet. Les protocoles de couche transport disposent de services qui segmentent les données d'application en blocs de données de taille appropriée (Figure 2). Il s'agit notamment de l'encapsulation devant s'appliquer à chaque bloc de données. Un en-tête, utilisé pour la réorganisation, est ajouté à chaque bloc de données. Cet en-tête est utilisé pour suivre le flux de données.

Au niveau du destinataire, la couche transport doit pouvoir reconstituer un flux de données complet utile pour la couche application à partir des blocs de données. Les protocoles intervenant au niveau de la couche transport gèrent la façon dont les informations d'en-tête de la couche transport sont utilisées pour réassembler les blocs de données en flux qui seront transmis à la couche application.

Identification des applications

De nombreux services ou applications peuvent s'exécuter sur chaque hôte du réseau. Pour que les flux de données atteignent les applications auxquelles ils sont destinés, la couche transport doit identifier l'application cible (Figure 3). Pour cela, la couche transport affecte un identificateur à chaque application. Cet identificateur est appelé numéro de port. Chaque processus logiciel ayant besoin d'accéder au réseau se voit affecter un numéro de port unique sur son hôte. La couche transport utilise des ports pour identifier l'application ou le service.

7.1.1.3 Multiplexage de conversations

Multiplexage de conversations

L'envoi de certains types de données (par exemple, un flux vidéo en continu) sur le réseau en tant que flux de communication complet peut utiliser toute la bande passante disponible et empêcher d'autres communications d'avoir lieu en même temps. Ceci rend également difficiles la reprise sur erreur et la retransmission des données endommagées.

La figure montre que la segmentation des données en parties plus petites permet à plusieurs communications différentes, provenant de nombreux utilisateurs, d'être imbriquées (multiplexées) sur le même réseau. La segmentation des données par les protocoles de couche transport permet d'envoyer et de recevoir des données tout en exécutant plusieurs applications simultanément sur un ordinateur.

Sans segmentation, une seule application pourrait recevoir des données. Par exemple, pour un flux vidéo en continu, le support serait monopolisé par le flux de communication, au lieu d'être partagé. Il serait impossible de recevoir des e-mails, de parler sur une messagerie instantanée et d'afficher des pages Web tout en regardant la vidéo.

Pour identifier chaque segment de données, la couche transport ajoute un en-tête contenant des données binaires au segment. Cet en-tête contient des champs de bits. Ce sont les valeurs contenues dans ces champs qui permettent aux différents protocoles de couche transport d'exécuter des fonctions diverses de gestion des communications de données.

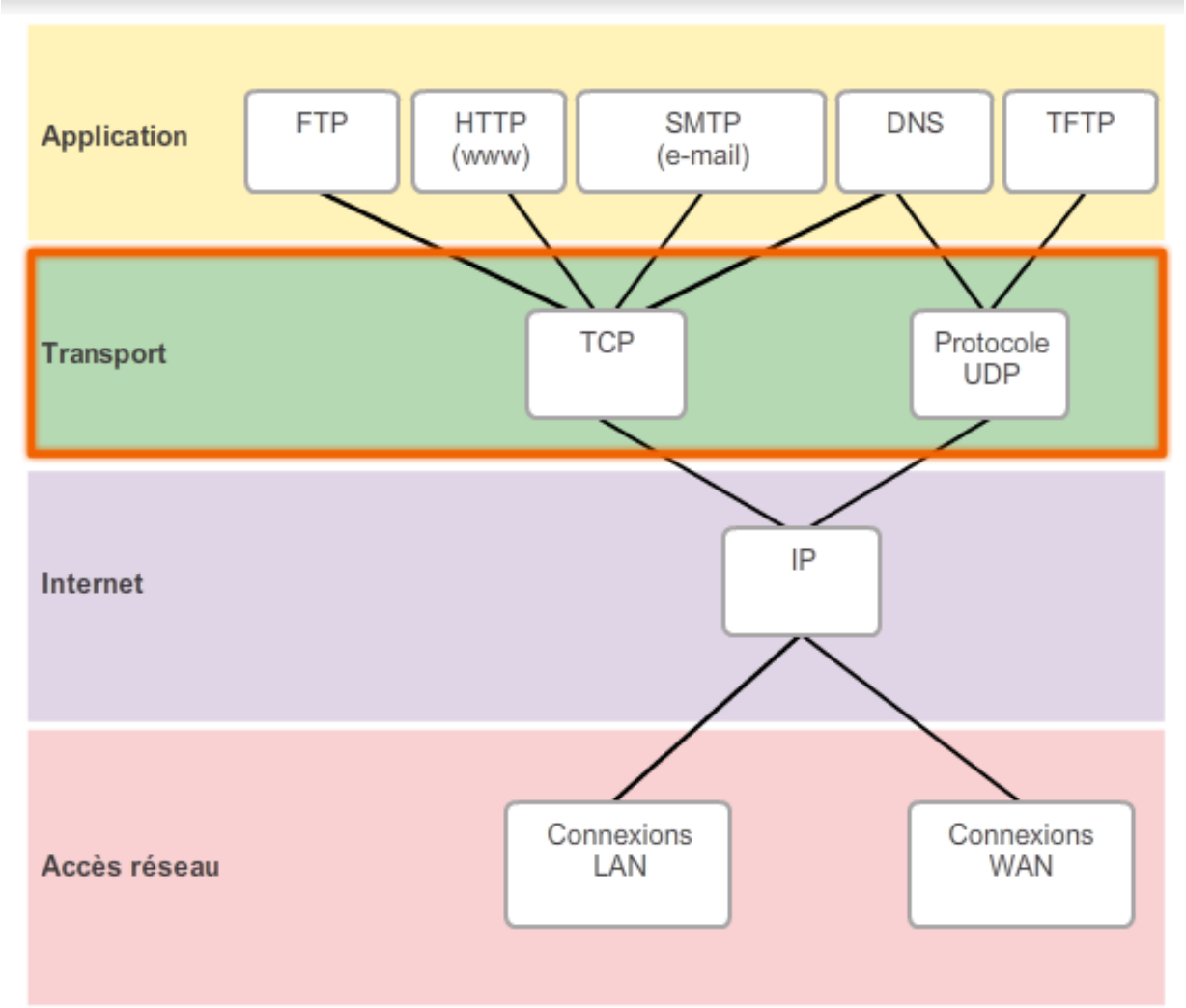
7.1.1.4 Fiabilité de la couche transport

La couche transport est également responsable de la gestion des exigences de fiabilité d'une conversation. Des applications différentes ont des exigences différentes en matière de fiabilité du transport.

Le protocole IP ne s'occupe que de la structure, de l'adressage et du routage des paquets. Il ne fixe pas le mode d'acheminement ou de transport des paquets. Les protocoles de transport

définissent comment transmettre les messages entre les hôtes. La suite de protocoles TCP/IP propose deux protocoles de couche transport, TCP et UDP, comme illustré dans la figure ci-contre. Le protocole IP utilise ces protocoles de transport pour permettre aux hôtes de communiquer et de transmettre des données.

Le protocole TCP est un protocole de couche transport fiable et complet, qui garantit que toutes les données arrivent à destination. En revanche, le protocole UDP est un protocole de couche transport très simple qui ne permet pas de garantir la fiabilité.



7.1.1.5 TCP

Comme indiqué précédemment, le protocole TCP est un protocole de transport fiable, ce qui signifie qu'il comprend des processus permettant d'assurer un acheminement fiable des données entre les applications par l'utilisation d'accusés de réception. Le transport TCP revient à envoyer des paquets qui sont suivis de la source à la destination. Si l'expédition de FedEx est divisée en plusieurs colis, un client peut vérifier en ligne l'ordre des livraisons.

Avec le protocole TCP, les trois fonctions de fiabilité de base sont :

- le suivi des segments de données transmis ;
- les accusés de réception des données ;
- la retransmission des données n'ayant pas fait l'objet d'un accusé de réception.

TCP découpe un message en petits morceaux appelés segments. Les segments, numérotés en séquence, sont ensuite passés au processus IP pour être assemblés en paquets. TCP conserve une trace du nombre de segments qui ont été envoyés à un hôte donné à partir d'une application spécifique. Si l'expéditeur ne reçoit pas d'accusé de réception au bout d'un certain temps, il suppose que les segments ont été perdus, et il les retransmet. Seule la partie du message qui a été perdue est renvoyée, pas l'intégralité. Sur l'hôte récepteur, TCP est responsable de la reconstitution des segments de message et de leur transmission à l'application. Les protocoles FTP (File Transfer Protocol et HTTP (Hypertext Transfer Protocol) sont des exemples d'applications qui utilisent le protocole TCP pour assurer l'acheminement des données.

Cliquez sur le bouton Lecture dans la figure pour voir une animation présentant des segments TCP transmis par l'expéditeur au destinataire.

Ces processus assurant la fiabilité augmentent la surcharge des ressources du réseau du fait des opérations d'accusé de réception, de suivi et de retransmission. Pour prendre en charge ces opérations assurant la fiabilité, un nombre plus important de données de contrôle est échangé entre les hôtes qui expédient et ceux qui reçoivent les données. Ces informations de contrôle sont contenues dans un en-tête TCP.

7.1.1.6 Protocole UDP

Tandis que les fonctionnalités de fiabilité TCP assurent l'efficacité des communications entre les applications, elles engendrent également une surcharge supplémentaire et des éventuels retards de transmission. Un compromis doit être établi entre la valeur accordée à la fiabilité et la charge qu'elle représente sur le réseau. Imposer une surcharge pour garantir la fiabilité de certaines applications peut réduire l'utilité de l'application et peut même porter préjudice à l'application. Dans ce cas, le protocole UDP représente un meilleur protocole de transport.

Le protocole UDP fournit uniquement des fonctions de base permettant d'acheminer des segments de données entre les applications appropriées avec peu de surcharge et de vérification des données. Le protocole UDP est un protocole d'acheminement au mieux. Dans le contexte des réseaux, l'acheminement au mieux est considéré comme n'étant pas fiable car aucun accusé de réception ne confirme que les données sont arrivées à destination. Avec le protocole UDP, aucun processus de couche transport ne signale à l'expéditeur si la transmission a réussi.

L'UDP revient à poster une lettre normale, sans accusé de réception. L'expéditeur de la lettre ne sait pas si le destinataire peut recevoir la lettre et le bureau de poste ne doit ni suivre la lettre ni informer l'expéditeur si la lettre n'arrive pas à la destination finale.

Cliquez sur le bouton Lecture dans la figure pour voir une animation des segments UDP transmis par l'expéditeur au destinataire.

7.1.1.7 Le bon protocole de couche transport pour la bonne application

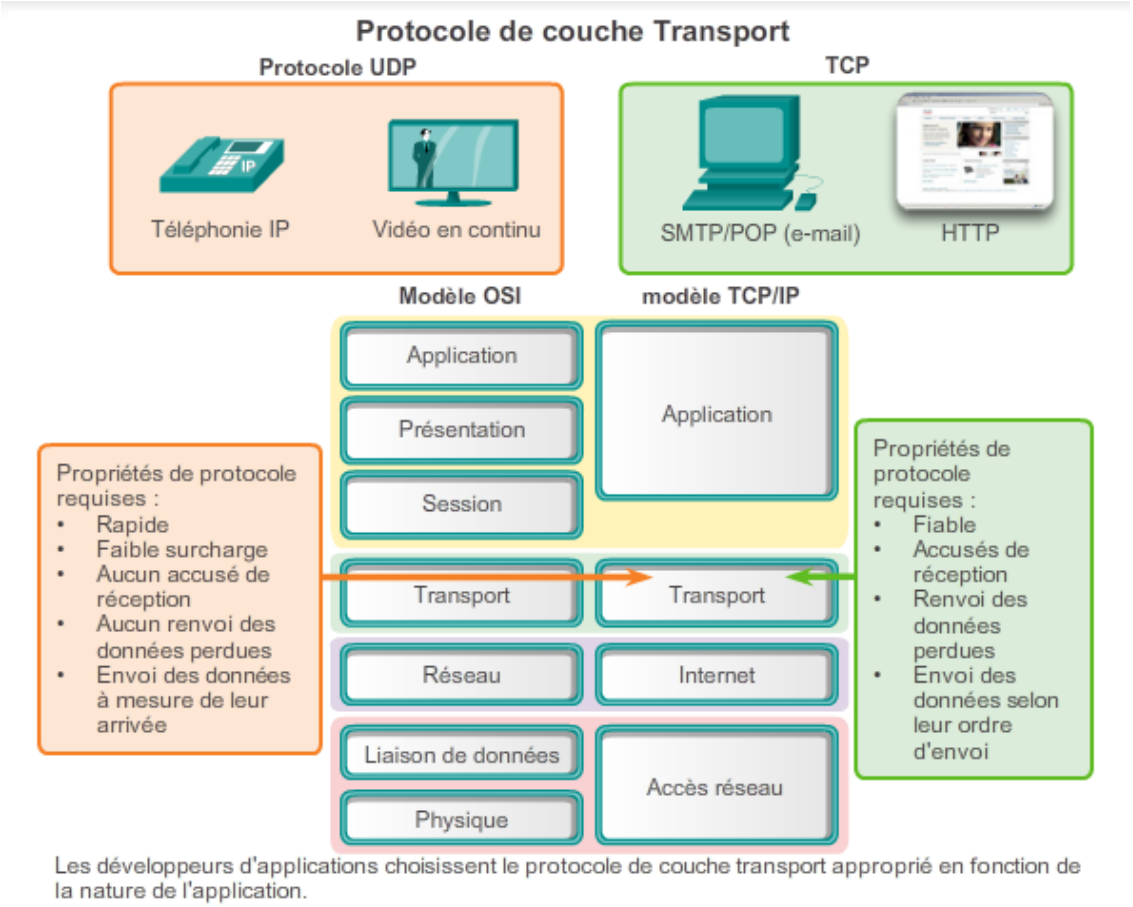
Les protocoles TCP et UDP sont des protocoles de transport valides. En fonction des besoins des applications, un ou deux de ces protocoles de transport peuvent être utilisés. Les développeurs d'applications doivent déterminer quel type de protocole de transport est approprié en fonction des exigences des applications.

Pour certaines applications, les segments doivent arriver dans un ordre donné pour être traités correctement. Pour d'autres applications, toutes les données doivent être entièrement reçues pour être utilisées. Dans les deux cas, le protocole TCP est utilisé comme protocole de transport. Par exemple, les applications telles que les bases de données, les navigateurs Web et les clients de messagerie ont besoin que toutes les données envoyées arrivent à destination dans leur état d'origine. Toute donnée manquante risque de corrompre la communication en la rendant incomplète ou illisible. Par conséquent, ces applications sont conçues pour utiliser le protocole TCP. On considère que cette surcharge supplémentaire pour le réseau est indispensable pour ces applications.

Dans d'autres cas, une application peut tolérer une certaine perte lors de la transmission de données sur le réseau, mais pas les retards de transmission. Le protocole UDP est le choix idéal pour ces applications, car il implique moins de surcharge sur le réseau. Le protocole UDP est à privilégier pour la lecture audio/vidéo en continu et la voix sur IP (VoIP). Les accusés de réception ralentiraient la livraison, et les retransmissions ne sont pas souhaitables.

Si, par exemple, un ou deux segments d'un flux vidéo en continu n'arrivent pas à destination, cela ne fait que créer une interruption momentanée du flux. Cela peut se traduire par une distorsion de l'image que l'utilisateur ne remarquera peut-être même pas. Cependant, l'image produite par un flux vidéo en continu serait fortement dégradée si le périphérique de destination devait rendre compte des données perdues et retarder la lecture le temps qu'elles arrivent. Dans ce cas, il est donc préférable de fournir la meilleure qualité vidéo possible en fonction des segments reçus et de renoncer à la fiabilité.

La radio sur Internet est un autre exemple d'application utilisant le protocole UDP. Si une partie du message est perdue pendant sa transmission via le réseau, elle n'est pas retransmise. Si certains paquets manquent, il se peut que la personne qui écoute entende de légères interruptions dans le son. Si TCP était utilisé et si les paquets perdus étaient renvoyés, la transmission serait interrompue pour recevoir ces paquets, et l'interruption se remarquerait davantage.



7.1.2 Présentation des protocoles TCP et UDP

7.1.2.1 Présentation du protocole TCP

Pour comprendre les différences entre les protocoles TCP et UDP, il est important de comprendre comment chaque protocole utilise des fonctions spécifiques de fiabilité et comment il effectue le suivi des communications.

Protocole TCP (Transmission Control Protocol)

Le protocole TCP a été initialement décrit dans le document RFC 793. Outre la prise en charge des fonctions de base de segmentation et de réorganisation des données, le protocole TCP, comme l'illustre la figure, fournit également :

- des conversations orientées connexion en établissant des sessions ;
- un acheminement fiable ;
- une reconstitution ordonnée des données ;
- le contrôle de flux.

Établissement de session

Le protocole TCP est un protocole orienté connexion. Un protocole orienté connexion est un protocole qui négocie et établit une connexion permanente (ou session) entre les périphériques source et de destination avant de transmettre du trafic. L'établissement de session prépare les périphériques à communiquer entre eux. Grâce à l'établissement de la session, les périphériques négocient la quantité de trafic pouvant être transmise à un moment donné et les données de communication peuvent être étroitement gérées. La session est interrompue une fois que toutes les communications sont terminées.

Acheminement fiable

Le protocole TCP est en mesure d'assurer l'acheminement fiable des données. Dans le contexte des réseaux, la fiabilité consiste à veiller à ce que chaque bloc de données envoyé par la source parvienne à destination. Bien des circonstances peuvent entraîner la corruption ou la perte d'un bloc de données lors de son transfert sur le réseau. Le protocole TCP peut garantir que tous les blocs atteignent leur destination en demandant au périphérique source de retransmettre les données perdues ou endommagées.

Livraison dans le même ordre

Étant donné que les réseaux peuvent fournir plusieurs routes dont les débits de transmission varient, il se peut que les données arrivent dans le désordre. En numérotant et en ordonnant les segments, le protocole TCP s'assure que ces segments sont remis dans le bon ordre.

Contrôle de flux

Les hôtes du réseau disposent de ressources limitées, par exemple en ce qui concerne la mémoire ou la bande passante. Quand le protocole TCP détermine que ces ressources sont surexploitées, il peut demander à l'application qui envoie les données d'en réduire le flux. Cette opération consiste à réguler la quantité de données transmises par la source. Le contrôle du flux contribue à prévenir la perte de segments sur le réseau et à rendre inutiles les retransmissions.

7.1.2.2 Rôle du protocole TCP

Une fois que le protocole TCP établit une session, il peut alors effectuer le suivi de la conversation dans cette session. En raison de la capacité de suivi des conversations réelles du protocole TCP, ce dernier est considéré comme un protocole avec état. Un protocole avec état est un protocole qui contrôle l'état de la session de communication. Par exemple, lorsque les données sont transmises à l'aide du protocole TCP, l'expéditeur s'attend à ce que la destination accuse réception des données. Le protocole TCP suit les informations qu'il a envoyées et sait quelles informations ont été reçues. Si aucun accusé de réception n'est reçu, l'expéditeur suppose que les données ne sont pas arrivées et les renvoie. La session avec état commence par l'établissement d'une session et se termine lorsque la session est interrompue.

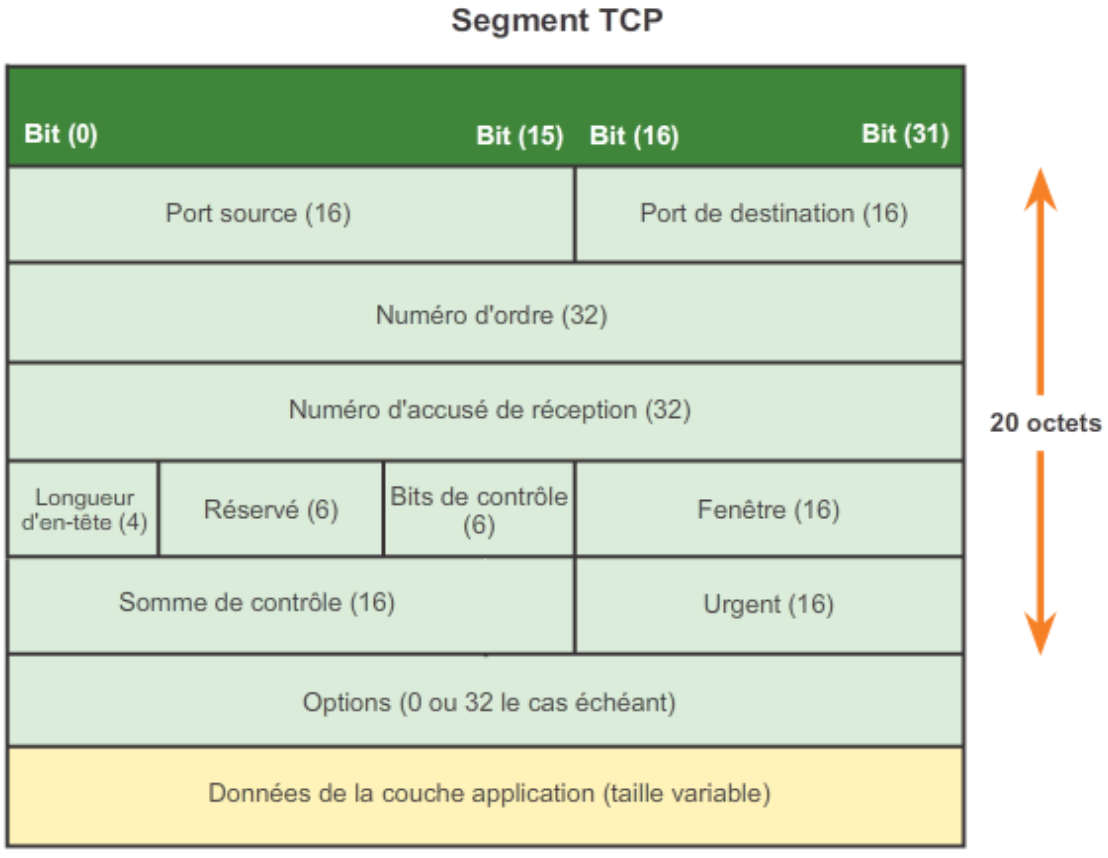
Remarque : la mise à jour de ces informations d'état nécessite des ressources qui ne sont pas nécessaires pour un protocole sans état, tel que le protocole UDP.

Le protocole TCP implique une surcharge pour bénéficier de ces fonctionnalités. Comme l'illustre la figure, chaque segment TCP utilise 20 octets dans l'en-tête pour encapsuler les

données de la couche application. C'est bien plus qu'un segment UDP, qui ne représente que 8 octets de surcharge. Cette surcharge comprend :

- **Un numéro d'ordre (32 bits)** – utilisé pour réorganiser les données.
- **Un numéro d'accusé de réception (32 bits)** – indique les données qui ont été reçues.
- **Le champ Longueur d'en-tête (4 bits)** – connue sous le nom de « décalage de données ». Indique la longueur de l'en-tête du segment TCP.
- **Le champ Réservé (6 bits)** - champ réservé pour les futures évolutions.
- **Des bits de contrôle (6 bits)** – comprennent des codes de bits, ou indicateurs, indiquant l'objectif et la fonction du segment TCP.
- **La taille de fenêtre (16 bits)** – indique le nombre de segments qui peuvent être acceptés en même temps.
- **La somme de contrôle (16 bits)** – utilisée pour le contrôle des erreurs sur l'en-tête et les données de segment.
- **Le champ Urgent (16 bits)** – indique si les données sont urgentes.

Le protocole TCP est par exemple utilisé par les navigateurs Web, les messageries et les applications de transfert de fichiers.



7.1.2.3 Présentation de l'UDP

protocole UDP (User Datagram Protocol)

Le protocole UDP est un protocole de transport d'acheminement au mieux, décrit dans le document RFC 768. Le protocole UDP est un protocole de transport léger qui offre les mêmes fonctions de segmentation et de réorganisation des données que le protocole TCP, mais sans la fiabilité et le contrôle de flux du protocole TCP. C'est un protocole simple, qui est généralement décrit en indiquant ce qu'il ne fait pas par rapport au protocole TCP.

Comme l'illustre la figure, les fonctionnalités suivantes constituent le protocole UDP :

- **Sans connexion** – le protocole UDP n'établit pas de connexion entre les hôtes avant que les données puissent être envoyées et reçues.

- **Acheminement non fiable** – le protocole UDP ne fournit pas de services garantissant que les données sont acheminées de façon fiable. Il n'existe pas de processus dans le protocole UDP permettant de faire retransmettre à l'expéditeur les données perdues ou endommagées.

- **Aucune reconstitution ordonnée des données** – parfois, les données sont reçues dans un ordre différent de celui dans lequel elles ont été envoyées. Le protocole UDP n'offre aucun mécanisme permettant de réorganiser les données dans leur ordre initial. Les données sont simplement remises à l'application dans l'ordre où elles arrivent.

- **Aucun contrôle de flux** – le protocole UDP ne propose aucun service permettant de contrôler la quantité de données envoyées par la source pour éviter de submerger le périphérique de destination. La source envoie les données. Si les ressources sur l'hôte de destination sont surexploitées, l'hôte de destination abandonne généralement les données envoyées jusqu'à ce que des ressources soient disponibles. Contrairement au protocole TCP, le protocole UDP ne fournit aucun mécanisme permettant de retransmettre automatiquement les données abandonnées.

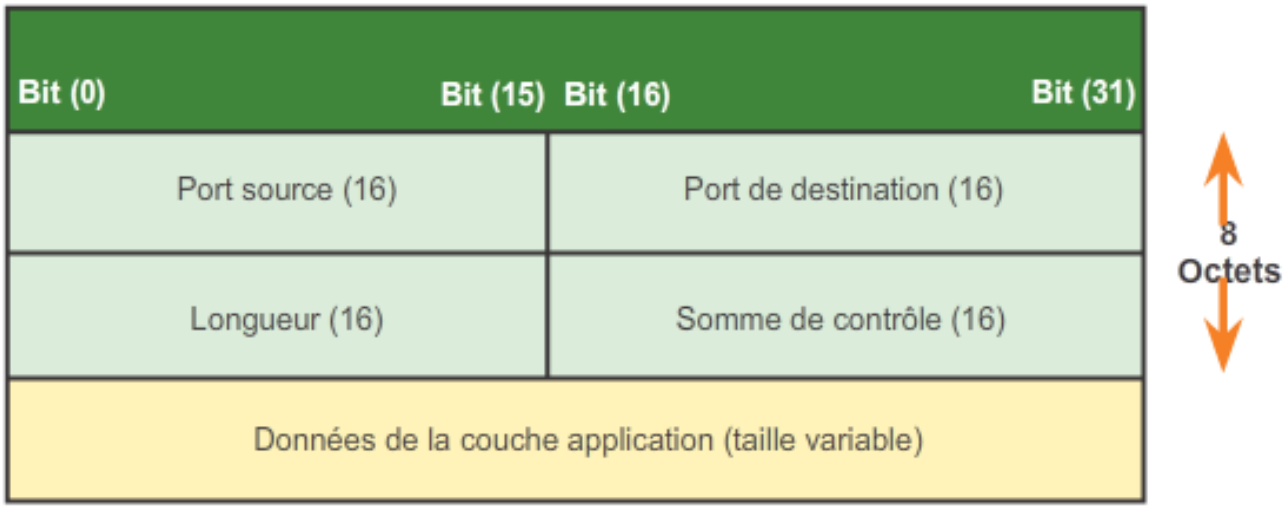
7.1.2.4 Rôle du protocole UDP

Bien que le protocole UDP n'inclue pas les mécanismes de fiabilité et de contrôle de flux du protocole TCP, comme l'illustre la figure, la faible surcharge pour l'acheminement des données du protocole UDP fait de ce dernier un protocole de transport idéal pour les applications qui peuvent tolérer certaines pertes de données. Les blocs de communications utilisés dans le protocole UDP sont appelés des datagrammes. Ces datagrammes sont envoyés « au mieux » par le protocole de couche transport. Le système de noms de domaine (DNS), la transmission vidéo en continu et la voix sur IP (VoIP) comptent parmi les applications utilisant le protocole UDP.

L'une des conditions les plus importantes pour fournir une vidéo en direct et faire transiter des données vocales sur un réseau est que le flux de données soit rapide. Les applications vidéo et de communication vocale peuvent tolérer certaines pertes de données, qui ont un impact faible ou nul, et sont donc parfaitement adaptées au protocole UDP.

UDP est un protocole sans état, c'est-à-dire que ni le client ni le serveur ne sont tenus de surveiller l'état de la session de communication. Comme l'illustre la figure, le protocole UDP n'est pas concerné par la fiabilité et le contrôle de flux. Les données peuvent être perdues ou reçues dans le désordre sans qu'aucun mécanisme UDP ne puisse récupérer ou réorganiser les données. Si la fiabilité est nécessaire dans le cadre de l'utilisation d'UDP comme protocole de transport, elle doit être prise en charge par l'application.

Datagramme UDP



7.1.2.5 Séparation de communications multiples

La couche transport doit pouvoir segmenter et gérer plusieurs communications ayant différentes exigences relatives au transport. Prenons comme exemple un utilisateur connecté à un réseau sur un périphérique final. L'utilisateur envoie et reçoit simultanément des e-mails et des messages instantanés, consulte des sites Web et passe un appel VoIP. Chacune de ces applications envoie des données sur le réseau et en reçoit simultanément, et ce malgré leurs différents besoins en termes de fiabilité. De plus, les données de l'appel VoIP ne sont pas orientées vers le navigateur Web et le texte des messages instantanés ne finit pas dans un e-mail.

Pour garantir la fiabilité, les utilisateurs ont besoin que les e-mails et les pages Web soient intégralement reçus et traités, afin que les informations soient considérées comme utiles. De légers retards dans le chargement des e-mails ou des pages Web sont généralement acceptables, tant que les produits finis s'affichent dans leur intégralité et correctement. Dans cet exemple, le réseau gère la réexpédition ou le remplacement des informations manquantes, et n'affiche pas le produit fini jusqu'à ce que tout soit reçu et correctement assemblé.

Dans le cas d'une conversation téléphonique, l'absence de quelques mots peut par contre être considérée comme acceptable. Même si certaines petites parties de quelques mots sont manquées, il est possible de déduire les mots manquants en fonction du contexte de la

conversation ou de demander à l'autre interlocuteur de répéter ce qui a été dit. Cela est considéré comme étant préférable aux retards causés si le réseau devait gérer et renvoyer les segments manquants. Dans notre exemple, c'est l'utilisateur, et non le réseau, qui gère la réexpédition ou la reconstitution des informations manquantes.

Comme l'illustre la figure, pour que les protocoles TCP et UDP gèrent ces conversations simultanées avec des besoins variables, les services TCP et UDP doivent surveiller les différentes applications en train de communiquer. Pour différencier les segments et les datagrammes de chaque application, les protocoles TCP et UDP utilisent chacun des champs d'en-tête identifiant ces applications de façon unique. Ces identificateurs uniques sont les numéros de port.

7.1.2.6 Adressage de ports TCP et UDP

L'en-tête de chaque segment ou datagramme contient un port source et un port de destination. Le numéro de port source est le numéro associé à l'application d'origine sur l'hôte local pour cette communication. Comme l'illustre la figure, le numéro de port de destination est le numéro de cette communication associé à l'application de destination sur l'hôte distant.

Lorsqu'un message est transmis à l'aide du protocole TCP ou UDP, les protocoles et services demandés sont identifiés par un numéro de port. Un port est un identifiant numérique, présent dans chaque segment, qui est utilisé pour conserver la trace de certaines conversations et de certains services de destination demandés. Chaque message envoyé par un hôte contient un port source et un port de destination.

Port de destination

Le client place un numéro de port de destination dans le segment pour informer le serveur de destination du service demandé. Par exemple, le port 80 renvoie au service HTTP ou Web. Lorsque le client spécifie le port 80 comme port de destination, le serveur qui reçoit le message sait que des services Web sont demandés. Un serveur peut proposer plusieurs services simultanément. Par exemple, il peut proposer des services Web sur le port 80 et, en même temps, l'établissement d'une connexion FTP sur le port 21.

Port source

Le numéro du port source est généré de manière aléatoire par le périphérique émetteur pour identifier une conversation entre deux périphériques. Ainsi, plusieurs conversations peuvent s'effectuer simultanément. En d'autres termes, un périphérique peut envoyer plusieurs requêtes de service HTTP à un serveur Web en même temps. Un suivi des différentes conversations est effectué sur la base des ports sources.

7.1.2.7 Adressage de ports TCP et UDP (suite)

Les ports sources et de destination sont placés à l'intérieur du segment. Les segments sont ensuite encapsulés dans un paquet IP. Le paquet IP contient l'adresse IP de la source et de la

destination. La combinaison des adresses IP source et de destination ainsi que des numéros de port source et de destination est appelée un socket. L'interface de connexion sert à identifier le serveur et le service demandés par le client. Chaque jour, des milliers d'hôtes communiquent avec des millions de serveurs différents. Ces communications sont identifiées par les sockets.

La combinaison du numéro de port de la couche transport et de l'adresse IP de la couche réseau de l'hôte suffit à identifier de manière unique un processus d'application particulier exécuté sur un périphérique hôte individuel. Cette combinaison est appelée un socket. Une paire de sockets, composée des adresses IP et numéros de port source et de destination, est également unique et identifie la conversation spécifique entre les deux hôtes.

Un socket client peut se présenter comme suit, 1099 représentant le numéro de port source : 192.168.1.5:1099.

Le socket d'un serveur Web peut avoir la forme suivante : 192.168.1.7:80

Ensemble, ces deux sockets constituent une paire de sockets : 192.168.1.5:1099, 192.168.1.7:80.

Avec la création de sockets, les points de communication sont connus de sorte que les données peuvent passer d'une application sur un hôte à une application sur un autre. Les sockets permettent à plusieurs processus exécutés sur un client de se différencier les uns des autres, et aux multiples connexions à un processus serveur de se distinguer les unes des autres.

Le port source d'une requête de client est généré aléatoirement. Le numéro de port fait office d'adresse de retour pour l'application envoyant la requête. La couche transport effectue le suivi du port et de l'application à l'origine de la requête afin que la réponse, quand elle sera envoyée, soit transmise à l'application appropriée. Le numéro de port de l'application envoyant la requête sert de numéro de port de destination dans la réponse renvoyée depuis le serveur.

7.1.2.8 Adressage de ports TCP et UDP (suite)

L'Internet Assigned Numbers Authority (IANA) attribue les numéros de port. L'IANA est une agence de normalisation responsable de l'affectation de diverses normes d'adressage.

Il existe différents types de numéros de port, comme illustré à la Figure 1 :

- **Ports réservés (numéros 0 à 1023)** – Ces numéros sont réservés à des services et applications. Ils sont généralement utilisés pour les applications telles que HTTP (serveur Web), Internet Message Access Protocol (IMAP)/Simple Mail Transfer Protocol (SMTP) (serveur de messagerie) et Telnet. En définissant ces ports réservés pour une utilisation par des applications serveur, il est possible de programmer les applications clientes de façon à ce qu'elles demandent à être connectées à un port précis et au service qui lui est associé.

- **Ports inscrits (numéros 1024 à 49151)** – Ces numéros de port sont affectés à des processus ou applications d'utilisateurs. Ces processus sont essentiellement des applications particulières qu'un utilisateur a choisi d'installer plutôt que des applications courantes qui recevraient un numéro de port réservé. Un client peut également sélectionner dynamiquement ces ports en tant que ports source lorsqu'ils ne sont pas utilisés par une ressource serveur.

- **Ports privés ou dynamiques (numéros 49152 à 65535)** – Également appelés ports éphémères, ces ports sont généralement affectés de façon dynamique à des applications clientes lorsqu'une connexion à un service est initiée par un client. Le port dynamique est très souvent utilisé pour identifier l'application cliente durant la communication, alors que le client utilise le port réservé pour identifier et se connecter au service demandé au serveur. Il est relativement rare pour un client de se connecter à un service par le biais d'un port dynamique ou privé (bien que certains programmes de partage de fichiers peer-to-peer utilisent ces ports).

La Figure 2 représente certains des ports réservés et inscrits dans le cadre du protocole TCP. La Figure 3 représente certains des ports réservés et inscrits dans le cadre du protocole UDP.

Utilisation du protocole TCP et du protocole UDP

Certaines applications peuvent utiliser à la fois le protocole TCP et le protocole UDP (Figure 4). En effet, la faible surcharge du protocole UDP permet au service DNS de gérer très rapidement de nombreuses requêtes de clients. Parfois, cependant, l'envoi des informations demandées exige la fiabilité du protocole TCP. Dans ce cas, le port réservé 53 est utilisé par les deux protocoles en association avec ce service.

Une liste à jour des numéros de port et des applications associées est disponible sur le site Web de l'organisme IANA.

7.1.2.9 Adressage de ports TCP et UDP (suite)

Il est parfois nécessaire de savoir quelles connexions TCP actives sont ouvertes et s'exécutent sur un hôte en réseau. L'utilitaire netstat est un utilitaire de réseau important qui peut être utilisé pour vérifier ces connexions. Il répertorie le protocole utilisé, l'adresse et le numéro de port locaux, l'adresse et le numéro de port distants, et l'état de la connexion.

Les connexions TCP inexpliquées peuvent constituer un risque majeur, car elles peuvent indiquer que quelque chose ou que quelqu'un est connecté à l'hôte local. En outre, les connexions TCP inutiles consomment des ressources système importantes et ralentissent donc les performances de l'hôte. L'utilitaire netstat doit être utilisé pour examiner les connexions ouvertes sur un hôte lorsque les performances semblent se dégrader.

La commande **netstat** dispose de nombreuses options utiles. Cliquez sur les boutons des figures 1 à 5 pour voir les différents résultats de la commande **netstat**.

7.1.2.10 Segmentation TCP et UDP

Dans un chapitre précédent, nous vous avons expliqué qu'une unité de données de protocole (PDU) est élaborée en faisant transiter les données d'une application par diverses couches afin de créer une PDU qui est ensuite transmise sur le support. Une fois les données parvenues sur l'hôte de destination, le processus est inversé jusqu'à ce que les données puissent être communiquées à l'application.

Certaines applications transmettent de très importants volumes de données pouvant parfois atteindre plusieurs gigaoctets. Transmettre l'ensemble de ces données en un envoi massif serait peu pratique car aucun autre trafic ne pourrait être transmis sur le réseau pendant l'envoi de ces données. De plus, l'envoi d'une grosse quantité de données peut prendre de plusieurs minutes à plusieurs heures. En outre, en cas d'erreurs, l'ensemble du fichier de données serait perdu ou devrait être renvoyé. La mémoire tampon des périphériques réseau ne serait pas suffisante pour stocker autant de données pendant leur transmission ou leur réception. La limite varie selon la technologie réseau employée et le support physique particulier qui est utilisé.

Diviser les données d'application en blocs permet de s'assurer que les données sont transmises en tenant compte des limites du support et que les données provenant d'applications différentes peuvent faire l'objet d'un multiplexage sur le support.

Les protocoles TCP et UDP traitent différemment la segmentation.

Comme l'illustre la figure, chaque en-tête de segment TCP contient un numéro d'ordre permettant aux fonctions de la couche transport sur l'hôte de destination de réassembler les segments dans l'ordre dans lequel ils ont été transmis. L'application de destination peut ainsi disposer des données sous la forme exacte voulue par l'expéditeur.

Bien que les services utilisant le protocole UDP effectuent également un suivi des conversations entre les applications, ils ne prêtent pas attention à l'ordre dans lequel les informations ont été transmises ni au maintien de la connexion. Un en-tête UDP ne contient pas de numéro d'ordre. La conception du protocole UDP est plus simple et produit moins de surcharge que le protocole TCP, de sorte que le transfert de données est plus rapide.

Il se peut que les informations arrivent dans un ordre différent de celui dans lequel elles ont été transmises car les différents paquets peuvent emprunter des chemins différents sur le réseau. Les applications qui utilisent le protocole UDP doivent tolérer le fait que les données peuvent arriver dans un ordre différent de celui dans lequel elles ont été envoyées.

7.2 TCP et UDP

7.2.1 Communication TCP

7.2.1.1 Acheminement fiable TCP

La fiabilité est le principal élément différenciateur entre les protocoles TCP et UDP. La fiabilité des communications TCP est obtenue grâce aux sessions orientées connexion. Avant qu'un hôte utilisant le protocole TCP n'envoie des données à un autre hôte, le protocole TCP initie un processus destiné à établir une connexion avec la destination. Cette connexion rend possible le suivi d'une session ou d'un flux de communication entre les hôtes. Ce processus veille à ce que chaque hôte soit notifié du flux de communication et qu'il y soit préparé. Une conversation TCP nécessite l'établissement d'une session entre les hôtes dans les deux directions, comme illustré dans l'animation.

Une fois une session établie et le transfert des données commencé, la destination envoie des accusés de réception à la source pour les segments qu'elle reçoit. Ces accusés constituent l'élément de base de la fiabilité dans la session TCP. Quand la source reçoit un accusé de réception, elle sait que les données ont bien été reçues et qu'elle peut cesser d'en effectuer le suivi. Si la source ne reçoit pas d'accusé de réception dans un délai prédéterminé, elle retransmet ces données vers la destination.

La surcharge provoquée par l'utilisation du protocole TCP provient en partie du trafic réseau généré par les accusés de réception et les retransmissions. L'établissement des sessions crée une surcharge prenant la forme d'un échange de segments supplémentaires. Une surcharge supplémentaire provoquée par la nécessité d'effectuer un suivi des segments pour lesquels on attend un accusé de réception et par le processus de retransmission pèse également sur les hôtes individuels.

7.2.1.2 Processus serveur TCP

Les processus d'application s'exécutent sur les serveurs. Un seul serveur peut exécuter plusieurs processus d'application simultanément. Ces processus attendent qu'un client lance une requête d'informations ou d'autres services.

Chaque processus applicatif qui s'exécute sur le serveur est configuré par défaut, ou manuellement par un administrateur système, pour utiliser un numéro de port. Deux services ne peuvent pas être affectés au même numéro de port d'un serveur au sein des mêmes services de la couche transport. Il est impossible qu'une application de serveur Web et une application de transfert de fichiers s'exécutant sur un hôte soient toutes deux configurées pour utiliser le même port (par exemple le port TCP 8080). Une application de serveur active affectée à un port spécifique est considérée comme étant ouverte, ce qui signifie que la couche transport accepte et traite les segments adressés à ce port. Toute requête entrante d'un client qui est adressée au socket correct est acceptée et les données sont transmises à l'application de serveur. De nombreux ports peuvent être ouverts simultanément sur un serveur, chacun étant destiné à une application de serveur active. Il est courant qu'un serveur fournisse plusieurs services simultanément, par exemple en tant que serveur Web et en tant que serveur FTP.

Limiter l'accès au serveur aux seuls ports associés aux services et applications devant être accessibles aux demandeurs autorisés est un moyen d'améliorer la sécurité sur le serveur.

Voir les figures 1 à 5 pour consulter l'affectation standard des ports source et de destination dans le cadre des opérations client-serveur TCP.

7.2.1.3 Établissement et fermeture d'une connexion TCP

Dans certaines cultures, lorsque deux personnes se rencontrent, elles se saluent en se serrant la main. Le fait de se serrer la main est perçu par les deux personnes comme un signe amical. D'une certaine manière, il en va de même pour les connexions sur le réseau. La première étape de la connexion nécessite la synchronisation. La deuxième étape consiste à accuser réception de la requête de synchronisation initiale et à synchroniser les paramètres de connexion dans la direction opposée. La troisième étape de connexion consiste à envoyer un accusé réception indiquant à la destination que la connexion peut être établie des deux côtés.

Lorsque deux hôtes communiquent à l'aide du protocole TCP, une connexion est établie avant que les données ne puissent être échangées. Une fois la communication terminée, les sessions sont fermées et il est mis fin à la connexion. Les mécanismes de connexion et de session permettent l'activation de la fonction de fiabilité du protocole TCP. Consultez la figure ci-contre pour découvrir les étapes de l'établissement et de la fermeture d'une connexion TCP.

Les hôtes suivent chaque segment de données au sein d'une session et échangent des informations sur les données reçues grâce aux informations contenues dans l'en-tête TCP. Le protocole TCP est un protocole bidirectionnel simultané, où chaque connexion représente deux flux de communication unidirectionnelle, ou sessions. Pour établir la connexion, l'hôte effectue une connexion en trois étapes. Les bits de contrôle de l'en-tête TCP indiquent la progression et l'état de la connexion. La connexion en trois étapes :

- Vérifie que le périphérique de destination est bien présent sur le réseau ;
- S'assure que le périphérique de destination a un service actif et qu'il accepte les requêtes sur le numéro de port de destination que le client qui démarre la session a l'intention d'utiliser ;
- Informe le périphérique de destination que le client source entend établir une session de communication sur ce numéro de port.

Dans le cadre des connexions TCP, l'hôte client établit la connexion avec le serveur. Les trois étapes de l'établissement d'une connexion TCP sont les suivantes :

Étape 1. Le client demande l'établissement d'une session de communication client-serveur avec le serveur.

Étape 2. Le serveur accuse réception de la session de communication client-serveur et demande l'établissement d'une session de communication serveur-client.

Étape 3. Le client accuse réception de la session de communication serveur-client.

Dans la figure, cliquez sur les boutons 1 à 3 pour en savoir plus sur l'établissement d'une connexion TCP.

Pour comprendre le processus de connexion en trois étapes, examinez les différentes valeurs échangées par les deux hôtes. Dans l'en-tête du segment TCP se trouvent six champs de 1 bit contenant des informations de contrôle qui servent à gérer les processus TCP. Il s'agit des champs :

- **URG** : pointeur de données urgentes valide
- **ACK** : champ d'accusé de réception valide
- **PSH** : fonction de livraison des données sans attendre le remplissage des tampons (Push)
- **RST** : réinitialisation de la connexion
- **SYN** : synchronisation des numéros d'ordre
- **FIN** : arrêt de l'envoi de données par l'expéditeur

Les champs ACK et SYN sont appropriés à notre analyse de la connexion en trois étapes.

7.2.1.4 Analyse de la connexion TCP en trois étapes - Étape 1

En utilisant les informations du logiciel d'analyse de protocoles, par exemple les résultats de Wireshark, vous pouvez examiner le fonctionnement de la connexion TCP en trois étapes :

Étape 1 : Le client demande l'établissement d'une session de communication client-serveur avec le serveur.

Un client TCP initie une connexion en trois étapes en envoyant un segment contenant l'indicateur de contrôle SYN qui indique une valeur initiale dans le champ de numéro d'ordre de l'en-tête. Cette valeur initiale du numéro d'ordre, appelée ISN (Initial Sequence Number), est choisie de façon aléatoire et sert à commencer le suivi du flux de données entre le client et le serveur pour cette session. L'ISN figurant dans l'en-tête de chaque segment est incrémenté de un pour chaque octet de données envoyé par le client au serveur tandis que la conversation de données se poursuit.

Comme l'illustre la figure ci-contre, le résultat d'un analyseur de protocole affiche l'indicateur de contrôle SYN et le numéro d'ordre relatif.

L'indicateur de contrôle SYN est défini et le numéro d'ordre relatif est égal à 0. Bien que l'analyseur de protocole dans le graphique présente les valeurs relatives des numéros d'ordre et d'accusé de réception, les valeurs réelles sont des nombres binaires de 32 bits. La figure illustre les quatre octets au format hexadécimal.

7.2.1.5 Analyse de la connexion TCP en trois étapes - Étape 2

Étape 2 : Le serveur accuse réception de la session de communication client-serveur et demande l'établissement d'une session de communication serveur-client.

Le serveur TCP doit accuser réception du segment SYN provenant du client pour établir la session du client vers le serveur. Pour cela, le serveur renvoie au client un segment accompagné de l'indicateur ACK indiquant que le numéro d'accusé de réception est valide. Grâce à cet indicateur présent dans le segment, le client identifie ceci comme un accusé de réception indiquant que le serveur a reçu le SYN du client TCP.

La valeur du champ de numéro d'accusé de réception est égale à l'ISN + 1. Cela établit une session du client au serveur. L'indicateur ACK demeure défini pour le reste de la session. Souvenez-vous que la communication entre le client et le serveur est composée de deux sessions unidirectionnelles : une allant du client vers le serveur et l'autre du serveur vers le client. Dans le cadre de la deuxième étape de la connexion en trois étapes, le serveur doit déclencher la réponse au client. Pour lancer cette session, le serveur utilise l'indicateur SYN comme le client l'a fait. Il inclut l'indicateur de contrôle SYN dans l'en-tête pour établir une session du serveur vers le client. L'indicateur SYN précise que la valeur initiale du champ de numéro d'ordre se trouve dans l'en-tête. Cette valeur sert à effectuer le suivi du flux de données dans cette session, du serveur vers le client.

Comme l'illustre la figure ci-contre, les résultats de l'analyseur de protocole montrent que les indicateurs de contrôle ACK et SYN sont définis et les numéros d'ordre et d'accusé de réception relatifs sont affichés.

7.2.1.6 Analyse de la connexion TCP en trois étapes - Étape 3

Étape 3 : Le client accuse réception de la session de communication serveur-client.

Enfin, le client TCP répond à l'aide d'un segment contenant un ACK qui constitue la réponse au SYN TCP envoyé par le serveur. Ce segment ne contient pas de données de l'utilisateur. La valeur du champ de numéro d'accusé de réception est supérieure de 1 au numéro d'ordre initial reçu du serveur. Quand les deux sessions sont établies entre le client et le serveur, tous les segments supplémentaires échangés dans cette communication comportent l'indicateur ACK défini.

Comme l'illustre la figure ci-contre, les résultats de l'analyseur de protocole montrent l'indicateur de contrôle ACK défini et les numéros relatifs d'ordre et d'accusé de réception.

Il est possible de sécuriser le réseau de données en :

- Refusant l'établissement de sessions TCP ;

- Autorisant uniquement l'établissement de sessions pour des services spécifiques ;
- Autorisant uniquement le trafic faisant déjà partie de sessions établies.

Ces mesures de sécurité peuvent être implémentées pour toutes les sessions TCP ou uniquement pour certaines sessions.

7.2.1.7 Analyse de l'interruption d'une session TCP

Pour mettre fin à une connexion, l'indicateur de contrôle FIN (Finish) doit être défini dans l'en-tête de segment. Pour mettre fin à chaque session TCP unidirectionnelle, on utilise un échange en deux étapes, constitué d'un segment FIN et d'un segment ACK. Par conséquent, pour mettre fin à une seule conversation TCP, quatre échanges sont nécessaires pour mettre fin aux deux sessions (voir la Figure 1).

Remarque : les termes client et serveur sont utilisés ici pour simplifier l'explication, mais le processus d'interruption peut être initié par n'importe lequel des deux hôtes ayant une session ouverte :

Étape 1 : quand le client n'a plus de données à envoyer dans le flux, il envoie un segment dont l'indicateur FIN est défini.

Étape 2 : le serveur envoie un segment ACK pour informer de la bonne réception du segment FIN, afin de fermer la session du client au serveur.

Étape 3 : le serveur envoie un segment FIN au client pour mettre fin à la session du serveur au client.

Étape 4 : le client répond à l'aide d'un segment ACK pour accuser réception du segment FIN envoyé par le serveur.

Quand le client n'a plus aucune donnée à transférer, il définit l'indicateur FIN dans l'en-tête d'un segment. Ensuite, le serveur de la connexion envoie un segment normal contenant des données dont l'indicateur ACK est défini en utilisant le numéro d'accusé de réception, confirmant ainsi que tous les octets de données ont été reçus. Quand la réception de tous les segments a été confirmée, la session est fermée.

La session dans l'autre sens est fermée selon le même processus. Le récepteur indique qu'il n'y a plus de données à envoyer en définissant l'indicateur FIN dans l'en-tête d'un segment envoyé à la source. Un accusé de réception confirme que tous les octets de données ont été reçus et que cette session, à son tour, se ferme.

Voir les figures 2 et 3 pour voir les indicateurs de contrôle FIN et ACK définis dans l'en-tête de segment, permettant ainsi l'interruption d'une session HTTP.

Il est également possible de fermer la connexion à l'aide d'une connexion en trois étapes. Quand le client n'a plus de données à envoyer, il envoie un segment FIN au serveur. Si le

serveur n'a plus de données à envoyer, il peut répondre en définissant les indicateurs FIN et ACK simultanément et en combinant ainsi deux étapes en une. Le client répond par un segment ACK.

7.2.2 Fiabilité et contrôle de flux

7.2.2.1 Fiabilité du protocole TCP – Livraison ordonnée

Remise en ordre des segments

Quand des services envoient des données à l'aide du protocole TCP, il arrive que les segments parviennent à destination dans le désordre. Pour que le destinataire puisse comprendre le message d'origine, il faut que les données contenues dans ces segments soient réagencées dans leur ordre d'origine. Pour cela, des numéros d'ordre sont affectés à l'en-tête de chaque paquet.

Lors de la configuration de la session, un numéro d'ordre initial, ou ISN, est défini. L'ISN représente la valeur de début des octets de cette session qui est transmise à l'application destinataire. Lors de la transmission des données pendant la session, le numéro d'ordre est incrémenté du nombre d'octets ayant été transmis. Ce suivi des octets de données permet d'identifier chaque segment et d'en accuser réception individuellement. Il est ainsi possible d'identifier les segments manquants.

Les numéros d'ordre des segments assurent la fiabilité en indiquant comment réassembler et réorganiser les segments reçus, comme l'illustre la figure ci-contre.

Le processus TCP récepteur place les données d'un segment dans une mémoire tampon de réception. Les segments sont remis dans l'ordre correct et sont transmis à la couche application une fois qu'ils ont été réassemblés. Tous les segments reçus dont les numéros d'ordre ne sont pas contigus sont conservés en vue d'un traitement ultérieur. Ensuite, ces segments sont traités dans l'ordre quand les segments contenant les octets manquants sont reçus.

7.2.2.2 Fiabilité du protocole TCP – Accusé de réception et taille de fenêtre

Confirmation de la réception des segments

L'une des fonctions du protocole TCP consiste à garantir que chaque segment atteigne sa destination. Les services TCP sur l'hôte de destination accusent réception des données reçues à l'application source.

Le numéro d'ordre (SEQ) et le numéro d'accusé de réception (ACK) sont utilisés ensemble pour confirmer la réception des octets de données contenus dans les segments envoyés. Le numéro SEQ indique le nombre relatif d'octets qui ont été transmis dans cette session, y compris les octets dans le segment actuel. Le protocole TCP utilise le numéro ACK renvoyé à la source pour indiquer l'octet suivant que le destinataire s'attend à recevoir. C'est ce que l'on appelle un accusé de réception prévisionnel.

La source est informée que la destination a reçu tous les octets de ce flux de données jusqu'à l'octet indiqué par le numéro ACK, mais sans inclure ce dernier. L'hôte expéditeur est censé envoyer un segment qui utilise un numéro d'ordre égal au numéro ACK.

Souvenez-vous qu'en fait chaque connexion est composée de deux sessions unidirectionnelles. Les numéros SEQ et ACK sont échangés dans les deux sens.

Dans l'exemple de la figure ci-contre, l'hôte de gauche envoie des données à l'hôte de droite. Il envoie un segment contenant 10 octets de données pour cette session et un numéro d'ordre égal à 1 dans l'en-tête.

L'hôte récepteur reçoit le segment au niveau de la couche 4 et détermine que le numéro d'ordre est 1 et qu'il y a 10 octets de données. L'hôte renvoie alors un segment à l'hôte de gauche pour accuser la réception de ces données. Dans ce segment, l'hôte définit le numéro ACK sur 11 pour indiquer que le prochain octet de données qu'il prévoit de recevoir dans cette session est l'octet numéro 11. Quand l'hôte expéditeur reçoit cet accusé de réception, il peut envoyer le segment suivant contenant des données pour cette session commençant par l'octet numéro 11.

Dans notre exemple, si l'hôte expéditeur devait attendre un accusé de réception tous les 10 octets, le réseau subirait une forte surcharge. Pour réduire la surcharge due à ces accusés de réception, plusieurs segments de données peuvent être envoyés et faire l'objet d'un accusé de réception grâce à un seul message TCP en retour. Cet accusé de réception contient un numéro ACK basé sur le nombre total d'octets reçus dans la session. Prenons l'exemple d'un numéro d'ordre de début égal à 2000. Si 10 segments de 1 000 octets chacun étaient reçus, le numéro ACK 12001 serait renvoyé à la source.

La quantité de données qu'une source peut transmettre avant qu'un accusé de réception soit reçu est la « taille de fenêtre », qui est un champ de l'en-tête TCP qui permet de gérer les données perdues et le contrôle de flux.

7.2.2.3 Fiabilité du protocole TCP – Perte de données et retransmission

Traitement des pertes de segments

Qu'un réseau soit bien conçu ou non, il arrive que des données se perdent. Par conséquent, le protocole TCP fournit des méthodes de gestion des pertes de segments. Parmi elles se trouve un mécanisme de retransmission des segments contenant des données sans accusé de réception.

En général, un service sur l'hôte de destination utilisant le protocole TCP ne génère d'accusé de réception que pour les séquences contiguës d'octets. Si un ou plusieurs segments sont manquants, seules les données dans la première séquence contiguë d'octets sont reconnues. Par exemple, si les segments avec des numéros allant de 1500 à 3000 et de 3400 à 3500 sont reçus, le numéro ACK est 3001. Cela est dû au fait qu'il existe des segments avec les numéros SEQ 3001 à 3399 qui n'ont pas été reçus.

Lorsque le protocole TCP sur l'hôte source ne reçoit pas d'accusé de réception après un délai prédéterminé, il revient au dernier numéro ACK reçu et retransmet les données à partir de ce point. Le processus de retransmission n'est pas spécifié par le document RFC, mais il incombe à l'implémentation particulière du protocole TCP de le déterminer.

Dans une implémentation TCP classique, un hôte peut transmettre un segment, placer une copie du segment dans une file d'attente de retransmission et lancer un minuteur. Quand l'accusé de réception des données est reçu, le segment est supprimé de la file d'attente. Si l'accusé de réception n'est pas reçu avant l'écoulement du délai prévu, le segment est retransmis.

Cliquez sur le bouton Lecture de la figure pour voir l'animation expliquant la retransmission des segments perdus.

Aujourd'hui, les hôtes peuvent également utiliser une fonction facultative appelée « accusés de réception sélectifs » (SACK). Si les deux hôtes prennent en charge les accusés de réception sélectifs, la destination peut accuser réception des octets de segments ne se suivant pas et l'hôte ne retransmettra que les données manquantes.

7.2.2.4 Contrôle de flux TCP – Taille de fenêtre et accusés de réception

Contrôle de flux

Le protocole TCP inclut également des mécanismes de contrôle de flux. Le contrôle de flux aide à maintenir la fiabilité des transmissions TCP en réglant le flux de données entre la source et la destination pour une session donnée. Le contrôle de flux consiste à limiter la quantité de données de segments transférées en une seule fois et à demander des accusés de réception avant de transmettre davantage de données.

Pour effectuer le contrôle de flux, la première chose que le protocole TCP doit déterminer est la quantité de données de segments que le périphérique de destination peut accepter. L'en-tête TCP comprend un champ de 16 bits appelé la taille de fenêtre. Il s'agit du nombre d'octets que le périphérique de destination d'une session TCP peut accepter et traiter en une seule fois. La taille de fenêtre initiale est convenue lors du démarrage de la session, via la connexion en trois étapes entre la source et la destination. Une fois cette taille approuvée, le périphérique source doit limiter la quantité de données de segments envoyées au périphérique de destination en fonction de la taille de fenêtre. Une fois que le périphérique source a reçu un accusé de réception l'informant que les segments de données ont été reçus, il peut continuer à envoyer des données pour la session.

Pendant le délai d'attente de l'accusé de réception, l'expéditeur n'envoie pas de segment supplémentaire. Quand le réseau est encombré ou que les ressources de l'hôte récepteur subissent une forte pression, le délai peut augmenter. Plus ce délai s'allonge, plus le taux de transmission effectif des données de cette session diminue. Le ralentissement de la transmission de données de chaque session permet de réduire les conflits d'utilisation des ressources sur le réseau et sur le périphérique de destination lorsque plusieurs sessions sont en cours.

La figure ci-contre présente une représentation simplifiée de la taille de fenêtre et des accusés de réception. Dans cet exemple, la taille de fenêtre initiale d'une session TCP représentée est définie à 3000 octets. Lorsque l'expéditeur a transmis 3 000 octets, il attend l'accusé de réception de ces octets avant de transmettre d'autres segments de cette session. Une fois que l'expéditeur a reçu l'accusé de réception provenant du destinataire, il peut transmettre 3 000 octets supplémentaires.

Le protocole TCP utilise les tailles de fenêtre pour maintenir le plus haut débit de transmission possible sur le réseau et le périphérique de destination, tout en réduisant la perte et les retransmissions de données.

7.2.2.5 Contrôle de flux TCP – Suppression d'encombrement

Réduction de la taille de fenêtre

L'utilisation de tailles de fenêtres dynamiques permet également de contrôler le flux de données. Quand les ressources réseau sont soumises à de fortes contraintes, le protocole TCP peut réduire la taille de fenêtre afin d'imposer l'envoi plus fréquent d'accusés de réception pour les segments reçus. Ceci a pour effet de ralentir le taux de transmission car la source attend des accusés de réception des données plus fréquents.

L'hôte destinataire renvoie la valeur de taille de fenêtre à l'hôte expéditeur pour indiquer le nombre d'octets qu'il est prêt à recevoir. Si la destination doit ralentir le débit de communication parce que la mémoire tampon est limitée, elle peut envoyer une valeur de taille de fenêtre plus petite à la source en l'intégrant à un accusé de réception.

Comme l'illustre la figure ci-contre, si un hôte destinataire subit un encombrement, il peut répondre à l'hôte expéditeur en envoyant un segment dont la taille de fenêtre est réduite. Dans la figure ci-contre, on peut voir que l'un des segments a été perdu. Dans cette conversation, le destinataire a changé le champ de fenêtre dans l'en-tête TCP des segments renvoyés en le ramenant de 3 000 à 1 500. L'expéditeur a donc été obligé de réduire la taille de fenêtre à 1 500.

Après une période de transmission sans perte de données ni contrainte excessive sur les ressources, le destinataire commence à augmenter la taille de fenêtre, ce qui réduit la surcharge du réseau, car un nombre réduit d'accusés de réception doivent être envoyés. La taille de fenêtre continue à augmenter jusqu'à ce qu'une perte de données survienne, laquelle entraîne une réduction de la taille de fenêtre.

Ces augmentations et réductions dynamiques de la taille de fenêtre sont continues dans le cadre du protocole TCP. Dans les réseaux très efficaces, les tailles de fenêtre peuvent être très élevées car les données ne sont pas perdues. Dans les réseaux pour lesquels l'infrastructure sous-jacente est moins robuste, la taille de fenêtre demeure généralement assez faible.

7.2.3 Communication UDP

7.2.3.1 Faible surcharge et fiabilité du protocole UDP

Le protocole UDP est un protocole simple offrant des fonctions de couche transport de base. Il crée beaucoup moins de surcharge que le protocole TCP car il n'est pas orienté connexion et ne propose pas de mécanismes sophistiqués de fiabilité (retransmission, séquençage et contrôle de flux).

Cela ne signifie pas que les applications utilisant le protocole UDP ne sont jamais fiables, ni que le protocole UDP n'est pas efficace. Cela signifie simplement que ces fonctions ne sont pas fournies par le protocole de couche transport et qu'elles doivent être implémentées à un autre niveau, le cas échéant.

Bien que le volume total de trafic UDP d'un réseau standard soit relativement faible, des protocoles importants de couche application utilisent le protocole UDP, notamment :

- Système de noms de domaine (DNS)
- SNMP (Simple Network Management Protocol)
- Protocole DHCP (Dynamic Host Configuration Protocol)
- Protocole RIP (Routing Information Protocol)
- TFTP (Trivial File Transfer Protocol)
- Téléphonie IP ou voix sur IP (VoIP)
- Jeux en ligne

Certaines applications, comme les jeux en ligne ou la VoIP, peuvent tolérer la perte d'une certaine quantité de données. Si ces applications utilisaient le protocole TCP, elles risqueraient d'être confrontées à des retards importants lorsque le protocole TCP détecterait les pertes de données et retransmettrait les données. Ces délais seraient plus préjudiciables à l'application que la perte d'une petite quantité de données. Certaines applications, comme le système DNS, renvoient simplement la requête si aucune réponse n'est reçue. Par conséquent, elles n'ont pas besoin du protocole TCP pour garantir l'acheminement des messages.

La faible surcharge qu'engendre le protocole UDP rend celui-ci très intéressant pour de telles applications.

7.2.3.2 Réassemblage de datagrammes UDP

Comme le protocole UDP n'est pas orienté connexion, les sessions ne sont pas établies avant que la communication n'ait lieu comme c'est le cas avec le protocole TCP. On dit que le protocole UDP est basé sur les transactions : en d'autres termes, quand une application doit envoyer des données, elle les envoie tout simplement.

De nombreuses applications utilisant le protocole UDP envoient de petites quantités de données pouvant tenir dans un seul segment. Cependant, certaines applications envoient des volumes de données plus importants qui doivent être découpés en plusieurs segments. L'unité de données de protocole UDP est appelée un datagramme, bien que les termes segment et datagramme soient parfois utilisés indifféremment pour décrire une unité de données de protocole de la couche transport.

Quand plusieurs datagrammes sont envoyés vers une destination, ils peuvent emprunter des chemins différents et arriver dans le désordre. Le protocole UDP n'effectue pas de suivi des numéros d'ordre comme le fait le protocole TCP. Le protocole UDP ne peut pas réassembler les datagrammes dans leur ordre de transmission, comme illustré dans la figure.

Le protocole UDP se contente donc de réassembler les données dans l'ordre dans lequel elles ont été reçues, puis de les transmettre à l'application. Si l'ordre des données est important pour l'application, cette dernière doit identifier l'ordre correct et déterminer le mode de traitement des données.

7.2.3.3 Processus et requêtes des serveurs UDP

Comme c'est le cas avec des applications basées sur le protocole TCP, des numéros de port réservés ou inscrits sont affectés aux applications serveur basées sur le protocole UDP. Quand ces applications ou processus s'exécutent sur un serveur, ils ou elles acceptent les données correspondant au numéro de port attribué. Quand le protocole UDP reçoit un datagramme destiné à l'un de ces ports, il transmet les données applicatives à l'application appropriée d'après son numéro de port.

7.2.3.4 Processus des clients UDP

Comme c'est le cas avec le protocole TCP, la communication client-serveur est initiée par une application cliente qui demande des données à un processus serveur. Le processus client UDP sélectionne aléatoirement un numéro de port dans une plage de numéros de port dynamiques et l'utilise comme port source pour la conversation. Le port de destination est généralement le numéro de port réservé ou inscrit affecté au processus serveur.

Le choix aléatoire des numéros de port source présente également un avantage en matière de sécurité. Quand il existe un modèle prévisible de sélection du port de destination, il est plus facile pour un intrus de simuler un accès à un client en tentant de se connecter au numéro de port le plus susceptible d'être ouvert.

Étant donné que le protocole UDP ne crée pas de session, dès que les données sont prêtes à être envoyées et que les ports sont identifiés, le protocole UDP peut créer des datagrammes et les transmettre à la couche réseau, pour qu'ils soient adressés et envoyés sur le réseau.

Une fois qu'un client a choisi le port source et le port de destination, la même paire de ports est utilisée dans l'en-tête de tous les datagrammes employés dans la transaction. Quand des

données sont renvoyées du serveur vers le client, les numéros de port source et de port de destination sont inversés dans l'en-tête du datagramme.

Parcourez les figures du côté droit de l'écran pour voir les détails des processus client UDP.

7.2.4 TCP ou UDP, telle est la question

7.2.4.1 Applications utilisant le protocole TCP

De nombreuses applications ont besoin de la fiabilité et des autres services proposés par le protocole TCP. Ce sont des applications qui peuvent tolérer certains retards ou certaines baisses de performances en raison de la charge imposée par le protocole TCP.

Cela fait du protocole TCP une solution adaptée pour les applications qui ont besoin d'un transport fiable et qui peuvent tolérer certains retards. Le protocole TCP illustre parfaitement les rôles spécifiques des différentes couches de la pile de protocoles TCP/IP. Comme le protocole TCP de couche transport gère toutes les tâches associées à la segmentation du flux de données, à la fiabilité, au contrôle de flux et à la réorganisation des segments, il permet aux applications de ne pas avoir à gérer ces tâches. Les applications peuvent simplement envoyer le flux de données à la couche transport et utiliser les services du protocole TCP.

La figure ci-contre illustre certaines des applications courantes utilisant le protocole TCP :

- protocole HTTP (HyperText Transfer Protocol)
- Protocole FTP (File Transfer Protocol)
- Protocole SMTP (Simple Mail Transfer Protocol)
- Telnet

7.2.4.2 Applications utilisant le protocole UDP

Il existe trois types d'application plus adaptés au protocole UDP :

- les applications pouvant tolérer certaines pertes de données mais aucun retard ;
- les applications avec des transactions simples de requête et de réponse ;
- les communications unidirectionnelles pour lesquelles la fiabilité n'est pas requise ou peut être prise en charge par l'application.

De nombreuses applications vidéo et multimédias, telles que la VoIP et la télévision sur IP (IPTV), utilisent le protocole UDP. Ces applications peuvent tolérer une certaine perte de données avec un impact nul ou très faible sur la qualité. Les mécanismes de fiabilité du protocole TCP entraînent un certain délai pouvant affecter la qualité du son et de la vidéo reçus.

Les applications qui utilisent des transactions simples de requête et de réponse sont également adaptées au protocole UDP. Ce sont les applications dans le cadre desquelles un hôte envoie une requête qui peut se solder ou non par une réponse. Voici certaines de ces applications :

- DHCP
- DNS – peut également utiliser le protocole TCP
- SNMP
- TFTP

Certaines applications gèrent elles-mêmes la fiabilité des communications. Celles-ci n'ont pas besoin des services du protocole TCP et peuvent exploiter l'UDP comme protocole de couche transport. Le protocole TFTP illustre bien cela. Il possède ses propres mécanismes de contrôle de flux, de détection des erreurs, d'accusés de réception et de reprise après erreur. Il n'a donc pas besoin de s'appuyer sur le protocole TCP pour ces services.

CHAPITRE 8: ADRESSAGE IP

Introduction

L'adressage est l'une des fonctions principales des protocoles de couche réseau. Il permet de mettre en œuvre la transmission de données entre des hôtes situés sur un même réseau ou sur des réseaux différents. La version 4 (IPv4) et la version 6 (IPv6) du protocole IP fournissent un adressage hiérarchique pour les paquets qui transportent les données.

L'élaboration, la mise en œuvre et la gestion d'un modèle d'adressage IP garantissent un fonctionnement optimal des réseaux.

Ce chapitre décrit en détail la structure des adresses IP et leur application dans la création et le test de réseaux et de sous-réseaux IP.

Internet of Everything (IoE)

Si la nature, le trafic, le transport, les réseaux et l'exploration de l'espace dépendent du partage des informations numériques, comment ces informations peuvent-elles être identifiées de la source à la destination ?

Dans cet exercice, vous commencerez à réfléchir aux composants de l'IoE, mais également à l'adressage de tous les éléments dans cet univers !

- Lisez les blogs/actualités fournis par John Chambers concernant l'Internet of Everything – IoE – http://blogs.cisco.com/news/internet-of-everything-2. Regardez la vidéo au milieu de cette page.

- Ensuite, rendez-vous sur la page principale de l'IoE – http://www.cisco.com/web/tomorrow-starts-here/index.html. Cliquez sur une catégorie qui vous intéresse.

- Consultez la vidéo, le blog ou le fichier PDF correspondant à la catégorie qui vous intéresse.

- Écrivez 5 questions ou commentaire sur ce que vous avez vu ou lu. Partagez ensuite ces remarques avec la classe.

8.1 Adresses réseau IPv4

8.1.1 Structure de l'adresse IPv4

8.1.1.1 Notation binaire

Pour comprendre le fonctionnement des périphériques réseau, il convient d'aborder les adresses et les autres données de la même manière que les périphériques, c'est-à-dire en notation binaire. La notation binaire est une représentation d'informations qui n'utilise que des 1 et des 0. Les ordinateurs communiquent à l'aide de données binaires. Les données binaires peuvent être utilisées pour représenter de nombreux types de données. Par exemple, lorsque vous tapez sur un clavier, les lettres apparaissent à l'écran dans un format que vous pouvez

lire et comprendre. Cependant, l'ordinateur convertit chaque lettre en une série de chiffres binaires pour le stockage et le transport. Pour effectuer cette conversion, l'ordinateur utilise le code ASCII (American Standard Code for Information Interchange).

Selon l'ASCII, la lettre « A » est représentée sous forme binaire par 01000001, alors que la lettre « a » est représentée sous forme binaire par 01100001. Utilisez le convertisseur ASCII de la Figure 1 pour convertir des caractères ASCII en binaire.

Il n'est généralement pas nécessaire de connaître la conversion binaire des lettres, mais il est très important de comprendre l'utilisation du format binaire pour l'adressage IP. Chaque périphérique d'un réseau doit être identifié par une adresse binaire unique. Dans les réseaux IPv4, cette adresse est représentée par une chaîne de 32 bits (composée de 1 et de 0). Au niveau de la couche réseau, les paquets incluent ces informations d'identification uniques pour les systèmes source et de destination. Par conséquent, dans un réseau IPv4, chaque paquet inclut une adresse source de 32 bits et une adresse de destination de 32 bits dans l'en-tête de couche 3.

Pour la plupart des utilisateurs, il est difficile d'interpréter une chaîne de 32 bits et il est encore plus difficile de la mémoriser. Par conséquent, nous représentons les adresses IPv4 au format décimal à point et non au format binaire. De ce fait, nous traitons chaque octet en tant que nombre décimal compris dans une plage de 0 à 255. Pour comprendre ce processus, il est nécessaire d'avoir certaines compétences en matière de conversion de nombres binaires en nombres décimaux.

Numération pondérée

Pour maîtriser la conversion entre les nombres binaires et décimaux, il convient de comprendre ce qu'est le système de numérotation appelé numération pondérée. En numération pondérée, un caractère peut représenter différentes valeurs selon la position qu'il occupe. Dans le système décimal, la base est 10. Dans le système binaire, nous utilisons la base 2. Plus précisément, la valeur qu'un chiffre représente est le chiffre multiplié par la base élevé à la puissance correspondant à sa position. Quelques exemples nous permettront de mieux comprendre le fonctionnement de ce système.

Pour le nombre décimal 192, la valeur que le chiffre 1 représente est 1*10^2 (1 fois 10 à la puissance 2). Le 1 se trouve dans la position appelée « centaine ». La numération pondérée fait référence à cette position comme étant la position base^2 puisque la base est 10 et la puissance 2. Le chiffre 9 représente 9*10^1 (9 fois 10 puissance 1). La numération pondérée du nombre décimal 192 est illustrée à la Figure 2.

Avec la numération pondérée en base 10, 192 représente :

192 = (1 * 10^2) + (9 * 10^1) + (2 * 10^0)

ou

192 = (1 * 100) + (9 * 10) + (2 * 1

8.1.1.2 Système binaire

Pour l'IPv4, les adresses sont des nombres binaires de 32 bits. Cependant, pour une plus grande facilité d'utilisation, les schémas binaires représentant les adresses IPv4 sont exprimés en notation décimale à point. Cela est effectué en séparant tout d'abord tous les octets (8 bits) du schéma binaire de 32 bits par un point. Le nom d'« octet » s'explique par le fait que chaque nombre décimal représente 8 bits.

L'adresse binaire

11000000 10101000 00001010 00001010

est exprimée en décimale à point de la manière suivante :

192.168.10.10

Dans la Figure 1, cliquez sur chaque bouton pour voir comment l'adresse binaire de 32 bits est représentée par des octets sous forme de décimales à point.

Mais comment sont déterminés les équivalents décimaux réels ?

Système binaire

Dans le système binaire, la base est 2. Par conséquent, chaque position représente une augmentation de la puissance de 2. Dans les nombres binaires de 8 bits, les positions représentent les quantités suivantes :

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 64 32 16 8 4 2 1

Le système de base 2 ne comprend que deux chiffres : 0 et 1.

Lorsque nous interprétons un octet dans sa forme décimale, nous obtenons le nombre que les positions représentent si le chiffre est 1 et aucun nombre si le chiffre est 0, comme illustré à la Figure 1.

La Figure 2 illustre la représentation binaire du nombre décimal 192. Un 1 dans une certaine position indique que nous ajoutons cette valeur au total. Un 0 signifie que nous n'ajoutons pas cette valeur. Le nombre binaire 11000000 a un 1 en position 2^7 (valeur décimale : 128) et un 1 en position 2^6 (valeur décimale : 64). Les bits restants sont des 0, donc nous n'ajoutons pas les valeurs décimales correspondantes. Le résultat de l'addition 128+64 est 192, l'équivalent décimal de 11000000.

Voici deux exemples :

Exemple 1 : un octet contenant uniquement des 1, 11111111

Un 1 dans chaque position indique que la valeur de cette position est ajoutée au total. Un octet composé uniquement de 1 implique que les valeurs de chaque position sont incluses dans le total, par conséquent, le total de tous les 1 est égal à 255.

128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

Exemple 2 : un octet contenant uniquement des 0, 00000000

Un 0 dans chaque position indique que la valeur de cette position n'est pas ajoutée au total. Avec un 0 dans chacune des positions, un total de 0 est obtenu.

0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0

Une combinaison différente de uns et de zéros donne une valeur décimale différente.

8.1.1.3 Conversion d'une adresse binaire en adresse décimale

Chaque octet est constitué de 8 bits, qui ont chacun une valeur de 0 ou 1. Les quatre groupes de 8 bits ont le même ensemble de valeurs valides, comprises entre 0 et 255 (inclus). La valeur de chaque position de bit, de la droite vers la gauche, est 1, 2, 4, 8, 16, 32, 64 et 128.

Déterminez la valeur de l'octet en ajoutant les valeurs de positions chaque fois qu'un 1 binaire est présent.

- Si, dans un rang, la valeur est 0, n'ajoutez pas de valeur.
- Si les 8 bits sont des 0, 00000000, la valeur de l'octet est 0.
- Si les 8 bits sont des 1, 11111111, la valeur de l'octet est 255 (128+64+32+16+8+4+2+1).
- Si les 8 bits sont mixtes, les valeurs sont ajoutées. Par exemple, l'octet 00100111 a une valeur de 39 (32+4+2+1).

Ainsi, la valeur de chacun des quatre octets peut aller de 0 à 255 au maximum.

En utilisant l'adresse IPv4 de 32 bits 11000000101010000000101000001010, convertissez la représentation binaire en notation décimale à point en procédant comme suit :

Étape 1. Diviser les 32 bits en 4 octets.

Étape 2. Convertir chaque octet en nombre décimal.

Étape 3. Ajouter un point entre chaque nombre décimal.

Cliquez sur Lecture dans la figure pour voir comment une adresse binaire est convertie en décimale à point.

8.1.1.5 Conversion de nombres décimaux en nombres binaires

En plus d'être capable de convertir un nombre binaire en nombre décimal, il est également nécessaire de comprendre la conversion d'un nombre décimal en binaire.

Puisque nous représentons les adresses IPv4 sous forme de décimales à point, il suffit que nous examinions le processus de conversion d'un nombre binaire de 8 bits en valeurs décimales comprises entre 0 et 255 pour chaque octet d'une adresse IPv4.

Déterminons d'abord si le nombre décimal est supérieur ou égal à la valeur décimale la plus grande représentée par le bit de poids fort. À la position le plus à gauche, nous déterminons si la valeur d'octet est supérieure ou égale à 128. Si la valeur d'octet est inférieure à 128, nous plaçons un 0 dans cette position binaire pour la valeur décimale 128 et nous passons à la position de bit correspondant à la valeur décimale 64.

Si la valeur de l'octet à la position correspondant à la valeur décimale 128 est supérieure ou égale à 128, nous plaçons un 1 dans cette position binaire et soustrayons 128 à la valeur à convertir. Nous comparons le reste de cette opération à la plus petite valeur suivante, 64. Nous répétons cette procédure pour toutes les positions de bit restantes.

Cliquez sur les figures 1 à 6 pour afficher le processus de conversion du nombre 168 en équivalent binaire, 10101000

Suivez les étapes de conversion des figures pour observer la conversion d'une adresse IP en nombres binaires.

Figure 1 : Convertissez 192 en binaire.

Figure 2 : Convertissez 168 en binaire.

Figure 3 : Convertissez 10 en binaire.

Figure 4 : Convertissez 10 en binaire.

Figure 5 : Combinez les octets convertis en commençant par le premier octet

8.1.2 Masque de sous-réseau IPv4

8.1.2.1 Partie réseau et partie hôte d'une adresse IPv4

Comprendre la notation binaire est important pour déterminer si deux hôtes sont sur le même réseau. Rappelez-vous qu'une adresse IP est une adresse hiérarchique qui se compose de deux parties : une partie réseau et une partie hôte. Lorsque vous déterminez la partie réseau et la partie hôte, il est nécessaire d'examiner non pas la valeur décimale, mais le flux de 32 bits.

Dans le flux de 32 bits, une partie des bits constitue la partie réseau et une autre partie des bits compose la partie hôte.

Les bits de la partie réseau de l'adresse doivent être identiques pour tous les périphériques installés sur le même réseau. Les bits de la partie hôte de l'adresse doivent être uniques, pour identifier un hôte spécifique dans un réseau. Que les nombres décimaux entre deux adresses IPv4 correspondent ou non, si deux hôtes ont les mêmes bits comme partie réseau du flux de 32 bits, ces deux hôtes résident sur le même réseau.

Les hôtes savent-ils quelle partie du flux de 32 bits représente la partie réseau et quelle partie correspond à la partie hôte ? Le masque de sous-réseau permet de le savoir.

Lorsqu'un hôte IP est configuré, un masque de sous-réseau est attribué avec une adresse IP. Comme l'adresse IP, le masque de sous-réseau est constitué de 32 bits. Le masque de sous-réseau indique quelle partie de l'adresse IP correspond au réseau et quelle partie correspond à l'hôte.

Le masque de sous-réseau est comparé à l'adresse IP de gauche à droite, bit par bit. Les 1 dans le masque de sous-réseau représentent la partie réseau, et les 0 représentent la partie hôte. Comme l'illustre la Figure 1, le masque de sous-réseau est créé en plaçant le nombre binaire 1 dans chaque position de bit qui représente la partie réseau et en plaçant le nombre binaire 0 dans chaque position de bit qui représente la partie hôte. Notez que le masque de sous-réseau ne contient pas réellement la partie réseau ou hôte d'une adresse IPv4 : il indique uniquement à l'ordinateur où rechercher ces parties dans une adresse IPv4 donnée.

Tout comme les adresses IPv4, le masque de sous-réseau est représenté sous forme de notation décimale à point pour une plus grande facilité d'utilisation. Le masque de sous-réseau est configuré sur un périphérique hôte, en conjonction avec l'adresse IPv4, et est nécessaire pour que l'hôte puisse déterminer le réseau auquel il appartient. La Figure 2 montre les masques de sous-réseau valides d'un octet IPv4

8.1.2.2 Examen de la longueur du préfixe

Préfixes réseau

La longueur de préfixe est une autre façon d'exprimer le masque de sous-réseau. La longueur de préfixe correspond au nombre de bits définis sur 1 dans le masque de sous-réseau. Elle est notée au moyen de la « notation de barre oblique », à savoir un « / » suivi du nombre de bits définis sur 1. Par exemple, si le masque de sous-réseau est 255.255.255.0, il existe 24 bits définis sur 1 dans la version binaire du masque de sous-réseau. La longueur du préfixe est donc de 24 bits, soit /24. Le préfixe et le masque de sous-réseau constituent des moyens distincts de représenter la même chose : la partie réseau d'une adresse.

Les réseaux ne se voient pas toujours attribuer un préfixe /24. En fonction du nombre d'hôtes sur le réseau, le préfixe attribué peut être différent. Un numéro de préfixe différent modifie la plage d'hôtes et l'adresse de diffusion pour chaque réseau.

Les figures illustrent différents préfixes sur la même adresse 10.1.1.0. La Figure 1 illustre les préfixes /24 à /26. La Figure 2 illustre les préfixes /27 à /28.

Vous remarquerez que l'adresse réseau peut rester inchangée, mais que la plage d'hôtes et l'adresse de diffusion varient selon les longueurs de préfixe. Dans les figures, vous pouvez voir que le nombre d'hôtes accessibles sur le réseau change également.

8.1.2.3 Réseau, hôte et adresses de diffusion IPv4

Il existe trois sortes d'adresse comprises dans la plage d'adresses de chaque réseau IPv4 :

- Adresse réseau
- Adresses d'hôte
- Adresse de diffusion

Adresse réseau

L'adresse réseau est généralement utilisée pour faire référence à un réseau. Le masque de sous-réseau ou la longueur du préfixe peuvent aussi être utilisés pour décrire une adresse réseau. Par exemple, le réseau illustré à la Figure 1 peut être appelé le réseau 10.1.1.0, le réseau 10.1.1.0 255.255.255.0 ou le réseau 10.1.1.0/24. Tous les hôtes du réseau 10.1.1.0/24 auront la même partie réseau.

Comme l'illustre la Figure 2, dans la plage d'adresses IPv4 d'un réseau, la première adresse est réservée à l'adresse réseau. La partie adresse de cette adresse comprend uniquement des 0. Tous les hôtes du réseau partagent la même adresse réseau.

Adresse de l'hôte

Chaque périphérique final nécessite une adresse unique pour communiquer sur le réseau. Avec les adresses IPv4, les valeurs comprises entre l'adresse réseau et l'adresse de diffusion peuvent être attribuées aux périphériques finaux d'un réseau. Comme l'illustre la Figure 3, la partie hôte de cette adresse est composée de n'importe quelle combinaison de bits 0 et 1, mais ne peut pas contenir uniquement des bits 0 ou 1.

Adresse de diffusion

L'adresse de diffusion IPv4 est une adresse spécifique, attribuée à chaque réseau. Elle permet de transmettre des données à l'ensemble des hôtes d'un réseau. Pour envoyer les données à tous les hôtes d'un réseau en une seule fois, un hôte peut envoyer un paquet adressé à l'adresse de diffusion du réseau : chaque hôte du réseau qui recevra ce paquet en traitera le contenu.

L'adresse de diffusion correspond à la plus grande adresse de la plage d'adresses d'un réseau. Il s'agit de l'adresse dans laquelle les bits de la partie hôte sont tous des « 1 ». Un octet au format binaire ne comportant que des 1 correspond au nombre 255 en notation décimale. Par conséquent, comme illustré à la Figure 4, pour le réseau 10.1.1.0/24, dans lequel le dernier octet est utilisé pour la partie hôte, l'adresse de diffusion serait 10.1.1.255. Notez que la partie

hôte n'est pas toujours un octet entier. Cette adresse est également désignée sous le nom de diffusion dirigée.

8.1.2.4 Première et dernière adresses d'hôte

Pour s'assurer que tous les hôtes d'un réseau disposent d'une adresse IP unique provenant de cette plage réseau, il est important d'identifier la première adresse d'hôte et la dernière adresse d'hôte. Les hôtes d'un réseau se voient attribuer des adresses IP comprises dans cette plage.

Première adresse d'hôte

Comme le montre la Figure 1, la partie hôte de la première adresse d'hôte ne contient que des bits 0 à l'exception d'un bit 1 en tant que bit de poids faible ou bit le plus à droite. Cette adresse est toujours supérieure de 1 à l'adresse réseau. Dans cet exemple, la première adresse d'hôte du réseau 10.1.1.0/24 est 10.1.1.1. De nombreux schémas d'adressage utilisent la première adresse d'hôte pour le routeur ou la passerelle par défaut.

Dernière adresse d'hôte

La partie hôte de la dernière adresse d'hôte ne contient que des bits 1 à l'exception d'un bit 0 en tant que bit de poids faible ou bit le plus à droite. Cette adresse est toujours inférieure de un à l'adresse de diffusion. Comme le montre la Figure 2, la dernière adresse d'hôte du réseau 10.1.1.0/24 est 10.1.1.254.

8.1.2.5 Opération AND au niveau du bit

Lorsqu'une adresse IPv4 est attribuée à un périphérique, ce dernier utilise le masque de sous-réseau pour savoir à quelle adresse réseau il appartient. L'adresse réseau est l'adresse représentant tous les périphériques du même réseau.

En envoyant des données réseau, le périphérique utilise ces informations pour déterminer s'il peut envoyer des paquets en local ou s'il doit envoyer les paquets à une passerelle par défaut pour l'acheminement à distance. Lorsqu'un hôte envoie un paquet, il compare la partie réseau de sa propre adresse IP à la partie réseau de l'adresse IP de destination, grâce aux masques de sous-réseau. Si les bits de réseau correspondent, l'hôte source et l'hôte de destination sont sur le même réseau, et le paquet peut être transmis localement. S'ils ne correspondent pas, l'hôte expéditeur transmet le paquet à la passerelle par défaut, afin qu'il soit envoyé à l'autre réseau.

Opération AND

Il s'agit de l'une des trois opérations binaires de base, appliquées en logique numérique. Les deux autres sont les opérations OR (OU) et NOT (NON). Bien que les trois soient utilisées dans les réseaux de données, l'opération AND permet de déterminer l'adresse réseau. De ce fait, nous aborderons uniquement l'opération logique AND. L'opération logique AND consiste à comparer deux bits, ce qui donne le résultat suivant :

1 AND 1 = 1 (Figure 1)

0 AND 1 = 0 (Figure 2)

0 AND 0 = 0 (Figure 3)

1 AND 0 = 0 (Figure 4)

L'adresse d'hôte IPv4 est logiquement ajoutée par une opération AND (bit par bit) à son masque de sous-réseau pour déterminer l'adresse à laquelle l'hôte est associé. Lorsque cette opération AND est appliquée entre l'adresse et le masque de sous-réseau, le résultat obtenu est l'adresse réseau

8.1.2.6 Importance de l'opération AND

Toute opération AND entre un bit d'adresse ajouté à une valeur de bit 1 du masque de sous-réseau a pour résultat la valeur d'origine du bit de l'adresse. Ainsi, 0 (de l'adresse IPv4) AND 1 (du masque de sous-réseau) = 0. 1 (de l'adresse IPv4) AND 1(du masque de sous-réseau) = 1. Par conséquent, toute opération « AND 0 » a comme résultat 0. Ces propriétés de l'opération AND sont utilisées avec le masque de sous-réseau pour « masquer » les bits d'hôte d'une adresse IPv4. Le bit correspondant du masque de sous-réseau est ajouté à chaque bit de l'adresse par le biais d'une opération AND.

Puisque les bits du masque de sous-réseau qui représentent les bits d'hôte sont des 0, la partie hôte de l'adresse réseau résultante comporte uniquement des 0. Rappelez-vous qu'une adresse IPv4 comportant uniquement des 0 dans la partie hôte représente l'adresse réseau.

De même, tous les bits du masque de sous-réseau indiquant la partie réseau sont uniquement des 1. Lorsque tous les 1 sont ajoutés au bit d'adresse correspondant (via l'opération AND), les bits qui en résultent sont identiques aux bits d'adresse d'origine.

Comme l'illustre la figure ci-contre, les bits 1 du masque de sous-réseau impliquent que la partie réseau de l'adresse réseau a les mêmes bits que la partie réseau de l'hôte. La partie hôte de l'adresse réseau ne sera alors composée que de 0.

Pour une adresse IP spécifique et son sous-réseau, l'opération AND permet de déterminer à quel sous-réseau l'adresse appartient, ainsi que les adresses appartenant au même sous-réseau. N'oubliez pas que si deux adresses se trouvent sur le même réseau ou sous-réseau, elles sont considérées comme locales et peuvent donc communiquer directement entre elles. Les adresses qui ne sont pas sur le même réseau ou sous-réseau sont considérées comme distantes et doivent donc avoir un périphérique de couche 3 (tel qu'un routeur ou un commutateur de couche 3) entre elles pour communiquer.

Dans le cadre de la vérification/du dépannage d'un réseau, il faut souvent déterminer si deux hôtes sont sur le même réseau local. Cela n'est possible que si l'on se pose dans la perspective des périphériques réseau. Suite à une mauvaise configuration, un hôte peut s'identifier sur un réseau qui n'était pas celui prévu à l'origine. Cela peut créer un fonctionnement imprévisible, sauf si le problème est identifié en examinant les processus d'opération AND utilisés par l'hôte.

8.1.3 Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

8.1.3.1 Attribution d'une adresse IPv4 statique à un hôte

Adresses pour les périphériques d'utilisateurs

Dans la plupart des réseaux de données, l'immense majorité des hôtes sont des périphériques finaux, tels que des ordinateurs, des téléphones IP, des imprimantes, des tablettes et des smartphones. Dans la mesure où ces hôtes représentent le plus grand nombre de périphériques au sein d'un réseau, le plus grand nombre d'adresses doit leur être attribué. Ces hôtes se voient attribuer des adresses IP de la plage d'adresses disponibles dans le réseau. Les adresses IP peuvent être attribuées de manière statique ou de manière dynamique.

Attribution statique

Avec une attribution statique, l'administrateur réseau doit configurer manuellement les informations réseau relatives à un hôte. La Figure 1 illustre la fenêtre des propriétés de la carte réseau. Pour configurer une adresse IPv4 statique, sélectionnez IPv4 sur l'écran de la carte réseau, puis tapez l'adresse, le masque de sous-réseau et la passerelle par défaut, tous statiques. La Figure 2 présente les informations nécessaires pour une configuration statique : l'adresse IP, le masque de sous-réseau et la passerelle par défaut.

Il existe plusieurs avantages à choisir l'adressage statique. Par exemple, il est utile pour les imprimantes, les serveurs et les autres périphériques réseau qui ne changent pas souvent d'emplacement et qui doivent être accessibles pour les clients du réseau en fonction d'une adresse IP fixe. Si les hôtes ont l'habitude d'accéder à un serveur à une adresse IP particulière, cela peut poser des problèmes en cas de modification de cette adresse. De plus, l'attribution statique des informations d'adressage permet de mieux contrôler les ressources réseau. Par exemple, il est possible de créer des filtres d'accès basés sur le trafic vers et à partir d'une adresse IP spécifique. Cependant, l'adressage statique prend du temps car il doit être paramétré sur chaque hôte.

Lorsque l'adressage IP statique est utilisé, il convient de tenir à jour une liste exacte des adresses IP attribuées à chaque périphérique. Ces adresses étant permanentes, en principe, elles ne seront pas réutilisées

8.1.3.2 Attribution d'une adresse IPv4 dynamique à un hôte

Attribution dynamique

Sur les réseaux locaux, il n'est pas rare que les utilisateurs changent fréquemment. Les nouveaux utilisateurs arrivent avec des ordinateurs portables et ont besoin d'une connexion. D'autres disposent de nouvelles stations de travail ou d'autres périphériques réseau, tels que des smartphones, qui doivent être connectés. Plutôt que de demander à l'administrateur réseau

d'attribuer des adresses IP à chaque station de travail, il est plus facile d'attribuer ces adresses automatiquement. Cette opération est réalisée à l'aide du protocole DHCP (Dynamic Host Configuration Protocol), comme illustré à la Figure 1.

Le protocole DHCP permet l'attribution automatique des informations d'adressage, telles que l'adresse IP, le masque de sous-réseau, la passerelle par défaut et d'autres paramètres. La configuration du serveur DHCP nécessite qu'un bloc d'adresses, appelé pool d'adresses, soit utilisé pour l'attribution aux clients DHCP d'un réseau. Les adresses attribuées à ce pool doivent être définies de manière à exclure toutes les adresses statiques utilisées par d'autres périphériques.

Le protocole DHCP est généralement la méthode d'attribution d'adresses IPv4 privilégiée pour les réseaux de grande taille, car le personnel de support du réseau est dégagé de cette tâche et le risque d'erreur de saisie est presque éliminé.

L'autre avantage de l'attribution dynamique réside dans le fait que les adresses ne sont pas permanentes pour les hôtes, elles sont uniquement « louées » pour une certaine durée. Si l'hôte est mis hors tension ou retiré du réseau, l'adresse est retournée au pool pour être réutilisée. Cela est particulièrement intéressant pour les utilisateurs mobiles qui se connectent et se déconnectent d'un réseau.

Si le protocole DHCP est activé sur un périphérique hôte, la commande **ipconfig** peut être utilisée pour afficher les informations sur l'adresse IP attribuée par le serveur DHCP, comme illustré à la Figure 2.

8.1.3.3 Transmission monodiffusion

Dans un réseau IPv4, les hôtes peuvent communiquer de trois façons :

- **Monodiffusion** : processus consistant à envoyer un paquet d'un hôte à un autre hôte spécifique.
- **Diffusion** : processus consistant à envoyer un paquet d'un hôte à tous les hôtes du réseau.
- **Multidiffusion** : processus consistant à envoyer un paquet d'un hôte à un groupe d'hôtes en particulier (qui peuvent se trouver sur différents réseaux).

Ces trois types de transmission sont utilisés différemment dans les réseaux de données. Dans les trois cas, l'adresse IPv4 de l'hôte émetteur est placée dans l'en-tête du paquet comme adresse source.

Trafic monodiffusion

La monodiffusion est utilisée dans les communications normales d'hôte à hôte tant entre client et serveur que dans un réseau peer-to-peer. Les paquets de type monodiffusion utilisent les adresses de périphérique de destination comme adresses de destination et peuvent être routés sur un interréseau.

Lancez l'animation pour visualiser un exemple de monodiffusion.

Dans un réseau IPv4, les adresses de monodiffusion appliquées à un périphérique final sont désignées sous le nom d'adresses d'hôte. Dans une monodiffusion, les adresses d'hôte attribuées aux deux périphériques finaux sont utilisées comme adresses IPv4 source et de destination. Durant l'encapsulation, l'hôte source place dans l'en-tête du paquet monodiffusion son adresse IPv4 comme adresse source et l'adresse IPv4 de l'hôte de destination comme adresse de destination. Même si la destination spécifiée dans un paquet est une monodiffusion, une diffusion ou une multidiffusion, l'adresse source d'un paquet est toujours l'adresse de monodiffusion de l'hôte d'origine.

Remarque : dans ce cours, sauf indication contraire, toutes les transmissions entre les périphériques sont de type monodiffusion.

Les adresses d'hôte IPv4 sont des adresses de monodiffusion et se trouvent dans la plage d'adresses 0.0.0.0 à 223.255.255.255. Toutefois, dans cette plage, de nombreuses adresses sont réservées à un usage spécifique. Ces adresses seront abordées plus loin dans ce chapitre.

8.1.3.4 Transmission de diffusion

Transmission de diffusion

Le trafic de diffusion est utilisé pour envoyer des paquets à tous les hôtes du réseau grâce à l'adresse de diffusion du réseau. Avec une diffusion, le paquet contient une adresse IP de destination avec uniquement des un (1) dans la partie hôte. Cela signifie que tous les hôtes se trouvant sur ce réseau local (domaine de diffusion) recevront le paquet et le regarderont. De nombreux protocoles réseau, tels que DHCP, utilisent les diffusions. Lorsqu'un hôte reçoit un paquet envoyé à l'adresse de diffusion du réseau, il traite le paquet comme il le ferait pour un paquet adressé à son adresse de monodiffusion.

Voici quelques cas d'utilisation des transmissions de diffusion :

- Mappage des adresses d'une couche supérieure à des adresses d'une couche inférieure
- Demande d'une adresse
- Contrairement à une transmission de type monodiffusion où les paquets peuvent être routés via l'interréseau, les paquets de diffusion sont habituellement limités au réseau local. Cette limitation dépend de la configuration de la passerelle et du type de diffusion. Il existe deux types de diffusion : la diffusion dirigée et la diffusion limitée.

Diffusion dirigée

Une diffusion dirigée est envoyée à tous les hôtes d'un réseau particulier. Ce type de diffusion permet l'envoi d'une diffusion à tous les hôtes d'un réseau qui n'est pas local. Par exemple, pour qu'un hôte situé en dehors du réseau 172.16.4.0/24 communique avec tous les hôtes de ce réseau, l'adresse de destination du paquet doit être 172.16.4.255. Bien que, par défaut, les routeurs n'acheminent pas les diffusions dirigées, ils peuvent être configurés de manière à le faire.

Diffusion limitée

La diffusion limitée permet une transmission qui est limitée aux hôtes du réseau local. Ces paquets utilisent toujours l'adresse IPv4 de destination 255.255.255.255. Les routeurs ne transmettent pas les diffusions limitées. C'est la raison pour laquelle un réseau IPv4 est également appelé « domaine de diffusion ». Les routeurs forment les limites d'un domaine de diffusion.

Par exemple, un hôte du réseau 172.16.4.0/24 envoie une diffusion à tous les hôtes de son réseau à l'aide d'un paquet dont l'adresse de destination est 255.255.255.255.

Lancez l'animation pour voir un exemple de diffusion limitée.

Lorsqu'un paquet est diffusé, il utilise les ressources du réseau et est traité par chaque hôte destinataire sur le réseau. Ainsi, le trafic de diffusion devrait être limité de sorte qu'il ne réduise pas les performances du réseau ou des périphériques. Dans la mesure où les routeurs séparent les domaines de diffusion, la création de sous-réseaux, pour les réseaux qui doivent prendre en charge un volume de trafic très important, peut en améliorer les performances.

8.1.3.5 Transmission multidiffusion

Transmission multidiffusion

La transmission multidiffusion permet de conserver la bande passante d'un réseau IPv4. Elle réduit le trafic en permettant à un hôte d'envoyer un paquet à un groupe d'hôtes spécifiques qui font partie d'un groupe de multidiffusion. Pour atteindre plusieurs hôtes de destination à l'aide d'une transmission de type monodiffusion, un hôte source a besoin d'envoyer un paquet qu'il adresse à chaque hôte. Dans une transmission multidiffusion, l'hôte source peut envoyer un seul paquet, qui parviendra à des milliers d'hôtes de destination. L'interréseau doit répliquer des flux de multidiffusion de façon efficace, afin qu'ils atteignent uniquement les destinataires visés.

Voici quelques exemples de transmission multidiffusion :

- Diffusions vidéo et audio
- Échange d'informations de routage entre des protocoles de routage
- Distribution de logiciels
- Jeu en ligne

Adresses de multidiffusion

L'IPv4 utilise un bloc d'adresses réservées pour s'adresser à des groupes de multidiffusion. Cette plage d'adresses va de 224.0.0.0 à 239.255.255.255. La plage d'adresses de multidiffusion est divisée en différents types d'adresse : les adresses link-local réservées et les adresses d'étendue globale. Il existe un autre type d'adresse de multidiffusion, dit adresses d'étendue administrative ou d'étendue limitée.

Les adresses de multidiffusion IPv4 du bloc 224.0.0.0 - 224.0.0.255 sont des adresses de liaison locales réservées. Ces adresses s'appliquent aux groupes de multidiffusion d'un réseau local. Un routeur connecté au réseau local sait que les paquets sont adressés à un groupe de multidiffusion link-local et ne transmet jamais ces paquets. Les adresses link-local réservées s'appliquent principalement aux protocoles de routage qui utilisent le type de transmission multidiffusion pour échanger des informations de routage.

Les adresses d'étendue globale vont de 224.0.1.0 à 238.255.255.255. Elles peuvent aussi être utilisées dans la multidiffusion de données sur Internet. Par exemple, 224.0.1.1 est une adresse réservée au protocole NTP (Network Time Protocol) pour synchroniser les horloges des périphériques réseau.

Clients multidiffusion

Les hôtes qui reçoivent des données de multidiffusion spécifiques sont appelés des « clients multidiffusion ». Ces clients font appel à des services demandés par un programme client pour s'abonner au groupe de multidiffusion.

Chaque groupe de multidiffusion est représenté par une seule adresse de destination multidiffusion IPv4. Lorsqu'un hôte IPv4 s'abonne à un groupe de multidiffusion, il traite les paquets adressés à cette adresse de multidiffusion, ainsi que ceux adressés à son adresse de monodiffusion, qui a été attribuée à lui seul.

L'animation présente la façon dont les clients acceptent des paquets multidiffusion.

8.1.4 Les types d'adresses IPv4

8.1.4.1 Adresses IPv4 publiques et adresses IP privées

Bien que la majorité des adresses d'hôte IPv4 soient des adresses publiques utilisées dans les réseaux accessibles sur Internet, d'autres blocs d'adresses sont attribués à des réseaux qui ne nécessitent pas d'accès à Internet, ou uniquement un accès limité. Ces adresses sont appelées des adresses privées.

Adresses privées

Voici ces plages d'adresses privées :

10.0.0.0 à 10.255.255.255 (10.0.0.0/8)

172.16.0.0 à 172.31.255.255 (172.16.0.0/12)

192.168.0.0 à 192.168.255.255 (192.168.0.0/16)

Les adresses privées sont définies dans le RFC 1918, « Address Allocation for Private Internets » et sont parfois appelées adresses RFC 1918. Les blocs d'adresses d'espace privé, comme l'illustre la figure, sont utilisés dans les réseaux privés. Les hôtes qui n'ont pas besoin

d'accéder à Internet peuvent utiliser des adresses privées. Cependant, au sein du réseau privé, les hôtes ont toujours besoin d'adresses IP uniques dans l'espace privé.

Plusieurs hôtes de réseaux différents peuvent utiliser les mêmes adresses d'espace privé. Les paquets qui utilisent ces adresses comme source ou destination ne doivent pas être visibles sur Internet. Le routeur ou le périphérique pare-feu, en périphérie de ces réseaux privés, doivent bloquer ou traduire ces adresses. Même si ces paquets parvenaient sur Internet, les routeurs ne disposeraient pas de routes pour les acheminer vers le réseau privé en question.

Dans le RFC 6598, l'IANA a réservé un autre groupe d'adresses connu sous le nom d'espace d'adressage partagé. Comme avec l'espace d'adressage privé du RFC 1918, les adresses partagées de l'espace d'adressage ne sont pas globalement routables. Toutefois, ces adresses sont conçues uniquement pour les réseaux de fournisseurs de services. Le bloc d'adresses partagé est 100.64.0.0/10.

Adresses publiques

La grande majorité des adresses de la plage d'hôtes multidiffusion IPv4 sont des adresses publiques. Ces adresses sont normalement attribuées à des hôtes publiquement accessibles depuis Internet. Même dans ces blocs d'adresses IPv4, de nombreuses adresses sont réservées à des usages particuliers

8.1.4.3 Les adresses IPv4 réservées

Certaines adresses ne peuvent pas être attribuées à des hôtes. D'autres adresses spéciales le peuvent, mais avec des restrictions concernant la façon dont les hôtes interagissent avec le réseau.

Adresses réseau et de diffusion

Comme nous l'avons vu, dans chaque réseau, la première et la dernière adresses ne peuvent pas être attribuées à des hôtes. Il s'agit respectivement de l'adresse réseau et de l'adresse de diffusion.

Bouclage

L'adresse de bouclage IPv4 127.0.0.1 est une autre adresse réservée. Il s'agit d'une adresse spéciale que les hôtes utilisent pour diriger le trafic vers eux-mêmes. L'adresse de bouclage crée un moyen rapide, pour les applications et les services TCP/IP actifs sur le même périphérique, de communiquer entre eux. En utilisant l'adresse de bouclage à la place de l'adresse d'hôte IPv4 attribuée, deux services actifs sur le même hôte peuvent contourner les couches les plus basses de la pile TCP/IP. Vous pouvez également envoyer une requête ping à l'adresse de bouclage afin de tester la configuration TCP/IP de l'hôte local.

Bien que seule l'adresse 127.0.0.1 soit utilisée, les adresses de la plage 127.0.0.0-127.255.255.255 sont réservées. Toutes les adresses de ce bloc sont envoyées en boucle sur l'hôte local. Aucune des adresses de cette plage ne devrait jamais apparaître sur un réseau quel qu'il soit.

Adresses link-local

Les adresses IPv4 du bloc d'adresses 169.254.0.0 à 169.254.255.255 (169.254.0.0/16) sont conçues comme des adresses link-local. Elles peuvent être automatiquement attribuées à l'hôte local par le système d'exploitation, dans les environnements où aucune configuration IP n'est disponible. Elles peuvent être utilisées dans un réseau peer-to-peer restreint ou pour un hôte qui ne parviendrait pas à obtenir automatiquement une adresse auprès d'un serveur DHCP.

Les transmissions basées sur des adresses IPv4 link-local ne conviennent que dans le cadre d'une communication avec d'autres périphériques connectés au même réseau, comme indiqué dans la figure. Un hôte ne peut pas envoyer de paquet avec une adresse de destination IPv4 link-local à un autre routeur pour qu'il soit acheminé. De plus, sur l'hôte, le paramètre IPv4 de durée de vie (TTL) doit être défini sur 1 pour ces paquets.

Les adresses link-local ne fournissent pas de services en dehors du réseau local. Toutefois, de nombreuses applications client/serveur et peer to peer fonctionneront correctement avec des adresses link-local IPv4.

Adresses TEST-NET

Le bloc d'adresses 192.0.2.0 à 192.0.2.255 (192.0.2.0/24) est réservé à des fins pédagogiques. Ces adresses peuvent être utilisées dans la documentation et dans des exemples de réseau. Contrairement aux adresses expérimentales, les périphériques réseau accepteront ces adresses dans leur configuration. Ces adresses apparaissent souvent avec des noms de domaine exemple.com ou exemple.net dans les requêtes pour commentaires et la documentation de fournisseur et de protocole. Les adresses de cette plage ne doivent pas être visibles sur Internet.

Adresses expérimentales

Les adresses du bloc 240.0.0.0 à 255.255.255.254 sont répertoriées comme étant réservées pour une utilisation future (RFC 3330). Actuellement, ces adresses ne peuvent être utilisées qu'à des fins de recherche ou d'expérimentation, mais ne peuvent pas être utilisées dans un réseau IPv4. Cependant, selon le RFC 3330, elles peuvent techniquement être converties en adresses utilisables dans le futur.

8.1.4.4 L'ancien système d'adressage par classe

À l'origine, le RFC 1700, « Assigned Numbers », regroupait les plages monodiffusion selon différentes tailles, appelées des adresses de classe A, B et C. Il établissait également des adresses de classe D (multidiffusion) et de classe E (expérimentales), comme nous l'avons déjà vu. Les classes d'adresses de monodiffusion A, B et C définissaient des réseaux de taille spécifique et des blocs d'adresses spécifiques pour ces réseaux. Une entreprise ou une organisation se voyait attribuer un réseau entier de bloc d'adresses de classe A, B ou C. L'utilisation de l'espace d'adressage s'appelait adressage par classe.

Blocs d'adresses A

Un bloc d'adresses de classe A a été créé pour prendre en charge les réseaux de très grande taille, comportant plus de 16 millions d'adresses d'hôte. Les adresses IPv4 de classe A utilisaient un préfixe /8 invariable, le premier octet indiquant l'adresse réseau. Les trois octets restants correspondaient aux adresses d'hôte. Toutes les adresses de classe A nécessitaient que le bit de poids fort du premier octet soit un zéro. Cela implique qu'il n'y avait que 128 réseaux de classe A disponibles, de 0.0.0.0/8 à 127.0.0.0/8. Même si les adresses de classe A réservaient la moitié de l'espace d'adressage, elles ne pouvaient être attribuées qu'à 120 entreprises ou organisations, en raison de leur limite de 128 réseaux.

Blocs d'adresses B

L'espace d'adressage de classe B a été créé pour répondre aux besoins des réseaux de taille moyenne ou de grande taille, comportant jusqu'à 65 000 hôtes. Les adresses IP de classe B utilisaient les deux premiers octets pour indiquer l'adresse réseau. Les deux octets suivants correspondaient aux adresses d'hôte. Comme avec la classe A, l'espace d'adressage pour les classes d'adresses restantes devait être réservé. Pour les adresses de classe B, les deux bits de poids fort du premier octet étaient 10. Cela limitait le bloc d'adresses de classe B de 128.0.0.0/16 à 191.255.0.0/16. La classe B attribuait les adresses plus efficacement que la classe A, car elle répartissait de manière équitable 25 % de l'espace d'adressage IPv4 total sur environ 16 000 réseaux.

Blocs d'adresses C

L'espace d'adressage de la classe C était le plus disponible des anciennes classes d'adresses. Cet espace d'adressage était réservé aux réseaux de petite taille, comportant 254 hôtes au maximum. Les blocs d'adresses de classe C utilisaient le préfixe /24. Ainsi, un réseau de classe C ne pouvait utiliser que le dernier octet pour les adresses d'hôte, les trois premiers octets correspondant à l'adresse réseau. Les blocs d'adresses de classe C réservaient l'espace d'adressage à l'aide d'une valeur fixe de 110 pour les trois bits de poids fort du premier octet. Cela limitait le bloc d'adresses de classe C de 192.0.0.0/24 à 223.255.255.0/24. Bien qu'il occupait seulement 12,5 % de l'espace d'adressage IPv4, il pouvait attribuer des adresses à 2 millions de réseaux.

La Figure 1 montre comment ces classes d'adresses sont divisées.

Limites de l'adressage par classe

Les besoins de certaines entreprises ou organisations sont couverts par ces trois classes. L'attribution par classe des adresses IP gaspillait souvent de nombreuses adresses, ce qui épuisait la disponibilité des adresses IPv4. Par exemple, une entreprise avec un réseau de 260 hôtes devait se voir attribuer une adresse de classe B avec plus de 65 000 adresses.

Bien que ce système par classe ait été abandonné à la fin des années 90, il n'a pas entièrement disparu dans certains des réseaux modernes. Par exemple, lorsque vous attribuez une adresse IPv4 à un ordinateur, le système d'exploitation examine l'adresse en question pour déterminer si elle est de classe A, B ou C. Le système d'exploitation déduit ensuite le préfixe utilisé par cette classe et effectue l'attribution du masque de sous-réseau par défaut.

Adressage sans classe

Le système utilisé aujourd'hui porte le nom d'adressage sans classe. Son nom formel est le routage CIDR (Classless Inter-Domain Routing, routage interdomaine sans classe). L'attribution par classe d'adresses IPv4 était inefficace, car elle permettait uniquement l'utilisation de longueurs de préfixe /8, /16 ou /24, chacune d'un espace d'adresses distinct. En 1993, l'IETF a créé un nouvel ensemble de normes permettant aux fournisseurs de services d'attribuer des adresses IPv4 sur n'importe quelle limite binaire (longueur de préfixe) au lieu d'utiliser uniquement les classes A, B ou C.

L'IETF savait que le CIDR était uniquement une solution temporaire et qu'un nouveau protocole IP devait être développé pour s'adapter à la croissance rapide du nombre d'utilisateurs d'Internet. En 1994, l'IETF a commencé à chercher un successeur à l'IPv4, à savoir le futur protocole IPv6.

La Figure 2 illustre les plages d'adresses par classe.

8.1.4.5 L'attribution des adresses IP

Pour que les hôtes réseau (par exemple les serveurs Web) des entreprises ou des organisations soient accessibles depuis Internet, les organisations et entreprises en question doivent disposer d'un bloc d'adresses publiques. N'oubliez pas que les adresses publiques doivent être uniques et que l'utilisation des adresses publiques est régulée et dépend de chaque organisation. Cela vaut pour les adresses IPv4 et IPv6.

IANA et RIR

L'IANA (Internet Assigned Numbers Authority, http://www.iana.org) gère l'attribution des adresses IPv4 et IPv6. Jusque dans le milieu des années 1990, l'ensemble de l'espace d'adressage IPv4 était géré directement par l'IANA. À cette époque, la gestion de l'espace d'adressage IPv4 restant était répartie entre différents autres registres, selon le type d'utilisation ou la zone géographique. Ces sociétés d'enregistrement s'appellent des registres Internet régionaux, comme présenté dans la figure.

Voici les principaux registres :

- AfriNIC (African Network Information Centre) - Région Afrique http://www.afrinic.net
- APNIC (Asia Pacific Network Information Centre) - Région Asie/Pacifique http://www.apnic.net
- ARIN (American Registry for Internet Numbers) - Région Amérique du Nord http://www.arin.net
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) - Amérique du Sud et certaines îles des Caraïbes http://www.lacnic.net
- RIPE NCC (Réseaux IP européens) - Europe, Moyen Orient, Asie centrale http://www.ripe.net

FAI

Les RIR sont chargés d'attribuer des adresses IP aux FAI. La plupart des entreprises ou organisations obtiennent leur bloc d'adresses IPv4 auprès d'un FAI. Le FAI fournit généralement un petit nombre d'adresses IPv4 utilisables (6 ou 14) à leurs clients, dans le cadre des services d'accès qu'ils offrent. Il est possible d'obtenir, pour un coût supplémentaire, de plus grands blocs d'adresses sur base de justificatifs des besoins.

En quelque sorte, le FAI prête ou loue ces adresses. Lorsque nous changeons de FAI, le nouveau FAI nous fournit des adresses à partir des blocs d'adresses qui lui ont été attribués. L'ancien FAI retourne les blocs qu'il nous a prêtés à leur pool d'adresses, pour qu'un autre client puisse les emprunter.

Les adresses IPv6 peuvent être obtenues à partir du FAI ou, dans certains cas, directement à partir du RIR. La taille des adresses IPv6 et des blocs d'adresses standard sera abordée plus loin dans ce chapitre.

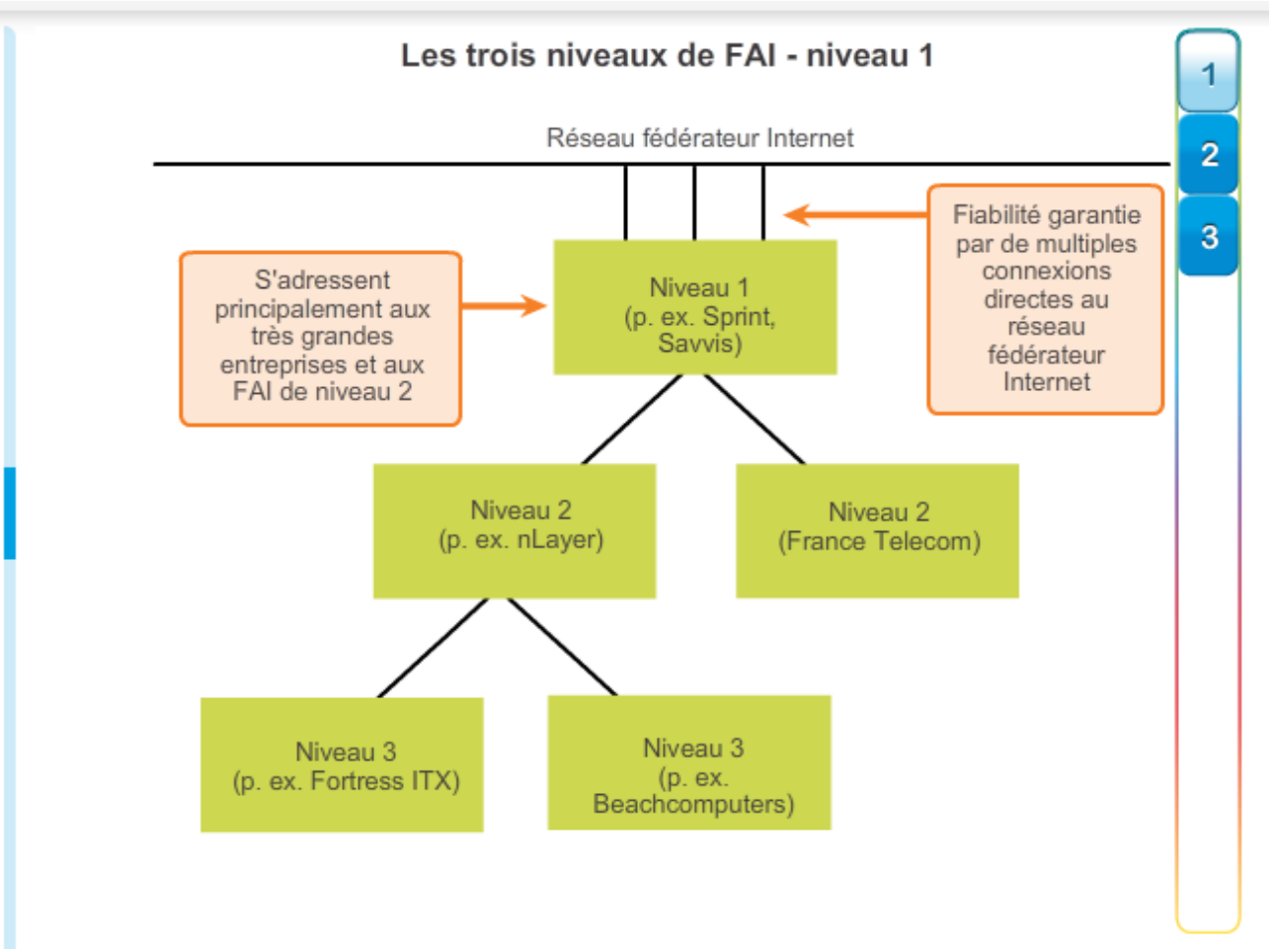
Services des fournisseurs de services Internet

Pour accéder à Internet, nous devons connecter notre réseau de données à Internet par l'intermédiaire d'un FAI (Fournisseur d'accès Internet), également appelé FSI (Fournisseur de services Internet).

Les FAI disposent de leur propre ensemble de réseaux de données internes pour gérer la connectivité Internet et fournir les services d'accès associés. Les services DNS, de messagerie et d'hébergement de site Web sont les principaux services offerts par les FAI à leurs clients. En fonction du niveau de service requis et disponible, les clients utilisent un FAI de niveau différent.

Niveaux de FAI

Les FAI sont regroupés au sein d'une hiérarchie, en fonction de leur niveau de connectivité au réseau fédérateur Internet. Les niveaux les plus bas obtiennent une connectivité au réseau fédérateur via une connexion à un FAI de niveau supérieur, comme indiqué dans les figures ci-contre.



Niveau 1

Comme l'illustre la Figure 1, au sommet de la hiérarchie des FAI se trouvent les FAI de niveau 1. Ces derniers sont de grands fournisseurs au niveau national ou international, directement connectés au réseau fédérateur Internet. Les clients des FAI de niveau 1 sont, soit des FAI de niveau inférieur dans la hiérarchie, soit des grandes sociétés ou des administrations. Dans la mesure où ces FAI se trouvent au sommet de la connectivité Internet, ils mettent en œuvre des connexions et des services extrêmement fiables. Des connexions multiples au réseau fédérateur Internet comptent parmi les technologies utilisées pour garantir cette fiabilité.

Pour les clients, les principaux avantages d'un FAI de niveau 1 sont la fiabilité et le débit de données. Ces clients étant seulement séparés d'Internet d'une connexion, les risques d'interruption de service ou de goulots d'étranglement du trafic restent très faibles. Pour les clients, l'inconvénient majeur d'un FAI de niveau 1 reste son coût élevé des services d'accès.

Niveau 2

Comme l'illustre la Figure 2, les FAI de niveau 2 dépendent des FAI de niveau 1 pour les services Internet. Les petites entreprises font le plus souvent appel aux FAI de niveau 2. En règle générale, ils offrent davantage de services que les deux autres niveaux inférieurs de FAI. Les FAI de niveau 2 disposent en principe de leurs propres ressources informatiques pour leurs propres services, par exemple les serveurs DNS, les serveurs de messagerie et les

serveurs Web. Parmi les autres services offerts par des FAI de niveau 2, citons le développement et la gestion de site Web, des services de commerce électronique/boutique en ligne et des services VoIP.

Par rapport aux FAI de niveau 1, le principal inconvénient des FAI de niveau 2 est un accès Internet plus lent. Dans la mesure où les FAI de niveau 2 sont séparés du réseau fédérateur Internet d'au moins une connexion, l'accès qu'ils offrent est généralement moins fiable que celui des FAI de niveau 1.

Niveau 3

Comme l'illustre la Figure 3, les FAI de niveau 3 achètent les services Internet auprès des FAI de niveau 2. Les clients de ces FAI sont généralement des particuliers dans une zone géographique précise. En principe, ces clients n'ont pas besoin de la plupart des services que nécessitent des clients de niveau 2. Leur premier besoin est une connectivité et un support technique.

Ces clients ont souvent un manque ou une insuffisance de connaissances dans les domaines de l'informatique et des réseaux. Les FAI de niveau 3 offrent souvent à leurs clients une connectivité Internet dans le cadre de contrats de services informatiques et de réseau. Bien qu'ils offrent un accès moins fiable et une bande passante réduite par rapport aux fournisseurs de niveau 1 et 2, ils sont également retenus par les petites et moyennes entreprises.

8.2 Les adresses réseau IPv6

8.2.1 Les problèmes liés au protocole IPv4

8.2.1.1 Ce qui rend IPv6 nécessaire

L'IPv6 est conçu pour être le successeur de l'IPv4. L'IPv6 possède un plus grand espace d'adressage (128 bits) pour un total de 340 undécillions d'adresses disponibles (ce qui correspond au nombre 340 suivi de 36 zéros). Toutefois, l'IPv6 apporte bien plus que des adresses plus longues. Lorsque l'IETF a commencé à développer un successeur à l'IPv4, l'organisme a utilisé cette opportunité pour corriger les limites de l'IPv4 et améliorer ce protocole. Par exemple, l'ICMPv6 (Internet Control Message Protocol version 6) inclut la configuration automatique et la résolution d'adresse, fonctions non présentes dans le protocole ICMP pour l'IPv4 (ICMPv4). L'ICMPv4 et l'ICMPv6 seront étudiés plus loin dans ce chapitre.

La nécessité du protocole IPv6

Le manque d'espace d'adressage IPv4 a été le facteur le plus important pour passer à l'IPv6. Comme l'Afrique, l'Asie et d'autres parties du monde sont de plus en plus connectées à Internet, il n'y a pas suffisamment d'adresses IPv4 pour prendre en charge cette croissance. Le lundi 31 janvier 2011, l'IANA a attribué les deux derniers blocs d'adresses IPv4 /8 aux organismes d'enregistrement Internet locaux (RIR). Les différentes prévisions indiquent que les cinq RIR auront épuisé les adresses IPv4 entre 2015 et 2020. À ce stade, les adresses IPv4 restantes ont été attribuées aux FAI.

L'IPv4 fournit théoriquement 4,3 milliards d'adresses au maximum. Les adresses privées RFC 1918, en association avec la fonction NAT, ont été utilisées pour limiter le manque d'espace d'adressage IPv4. La fonction NAT comporte des restrictions gênant fortement les communications peer-to-peer.

Internet des objets

L'Internet moderne est sensiblement différent de l'Internet des dernières décennies. Aujourd'hui, Internet est principalement utilisé pour le courrier électronique, les pages Web et le transfert de fichiers entre les ordinateurs. Internet évolue pour devenir un « Internet des objets ». Les périphériques pouvant accédant à Internet ne sont plus seulement des ordinateurs, des tablettes et des smartphones. Les périphériques connectés et équipés de capteurs de demain comprennent tous les objets du quotidien, y compris les automobiles, les périphériques biomédicaux, les appareils électroménagers et même les écosystèmes naturels. Imaginez qu'une conférence sur un site client est automatiquement planifiée sur votre application de calendrier et doit commencer une heure avant vos horaires de travail normaux. Cela peut vous poser problème, notamment si vous oubliez de vérifier le calendrier ou de régler votre réveil en conséquence. Imaginez maintenant que votre application de calendrier communique ces informations directement à votre réveil et à votre automobile. Votre voiture se met en marche automatiquement pour dégeler le pare-brise avant votre arrivée et vous indique la route pour vous rendre sur le site client.

Avec un nombre d'utilisateurs d'Internet augmentant sans cesse, un espace d'adressage IPv4 limité, des problèmes liés à la fonction NAT et l'Internet des objets, le temps est venu de lancer la transition vers l'IPv6

8.2.1.2 La coexistence des protocoles IPv4 et IPv6

La transition vers l'IPv6 n'aura pas lieu à une date fixe. À l'avenir, l'IPv4 et l'IPv6 devront coexister. La transition vers l'IPv6 durera probablement plusieurs années. L'IETF a créé divers protocoles et outils pour aider les administrateurs réseau à migrer leurs réseaux vers l'IPv6. Les techniques de migration peuvent être classées en trois catégories :

- **Double pile** – comme illustré à la Figure 1, la double pile permet à l'IPv4 et à l'IPv6 de coexister sur le même réseau. Les périphériques double pile exécutent les piles de protocoles IPv4 et IPv6 simultanément.

- **Tunneling** – comme illustré à la Figure 2, le tunneling est une méthode de transport des paquets IPv6 via un réseau IPv4. Les paquets IPv6 sont encapsulés dans des paquets IPv4, de la même manière que d'autres types de données.

- **Traduction** – comme illustré à la Figure 3, les périphériques IPv6 peuvent utiliser la traduction d'adresses réseau 64 (NAT64) pour communiquer avec les périphériques IPv4 à l'aide d'une technique de traduction similaire à la NAT pour l'IPv4. Un paquet IPv6 est traduit en un paquet IPv4, et inversement.

8.2.2 Adressage IPv6

8.2.2.1 Système de notation hexadécimale

Contrairement aux adresses IPv4 qui sont exprimées en notation décimale à point, les adresses IPv6 sont représentées à l'aide de valeurs hexadécimales. Vous avez déjà vu le format hexadécimal dans le volet Packet Byte de Wireshark. Dans Wireshark, le format hexadécimal est utilisé pour représenter les valeurs binaires des trames et des paquets. Le système hexadécimal est également utilisé pour représenter les adresses MAC Ethernet.

Numérotation hexadécimale

Ce type de numérotation est un moyen pratique de représenter des valeurs binaires. Le système de numérotation décimale est en base dix, le système binaire en base deux et le système hexadécimal est en base seize.

Le système de numération en base 16 utilise les chiffres 0 à 9 et les lettres A à F. La Figure 1 montre les équivalents binaires et décimaux, ainsi que les valeurs hexadécimales. Il existe 16 combinaisons uniques de quatre bits, de 0000 à 1111. Le système hexadécimal à 16 caractères est le système de numération idéal, car quatre bits peuvent être représentés par une valeur hexadécimale unique.

1

2

Représentation de valeurs hexadécimales

Hexadécimal	Décimal	Binaire
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Comprendre le format binaire

Sachant que 8 bits (un octet) est un regroupement binaire courant, la plage binaire de 00000000 à 11111111 correspond, dans le format hexadécimal, à la plage de 00 à FF. Les zéros de gauche peuvent être affichés pour compléter la représentation de 8 bits. Par exemple, la valeur binaire 0000 1010 correspond à 0A au format hexadécimal.

Représentation de valeurs hexadécimales

Remarque : il est important de distinguer les valeurs hexadécimales des valeurs décimales en ce qui concerne les caractères 0 à 9.

Le système hexadécimal est généralement représenté à l'écrit par la valeur concernée précédée par 0x (par exemple, 0x73) ou suivie de l'indice 16. Moins souvent, une valeur peut être suivie d'un H, par exemple 73H. Toutefois, dans la mesure où le texte sous forme d'exposant n'est pas reconnu dans les environnements de ligne de commande ou de programmation, la représentation technique hexadécimale est précédée d'un 0x. Par conséquent, les exemples ci-dessus doivent correspondre respectivement à 0x0A et 0x73.

Conversions hexadécimales

Les conversions numériques entre des valeurs décimales et hexadécimales sont très simples, bien que la division ou la multiplication par 16 ne soit pas toujours très commode.

Avec un peu de pratique, il est possible de reconnaître les configurations binaires qui correspondent aux valeurs décimales et hexadécimales. La figure 2 illustre ces configurations pour des valeurs de 8 bits données.

Conversions au format hexadécimal des octets binaires

Hexadécimal	Décimal	Binaire
00	0	0000 0000
01	1	0000 0001
02	2	0000 0010
03	3	0000 0011
04	4	0000 0100
05	5	0000 0101
06	6	0000 0110
07	7	0000 0111
08	8	0000 1000
0A	10	0000 1010
0F	15	0000 1111
10	16	0001 0000
20	32	0010 0000
40	64	0100 0000
80	128	1000 0000
C0	192	1100 0000
CA	202	1100 1010
F0	240	1111 0000
FF	255	1111 1111

1
2

8.2.2.2 Représentation de l'adresse IPv6

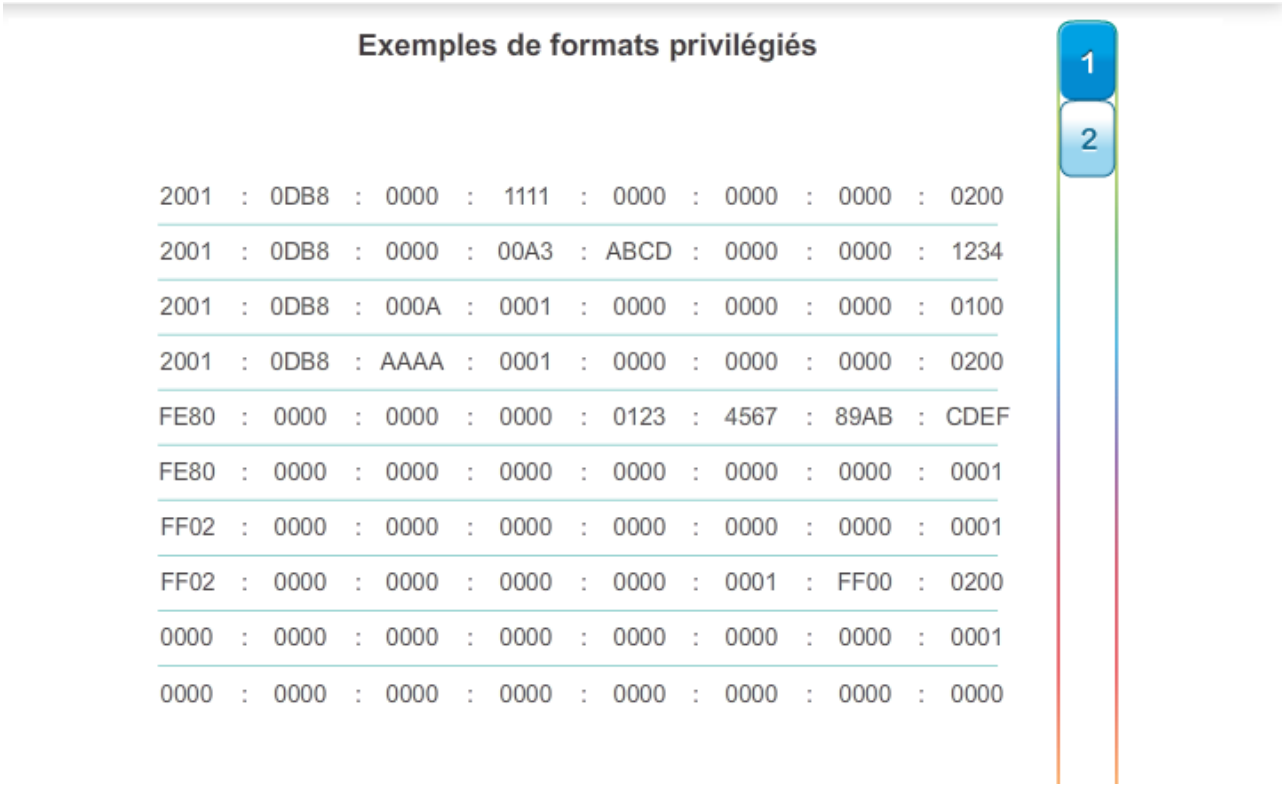
Les adresses IPv6 ont une longueur de 128 bits et sont notées sous forme de chaînes de valeurs hexadécimales. Tous les groupes de 4 bits sont représentés par un caractère hexadécimal unique ; pour un total de 32 valeurs hexadécimales. Les adresses IPv6 ne sont pas sensibles à la casse et peuvent être notées en minuscules ou en majuscules.

Format privilégié

Comme l'illustre la Figure 1, le format privilégié pour noter une adresse IPv6 est x:x:x:x:x:x:x:x, chaque « x » comportant quatre valeurs hexadécimales. Pour faire référence aux 8 bits d'une adresse IPv4, nous utilisons le terme « octet ». Pour les adresses IPv6, « hextet » est le terme non officiel utilisé pour désigner un segment de 16 bits ou de quatre valeurs hexadécimales. Chaque « x » est un hextet simple, 16 bits, ou quatre caractères hexadécimaux.

Le format privilégié implique que l'adresse IPv6 soit écrite à l'aide de 32 caractères hexadécimaux. Cela ne signifie pas nécessairement que c'est la solution idéale pour représenter une adresse IPv6. Dans les pages suivantes, nous verrons deux règles permettant de réduire le nombre de caractères requis pour représenter une adresse IPv6.

La Figure 2 présente des adresses IPv6 dans le format privilégié.



8.2.2.3 Règle n° 1 - Omettre les zéros en début de segment

La première règle permettant d'abréger la notation des adresses IPv6 est l'omission des zéros en début de segment de 16 bits (ou d'hextet). Par exemple :

- 01AB est équivalent à 1AB
- 09F0 est équivalent à 9F0
- 0A00 est équivalent à A00
- 00AB est équivalent à AB

Cette règle s'applique uniquement aux zéros de début de segment et NON aux zéros suivants. L'omission de ces derniers rendrait une adresse ambiguë. Par exemple, l'hextet « ABC » pourrait être « 0ABC » ou « ABC0 ».

Les figures 1 à 8 illustrent plusieurs exemples de la façon dont il est possible d'omettre les zéros de début de segment pour réduire la taille des adresses IPv6. Pour chaque exemple, le format privilégié est affiché. Notez que l'omission des zéros de début de segment entraîne un raccourcissement de l'adresse dans la plupart des cas.

8.2.2.4 Règle n° 2 - Omettre les séquences composées uniquement de zéros

La deuxième règle permettant d'abréger la notation des adresses IPv6 est qu'une suite de deux fois deux-points (::) peut remplacer toute chaîne unique et contiguë d'un ou plusieurs segments de 16 bits (hextets) comprenant uniquement des zéros.

Une suite de deux fois deux-points (::) peut être utilisée une seule fois par adresse : sinon, il serait possible d'aboutir sur plusieurs adresses différentes. Lorsque l'omission des zéros de début de segment est utilisée, la notation des adresses IPv6 peut être considérablement réduite. Il s'agit du « format compressé ».

Adresse non valide :

- 2001:0DB8::ABCD::1234

Extensions possibles des adresses ambiguës compressées :

- 2001:0DB8::ABCD:0000:0000:1234
- 2001:0DB8::ABCD:0000:0000:0000:1234
- 2001:0DB8:0000:ABCD::1234
- 2001:0DB8:0000:0000:ABCD::1234

Les figures 1 à 7 illustrent plusieurs exemples de la façon dont il est possible d'utiliser une suite de deux fois deux-points (::) et d'omettre les zéros de début de segment pour réduire la taille d'une adresse IPv6.

8.2.3 Les types d'adresses IPv6

8.2.3.1 Types d'adresses IPv6

Il existe trois types d'adresses IPv6 :

- **Monodiffusion** – une adresse de monodiffusion IPv6 identifie une interface sur un périphérique IPv6 de façon unique. Comme le montre la figure ci-contre, une adresse source IPv6 doit être une adresse de monodiffusion.

- **Multidiffusion** – une adresse de multidiffusion IPv6 est utilisée pour envoyer un seul paquet IPv6 vers plusieurs destinations.

- **Anycast** – une adresse anycast IPv6 est une adresse de monodiffusion IPv6 qui peut être attribuée à plusieurs périphériques. Un paquet envoyé à une adresse anycast est acheminé vers le périphérique le plus proche ayant cette adresse. Les adresses anycast sortent du cadre de ce cours.

Contrairement à l'IPv4, l'IPv6 n'a pas d'adresse de diffusion. Cependant, il existe une adresse de multidiffusion à tous les nœuds IPv6 qui offre globalement les mêmes résultats.

8.2.3.2 Longueur de préfixe IPv6

Souvenez-vous que le préfixe (ou la partie réseau) d'une adresse IPv4 peut être identifié par un masque de sous-réseau ou une longueur de préfixe en notation décimale à point (notation de barre oblique). Par exemple, l'adresse IP 192.168.1.10 et le masque de sous-réseau en notation décimale à point 255.255.255.0 équivalent à 192.168.1.10/24.

L'IPv6 utilise la longueur de préfixe pour représenter le préfixe de l'adresse. Le protocole IPv6 n'utilise pas la notation décimale à point du masque de sous-réseau. La longueur de préfixe est utilisée pour indiquer la partie réseau d'une adresse IPv6 à l'aide de la notation adresse IPv6/longueur de préfixe.

La longueur de préfixe peut aller de 0 à 128. La longueur de préfixe IPv6 standard pour les réseaux locaux et la plupart des autres types de réseau est /64. Celle-ci signifie que le préfixe ou la partie réseau de l'adresse a une longueur de 64 bits, ce qui laisse 64 bits pour l'ID d'interface (partie hôte) de l'adresse.

8.2.3.3 Les adresses de monodiffusion globale IPv6

Une adresse de monodiffusion IPv6 identifie une interface sur un périphérique IPv6 de façon unique. Un paquet envoyé à une adresse de monodiffusion est reçu par l'interface correspondant à cette adresse. Comme c'est le cas avec l'IPv4, une adresse source IPv6 doit être une adresse de monodiffusion. L'adresse IPv6 de destination peut quant à elle être une adresse de monodiffusion ou de multidiffusion.

Il existe six types d'adresse de monodiffusion IPv6.

Monodiffusion globale

Une adresse de monodiffusion globale est similaire à une adresse IPv4 publique. Ces adresses sont uniques au monde et routables sur Internet. Les adresses de monodiffusion globale peuvent être configurées de manière statique ou attribuées de manière dynamique. Il existe des différences importantes entre la réception d'une adresse IPv6 dynamique par un périphérique et le DHCP pour l'IPv4.

Link-local

Les adresses link-local sont utilisées pour communiquer avec d'autres périphériques sur la même liaison locale. Dans le cadre de l'IPv6, le terme « link » (ou liaison) fait référence à un sous-réseau. Les adresses link-local sont confinées à une seule liaison. Leur caractère unique doit être confirmé uniquement sur cette liaison, car elles ne sont pas routable au-delà de la liaison. En d'autres termes, les routeurs ne transmettent aucun paquet avec une adresse source ou de destination link-local.

Bouclage

Une adresse de bouclage est utilisée par un hôte pour envoyer un paquet à lui-même. Cette adresse ne peut pas être attribuée à une interface physique. Tout comme avec une adresse de bouclage IPv4, vous pouvez envoyer une requête ping à une adresse de bouclage IPv6 pour tester la configuration TCP/IP de l'hôte local. L'adresse de bouclage IPv6 contient uniquement des 0, excepté le dernier bit. Elle est donc notée ::1/128, ou simplement ::1 au format compressé.

Adresse non spécifiée

Une adresse non spécifiée est une adresse contenant uniquement des 0 et notée ::/128 ou simplement :: au format compressé. Elle ne peut pas être attribuée à une interface et ne peut être utilisée que comme adresse source dans un paquet IPv6. Une adresse non spécifiée est utilisée comme adresse source lorsque le périphérique n'a pas encore d'adresse IPv6 permanente ou lorsque la source du paquet n'est pas pertinente pour la destination.

Adresse locale unique

Les adresses IPv6 locales uniques ont certains points communs avec les adresses RFC 1918 privées pour l'IPv4, mais ces deux types d'adresse diffèrent également sur certains points. Des adresses locales uniques sont utilisées pour l'adressage local au sein d'un site ou entre un nombre limité de sites. Ces adresses ne doivent pas être routables sur le réseau IPv6 global. Les adresses locales uniques sont comprises entre FC00::/7 et FDFF::/7.

Avec l'IPv4, les adresses privées sont associées aux fonctions NAT/PAT pour fournir une traduction « plusieurs vers un » d'adresses privées en adresses publiques. Cette opération est effectuée en raison du caractère restreint de l'espace d'adressage IPv4. De nombreux sites utilisent également le caractère privé des adresses RFC 1918 pour sécuriser ou masquer leur réseau et limiter les risques. Cependant, ce n'est pas le but premier de ces technologies et l'IETF a toujours recommandé que les sites prennent les précautions de sécurité nécessaires au niveau de leur routeur connecté à Internet. Bien que l'IPv6 fournisse un adressage spécifique selon les sites, il n'est pas censé être utilisé pour masquer les périphériques IPv6 internes de l'Internet IPv6. L'IETF conseille de limiter l'accès aux périphériques en respectant les meilleures pratiques en matière de mesures de sécurité.

Remarque : la norme IPv6 initiale définissait des adresses site-local et utilisait la plage de préfixes FEC0::/10. Cette norme était ambiguë sur certains points et les adresses site-local ont été désapprouvées par l'IETF au profit des adresses locales uniques.

IPv4 intégré

Le dernier type d'adresse de monodiffusion est l'adresse IPv4 intégrée. Ces adresses sont utilisées pour faciliter la transition de l'IPv4 vers l'IPv6. Les adresses IPv4 intégrées sortent du cadre de ce cours.

8.2.3.4 Les adresses de monodiffusion link-local IPv6

Une adresse link-local IPv6 permet à un périphérique de communiquer avec d'autres périphériques IPv6 sur la même liaison et uniquement sur cette liaison (sous-réseau). Les paquets associés à une adresse source ou de destination link-local ne peuvent pas être acheminés au-delà de leur liaison d'origine.

Contrairement aux adresses link-local IPv4, les adresses link-local IPv6 ont une influence importante sur divers aspects du réseau. L'adresse de monodiffusion globale n'est pas obligatoire. Cependant, chaque interface réseau IPv6 doit avoir une adresse link-local.

Si une adresse link-local n'est pas configurée manuellement sur une interface, le périphérique crée automatiquement sa propre adresse sans communiquer avec un serveur DHCP. Les hôtes IPv6 créent une adresse link-local IPv6 même si aucune adresse de monodiffusion globale IPv6 n'a été attribuée aux périphériques. Cela permet aux périphériques IPv6 de communiquer avec d'autres périphériques IPv6 sur le même sous-réseau. Cela inclut la communication avec la passerelle par défaut (routeur).

Les adresses link-local IPv6 se trouvent dans la plage FE80::/10. /10 Indique que les 10 premiers bits sont 1111 1110 10xx xxxx. Le premier hextet dispose d'une plage allant de 1111 1110 10**00 0000** (FE80) à 1111 1110 10**11 1111** (FEBF).

La Figure 1 présente un exemple de transmission à l'aide d'adresses link-local IPv6.

La Figure 2 illustre le format d'une adresse link-local IPv6.

Les adresses link-local IPv6 sont également utilisées par les protocoles de routage IPv6 pour échanger des messages et en tant qu'adresses de saut suivant dans la table de routage IPv6. Les adresses link-local sont décrites plus en détail dans un cours ultérieur.

Remarque : généralement, c'est l'adresse link-local du routeur et non l'adresse de monodiffusion globale qui est utilisée comme passerelle par défaut pour les autres périphériques sur la liaison.

8.2.4 Les adresses de monodiffusion globale IPv6

8.2.4.1 La structure d'une adresse de monodiffusion globale IPv6

Les adresses de monodiffusion globale IPv6 sont uniques au monde et routables (Internet IPv6). Ces adresses sont équivalentes aux adresses publiques IPv4. L'ICANN (Internet Committee for Assigned Names and Numbers), opérateur de l'IANA (Internet Assigned Numbers Authority), attribue des blocs d'adresses IPv6 aux cinq RIR. Actuellement, seules des adresses de monodiffusion globale dont les premiers bits sont 001 ou 2000::/3 sont attribuées. C'est uniquement 1/8e de l'espace d'adressage IPv6 total disponible : seule une infime partie est exclue pour les autres types d'adresse de monodiffusion et de multidiffusion.

Remarque : l'adresse 2001:0DB8::/32 a été réservée à des fins de documentation, par exemple pour être utilisée dans des exemples.

La Figure 1 illustre la structure et la plage d'adresses de monodiffusion globale.

Une adresse de monodiffusion globale se compose de trois parties :

- Préfixe de routage global
- ID de sous-réseau
- ID d'interface

Préfixe de routage global

Le préfixe de routage global est le préfixe ou la partie réseau de l'adresse attribué(e) par le fournisseur (par exemple un FAI) à un client ou à un site. Actuellement, les RIR attribuent le préfixe global de routage /48 aux clients. Ces clients incluent tous les clients potentiels, des réseaux d'entreprise aux réseaux particuliers. Cet espace d'adressage est plus que suffisant pour la plupart des clients.

La Figure 2 illustre la structure d'une adresse de monodiffusion globale utilisant le préfixe de routage global /48. Les préfixes /48 sont les préfixes de routage global les plus couramment attribués et seront utilisés dans la plupart des exemples de ce cours.

Par exemple, l'adresse IPv6 2001:0DB8:ACAD::/48 a un préfixe indiquant que les 48 premiers bits (3 hextets) (2001:0DB8:ACAD) constituent le préfixe ou la partie réseau de l'adresse. La suite de deux fois deux-points (::) avant la longueur de préfixe /48 signifie que le reste de l'adresse contient uniquement des 0.

ID de sous-réseau

L'ID de sous-réseau est utilisé par une entreprise pour identifier les sous-réseaux au sein de son site.

ID d'interface

L'ID d'interface IPv6 est similaire à la partie hôte d'une adresse IPv4. Le terme ID d'interface est utilisé car un hôte unique peut avoir plusieurs interfaces, chacune dotée d'une ou de plusieurs adresses IPv6.

Remarque : contrairement à l'adressage IPv4, avec IPv6, les adresses d'hôte contenant uniquement des 0 ou uniquement des 1 peuvent être attribuées à un périphérique. L'adresse contenant uniquement des 1 peut être utilisée, puisque les adresses de diffusion ne sont pas utilisées dans IPv6. L'adresse contenant uniquement des 0 peut également être utilisée, mais elle est réservée comme adresse anycast de routeur de sous-réseau, et elle ne doit être attribuée qu'aux routeurs.

Un moyen simple de lire la plupart des adresses IPv6 consiste à compter le nombre d'hextets. Comme l'illustre la Figure 3, dans une adresse de monodiffusion globale /64, les quatre premiers hextets sont réservés à la partie réseau de l'adresse, le quatrième hextet indiquant l'ID de sous-réseau. Les quatre hextets restants sont réservés pour l'ID d'interface

8.2.4.2 La configuration statique d'une adresse de monodiffusion globale

Configuration de routeur

La plupart des commandes de configuration et de vérification IPv6 de Cisco IOS sont semblables aux commandes utilisées pour l'IPv4. Dans de nombreux cas, la seule différence est l'utilisation d'**ipv6** au lieu d'**ip** dans les commandes.

La commande **interface** permettant de configurer une adresse de monodiffusion IPv6 sur une interface est **ipv6 address** *adresse IPv6/longueur du préfixe*.

Notez qu'il n'y a aucun espace entre l'*adresse IPv6* et la *longueur du préfixe*.

La configuration utilisée en exemple utilise la topologie de la Figure 1 et les sous-réseaux IPv6 suivants :

- 2001:0DB8:ACAD:0001:/64 (*ou* 2001:DB8:ACAD:1::/64)
- 2001:0DB8:ACAD:0002:/64 (*ou* 2001:DB8:ACAD:2::/64)
- 2001:0DB8:ACAD:0003:/64 (*ou* 2001:DB8:ACAD:3::/64)

Comme illustré à la Figure 2, les commandes nécessaires pour configurer l'adresse de monodiffusion globale IPv6 sur l'interface gigabit ethernet 0/0 du périphérique R1 sont :

Router(config)#interface GigabitEthernet 0/0

Router(config-if)#ipv6 address 2001:db8:acad:1::1/64

Router(config-if)#no shutdown

Configuration d'hôte

La configuration manuelle de l'adresse IPv6 sur un hôte est similaire à la configuration d'une adresse IPv4.

Comme l'illustre la Figure 3, l'adresse de la passerelle par défaut configurée pour le PC1 est 2001:DB8:ACAD:1::1, l'adresse de monodiffusion globale de l'interface gigabit ethernet du périphérique R1 sur le même réseau.

Utilisez le contrôleur de syntaxe de la Figure 4 pour configurer l'adresse de monodiffusion globale IPv6.

Tout comme avec l'IPv4, la configuration des adresses statiques sur les clients ne convient pas aux environnements de grande taille. Pour cette raison, la plupart des administrateurs de réseaux IPv6 utilisent l'attribution dynamique des adresses IPv6.

Il existe deux façons pour un périphérique d'obtenir automatiquement une adresse de monodiffusion globale IPv6 :

- Configuration automatique des adresses sans état (SLAAC)
- DHCPv6

8.2.4.3 La configuration dynamique d'une adresse de monodiffusion globale avec la méthode SLAAC

Configuration automatique des adresses sans état (SLAAC)

La configuration automatique des adresses sans état (SLAAC) est une méthode permettant à un périphérique d'obtenir son préfixe, la longueur de préfixe, et l'adresse de la passerelle par défaut depuis un *routeur IPv6*, sans l'intervention d'un serveur DHCPv6. Lorsque la SLAAC

est utilisée, les périphériques se basent sur les messages d'annonce de routeur ICMPv6 du routeur local pour obtenir les informations nécessaires.

Les routeurs IPv6 envoient régulièrement des messages d'annonce de routeur ICMPv6 à tous les périphériques IPv6 du réseau. Par défaut, les routeurs Cisco envoient des messages d'annonce de routeur toutes les 200 secondes à l'adresse du groupe de multidiffusion à tous les nœuds IPv6. Un périphérique IPv6 du réseau n'a pas à attendre ces messages. Il peut envoyer un message de sollicitation de routeur au routeur, en utilisant l'adresse du groupe de multidiffusion à tous les routeurs IPv6. Lorsqu'un routeur IPv6 reçoit un message de sollicitation, il répond immédiatement en envoyant un message d'annonce de routeur.

Même si une interface d'un routeur Cisco peut être configurée avec une adresse IPv6, cela ne fait pas du routeur un « routeur IPv6 ». Un routeur IPv6 est un routeur qui :

- transfère les paquets IPv6 entre les réseaux ;
- peut être configuré avec des routes IPv6 statiques ou un protocole de routage IPv6 dynamique ;
- envoie des messages d'annonce de routeur ICMPv6.

Le routage IPv6 n'est pas activé par défaut. Pour sélectionner l'IPv6 sur un routeur, la commande de configuration globale **ipv6 unicast-routing** doit être utilisée.

Remarque : les routeurs Cisco sont tous configurés pour l'IPv4 par défaut.

Le message d'annonce de routeur ICMPv6 contient le préfixe, la longueur du préfixe et d'autres informations destinées au périphérique IPv6. Le message d'annonce de routeur indique également au périphérique IPv6 comment obtenir ses informations d'adressage. Ce message peut contenir l'une des trois options suivantes, comme illustré à la figure ci-contre :

- **Option 1 – SLAAC uniquement** : le périphérique doit utiliser le préfixe, la longueur du préfixe et l'adresse de la passerelle par défaut contenus dans le message d'annonce de routeur. Aucune information n'est acquise auprès d'un serveur DHCPv6.
- **Option 2 – SLAAC et DHCPv6** : le périphérique doit utiliser le préfixe, la longueur du préfixe et l'adresse de la passerelle par défaut contenus dans le message d'annonce de routeur. Il existe d'autres informations à acquérir auprès d'un serveur DHCPv6 telles que l'adresse du serveur DNS. Le périphérique obtient ces informations supplémentaires par le biais du processus de découverte et d'interrogation d'un serveur DHCPv6. On parle alors de DHCPv6 sans état, car le serveur DHCPv6 n'a pas besoin d'attribuer ou de contrôler les allocations d'adresses IPv6, mais doit fournir des informations supplémentaires telles que l'adresse du serveur DNS.
- **Option 3 – DHCPv6 uniquement** : le périphérique ne doit pas utiliser les informations contenues dans le message d'annonce de routeur en tant qu'informations d'adressage. Au lieu de cela, le périphérique utilise le processus de découverte et d'interrogation d'un serveur DHCPv6 pour obtenir toutes ses informations d'adressage. Ces informations incluent une adresse de monodiffusion globale IPv6, la longueur du préfixe, une adresse de passerelle par défaut et les adresses des serveurs DNS. Dans ce

cas, le serveur DHCPv6 agit en tant que serveur DHCP avec état, tout comme le DHCP pour l'IPv4. Le serveur DHCPv6 attribue et contrôle les adresses IPv6 afin de ne pas attribuer la même adresse IPv6 à plusieurs périphériques.

Les routeurs envoient des messages d'annonce de routeur ICMPv6 en utilisant l'adresse link-local comme adresse source IPv6. Les périphériques utilisant SLAAC utilisent l'adresse link-local du routeur comme adresse de passerelle par défaut.

8.2.4.4 La configuration dynamique d'une adresse de monodiffusion globale avec la méthode DHCPv6

DHCPv6

Le protocole DHCP (Dynamic Host Configuration Protocol) pour l'IPv6 (DHCPv6) est comparable au DHCP pour l'IPv4. Un périphérique peut recevoir automatiquement ses informations d'adressage, y compris une adresse de monodiffusion globale, la longueur du préfixe, l'adresse de la passerelle par défaut et les adresses des serveurs DNS à l'aide des services d'un serveur DHCPv6.

Un périphérique peut recevoir une partie ou la totalité de ses informations d'adressage IPv6 depuis un serveur DHCPv6, selon que l'option 2 (SLAAC et DHCPv6) ou l'option 3 (DHCPv6 uniquement) est spécifiée dans le message d'annonce de routeur ICMPv6. En outre, le système d'exploitation de l'hôte peut choisir d'ignorer le message d'annonce de routeur et d'obtenir son adresse IPv6 et les autres informations directement à partir d'un serveur DHCPv6.

Avant de déployer des périphériques IPv6 dans un réseau, il est judicieux de commencer par vérifier si l'hôte peut observer les options dans le message d'annonce de routeur ICMPv6.

Un périphérique peut obtenir son adresse de monodiffusion globale IPv6 de manière dynamique et peut également être configuré avec plusieurs adresses IPv6 statiques sur la même interface. L'IPv6 permet à plusieurs adresses IPv6 appartenant au même réseau IPv6 d'être configurées sur la même interface.

Un périphérique peut également être configuré avec plusieurs adresses IPv6 de passerelle par défaut. Pour plus d'informations sur la sélection de l'adresse à utiliser comme adresse source IPv6 ou de l'adresse de passerelle par défaut à utiliser, reportez-vous au RFC 6724, « Default Address Selection for IPv6 ».

ID d'interface

Si le client n'utilise pas les informations contenues dans le message d'annonce de routeur et compte uniquement sur le DHCPv6, le serveur DHCPv6 fournit alors l'adresse de monodiffusion globale IPv6 complète, y compris le préfixe et l'ID d'interface.

Cependant, si l'option 1 (SLAAC uniquement) ou l'option 2 (SLAAC avec DHCPv6) est utilisée, le client n'obtient pas la partie ID d'interface réelle de l'adresse grâce à ces processus. Le périphérique client doit alors déterminer son propre ID d'interface de 64 bits, soit à l'aide de la méthode EUI-64 soit en générant un nombre aléatoire de 64 bits.

8.2.4.5 La génération aléatoire ou à l'aide de la méthode EUI-64

Processus de EUI-64

L'IEEE a créé l'EUI (Extended Unique Identifier), ou format EUI-64 modifié. Ce processus utilise l'adresse MAC Ethernet 48 bits d'un client et insère 16 autres bits au milieu de l'adresse MAC 48 bits pour créer un ID d'interface de 64 bits.

Les adresses MAC Ethernet sont généralement représentées au format hexadécimal et sont constituées de deux parties :

- **OUI (Organizationally Unique Identifier)** – l'OUI est un code de fournisseur de 24 bits (6 caractères hexadécimaux) attribué par l'IEEE.

- **ID de périphérique** – l'identifiant de périphérique est une valeur unique de 24 bits (6 caractères hexadécimaux) contenue dans un OUI standard.

Un ID d'interface EUI-64 est représenté au format binaire et comprend trois parties :

- Le code OUI sur 24 bits, provenant de l'adresse MAC du client, mais dont le septième bit (universellement/localement, U/L) est inversé. Cela signifie que si le septième bit est un 0, il devient un 1, et vice versa.

- La valeur de 16 bits FFFE intégrée (au format hexadécimal).

- L'ID de périphérique de 24 bits de l'adresse MAC du client.

Le processus EUI-64 est présenté à la Figure 1, avec l'adresse MAC gigabit ethernet FC99:4775:CEE0 du périphérique R1.

Étape 1 : coupez l'adresse MAC au niveau de la séparation entre l'OUI et l'ID de périphérique.

Étape 2 : insérez la valeur hexadécimale FFFE, à savoir 1111 1111 1111 1110 en binaire.

Étape 3 : convertissez les 2 premières valeurs hexadécimales de l'OUI en binaire et inversez le bit U/L (bit 7). Dans cet exemple, le 0 du bit 7 devient un 1.

Il en résulte un ID d'interface généré à l'aide de la méthode EUI-64, FE99:47FF:FE75:CEE0.

Remarque : l'utilisation du bit U/L et les raisons de son inversion sont expliquées dans le RFC 5342.

L'avantage de la méthode EUI-64 est que l'adresse MAC Ethernet peut être utilisée pour déterminer l'ID d'interface. Elle permet également aux administrateurs réseau de suivre facilement une adresse IPv6 jusqu'à un périphérique final en utilisant une adresse MAC unique. Toutefois, cela a entraîné des problèmes de confidentialité pour de nombreux utilisateurs. Ces derniers s'inquiètent du fait qu'il soit possible de remonter jusqu'à l'ordinateur physique en analysant les paquets. En raison de ces problèmes, un ID d'interface généré aléatoirement peut également être utilisé.

ID d'interface générés aléatoirement

Selon le système d'exploitation, un périphérique peut utiliser un ID d'interface généré aléatoirement plutôt que l'adresse MAC et le processus EUI-64. À partir de la version Windows Vista, Windows utilise un ID d'interface généré aléatoirement au lieu d'un ID créé avec le processus EUI-64. Windows XP et les systèmes d'exploitation précédents utilisaient la méthode EUI-64.

Il est simple de savoir si une adresse a été créée via la méthode EUI-64 : il suffit d'analyser la valeur FFFE située dans l'ID d'interface (voir la Figure 2).

Une fois l'ID d'interface établi, via le processus EUI-64 ou par génération aléatoire, il peut être combiné avec un préfixe IPv6 pour créer une adresse de monodiffusion globale ou une adresse link-local :

- **Adresse de monodiffusion globale** – s'il utilise la SLAAC, le périphérique reçoit son préfixe par l'intermédiaire du message d'annonce de routeur ICMPv6 et l'associe à l'ID d'interface.

- **Adresse link-local** – un préfixe link-local commence par FE80::/10. Un périphérique utilise généralement FE80::/64 comme préfixe/longueur de préfixe, suivi de l'ID d'interface.

8.2.4.6 Les adresses link-local dynamiques

S'il utilise la SLAAC (SLAAC uniquement ou SLAAC avec DHCPV6), un périphérique reçoit son préfixe et la longueur de préfixe dans un message d'annonce de routeur ICMPv6. Puisque le préfixe de l'adresse est déterminé par le message d'annonce de routeur, le périphérique doit fournir uniquement la partie ID d'interface de l'adresse. Comme indiqué précédemment, l'ID d'interface peut être automatiquement généré selon le processus EUI-64 ou, selon le système d'exploitation, généré aléatoirement. En utilisant les informations du message d'annonce de routeur et l'ID d'interface, le périphérique peut établir son adresse de monodiffusion globale.

Une fois qu'une adresse de monodiffusion globale est attribuée à une interface, le périphérique IPv6 génère automatiquement son adresse link-local. Les périphériques IPv6 doivent avoir au minimum une adresse link-local. Notez qu'une adresse link-local IPv6 permet à un périphérique de communiquer avec les autres périphériques IPv6 situés sur le même sous-réseau.

Les adresses link-local IPv6 servent à diverses fins :

- Un hôte utilise l'adresse link-local du routeur local en tant qu'adresse IPv6 de passerelle par défaut.

- Les routeurs échangent des messages du protocole de routage dynamique via des adresses link-local.

- Les tables de routage des routeurs utilisent l'adresse link-local pour identifier le routeur de saut suivant lors du transfert des paquets IPv6.

Une adresse link-local peut être établie dynamiquement ou configurée manuellement comme adresse link-local statique.

Adresse link-local affectée dynamiquement

L'adresse link-local est créée dynamiquement à l'aide du préfixe FE80::/10 et de l'ID d'interface.

Par défaut, les routeurs Cisco IOS utilisent la méthode EUI-64 pour générer l'ID d'interface de toutes les adresses link-local sur des interfaces IPv6. Pour les interfaces série, le routeur utilise l'adresse MAC d'une interface Ethernet. Notez qu'une adresse link-local doit être unique sur la liaison ou le réseau. Toutefois, un inconvénient de l'utilisation de l'adresse link-local attribuée dynamiquement est sa longueur : il est en effet difficile d'identifier et de mémoriser les adresses attribuées.

8.2.4.7 Adresses Link-Local statiques

Adresse link-local statique

Configurer manuellement l'adresse link-local permet de créer une adresse qui est reconnaissable et plus facile à mémoriser.

Les adresses link-local peuvent être configurées manuellement avec la même commande d'interface que celle utilisée pour créer des adresses de monodiffusion globale IPv6. Cependant, dans ce cas, un autre paramètre doit être utilisé :

Router(config-if)#ipv6 address link-local-address link-local

La Figure 1 montre qu'une adresse link-local possède un préfixe compris dans la plage FE80 à FEBF. Lorsqu'une adresse commence par cet hextet (segment de 16 bits), le paramètre link-local doit suivre l'adresse.

La Figure 2 montre la configuration d'une adresse link-local à l'aide de la commande **ipv6 address interface**. L'adresse link-local FE80::1 est utilisée pour être facilement reconnaissable comme appartenant au routeur R1. La même adresse link-local IPv6 est configurée sur toutes les interfaces du routeur R1. L'adresse FE80::1 peut être configurée sur chaque liaison, car elle ne doit être unique que sur cette liaison.

Tout comme le routeur R1, le routeur R2 peut être configuré avec FE80::2 comme adresse link-local IPv6 sur toutes ses interfaces.

8.2.4.8 Vérifier la configuration des adresses IPv6

Comme l'illustre la Figure 1, la commande permettant de vérifier la configuration de l'interface IPv6 est semblable à la commande utilisée pour l'IPv4.

La commande **show interface** affiche l'adresse MAC des interfaces Ethernet. Le processus EUI-64 utilise cette adresse MAC pour générer l'ID d'interface de l'adresse link-local. En outre, la commande **show ipv6 interface brief** affiche des résultats abrégés pour chacune des interfaces. Les termes [up/up] sur la même ligne que l'interface indiquent l'état de l'interface de couche 1/couche 2. Ces états correspondent aux colonnes Status et Protocol de la commande IPv4 équivalente.

Notez que chaque interface possède deux adresses IPv6. La deuxième adresse de chaque interface est l'adresse de monodiffusion globale qui a été configurée. La première adresse, celle qui commence par FE80, est l'adresse de monodiffusion link-local de l'interface. Souvenez-vous que l'adresse link-local est automatiquement ajoutée à l'interface lorsqu'une adresse de monodiffusion globale est attribuée.

En outre, notez que l'adresse link-local de l'interface série 0/0/0 du routeur R1 est identique à celle de l'interface gigabit ethernet 0/0. Les interfaces série n'ont pas d'adresses MAC Ethernet. Cisco IOS utilise donc l'adresse MAC de la première interface Ethernet disponible. Cela est possible car les interfaces link-local ne doivent être uniques que sur une liaison.

L'adresse link-local de l'interface du routeur est généralement l'adresse de la passerelle par défaut des périphériques sur cette liaison ou sur ce réseau.

Comme l'illustre la Figure 2, la commande **show ipv6 route** peut être utilisée pour vérifier que les adresses des interfaces IPv6 spécifiques et des réseaux IPv6 ont été installées dans la table de routage IPv6. La commande **show ipv6 route** n'affiche que les réseaux IPv6 et non les réseaux IPv4.

Dans la table de route, la lettre C placée en regard d'une route indique qu'il s'agit d'un réseau connecté directement. Lorsque l'interface de routeur est configurée avec une adresse de monodiffusion globale et lorsque son état est « up/up », le préfixe IPv6 et la longueur de préfixe sont ajoutés à la table de routage IPv6 en tant que route connectée.

L'adresse de monodiffusion globale IPv6 configurée sur l'interface est également insérée dans la table de routage en tant que route locale. Le préfixe de la route locale est /128. Des routes locales sont utilisées par la table de routage pour traiter efficacement les paquets dont l'adresse de destination est l'adresse de l'interface du routeur.

La commande **ping** pour l'IPv6 est identique à la commande utilisée avec l'IPv4, excepté qu'une adresse IPv6 est utilisée. Comme l'illustre la Figure 3, cette commande permet de vérifier la connectivité de couche 3 entre le routeur R1 et le PC1. Lorsque vous envoyez une requête ping à une adresse link-local d'un routeur, Cisco IOS invite l'utilisateur à entrer l'interface de sortie. Comme l'adresse link-local de destination peut être sur une ou plusieurs

de ses liaisons ou sur un ou plusieurs de ses réseaux, le routeur doit savoir à quelle interface envoyer la requête ping.

Utilisez le contrôleur de syntaxe de la Figure 4 pour vérifier la configuration des adresses IPv6.

8.2.5.1 Les adresses de multidiffusion IPv6 attribuées

Les adresses de multidiffusion IPv6

Les adresses de multidiffusion IPv6 sont semblables aux adresses de multidiffusion IPv4. Rappelez-vous qu'une adresse de multidiffusion est utilisée pour envoyer un paquet à un ou plusieurs destinataires (groupe de multidiffusion). Les adresses de multidiffusion IPv6 ont le préfixe FF00::/8.

Remarque : les adresses de multidiffusion ne peuvent être que des adresses de destination et non des adresses source.

Il existe deux types d'adresses de multidiffusion IPv6 :

- Les adresses de multidiffusion attribuées
- Les adresses de multidiffusion de nœud sollicité

Les adresses de multidiffusion attribuées

Les adresses de multidiffusion attribuées sont des adresses de multidiffusion réservées à des groupes ou périphériques prédéfinis. Une adresse de multidiffusion attribuée est une adresse unique utilisée pour joindre un groupe de périphériques exécutant un service ou un protocole commun. Les adresses de multidiffusion attribuées sont utilisées avec des protocoles spécifiques, tels que DHCPv6.

Les deux groupes suivants de multidiffusion IPv6 attribuée sont les plus courants :

- **Groupe de multidiffusion à tous les nœuds FF02::1** – il s'agit d'un groupe de multidiffusion que tous les périphériques IPv6 peuvent joindre. Un paquet envoyé à ce groupe est reçu et traité par toutes les interfaces IPv6 situées sur la liaison ou le réseau. Cette opération a le même effet qu'une adresse de diffusion IPv4. La figure illustre un exemple de communication via l'adresse de multidiffusion à tous les nœuds. Un routeur IPv6 envoie des messages d'annonce de routeur ICMPv6 au groupe de multidiffusion à tous les nœuds. Le message d'annonce de routeur indique à tous les périphériques IPv6 du réseau les informations d'adressage telles que le préfixe, la longueur du préfixe et la passerelle par défaut.
- **Groupe de multidiffusion à tous les routeurs FF02::2** – il s'agit d'un groupe de multidiffusion que tous les routeurs IPv6 peuvent joindre. Un routeur devient un membre de ce groupe lorsqu'il est activé en tant que routeur IPv6 avec la commande

de configuration globale **ipv6 unicast-routing**. Un paquet envoyé à ce groupe est reçu et traité par tous les routeurs IPv6 situés sur la liaison ou le réseau.

Les périphériques IPv6 envoient des messages de sollicitation de routeur ICMPv6 à l'adresse de multidiffusion à tous les routeurs. Le message de sollicitation de routeur demande un message d'annonce au routeur IPv6 pour faciliter la configuration d'adresse du périphérique

8.2.5.2 Les adresses de multidiffusion IPv6 de nœud sollicité

Une adresse de multidiffusion de nœud sollicité est semblable à une adresse de multidiffusion à tous les nœuds. Notez qu'une adresse de multidiffusion à tous les nœuds est en grande partie semblable à une adresse de diffusion IPv4. Tous les périphériques du réseau doivent traiter le trafic envoyé à l'adresse de multidiffusion à tous les nœuds. Pour réduire le nombre de périphériques qui doivent gérer le trafic, utilisez une adresse de multidiffusion de nœud sollicité.

Une adresse de multidiffusion de nœud sollicité est une adresse correspondant uniquement aux 24 derniers bits de l'adresse de monodiffusion globale IPv6 d'un périphérique. Les seuls périphériques qui n'ont pas besoin de traiter les paquets sont ceux dont l'ID d'interface dispose des 24 mêmes bits les moins significatifs (derniers bits de l'ID d'interface).

Une adresse de multidiffusion de nœud sollicité IPv6 est créée automatiquement lorsque l'adresse de monodiffusion globale ou l'adresse link-local est attribuée. L'adresse de multidiffusion de nœud sollicité IPv6 est créée grâce à la combinaison d'un préfixe spécifique, FF02:0:0:0:0:1:FF00::/104, et des 24 derniers bits de son adresse de monodiffusion.

L'adresse de multidiffusion de nœud sollicité comprend deux parties :

- **Le préfixe de multidiffusion FF02:0:0:0:0:1:FF00::/104 :** les 104 premiers bits de l'adresse de multidiffusion de nœud sollicité.

- **Les 24 bits les moins significatifs :** il s'agit des 24 derniers bits de l'adresse de multidiffusion de nœud sollicité. Ces bits sont copiés à partir des 24 derniers bits de l'adresse de monodiffusion globale ou de l'adresse de monodiffusion link-local du périphérique.

Il est possible que plusieurs périphériques aient la même adresse de multidiffusion de nœud sollicité. Bien que cela soit rare, cela peut se produire lorsque des périphériques ont les mêmes 24 derniers bits dans leur ID d'interface. Cela n'entraîne aucun problème, car le périphérique traite toujours le message encapsulé, qui inclut l'adresse IPv6 complète du périphérique en question.

8.3 Vérification de la connectivité

8.3.1 ICMP

8.3.1.1 Les messages ICMPv4 et ICMPv6

Bien que le protocole IP ne soit pas un protocole fiable, la suite TCP/IP permet d'envoyer des messages si certaines erreurs se produisent. Ces messages sont envoyés via les services du protocole ICMP. Ces messages ont pour objectif de fournir des commentaires sur les problèmes liés au traitement de paquets IP dans certaines circonstances. Les messages ICMP ne sont pas obligatoires et sont souvent interdits au sein des réseaux pour des raisons de sécurité.

Le protocole ICMP est disponible pour IPv4 et pour IPv6. ICMPv4 est le protocole de message des réseaux IPv4. L'ICMPv6 fournit ces mêmes services pour l'IPv6, mais inclut des fonctionnalités supplémentaires. Dans ce cours, le terme ICMP est utilisé pour faire référence à l'ICMPv4 et à l'ICMPv6.

Il existe différents types de messages ICMP, et les raisons pour lesquelles ils sont envoyés sont très diverses. Nous décrirons les messages les plus courants.

Les messages ICMP communs à ICMPv4 et à ICMPv6 sont notamment les suivants :

- Host confirmation (Confirmation de l'hôte)
- Destination or Service Unreachable (destination ou service inaccessible)
- Time exceeded (Délai dépassé)
- Route redirection (Redirection de la route)

Host Confirmation (Confirmation de l'hôte)

Un message ICMP Echo (Écho ICMP) permet de déterminer si un hôte est fonctionnel. L'hôte local envoie un message ICMP Echo Request (Requête d'écho) à un autre hôte. Si l'hôte est disponible, l'hôte de destination répond en envoyant une réponse d'écho. Dans la figure ci-contre, cliquez sur le bouton Lecture pour afficher une animation concernant les requêtes et les réponses d'écho ICMP. L'utilisation de messages ICM Echo est à la base de l'utilitaire ping.

Destination or Service Unreachable (destination ou service inaccessible)

Lorsqu'un hôte ou une passerelle reçoit un paquet impossible à acheminer, il ou elle peut utiliser un message ICMP de destination inaccessible pour avertir la source que la destination ou le service est inaccessible. Ce message comprend un code indiquant pourquoi le paquet n'a pas pu être acheminé.

Certains des codes de destination inaccessible pour l'ICMPv4 sont :

- 0 – réseau inaccessible.
- 1 – hôte inaccessible.
- 2 – protocole inaccessible.
- 3 – port inaccessible.

Remarque : l'ICMPv6 a des codes légèrement différents pour des messages de destination inaccessible.

Dépassement du délai

Un message de dépassement de délai ICMPv4 est utilisé par un routeur pour indiquer qu'il ne peut pas transférer un paquet car le champ TTL de durée de vie du paquet a atteint 0. Si un routeur reçoit un paquet et décrémente le champ TTL de durée de vie du paquet IPv4 pour atteindre zéro, il abandonne le paquet et envoie un message de dépassement de délai à l'hôte source.

Le protocole ICMPv6 envoie également un message de dépassement de délai si le routeur ne peut pas transmettre un paquet IPv6 en raison de son expiration. Les paquets IPv6 n'ont pas de champ de durée de vie TTL : le champ de limite de nombre de sauts est utilisé pour déterminer si le paquet a expiré.

Route redirection (Redirection de la route)

Un routeur peut envoyer un message de redirection ICMP Redirect pour notifier l'hôte sur un réseau, qu'une meilleure route est disponible jusqu'à une destination particulière. Ce message ne peut être utilisé que si l'hôte source appartient au même réseau physique que les deux passerelles.

L'ICMPv4 et l'ICMPv6 utilisent tous deux des messages de redirection de route.

8.3.1.2 Les messages de sollicitation et d'annonce de routeur ICMPv6

Les messages d'informations et d'erreur du protocole ICMPv6 sont très similaires aux messages de contrôle et d'erreur mis en œuvre par le protocole ICMPv4. Cependant, l'ICMPv6 offre de nouvelles fonctions et fonctionnalités avancées introuvables dans l'ICMPv4.

ICMPv6 inclut quatre nouveaux protocoles dans le cadre du protocole Neighbor Discovery Protocol (ND ou NDP) :

- Message de sollicitation de routeur
- Message d'annonce de routeur
- Message de sollicitation de voisin

- Message d'annonce de voisin

Messages de sollicitation et d'annonce de routeur

Les périphériques IPv6 peuvent être divisés en deux catégories : les routeurs et les hôtes. Les messages de sollicitation de routeur et d'annonce de routeur sont envoyés entre les hôtes et les routeurs.

- **Messages de sollicitation de routeur :** lorsqu'un hôte est configuré pour obtenir ses informations d'adressage à l'aide de la configuration automatique des adresses sans état (SLAAC), celui-ci envoie un message de sollicitation au routeur. Le message de sollicitation de routeur est envoyé sous forme de message de multidiffusion à tous les routeurs IPv6.

- **Messages d'annonce de routeur** : ces messages sont envoyés par les routeurs pour fournir les informations d'adressage aux hôtes via la SLAAC. Un message d'annonce de routeur peut inclure les informations d'adressage pour l'hôte telles que le préfixe et la longueur de préfixe. Un routeur envoie un message d'annonce de routeur régulièrement ou en réponse à un message de sollicitation. Par défaut, les routeurs Cisco envoient des messages d'annonce de routeur toutes les 200 secondes. Ces messages sont envoyés à l'adresse de multidiffusion à tous les nœuds IPv6. Un hôte utilisant la SLAAC utilise l'adresse link-local du routeur qui a envoyé le message d'annonce de routeur en tant que passerelle par défaut.

8.3.1.3 Les messages de sollicitation et d'annonce de voisin ICMPv6

Le protocole Neighbor Discovery Protocol (NDP) ICMPv6 comprend deux types de message supplémentaires : la sollicitation de voisin et l'annonce de voisin.

Les messages de sollicitation de voisin et d'annonce de voisin sont utilisés pour :

- La résolution d'adresse

- La détection d'adresses en double (DAD)

Résolution d'adresse

La résolution d'adresse est utilisée lorsqu'un périphérique du réseau local (LAN) connaît l'adresse de monodiffusion IPv6 d'une destination, mais pas son adresse MAC Ethernet. Pour déterminer l'adresse MAC de destination, le périphérique envoie un message de sollicitation de voisin à l'adresse du nœud sollicité. Le message inclut l'adresse IPv6 (de destination) connue. Le périphérique avec l'adresse IPv6 ciblée répond par un message d'annonce de voisin contenant son adresse MAC Ethernet.

Détection d'adresses en double

Lorsqu'une adresse de monodiffusion globale ou de monodiffusion link-local est attribuée à un périphérique, il est recommandé d'utiliser la détection d'adresses en double sur l'adresse pour s'assurer qu'elle est unique. Pour vérifier le caractère unique d'une adresse, le périphérique envoie un message de sollicitation de voisin avec sa propre adresse IPv6 comme adresse IPv6 ciblée. Si cette adresse est attribuée à un autre périphérique du réseau, ce dernier répond en envoyant un message d'annonce de voisin. Ce message informe le périphérique expéditeur que l'adresse est utilisée. Si un message d'annonce de voisin n'est pas renvoyé au bout d'un certain temps, l'adresse de monodiffusion est unique et peut être utilisée.

Remarque : la détection d'adresses en double n'est pas obligatoire, mais le RFC 4861 recommande de l'utiliser sur les adresses de monodiffusion.

8.3.2 Test et vérification

8.3.2.1 Ping - Tester la pile locale

La commande ping est un utilitaire de test qui utilise des messages de requête et de réponse d'écho ICMP pour tester la connectivité entre les hôtes. Le ping fonctionne avec les hôtes IPv4 et IPv6.

Pour tester la connectivité à un autre hôte sur un réseau, une requête d'écho est envoyée à l'adresse d'hôte au moyen de la commande **ping**. Si l'hôte à l'adresse spécifiée reçoit une requête d'écho, il répond en envoyant une réponse d'écho. Chaque fois qu'une réponse d'écho est reçue, la commande ping vous informe du temps qui s'écoule entre l'envoi de la requête et la réception de la réponse. Cela peut être utilisé pour mesurer les performances réseau.

La commande ping a une valeur de délai d'attente pour la réponse. Si aucune réponse n'est reçue dans ce délai, la commande ping affiche un message indiquant que la réponse n'a pas été reçue. Cela indique généralement qu'il y a un problème, mais cela peut également indiquer que des fonctions de sécurité de blocage des messages ping sont activées sur le réseau.

Une fois toutes les requêtes envoyées, l'utilitaire ping présente un sommaire qui inclut le taux de réussite et la durée de transmission moyenne à la destination.

Envoi d'une requête ping sur le bouclage local

La commande ping s'utilise également dans certaines activités de test et de vérification. C'est le cas par exemple d'un test de la configuration interne IPv4 ou IPv6 sur l'hôte local. Pour réaliser ce test, nous exécutons la commande ping sur l'adresse de bouclage locale 127.0.0.1 pour l'IPv4 (et ::1 pour l'IPv6). Le test de bouclage IPv4 est illustré dans la figure ci-contre.

Une réponse provenant de l'adresse 127.0.0.1 pour l'IPv4 ou ::1pour l'IPv6 indique que le protocole IP est correctement installé sur l'hôte. Cette réponse provient de la couche réseau. Toutefois, elle n'est pas une indication que les adresses, les masques ou les passerelles sont correctement configurés. Par ailleurs, elle n'indique rien sur l'état de la couche la plus basse de la pile réseau. Elle teste uniquement la configuration IP via la couche réseau du protocole IP. Si un message d'erreur est généré, cela indique que TCP/IP ne fonctionne pas sur l'hôte.

8.3.2.2 Ping - Tester la connectivité au réseau local

Vous pouvez également utiliser la commande ping pour tester la capacité d'un hôte à communiquer sur le réseau local. Cela consiste généralement à envoyer une requête ping à l'adresse IP de la passerelle de l'hôte. Une requête ping à la passerelle indique que l'hôte et l'interface du routeur qui sert de passerelle sont fonctionnels (ou non) sur le réseau local.

Pour ce test, l'adresse de la passerelle est souvent utilisée car le routeur est, en principe, toujours fonctionnel. Si l'adresse de la passerelle ne répond pas, une requête ping peut être envoyée à l'adresse IP d'un autre hôte sur le réseau local connu pour fonctionner.

Si une réponse est obtenue, soit de la passerelle, soit d'un autre hôte, cela signifie que les hôtes locaux peuvent communiquer sans problème sur le réseau local. Si la passerelle ne répond pas mais qu'un autre hôte répond, cela peut être révélateur d'un problème sur l'interface du routeur qui sert de passerelle.

Il se peut qu'une adresse de passerelle incorrecte ait été configurée sur l'hôte. Peut-être que l'interface du routeur est fonctionnelle, mais qu'une règle de sécurité en vigueur l'empêche de traiter des requêtes ping ou d'y répondre.

8.3.2.3 Ping - Tester la connectivité à distance

La commande ping peut aussi être utilisée pour tester la capacité d'un hôte local à communiquer sur un interréseau. L'hôte local peut envoyer une requête ping à un hôte fonctionnel IPv4 sur un réseau distant, comme présenté à la figure ci-contre.

Si cette requête ping aboutit, le fonctionnement d'une grande partie de l'interréseau peut être vérifié. Une requête ping réussie sur un interréseau confirme la communication sur le réseau local, le fonctionnement du routeur qui sert de passerelle et le fonctionnement de tous les autres routeurs sur le chemin entre le réseau local et le réseau de l'hôte distant.

En outre, la fonctionnalité de l'hôte distant peut être vérifiée. Si l'hôte distant ne peut pas communiquer en dehors de son réseau local, il ne répond pas.

Remarque : de nombreux administrateurs réseau limitent ou interdisent l'entrée des messages ICMP dans le réseau d'entreprise. Par conséquent, l'absence d'une réponse ping peut être due à des restrictions de sécurité.

8.3.2.4 Traceroute - Tester le chemin

La commande ping permet de tester la connectivité entre deux hôtes, mais ne fournit pas d'informations sur les détails des périphériques entre les hôtes. Traceroute (tracert) est un utilitaire qui génère une liste de sauts qui ont été traversés sur le chemin. Cette liste peut

fournir d'importantes informations pour la vérification et le dépannage. Si les données parviennent à destination, la commande affiche tous les routeurs situés entre les hôtes. Si les données restent bloquées au niveau d'un saut, l'adresse du dernier routeur ayant répondu à la commande peut fournir une indication sur l'endroit où se situe le problème ou sur d'éventuelles restrictions de sécurité.

Durée de transmission ou RTT (Round Trip Time)

L'exécution de la commande traceroute fournit la durée de transmission sur chacun des sauts rencontrés sur le chemin et indique si un saut n'a pas répondu. La durée de transmission correspond à la durée nécessaire à un paquet pour atteindre l'hôte distant, plus le temps mis par l'hôte pour répondre. Un astérisque (*) indique un paquet perdu ou sans réponse.

Cette information permet de localiser un routeur problématique sur le chemin. Si des temps de réponse longs ou des pertes de données caractérisent un saut particulier, cela indique que les ressources du routeur ou que ses connexions sont saturées.

Champs de durée de vie TTL IPv4 et limite de nombre de sauts IPv6

La commande traceroute utilise une fonction du champ de durée de vie TTL du protocole IPv4 et le champ de limite de nombre de sauts du protocole IPv6 dans les en-têtes de couche 3, ainsi que le message ICMP de dépassement de délai.

Lancez l'animation de la figure pour visualiser l'utilisation du paramètre TTL par l'utilitaire traceroute.

La première séquence des messages envoyés par traceroute contient un champ TTL de durée de vie égal à 1. Cela entraîne l'expiration du champ TTL de durée de vie du paquet IPv4 au niveau du premier routeur. Ce routeur répond ensuite en envoyant un message ICMPv4. L'utilitaire traceroute dispose à présent de l'adresse du premier saut.

Puis, il incrémente progressivement le champ TTL (2, 3, 4, etc.) pour chaque séquence de messages. Cela permet d'obtenir l'adresse de chaque saut, à mesure que les paquets expirent sur le chemin restant. Le champ TTL est incrémenté jusqu'à ce que la destination soit atteinte ou jusqu'à une valeur maximale prédéfinie.

Une fois que la destination finale est atteinte, l'hôte répond par un message ICMP Port Unreachable (port inaccessible) ou ICMP Echo Reply (réponse d'écho), à la place du message ICMP Time Exceeded (dépassement de délai).

CHAPITRE 9:

SEGMENTER DES RÉSEAUX IP EN SOUS-RÉSEAUX

Introduction

L'élaboration, la mise en œuvre et la gestion d'un modèle d'adressage IP garantissent un fonctionnement optimal des réseaux. Cela devient d'autant plus important lorsque le nombre de connexions d'hôtes à un réseau augmente. Lorsque vous aurez compris la structure hiérarchique de l'adresse IP et que vous saurez comment modifier cette hiérarchie afin de répondre plus efficacement aux besoins de routage, vous aurez déjà accompli une part essentielle de la planification du schéma d'adressage IP.

Dans l'adresse IPv4 initiale, il existe deux niveaux hiérarchiques : un réseau et un hôte. Ces deux niveaux d'adressage permettent de réaliser des regroupements de base qui facilitent l'acheminement des paquets vers un réseau de destination. Un routeur transmet les paquets en fonction de la partie réseau de l'adresse IP. Une fois que le réseau est localisé, la partie hôte de l'adresse permet l'identification du périphérique de destination.

Cependant, lorsque les réseaux s'étendent et comptent des centaines, voire des milliers d'hôtes, la hiérarchie à deux niveaux devient insuffisante.

Le fait de sous-diviser un réseau permet d'ajouter un niveau hiérarchique, pour obtenir trois niveaux : un réseau, un sous-réseau et un hôte. Le fait d'ajouter un niveau hiérarchique permet de créer des sous-groupes supplémentaires dans un réseau IP, qui facilitent l'acheminement rapide des paquets et le filtrage efficace en réduisant le trafic « local ».

Ce chapitre étudie en détail la création et l'attribution des adresses de réseaux et de sous-réseaux IP à l'aide du masque de sous-réseau.

Segmenter un réseau IPv4 en sous-réseaux

Segmentation du réseau

9.1.1.1 Pourquoi créer des sous-réseaux ?

Dans les premiers réseaux, il était courant que tous les ordinateurs et autres périphériques réseau d'une entreprise soient connectés à un seul et même réseau IP. Tous les périphériques de l'entreprise recevaient une adresse IP avec un ID de réseau correspondant. Ce type de configuration est appelé « réseau plat ». Dans un réseau de petite taille où le nombre de périphériques est limité, ce type de configuration peut convenir. En revanche, dès que le réseau s'étend, des problèmes majeurs peuvent apparaître.

Pensez à la façon dont les périphériques utilisent les diffusions pour localiser les services et les périphériques nécessaires sur un réseau local Ethernet. Souvenez-vous qu'une diffusion est envoyée à tous les hôtes sur un réseau IP. Le protocole DHCP (Dynamic Host Configuration Protocol) est un exemple de service réseau dépendant des diffusions. Les périphériques envoient les diffusions sur l'ensemble du réseau pour localiser le serveur DHCP. Sur un réseau de grande taille, cela peut créer un trafic important susceptible de ralentir les opérations réseau. De plus, étant donné que la diffusion est adressée à tous les périphériques, ceux-ci doivent tous accepter et gérer le trafic, ce qui augmente les besoins de traitement des périphériques. Si un périphérique doit traiter une quantité importante de diffusions, il peut

même ralentir ses opérations. De ce fait, les réseaux de plus grande envergure doivent être segmentés en sous-réseaux plus petits qui permettent la localisation de périphériques et de services dans de plus petits groupes.

Les petits espaces réseau obtenus lors de la segmentation du réseau sont appelés sous-réseaux. En anglais, on les appelle des « subnets ». Les administrateurs réseau ont la possibilité de regrouper les périphériques et les services dans des sous-réseaux définis par l'emplacement géographique (3e étage d'un bâtiment, par exemple), par division de l'entreprise (service des ventes, par exemple), par type de périphérique (imprimantes, serveurs, réseau étendu) ou par tout type de critère logique pour le réseau. La segmentation en sous-réseaux peut réduire le trafic global et améliorer les performances réseau.

Remarque : un sous-réseau est un réseau et ces termes peuvent être utilisés de manière interchangeable. La plupart des réseaux sont des sous-réseaux d'un bloc d'adresses plus grand.

9.1.1.2 Communication entre les sous-réseaux

Le routeur est indispensable à la communication des périphériques de différents réseaux. Les périphériques réseau utilisent l'interface du routeur reliée à leur réseau local comme passerelle par défaut. Le trafic destiné à un périphérique sur un réseau distant est traité par le routeur et transmis à sa destination. Pour déterminer si le trafic est local ou distant, le routeur utilise le masque de sous-réseau.

Dans un espace réseau comportant des sous-réseaux, le fonctionnement est exactement le même. Comme l'illustre la figure, la segmentation en sous-réseaux crée plusieurs réseaux logiques à partir d'un seul bloc d'adresses ou d'une adresse réseau. Chaque sous-réseau est traité comme un espace réseau distinct. Les périphériques d'un même sous-réseau doivent utiliser une adresse, un masque de sous-réseau et une passerelle par défaut qui correspondent au sous-réseau auquel ils appartiennent.

Le trafic ne peut pas être transféré entre les sous-réseaux sans l'intervention d'un routeur. Chaque interface du routeur doit disposer d'une adresse d'hôte IPv4 qui appartient au réseau ou au sous-réseau auquel elle est connectée.

La segmentation en sous-réseaux IP est fondamentale

9.1.2.1 Le plan

Comme l'illustre la figure, la planification des sous-réseaux nécessite d'étudier les besoins de l'entreprise en termes d'utilisation du réseau et la structure appropriée des sous-réseaux. L'étude des besoins réseau constitue le point de départ. Cela revient à examiner l'ensemble du réseau et à déterminer les principales divisions du réseau et leur segmentation. Pour dresser le plan d'adressage, il convient de définir les besoins de chaque sous-réseau concernant les critères suivants : taille, nombre d'hôtes par sous-réseau, méthode d'attribution des adresses d'hôte, hôtes nécessitant des adresses IP statiques et hôtes pouvant utiliser le protocole DHCP pour obtenir leurs informations d'adressage.

La taille du sous-réseau nécessite de prévoir le nombre d'hôtes qui auront besoin d'adresses d'hôte IP dans chaque sous-réseau du réseau privé subdivisé. Par exemple, dans une conception de réseau de campus, vous pouvez déterminer combien d'hôtes seront nécessaires sur les réseaux locaux de l'administration, de la faculté et des étudiants. Dans un réseau domestique, vous pouvez définir combien d'hôtes existent sur le réseau domestique local et combien appartiennent au réseau local du bureau à domicile.

Comme indiqué précédemment, le choix de la plage d'adresses IP privées utilisée sur un réseau local appartient à l'administrateur réseau et doit être établi avec soin pour garantir que suffisamment d'adresses d'hôte seront disponibles à la fois pour les hôtes actuellement connus et pour les extensions futures. Souvenez-vous que les plages d'adresses IP privées sont les suivantes :

- 10.0.0.0 avec le masque de sous-réseau 255.0.0.0
- 172.16.0.0 avec le masque de sous-réseau 255.240.0.0
- 192.168.0.0 avec le masque de sous-réseau 255.255.0.0

Le nombre d'adresses IP requises déterminera la ou les plages d'adresses d'hôte à utiliser. La segmentation en sous-réseaux de l'espace d'adresses IP privées sélectionné vous fournira les adresses d'hôte permettant de répondre aux besoins de votre réseau.

Les adresses publiques utilisées pour se connecter à Internet sont généralement attribuées par un fournisseur d'accès. Par conséquent, même si les mêmes principes de segmentation s'appliquent, cette opération n'est généralement pas la responsabilité de l'administrateur réseau de l'entreprise

9.1.2.2 Le plan - L'attribution des adresses

Créez des règles d'attribution des adresses IP dans chaque plage de sous-réseaux. Par exemple :

- Les imprimantes et les serveurs sont associés à des adresses IP statiques
- Les utilisateurs obtiennent des adresses IP de la part des serveurs DHCP à l'aide de sous-réseaux /24
- Les routeurs obtiennent les premières adresses d'hôte disponibles dans la plage

Deux facteurs très importants qui détermineront le choix du bloc d'adresses privées sont le nombre de sous-réseaux nécessaires et le nombre maximal d'hôtes requis par sous-réseau. Chacun de ces blocs d'adresses vous permettra d'attribuer correctement les adresses aux hôtes en fonction de la taille donnée du réseau et des hôtes nécessaires à l'heure actuelle et dans un avenir proche. Les besoins en termes d'espace IP détermineront la ou les plages d'hôtes à utiliser.

Dans les exemples qui suivent, la segmentation repose sur des blocs d'adresses dont les masques de sous-réseau sont 255.0.0.0, 255.255.0.0 et 255.255.255.0.

9.1.3.1 Notions de base sur les sous-réseaux

Chaque adresse réseau dispose d'une plage valide d'adresses d'hôte. Tous les équipements reliés au même réseau disposeront d'une adresse IPv4 d'hôte de ce réseau et d'un masque de sous-réseau ou d'un préfixe de réseau commun.

Le préfixe et le masque de sous-réseau constituent des moyens distincts de représenter la même chose : la partie réseau d'une adresse.

Pour créer des sous-réseaux IPv4, on utilise un ou plusieurs bits d'hôte en tant que bits réseau. Pour cela, il convient de développer le masque pour emprunter quelques bits de la partie hôte de l'adresse et créer d'autres bits réseau. Plus les bits d'hôte empruntés sont nombreux, plus le nombre de sous-réseaux qui peuvent être définis est important. Pour chaque bit emprunté, il faut doubler le nombre de sous-réseaux disponibles. Par exemple, si vous empruntez 1 bit, vous pouvez créer 2 sous-réseaux. Si vous empruntez 2 bits, 4 sous-réseaux sont créés, si vous empruntez 3 bits, 8 sous-réseaux sont créés et ainsi de suite. Toutefois, pour chaque bit emprunté, le nombre d'adresses disponibles par sous-réseau décroît.

Les bits peuvent être empruntés uniquement dans la partie hôte de l'adresse. La partie réseau de l'adresse est attribuée par le fournisseur d'accès et ne peut pas être modifiée.

Remarque : dans les exemples présentés sur les figures, seul le dernier octet est indiqué en binaire, car seuls les bits de la partie hôte peuvent être empruntés.

Comme l'illustre la Figure 1, le réseau 192.168.1.0/24 comporte 24 bits dans la partie réseau et 8 bits dans la partie hôte, ce qui est indiqué par le masque de sous-réseau 255.255.255.0 ou la notation /24. Sans segmentation, ce réseau prend en charge une seule interface de réseau local. Si un réseau local supplémentaire est nécessaire, le réseau doit être segmenté en sous-réseaux.

Sur la Figure 2, 1 bit est emprunté au bit le plus important (bit le plus à gauche) de la partie hôte, ce qui fait passer la partie réseau à 25 bits. Deux sous-réseaux sont ainsi créés. Ils sont identifiés à l'aide d'un 0 dans le bit emprunté pour le premier réseau et d'un 1 dans le bit emprunté pour le second réseau. Le masque de sous-réseau des deux réseaux utilise un 1 à la position du bit emprunté pour indiquer que ce bit se trouve désormais dans la partie réseau.

Comme l'illustre la Figure 3, lorsque l'on convertit l'octet binaire en décimal, on constate que la première adresse de sous-réseau est 192.168.1.0 et la deuxième adresse de sous-réseau est 192.168.1.128. Étant donné qu'un bit a été emprunté, le masque de sous-réseau de chaque sous-réseau est 255.255.255.128 ou /25

9.1.3.2 Les sous-réseaux dans la pratique

Dans l'exemple précédent, le réseau 192.168.1.0/24 a été segmenté en deux sous-réseaux :

192.168.1.0/25

192.168.1.128/25

Sur la Figure 1, observez que deux segments de réseau local sont reliés aux interfaces GigabitEthernet du routeur R1. Les sous-réseaux seront utilisés pour les segments reliés à ces interfaces. Pour qu'elles puissent servir de passerelle pour les périphériques du réseau local, chacune des interfaces du routeur doit obtenir une adresse IP appartenant à la plage d'adresses valides du sous-réseau attribué. Il est courant d'attribuer la première ou la dernière adresse disponible d'une plage réseau à l'interface du routeur.

Le premier sous-réseau, 192.168.1.0/25, est utilisé pour le réseau connecté à l'interface GigabitEthernet 0/0 et le second sous-réseau, 192.168.1.128/25, est utilisé pour le réseau connecté à l'interface GigabitEthernet 0/1. Avant d'attribuer une adresse IP à chacune de ces interfaces, il est nécessaire de déterminer la plage d'adresses IP valides pour chaque sous-réseau.

Voici quelques recommandations à appliquer à chacun des sous-réseaux :

- **Adresse réseau** : tous les bits 0 de la partie hôte de l'adresse.
- **Première adresse d'hôte** : tous les bits 0 et le bit 1 le plus à droite de la partie hôte de l'adresse.
- **Dernière adresse d'hôte** : tous les bits 1 et le bit 0 le plus à droite de la partie hôte de l'adresse.
- **Adresse de diffusion** : tous les bits 1 de la partie hôte de l'adresse.

Comme l'illustre la Figure 2, la première adresse d'hôte du réseau 192.168.1.0/25 est 192.168.1.1 et la dernière adresse d'hôte est 192.168.1.126. La Figure 3 montre que la première adresse d'hôte du réseau 192.168.1.128/25 est 192.168.1.129 et que la dernière adresse d'hôte est 192.168.1.254.

Pour attribuer la première adresse d'hôte de chaque sous-réseau à l'interface du routeur correspondante, exécutez la commande **ip address** en mode de configuration d'interface, comme illustré à la Figure 4. Notez que chaque sous-réseau utilise le masque de sous-réseau 255.255.255.128 pour indiquer que la partie réseau de l'adresse est 25 bits.

La configuration d'un hôte du réseau 192.168.1.128/25 est représentée à la Figure 5. Notez que l'adresse IP de la passerelle est l'adresse configurée sur l'interface G0/1 de R1, 192.168.1.129, et que le masque de sous-réseau est 255.255.255.128.

9.1.3.3 Les formules de calcul des sous-réseaux

Calculer les sous-réseaux

Utilisez la formule suivante pour calculer le nombre de sous-réseaux :

2^n (où n = le nombre de bits empruntés)

Comme l'illustre la Figure 1, pour l'exemple de 192.168.1.0/25, le calcul est le suivant :

2^1 = 2 sous-réseaux

Calculer les hôtes

Utilisez la formule suivante pour calculer le nombre d'hôtes par sous-réseau :

2^n (où n = le nombre de bits restants dans le champ d'hôte)

Comme l'illustre la Figure 2, pour l'exemple de 192.168.1.0/25, le calcul est le suivant :

2^7 = 128

Étant donné que les hôtes ne peuvent pas utiliser l'adresse réseau ni l'adresse de diffusion d'un sous-réseau, 2 de ces adresses ne peuvent pas être attribuées à des hôtes. Cela signifie que chaque sous-réseau dispose de 126 adresses d'hôte valides (128 - 2).

Donc, dans cet exemple, l'emprunt de 1 bit d'hôte du réseau permet la création de 2 sous-réseaux dont chacun peut prendre en charge un total de 126 hôtes.

9.1.3.4 Créer 4 sous-réseaux

Prenons l'exemple d'un interréseau nécessitant trois sous-réseaux.

Si on utilise le même bloc d'adresses, 192.168.1.0/24, des bits d'hôte doivent être empruntés pour créer au moins 3 sous-réseaux. En empruntant un seul bit, nous obtiendrions seulement deux sous-réseaux. Pour obtenir davantage de sous-réseaux, il faut emprunter plus de bits d'hôte. Calculez le nombre de sous-réseaux créés lorsque l'on emprunte 2 bits. Pour cela, utilisez la formule 2^nombre de bits empruntés :

2^2 = 4 sous-réseaux

L'emprunt de 2 bits crée 4 sous-réseaux, comme illustré à la Figure 1.

Souvenez-vous que le masque de sous-réseau doit être modifié en fonction des bits empruntés. Dans cet exemple, lorsque 2 bits sont empruntés, le dernier octet du masque

compte 2 bits de plus. En notation décimale, le masque est représenté sous la forme 255.255.255.192, car le dernier octet correspond à 1100 0000 au format binaire.

Calcul du nombre d'hôtes

Pour calculer le nombre d'hôtes, observez le dernier octet. Après l'emprunt de 2 bits pour le sous-réseau, il reste 6 bits d'hôte.

Appliquez la formule de calcul du nombre d'hôtes comme illustré à la Figure 2.

2^6 = 64

Toutefois, n'oubliez pas que tous les bits 0 de la partie hôte de l'adresse correspondent à l'adresse réseau, et que tous les 1 de la partie hôte correspondent à une adresse de diffusion. Par conséquent, il n'y a que 62 adresses d'hôte réellement disponibles pour chaque sous-réseau.

Comme l'illustre la Figure 3, la première adresse d'hôte du premier sous-réseau est 192.168.1.1 et la dernière adresse d'hôte est 192.168.1.62. La Figure 4 indique les plages des sous-réseaux 0 - 2. N'oubliez pas que chaque hôte doit disposer d'une adresse IP valide appartenant à la plage définie pour ce segment du réseau. Le sous-réseau attribué à l'interface du routeur détermine le segment auquel un hôte appartient.

La Figure 5 présente un exemple de configuration. Dans cette configuration, le premier réseau est attribué à l'interface GigabitEthernet 0/0, le second réseau est attribué à l'interface GigabitEthernet 0/1 et le troisième est attribué au réseau Série 0/0/0.

Si l'on utilise le même plan d'adressage, la première adresse d'hôte du sous-réseau est à nouveau attribuée à l'interface du routeur. Les hôtes de chaque sous-réseau utilisent l'adresse de l'interface du routeur comme adresse de passerelle par défaut.

- PC1 (192.168.1.2/26) utilise 192.168.1.1 (adresse de l'interface G0/0 de R1) comme adresse de passerelle par défaut
- PC2 (192.168.1.66/26) utilise 192.168.1.65 (adresse de l'interface G0/1 de R1) comme adresse de passerelle par défaut

Remarque : tous les périphériques du même sous-réseau seront associés à une adresse IPv4 d'hôte de la plage d'adresses d'hôte et utiliseront le même masque de sous-réseau.

9.1.3.5 Créer 8 sous-réseaux

À présent, prenons l'exemple d'un interréseau qui nécessite cinq sous-réseaux, comme illustré à la Figure 1.

Si on utilise le même bloc d'adresses, 192.168.1.0/24, des bits d'hôte doivent être empruntés pour créer au moins 5 sous-réseaux. En empruntant 2 bits, nous obtiendrions seulement 4 sous-réseaux, comme nous l'avons vu dans l'exemple précédent. Pour obtenir davantage de

sous-réseaux, il faut emprunter plus de bits d'hôte. Calculez le nombre de sous-réseaux créés si 3 bits sont empruntés. Utilisez pour cela la formule suivante :

2^3 = 8 sous-réseaux

Comme le montrent les Figures 2 et 3, en empruntant 3 bits, on obtient 8 sous-réseaux. Lorsque 3 bits sont empruntés, le dernier octet du masque de sous-réseau compte 3 bits de plus (/27). On obtient donc le masque de sous-réseau 255.255.255.224. Tous les périphériques sur ces sous-réseaux utiliseront le masque de sous-réseau 255.255.255.224 (/27).

Calcul du nombre d'hôtes

Pour calculer le nombre d'hôtes, observez le dernier octet. Après l'emprunt de 3 bits pour le sous-réseau, il reste 5 bits d'hôte.

Appliquez la formule pour calculer le nombre d'hôtes :

2^5 = 32, mais vous devez retirez 2 pour tous les 0 de la partie hôte de l'adresse réseau et tous les 1 de la partie hôte de l'adresse de diffusion.

Les sous-réseaux sont attribués aux segments réseau requis pour la topologie présentée à la Figure 4.

Si on utilise le même plan d'adressage, la première adresse d'hôte du sous-réseau est à nouveau attribuée à l'interface du routeur, comme le montre la Figure 5. Les hôtes de chaque sous-réseau utilisent l'adresse de l'interface du routeur comme adresse de passerelle par défaut.

- PC1 (192.168.1.2/27) utilise l'adresse 192.168.1.1 comme adresse de passerelle par défaut.
- PC2 (192.168.1.34/27) utilise l'adresse 192.168.1.33 comme adresse de passerelle par défaut.
- PC3 (192.168.1.98/27) utilise l'adresse 192.168.1.97 comme adresse de passerelle par défaut.
- PC4 (192.168.1.130/27) utilise l'adresse 192.168.1.129 comme adresse de passerelle par défaut.

9.1.3.10 Créer 100 sous-réseaux avec le préfixe /16

Dans les exemples précédents, nous avions un interréseau nécessitant 3 sous-réseaux et un autre nécessitant 5 sous-réseaux. Pour parvenir à créer quatre sous-réseaux, nous avons emprunté 2 bits parmi les 8 bits d'hôte disponibles avec une adresse IP dont le masque par défaut était 255.255.255.0 ou le préfixe /24. Le masque de sous-réseau obtenu était 255.255.255.192 et un total de 4 sous-réseaux possibles ont été créés. En appliquant la

formule de calcul du nombre d'hôtes de 2^6 - 2, nous avons déterminé que chacun des 4 sous-réseaux disposait de 62 adresses d'hôte maximum à attribuer aux nœuds.

Pour obtenir 5 sous-réseaux, nous avons emprunté 3 bits parmi les 8 bits d'hôte disponibles avec une adresse IP dont le masque par défaut était 255.255.255.0 ou le préfixe /24. Après avoir emprunté ces 3 bits à la partie hôte de l'adresse, il restait 5 bits d'hôte. Le masque de sous-réseau obtenu était 255.255.255.224, avec un total de 8 sous-réseaux créés et 30 adresses d'hôte par sous-réseau.

Prenons à présent l'exemple de grandes entreprises ou de campus dont l'interréseau requiert 100 sous-réseaux. Tout comme dans les exemples précédents, pour parvenir à créer 100 sous-réseaux, nous devons emprunter des bits à la partie hôte de l'adresse IP de l'interréseau existant. Comme précédemment, pour calculer le nombre de sous-réseaux, nous devons déterminer le nombre de bits d'hôte disponibles et utiliser la formule de calcul suivante des sous-réseaux : 2^nombre de bits empruntés moins 2. Si l'on reprend l'adresse IP du dernier exemple, soit 192.168.10.0/24, nous disposons de 8 bits d'hôte. Pour créer 100 sous-réseaux, nous devons donc emprunter 7 bits.

Calcul du nombre de sous-réseaux si 7 bits sont empruntés : 2^7 = 128 sous-réseaux.

Cependant, si l'on emprunte 7 bits, il ne reste qu'un seul bit d'hôte et si l'on applique la formule de calcul du nombre d'hôtes, on n'obtient aucun hôte sur ces sous-réseaux. Calcul du nombre d'hôtes s'il reste un bit : 2^1 = 2, on retire 2 pour l'adresse réseau et la diffusion réseau et l'on obtient un résultat de 0 hôte (2^1 - 2 = 0).

Dans une situation nécessitant un plus grand nombre de sous-réseaux, le réseau IP doit disposer de davantage de bits d'hôte à emprunter, par exemple une adresse IP dont le masque de sous-réseau par défaut est /16 ou 255.255.0.0. Les adresses dont le premier octet dispose d'une plage de 128 à 191 adresses ont un masque par défaut de 255.255.0.0 ou /16. Les adresses de cette plage possèdent 16 bits dans la partie réseau et 16 bits dans la partie hôte. Ces 16 bits représentent les bits qui peuvent être empruntés pour créer des sous-réseaux.

Si l'on utilise un nouveau bloc d'adresses IP, 172.16.0.0/16, des bits d'hôte doivent être empruntés pour créer au moins 100 sous-réseaux. Nous allons procéder de la gauche vers la droite à partir du premier bit d'hôte disponible et emprunter un seul bit à la fois jusqu'à obtenir le nombre de bits nécessaires pour créer 100 sous-réseaux. L'emprunt de 1 bit permet de créer 2 sous-réseaux, l'emprunt de 2 bits permet de créer 4 sous-réseaux, avec 3 bits l'on obtient 8 sous-réseaux et ainsi de suite. Calculez le nombre de sous-réseaux créés lorsque l'on emprunte 7 bits. Pour cela, utilisez la formule 2^nombre de bits empruntés :

2^7 = 128 sous-réseaux

En empruntant 7 bits, on obtient 128 sous-réseaux, comme montré sur la figure.

Souvenez-vous que le masque de sous-réseau doit être modifié en fonction des bits empruntés. Dans cet exemple, lorsque 7 bits sont empruntés, le troisième octet du masque compte 7 bits de plus. En notation décimale, le masque est représenté par 255.255.254.0 ou le préfixe /23, car le troisième octet est 11111110 au format binaire et le quatrième octet est 00000000 en binaire. La segmentation en sous-réseaux a lieu dans le troisième octet, avec les bits d'hôte dans les troisième et quatrième octets.

9.1.3.11 Calculer le nombre d'hôtes

Calcul du nombre d'hôtes

Pour calculer le nombre d'hôtes, observez le troisième et le quatrième octet. Après avoir emprunté 7 bits pour le sous-réseau, il reste un bit d'hôte dans le troisième octet et 8 bits d'hôte dans le quatrième octet.

Appliquez la formule de calcul du nombre d'hôtes comme illustré à la Figure 1.

2^9 = 512

Toutefois, n'oubliez pas que tous les bits 0 de la partie hôte de l'adresse correspondent à l'adresse réseau, et que tous les 1 de la partie hôte correspondent à une adresse de diffusion. Par conséquent, il n'y a que 510 adresses d'hôte réellement disponibles pour chaque sous-réseau.

Comme l'illustre la Figure 2, la première adresse d'hôte du premier sous-réseau est 172.16.0.1 et la dernière adresse d'hôte est 172.16.1.254. N'oubliez pas que chaque hôte doit disposer d'une adresse IP valide appartenant à la plage définie pour ce segment du réseau. Le sous-réseau attribué à l'interface du routeur détermine le segment auquel un hôte appartient.

Rappel :

Les bits peuvent être empruntés uniquement dans la partie hôte de l'adresse. La partie réseau de l'adresse est attribuée par le fournisseur d'accès et ne peut pas être modifiée. Par conséquent, les entreprises qui avaient besoin d'un grand nombre de sous-réseaux devaient en faire part à leur FAI afin qu'il leur attribue un bloc d'adresses IP dont le masque par défaut comportait suffisamment de bits pour créer les sous-réseaux nécessaires.

9.1.3.12 Calculer le nombre d'hôtes

Certaines entreprises, telles que les fournisseurs d'accès de petite envergure, peuvent même avoir besoin de plus de 100 sous-réseaux. Prenons par exemple une entreprise qui a besoin de 1 000 sous-réseaux. Comme toujours, pour créer des sous-réseaux, nous devons emprunter des bits à la partie hôte de l'adresse IP de l'interréseau existant. Comme précédemment, pour calculer le nombre de sous-réseaux, il faut déterminer le nombre de bits d'hôte disponibles. Dans notre situation, l'adresse IP attribuée par le FAI doit comporter suffisamment de bits d'hôte disponibles pour obtenir 1 000 sous-réseaux. Les adresses IP dont le premier octet propose la plage 1 à 126 ont le masque par défaut 255.0.0.0 ou /8. Cela signifie qu'il y a 8 bits dans la partie réseau et 24 bits d'hôte qui peuvent être empruntés pour créer des sous-réseaux.

Avec le bloc d'adresses 10.0.0.0/8, des bits d'hôte doivent être empruntés pour créer au moins 1 000 sous-réseaux. Nous allons procéder de la gauche vers la droite à partir du premier bit d'hôte disponible et emprunter un seul bit à la fois jusqu'à obtenir le nombre de bits nécessaires pour créer 1 000 sous-réseaux. Calculez le nombre de sous-réseaux créés lorsque l'on emprunte 10 bits. Pour cela, utilisez la formule 2^nombre de bits empruntés :

2^10 = 1024 sous-réseaux

L'emprunt de 10 bits crée 1 024 sous-réseaux, comme illustré à la Figure 1.

Souvenez-vous que le masque de sous-réseau doit être modifié en fonction des bits empruntés. Dans cet exemple, lorsque 10 bits sont empruntés, le troisième octet du masque compte 10 bits de plus. En notation décimale, le masque est représenté par 255.255.192.0 ou le préfixe /18, car le troisième octet du masque de sous-réseau est 11000000 au format binaire et le quatrième octet est 00000000 en binaire. La segmentation en sous-réseaux a lieu dans le troisième octet, mais n'oubliez pas que les bits d'hôte se trouvent dans les troisième et quatrième octets.

Calcul du nombre d'hôtes

Pour calculer le nombre d'hôtes, observez le troisième et le quatrième octet. Après avoir emprunté 10 bits pour le sous-réseau, il reste 6 bits d'hôte dans le troisième octet et 8 bits d'hôte dans le quatrième octet. Il reste donc un total de 14 bits d'hôte.

Appliquez la formule de calcul du nombre d'hôtes comme illustré à la Figure 2.

2^14 - 2 = 16382

La première adresse d'hôte du premier sous-réseau est 10.0.0.1 et la dernière adresse d'hôte est 10.0.63.254. N'oubliez pas que chaque hôte doit disposer d'une adresse IP valide appartenant à la plage définie pour ce segment du réseau. Le sous-réseau attribué à l'interface du routeur détermine le segment auquel un hôte appartient.

Remarque : tous les périphériques du même sous-réseau seront associés à une adresse IPv4 d'hôte de la plage d'adresses d'hôte et utiliseront le même masque de sous-réseau.

Déterminer le masque de sous-réseau

9.1.4.1 Segmenter le réseau en sous-réseaux en fonction des besoins des hôtes

Le choix du nombre de bits d'hôte à emprunter pour créer des sous-réseaux constitue une décision de planification importante. Deux critères doivent être pris en compte lors de la planification des sous-réseaux : le nombre d'adresses d'hôte requises sur chaque réseau et le nombre de sous-réseaux nécessaires. L'animation montre les sous-réseaux possibles pour le réseau 192.168.1.0. Le choix du nombre de bits pour l'ID de sous-réseau affecte à la fois le nombre de sous-réseaux possibles et le nombre d'adresses d'hôte que chaque sous-réseau peut contenir.

Observez la relation inverse entre le nombre de sous-réseaux et le nombre d'hôtes. Plus les bits empruntés pour créer des sous-réseaux sont nombreux, moins il y a de bits d'hôte disponibles et donc moins il y a d'hôtes par sous-réseau. Si le réseau requiert davantage d'adresses d'hôte, plus de bits d'hôte sont nécessaires, ce qui réduit le nombre de sous-réseaux.

Nombre d'hôtes

Lorsque vous empruntez des bits pour créer plusieurs sous-réseaux, vous devez laisser suffisamment de bits d'hôte pour le plus grand sous-réseau. Le nombre d'adresses d'hôte nécessaires dans le plus grand sous-réseau déterminera le nombre de bits qui doivent rester dans la partie hôte. La formule 2^n (où n est le nombre de bits d'hôte restant) permet de calculer le nombre d'adresses disponibles sur chaque sous-réseau. Souvenez-vous que 2 de ces adresses ne peuvent pas être utilisées. Le nombre d'adresses disponibles correspond donc à 2^n - 2

9.1.4.2 Segmenter le réseau en fonction de ses besoins

Parfois, c'est le nombre de sous-réseaux qui est plus important que le nombre d'adresses d'hôte par sous-réseau. Cela peut être le cas lorsqu'une entreprise décide de séparer le trafic réseau en fonction d'une structure interne ou de ses différents services. Par exemple, une entreprise peut choisir de placer tous les périphériques hôtes utilisés par les employés du service ingénierie sur un réseau et tous les périphériques hôtes utilisés par la direction sur un réseau distinct. Dans ce cas, c'est principalement le nombre de sous-réseaux requis qui détermine le nombre de bits à emprunter.

Souvenez-vous que le nombre de sous-réseaux créés lorsque des bits sont empruntés peut être calculé en utilisant la formule 2^n (où n est le nombre de bits empruntés). Il n'est pas nécessaire de soustraire des sous-réseaux créés puisqu'ils sont tous utilisables.

L'essentiel est d'équilibrer le nombre de sous-réseaux nécessaires et le nombre d'hôtes requis par le plus grand sous-réseau. Plus le nombre de bits empruntés pour créer des sous-réseaux est élevé, moins il y a d'hôtes disponibles par sous-réseau.

9.1.4.3 Segmenter le réseau pour répondre à ses besoins

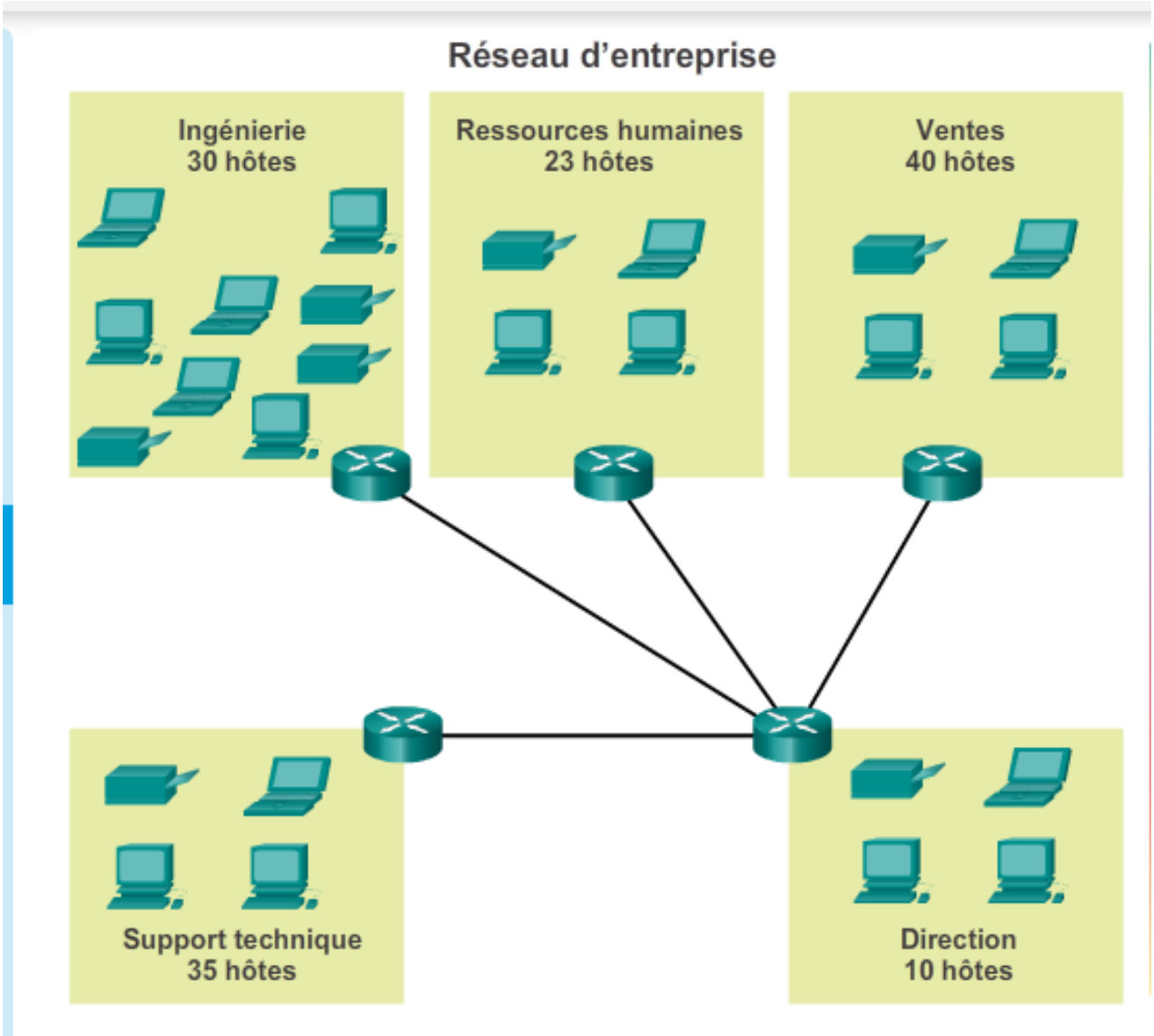
Dans les entreprises, chaque réseau est conçu pour accueillir un nombre limité d'hôtes. La segmentation en sous-réseaux de base consiste à créer suffisamment de sous-réseaux pour répondre aux besoins du réseau tout en fournissant suffisamment d'adresses d'hôte par sous-réseau.

Certains réseaux, tels que les liaisons de réseau étendu point à point, ne requièrent que deux hôtes. D'autres, comme le réseau local d'un grand bâtiment ou d'un service important, doivent accueillir des centaines d'hôtes. Les administrateurs réseau doivent développer un schéma d'adressage interréseau de façon à pouvoir accueillir le nombre maximal d'hôtes pour chaque réseau. Le nombre d'hôtes dans chaque division du réseau doit permettre un nombre plus important d'hôtes.

Déterminez le nombre total d'hôtes

Calculez d'abord le nombre total d'hôtes dont a besoin l'interréseau entier de l'entreprise. Vous devez utiliser un bloc d'adresses suffisamment grand pour accueillir tous les périphériques de tous les réseaux de l'entreprise. Ces périphériques sont notamment des périphériques d'utilisateurs, des serveurs, des périphériques intermédiaires et des interfaces de routeur.

Prenons l'exemple d'un interréseau d'entreprise qui doit accueillir 123 hôtes en tout sur ses cinq sites (voir Figure 1). Dans cet exemple, le fournisseur de services a attribué l'adresse réseau 172.20.0.0/21 (11 bits d'hôte). Comme l'indique la Figure 2, celle-ci permet d'obtenir 2 046 adresses d'hôte, ce qui dépasse les besoins d'adressage de cet interréseau.



Déterminez le nombre et la taille des réseaux

Ensuite, établissez le nombre de sous-réseaux requis et le nombre d'adresses d'hôte nécessaires sur chaque sous-réseau. D'après la topologie du réseau qui se compose de 5 segments de réseau local et de 4 connexions interréseau entre les routeurs, 9 sous-réseaux sont nécessaires. Le plus grand sous-réseau requiert 40 hôtes. Lors de la conception d'un schéma d'adressage, vous devez prévoir l'augmentation du nombre de sous-réseaux et du nombre d'hôtes par sous-réseau.

L'adresse réseau 172.16.0.0/22 comporte 10 bits d'hôte. Le plus grand sous-réseau nécessite 40 hôtes, aussi il faut au moins 6 bits d'hôte pour fournir l'adressage de 40 hôtes. Ce chiffre découle de la formule suivante : 2^6 - 2 = 62 hôtes. Les 4 premiers bits d'hôte peuvent être utilisés pour attribuer les sous-réseaux. En appliquant la formule de calcul du nombre de sous-réseaux, on obtient 16 sous-réseaux : 2^4 = 16. Comme l'interréseau en exemple requiert 9 sous-réseaux, cela répond à la demande et permet une certaine évolution.

Lorsque 4 bits sont empruntés, la nouvelle longueur de préfixe est /26 avec le masque de sous-réseau 255.255.255.192.

Comme le montre la Figure 1, la longueur de préfixe /26 permet de déterminer les 16 adresses de sous-réseau. Seule la partie sous-réseau de l'adresse est incrémentée. Les 22 bits initiaux de l'adresse réseau ne peuvent pas être modifiés et la partie hôte contient tous les bits 0.

Remarque : étant donné que la partie sous-réseau appartient à la fois au troisième et au quatrième octets, une de ces valeurs ou les deux seront différentes dans les adresses de sous-réseau.

Comme l'illustre la Figure 2, le réseau 172.16.0.0/22 d'origine était un seul réseau comportant 10 bits d'hôte et 1 022 adresses à attribuer aux hôtes. En empruntant 4 bits d'hôte, on obtient 16 sous-réseaux (0000 à 1111). Chaque sous-réseau comporte 6 bits d'hôte ou 62 adresses d'hôtes utilisables par sous-réseau.

Comme l'illustre la Figure 3, les sous-réseaux peuvent être attribués aux segments de réseau local et aux connexions de routeur à routeur.

Les avantages du masquage de sous-réseau de longueur variable

9.1.5.1 La segmentation traditionnelle en sous-réseaux n'est pas efficace

Avec la méthode classique de segmentation en sous-réseaux, le même nombre d'adresses est attribué à chaque sous-réseau. Si tous les sous-réseaux ont besoin d'un même nombre d'hôtes, l'utilisation de blocs d'adresses de taille fixe est judicieuse. Mais, bien souvent, ce n'est pas le cas.

Par exemple, la topologie représentée à la Figure 1 nécessite sept sous-réseaux, un pour chacun des quatre réseaux locaux et un autre pour chacune des trois connexions de réseau étendu entre les routeurs. Si l'on utilise la méthode classique de segmentation en sous-réseaux pour l'adresse 192.168.20.0/24, 3 bits peuvent être empruntés au dernier octet de la partie hôte pour obtenir les sept sous-réseaux requis. Comme l'illustre la Figure 2, en empruntant 3 bits, on obtient 8 sous-réseaux et on laisse 5 bits d'hôte avec 30 hôtes utilisables par sous-réseau. Ce schéma permet de créer les sous-réseaux nécessaires et de répondre aux besoins en hôtes du plus grand réseau local.

Bien que cette méthode classique satisfasse aux besoins du plus grand réseau local et divise l'espace d'adressage en un nombre approprié de sous-réseaux, de nombreuses adresses sont inutilisées.

Par exemple, seules deux adresses sont nécessaires dans chaque sous-réseau des trois liaisons de réseau étendu. Puisque chaque sous-réseau possède 30 adresses utilisables, 28 adresses sont inutilisées dans chacun de ces sous-réseaux. Comme l'illustre la Figure 3, ce sont au total 84 adresses qui sont inutilisées (28 x 3).

De plus, ce schéma ne laisse aucune place à un développement futur, puisqu'il réduit le nombre total de sous-réseaux disponibles. Cette utilisation inefficace des adresses est typique de la méthode classique de segmentation des réseaux par classe.

L'application d'un schéma de segmentation classique à ce scénario n'est pas très efficace. En fait, notre exemple illustre parfaitement bien comment le découpage d'un sous-réseau peut être utilisé pour optimiser l'attribution d'adresses.

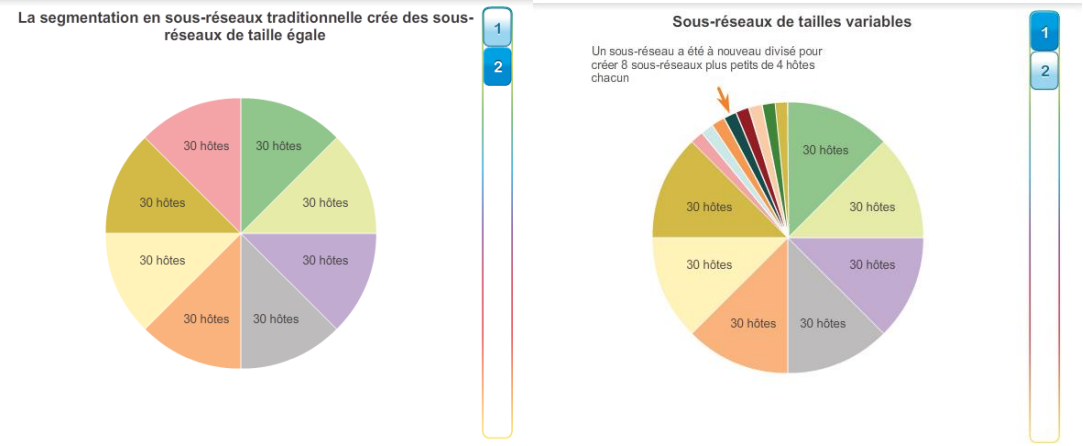
La segmentation des sous-réseaux, qui revient à utiliser le masquage de sous-réseau de longueur variable (VLSM) permet d'optimiser l'efficacité de l'adressage

9.1.5.2 Masquage de sous-réseau de longueur variable (VLSM)

Dans les exemples précédents de segmentation, vous constatez que le même masque de sous-réseau a été appliqué à tous les sous-réseaux. Cela signifie que chaque sous-réseau possède le même nombre d'adresses d'hôte disponibles.

Comme le montre la Figure 1, la méthode classique de segmentation crée des sous-réseaux de même taille. Chaque sous-réseau d'un schéma classique utilise le même masque de sous-réseau. Comme le montre la Figure 2, la méthode VLSM permet de diviser un espace réseau en parties inégales. Avec la méthode VLSM, le masque de sous-réseau varie selon le nombre de bits empruntés pour le sous-réseau, d'où la partie « variable » de cette méthode.

La création de sous-réseaux VLSM est similaire à la création de sous-réseaux classique car des bits sont empruntés pour créer des sous-réseaux. Les formules de calcul du nombre d'hôtes par sous-réseau et du nombre de sous-réseaux créés s'appliquent également. La différence réside dans le fait que la segmentation nécessite plus d'une opération. Avec le VLSM, le réseau est divisé en sous-réseaux qui sont eux-mêmes divisés en sous-réseaux. Ce processus peut être répété plusieurs fois de manière à créer des sous-réseaux de différentes tailles.



9.1.5.3 VLSM de base

Pour mieux comprendre le processus VLSM, revenez à l'exemple précédent.

Dans celui-ci (Figure 1), le réseau 192.168.20.0/24 a été divisé en huit sous-réseaux de taille égale et sept de ces sous-réseaux ont été attribués. Quatre sous-réseaux ont été utilisés pour les réseaux locaux et trois pour les connexions de réseau étendu entre les routeurs. Souvenez-vous que l'espace d'adressage inutilisé appartenait aux sous-réseaux des connexions de réseau étendu, car ces sous-réseaux nécessitaient seulement deux adresses utilisables : une pour chaque interface de routeur. La méthode VLSM peut être employée pour éviter cette perte. Elle permet de créer des sous-réseaux plus petits pour les connexions de réseau étendu.

Pour créer des sous-réseaux plus petits pour les liaisons de réseau étendu, l'un des sous-réseaux est divisé. Sur la Figure 2, le dernier sous-réseau, 192.168.20.224/27, est encore subdivisé.

Souvenez-vous que lorsque le nombre d'adresses d'hôte nécessaires est connu, la formule 2^n - 2 (où n représente le nombre de bits d'hôte restant) peut être appliquée. Pour obtenir deux adresses utilisables, 2 bits d'hôte doivent rester dans la partie hôte.

2^2 - 2 = 2

Étant donné que l'espace d'adresses 192.168.20.224/27 comporte 5 bits d'hôte, 3 bits peuvent être empruntés, ce qui laisse 2 bits dans la partie hôte.

Jusque-là, les calculs sont exactement les mêmes que pour la méthode classique. Il faut emprunter des bits et déterminer les plages des sous-réseaux.

Comme l'illustre la Figure 2, ce schéma de segmentation VLSM réduit le nombre d'adresses par sous-réseau jusqu'à la taille appropriée pour les réseaux étendus. Le fait de segmenter le sous-réseau 7 pour les réseaux étendus permet de conserver les sous-réseaux 4, 5, et 6 pour les futurs réseaux, mais également plusieurs autres sous-réseaux disponibles pour les réseaux étendus.

9.1.5.4 Le VLSM dans la pratique

Avec les sous-réseaux VLSM, les segments LAN et WAN peuvent être adressés sans perte inutile.

Les hôtes de chaque réseau local obtiennent une adresse d'hôte valide avec la plage de ce sous-réseau et le masque /27. L'interface de réseau local de chacun des quatre routeurs obtient un sous-réseau /27 et une ou plusieurs interfaces série obtiennent un sous-réseau /30.

Conformément au schéma d'adressage commun, la première adresse d'hôte IPv4 de chaque sous-réseau est attribuée à l'interface de réseau local du routeur. Les interfaces de réseau étendu des routeurs obtiennent les adresses IP et le masque des sous-réseaux /30.

Les Figures 1 à 4 présentent la configuration d'interface de chacun des routeurs.

Les hôtes de chaque sous-réseau obtiennent une adresse d'hôte IPv4 appartenant à la plage d'adresses d'hôte du sous-réseau et un masque approprié. Les hôtes utilisent l'adresse de l'interface de réseau local du routeur connecté comme adresse de passerelle par défaut.

- Les hôtes du bâtiment A (192.168.20.0/27) utilisent l'adresse 192.168.20.1 du routeur comme adresse de passerelle par défaut.

- Les hôtes du bâtiment B (192.168.20.32/27) utilisent l'adresse 192.168.20.33 du routeur comme adresse de passerelle par défaut.

- Les hôtes du bâtiment C (192.168.20.64/27) utilisent l'adresse 192.168.20.65 du routeur comme adresse de passerelle par défaut.

- Les hôtes du bâtiment D (192.168.20.96/27) utilisent l'adresse 192.168.20.97 du routeur comme adresse de passerelle par défaut.

9.1.5.5 Diagramme VLSM

Pour planifier des adresses, vous pouvez également faire appel à divers outils. Parmi ces derniers, le diagramme VLSM permet d'identifier les blocs d'adresses qui sont disponibles et ceux qui sont déjà attribués. Ce diagramme permet de ne pas attribuer des adresses déjà attribuées. Le tableau de VLSM peut être utilisé pour planifier l'attribution des adresses de l'exemple précédent.

Observation des sous-réseaux /27

Comme le montre la Figure 1, lorsque nous avons utilisé la méthode classique de segmentation, les sept premiers blocs d'adresses étaient attribués aux réseaux locaux et aux réseaux étendus. Souvenez-vous que ce schéma a entraîné la création de 8 sous-réseaux proposant chacun 30 adresses utilisables (/27). Même si ce schéma fonctionnait pour les segments de réseau local, de nombreuses adresses étaient gaspillées dans les segments de réseau étendu.

Lors de la conception du schéma d'adressage sur un nouveau réseau, les blocs d'adresses peuvent être attribués à l'aide d'une méthode qui réduit les pertes et maintient la contiguïté des blocs d'adresses inutilisées.

Attribution des blocs d'adresses VLSM

Comme l'illustre la Figure 2, afin d'utiliser plus efficacement l'espace d'adressage, des sous-réseaux /30 sont créés pour les liaisons de réseau étendu. Pour conserver ensemble les blocs d'adresses inutilisées, le dernier sous-réseau /27 a à nouveau été subdivisé pour créer des sous-réseaux /30. Les 3 premiers sous-réseaux ont été affectés aux liaisons de réseau étendu.

- Plage d'adresses d'hôte .224 /30 de 225 à 226 : liaison de réseau étendu entre R1 et R2
- Plage d'adresses d'hôte .228 /30 de 229 à 230 : liaison de réseau étendu entre R2 et R3
- Plage d'adresses d'hôte .232 /30 de 233 à 234 : liaison de réseau étendu entre R3 et R4
- Plage d'adresses d'hôte .236 /30 de 237 à 238 : disponible
- Plage d'adresses d'hôte .240 /30 de 241 à 242 : disponible
- Plage d'adresses d'hôte .244 /30 de 245 à 246 : disponible
- Plage d'adresses d'hôte .248 /30 de 249 à 250 : disponible
- Plage d'adresses d'hôte .252 /30 de 253 à 254 : disponible

Cette conception du schéma d'adressage laisse 3 sous-réseaux /27 et 5 sous-réseaux /30 inutilisés.

Schémas d'adressage

Conception structurée

9.2.1.1 Planification de l'adressage réseau

Comme l'illustre la figure, l'attribution d'un espace d'adressage de couche réseau dans le réseau d'entreprise doit être bien pensée. L'attribution d'adresses ne doit pas être laissée au hasard. Trois critères principaux sont à prendre en compte lors de la planification de l'attribution des adresses.

- **Éviter les doublons d'adresses :** chaque hôte d'un interréseau doit être associé à une adresse unique. Sans planification et documentation appropriées, une adresse pourrait être affectée à plusieurs hôtes, ce qui entraînerait des problèmes d'accès pour ces hôtes.
- **Assurer et contrôler l'accès :** certains hôtes, tels que les serveurs, fournissent des ressources aux hôtes internes ainsi qu'aux hôtes externes. L'adresse de couche 3 attribuée à un serveur

peut être utilisée pour contrôler l'accès à celui-ci. Si, toutefois, l'adresse est attribuée de manière aléatoire et n'est pas bien documentée, le contrôle d'accès devient plus difficile.

- **Surveiller la sécurité et les performances :** de même, la sécurité et les performances des hôtes du réseau et de l'ensemble du réseau doivent être surveillées. Dans le cadre de cette surveillance, le trafic réseau est examiné, à la recherche d'adresses qui génèrent ou reçoivent un nombre trop important de paquets. Lorsque l'adressage réseau est planifié et documenté correctement, les périphériques réseau posant problème peuvent facilement être identifiés.

Attribuer des adresses au sein d'un réseau

Dans un réseau, il existe quatre types différents de périphériques, notamment :

- Périphériques clients des utilisateurs finaux
- Serveurs et périphériques
- Hôtes accessibles depuis Internet
- Périphériques intermédiaires
- Passerelle

Lors du développement d'un schéma d'adressage IP, il est généralement recommandé de définir un modèle d'attribution des adresses à chaque type de périphérique. Cela apporte des avantages aux administrateurs pour l'ajout et la suppression des périphériques et le filtrage du trafic en fonction des adresses IP. En outre, la documentation devient plus simple.

9.2.1.2 Attribution d'adresses à des périphériques

Un plan d'adressage réseau peut impliquer l'utilisation d'une plage différente d'adresses dans chaque sous-réseau pour chaque type de périphérique.

Adresses des clients

En raison des difficultés associées à la gestion des adresses statiques, les périphériques des utilisateurs se voient souvent attribuer leur adresse de manière dynamique, à l'aide du protocole DHCP (Dynamic Host Configuration Protocol). Le protocole DHCP est généralement la méthode d'attribution d'adresses IP privilégiée pour les réseaux de grande taille, car le service d'assistance technique est dégagé de cette tâche et le risque d'erreur de saisie est quasiment éliminé.

Un autre avantage du protocole DHCP réside dans le fait qu'une adresse n'est pas attribuée définitivement à un hôte ; elle est seulement louée pour une période donnée. Par conséquent, si nous devons modifier le schéma de segmentation de notre réseau, nous n'avons pas besoin d'attribuer à nouveau toutes les adresses d'hôte de manière statique. Avec le protocole DHCP,

il suffit de configurer les informations du nouveau sous-réseau sur le serveur DHCP. Ensuite, les hôtes renouvellent automatiquement leurs adresses IP.

Adresses pour des serveurs et des périphériques

Toutes les ressources réseau, telles que les serveurs ou les imprimantes, doivent avoir une adresse IP statique, comme indiqué sur la figure. Les hôtes client accèdent à ces ressources au moyen des adresses IP de ces périphériques. Par conséquent, des adresses prévisibles sont nécessaires pour chacun de ces serveurs et périphériques.

Les serveurs et les périphériques forment un point de concentration pour le trafic réseau. De nombreux paquets sont envoyés aux adresses IPv4 de ces périphériques, mais également renvoyés par ces mêmes adresses. Lorsqu'il surveille le trafic réseau à l'aide d'un outil tel que Wireshark, l'administrateur réseau doit pouvoir identifier rapidement ces périphériques. La mise en œuvre d'un système de numérotation cohérent facilite cette identification.

Adresses pour les hôtes accessibles depuis Internet

Dans la plupart des interréseaux, seuls quelques périphériques sont accessibles par les hôtes depuis l'extérieur de l'entreprise. La majorité de ces périphériques sont de type serveur. À l'instar des périphériques d'un réseau qui fournissent des ressources réseau, les adresses IP de ces périphériques doivent être statiques.

Les serveurs accessibles depuis Internet doivent également être associés à une adresse publique. En outre, les changements d'adresse de l'un de ces périphériques le rendront inaccessible depuis Internet. Il arrive très souvent que ces périphériques appartiennent à un réseau numéroté à l'aide d'adresses privées. Cela implique que le routeur ou le pare-feu situé en périphérie du réseau doit être configuré de manière à traduire les adresses internes des serveurs en adresses publiques. En raison de cette configuration supplémentaire sur le périphérique intermédiaire, il est d'autant plus important que ces serveurs aient une adresse prévisible.

Adresses pour les périphériques intermédiaires

Les périphériques intermédiaires forment également un point de concentration pour le trafic réseau. La quasi-totalité du trafic à l'intérieur d'un réseau et entre les réseaux passe par des périphériques intermédiaires. Aussi, ces périphériques réseau fournissent-ils un emplacement propice à la gestion, à la surveillance et à la sécurité du réseau.

La plupart des périphériques intermédiaires se voient attribuer des adresses de couche 3, pour la gestion et/ou le fonctionnement des périphériques. Les périphériques de type concentrateur, commutateur et point d'accès sans fil ne nécessitent pas d'adresses IPv4 pour fonctionner en tant que périphériques intermédiaires. Toutefois, si nous devons accéder à ces périphériques en tant qu'hôtes pour configurer, surveiller ou dépanner le réseau, ils doivent être associés à des adresses.

Puisque nous devons savoir comment communiquer avec les périphériques intermédiaires, ils doivent avoir des adresses prévisibles. C'est la raison pour laquelle elles sont généralement attribuées manuellement. Par ailleurs, les adresses de ces périphériques doivent se trouver

dans une plage du bloc réseau différente de celle des adresses des périphériques des utilisateurs.

Adresse de la passerelle (routeurs et pare-feu)

Contrairement aux périphériques intermédiaires, les routeurs et les pare-feu possèdent une adresse IP attribuée à chaque interface. Chacune des interfaces se situe dans un réseau différent et sert de passerelle pour les hôtes de ce réseau. En règle générale, l'interface d'un routeur utilise l'adresse la plus grande ou la plus petite de la plage d'adresses du réseau. Cette attribution doit être uniforme pour l'ensemble des réseaux de l'entreprise. Ainsi, le personnel chargé du support réseau peut toujours déterminer la passerelle du réseau, quel que soit le réseau sur lequel il intervient.

Les interfaces des routeurs et des pare-feu forment un point de concentration du trafic pour l'entrée et la sortie du réseau. Dans la mesure où les hôtes de chaque réseau utilisent une interface de routeur et de pare-feu comme passerelle de sortie du réseau, de nombreux paquets traversent ces interfaces. Par conséquent, ces périphériques jouent un rôle majeur dans la sécurité des réseaux en filtrant les paquets sur base des adresses IP source et de destination. L'organisation des différents types de périphérique en groupes d'adressage logique optimise l'attribution des adresses et le filtrage des paquets.

Plages d'adresses IP

Réseau: 192.168.1.0/24

Utilisation	Premier	Dernier
Périphériques hôtes	.1	.229
Serveurs	.230	.239
Imprimantes	.240	.249
Périphériques intermédiaires	.250	.253
Passerelle (interface LAN du routeur)	.254	

9.3 Critères de conception à prendre en compte pour les réseaux IPv6

9.3.1 Segmentation en sous-réseaux d'un réseau IPv6

9.3.1.1 Segmenter le réseau en sous-réseaux à l'aide d'ID de sous-réseau

La segmentation en sous-réseaux IPv6 demande une approche différente de celle des sous-réseaux IPv4. En effet, l'approche IPv6 fait appel à tellement d'adresses que le motif de segmentation est tout autre. Un espace d'adressage IPv6 n'est pas segmenté en sous-réseaux pour conserver des adresses. En revanche, il est subdivisé pour prendre en charge la conception hiérarchique et logique du réseau. L'approche IPv4 consiste à gérer la pénurie d'adresses, mais la segmentation IPv6 consiste à créer une hiérarchie d'adressage en fonction du nombre de routeurs et de réseaux qu'ils prennent en charge.

Souvenez-vous qu'un bloc d'adresses IPv6 avec le préfixe /48 contient 16 bits pour l'ID de sous-réseau, comme le montre la Figure 1. La segmentation à l'aide de l'ID de sous-réseau à 16 bits peut générer jusqu'à 65 536 sous-réseaux /64 et ne nécessite pas d'emprunter de bits à l'ID d'interface ni à la partie hôte de l'adresse. Chaque sous-réseau IPv6 /64 contient environ dix-huit quintillions d'adresses, ce qui dépasse largement les besoins de tout segment de réseau IP.

Les sous-réseaux créés à partir de l'ID de sous-réseau sont faciles à représenter, puisqu'aucune conversion en binaire n'est requise. Pour déterminer le sous-réseau disponible suivant, il suffit de compter en hexadécimal. Comme le montre la Figure 2, cela revient à compter en hexadécimal dans la partie d'ID de sous-réseau.

Le préfixe global de routage est identique pour tous les sous-réseaux. Seul le quartet représentant l'ID de sous-réseau est incrémenté pour chaque sous-réseau

9.3.1.2 Attribution de sous-réseaux IPv6

Avec plus de 65 000 sous-réseaux disponibles, la mission de l'administrateur réseau revient à concevoir un schéma logique pour répondre aux besoins du réseau.

Comme le montre la Figure 1, cet exemple de topologie exige des sous-réseaux pour chaque réseau local ainsi que pour la liaison de réseau étendu entre R1 et R2. À la différence de l'exemple d'adressage IPv4, avec IPv6, le sous-réseau de la liaison WAN n'est pas divisé une nouvelle fois en sous-réseaux. Bien que cela entraîne un « gaspillage » d'adresses, ce n'est pas un problème avec l'approche IPv6.

Comme indiqué à la Figure 2, nous allons attribuer 5 sous-réseaux IPv6 avec le champ d'ID de sous-réseau 0001 à 0005 dans cet exemple. Chaque sous-réseau /64 propose plus d'adresses qu'il ne sera jamais nécessaire.

Comme l'illustre la Figure 3, un sous-réseau /64 est attribué à chaque segment LAN et à la liaison WAN.

Comme pour la configuration IPv4, la Figure 4 montre que chacune des interfaces du routeur a été configurée pour utiliser un sous-réseau IPv6 différent

9.3.1.3 Segmentation en sous-réseaux à partir de l'ID d'interface

Avec IPv6, il est possible d'emprunter des bits à l'ID d'interface pour créer des sous-réseaux IPv6 de la même manière que nous avons emprunté des bits à la partie hôte d'une adresse IPv4. Cette opération vise généralement à améliorer la sécurité en créant moins d'hôtes par sous-réseau et pas nécessairement pour créer des sous-réseaux supplémentaires.

Lorsque vous étendez l'ID de sous-réseau en empruntant des bits à l'ID d'interface, il est recommandé d'effectuer la segmentation au niveau d'une limite de quartet. Un quartet correspond à 4 bits ou un caractère hexadécimal. Comme l'illustre la figure, le préfixe de sous-réseau /64 est étendu de 4 bits ou 1 quartet, et devient donc /68. Cela réduit la taille de l'ID d'interface de 4 bits. Il passe donc de 64 à 60 bits.

La création de sous-réseaux sur les limites de quartet implique que seuls les masques de sous-réseau alignés sur les quartets sont utilisés. À partir de /64, les masques de sous-réseau alignés sur les quartets sont /68, /72, /76, /80, etc.

La segmentation au niveau d'une limite de quartet crée des sous-réseaux au moyen de la valeur hexadécimale supplémentaire. Dans l'exemple, le nouvel ID de sous-réseau comprend les 5 valeurs hexadécimales allant de 00000 à FFFFF.

Il est possible d'effectuer la segmentation au sein d'une limite de quartet avec un seul chiffre hexadécimal, mais ce n'est pas recommandé, voire inutile. Le fait de créer des sous-réseaux au sein d'une limite de quartet ne permet pas de déterminer facilement le préfixe à partir de l'ID d'interface Par exemple, si une longueur de préfixe /66 est utilisée, les deux premiers bits feraient partie de l'ID de sous-réseau et les deux bits suivants feraient partie de l'ID d'interface

CHAPITRE 10: COUCHE APPLICATION

Introduction

Nous utilisons Internet via le Web lorsque nous regardons des vidéos en continu, jouons à des jeux en ligne, chattons avec des amis, envoyons des e-mails et faisons des achats sur des sites Web. Les applications telles que celles utilisées pour fournir les services décrits offrent une interface humaine avec le réseau sous-jacent. Elles nous permettent d'envoyer et de recevoir des données relativement facilement. Il est généralement possible d'accéder à ces applications et de les utiliser sans savoir comment elles fonctionnent. Cependant, un professionnel des réseaux doit savoir dans quelle mesure une application est capable de formater, de transmettre et d'interpréter les messages envoyés et reçus via le réseau.

Grâce à sa structure en couches, le modèle OSI permet de visualiser plus facilement les mécanismes sous-jacents de la communication via le réseau.

Dans ce chapitre, nous allons examiner le rôle de la couche application. Nous découvrirons également comment les applications, les services et les protocoles de la couche application permettent une communication fiable via les réseaux de données.

10.0.1.2 Exercice - Recherche sur les applications

Que se passerait-il si...

Votre employeur a décidé d'installer des téléphones IP sur votre lieu de travail, ce qui va rendre le réseau inutilisable pendant une semaine.

Vous devez toutefois continuer à travailler. Vous avez des e-mails à envoyer et des devis à rédiger puis à faire valider par votre responsable. En raison de problèmes de sécurité potentiels, vous n'êtes pas autorisé à utiliser un système informatique ou un équipement personnel ou externe pour terminer votre travail.

Votre instructeur peut vous demander de répondre aux questions des deux scénarios ci-dessous ou de sélectionner un scénario (A. E-mails ou B. Devis à faire valider par le responsable). Répondez aux questions en détail pour les scénarios concernés. Soyez prêt à expliquer vos réponses en classe.

A. E-mail

- Quelles méthodes pouvez-vous utiliser pour envoyer vos e-mails ?
- Comment pouvez-vous envoyer le même message à plusieurs destinataires ?
- Comment pouvez-vous envoyer une pièce jointe de grande taille à plusieurs destinataires ?
- Ces méthodes sont-elles rentables pour l'entreprise ?
- Violent-elles certaines politiques de sécurité de l'entreprise ?

B. Devis à faire valider par le responsable

- Des applications de bureau sont installées sur votre ordinateur. Sera-t-il simple de rédiger le devis que votre responsable doit valider pour le nouveau contrat à envoyer avant la fin de la semaine ? À quelles limitations serez-vous confronté en essayant de rédiger le devis ?

- Comment présenterez-vous le devis à faire valider à votre responsable ? Comment pensez-vous que votre responsable enverra le devis au client ?

- Ces méthodes sont-elles rentables pour l'entreprise ? Justifiez votre réponse.

Instructions de l'exercice en classe - Que se passerait-il si...

Protocoles de couche Application

Application, session et présentation

10.1.1.1 Révision des modèles OSI et TCP/IP

Comme le montre la figure, les professionnels des réseaux utilisent les modèles OSI et TCP/IP pour communiquer verbalement et dans la documentation technique écrite. Ils leur permettent de décrire le comportement des protocoles et des applications.

Dans le modèle OSI, les données sont transmises d'une couche à l'autre, en partant de la couche application sur l'hôte émetteur, puis en descendant dans la hiérarchie jusqu'à la couche physique, pour ensuite transiter sur le canal de communication vers l'hôte de destination, où les données remontent la hiérarchie jusqu'à la couche application.

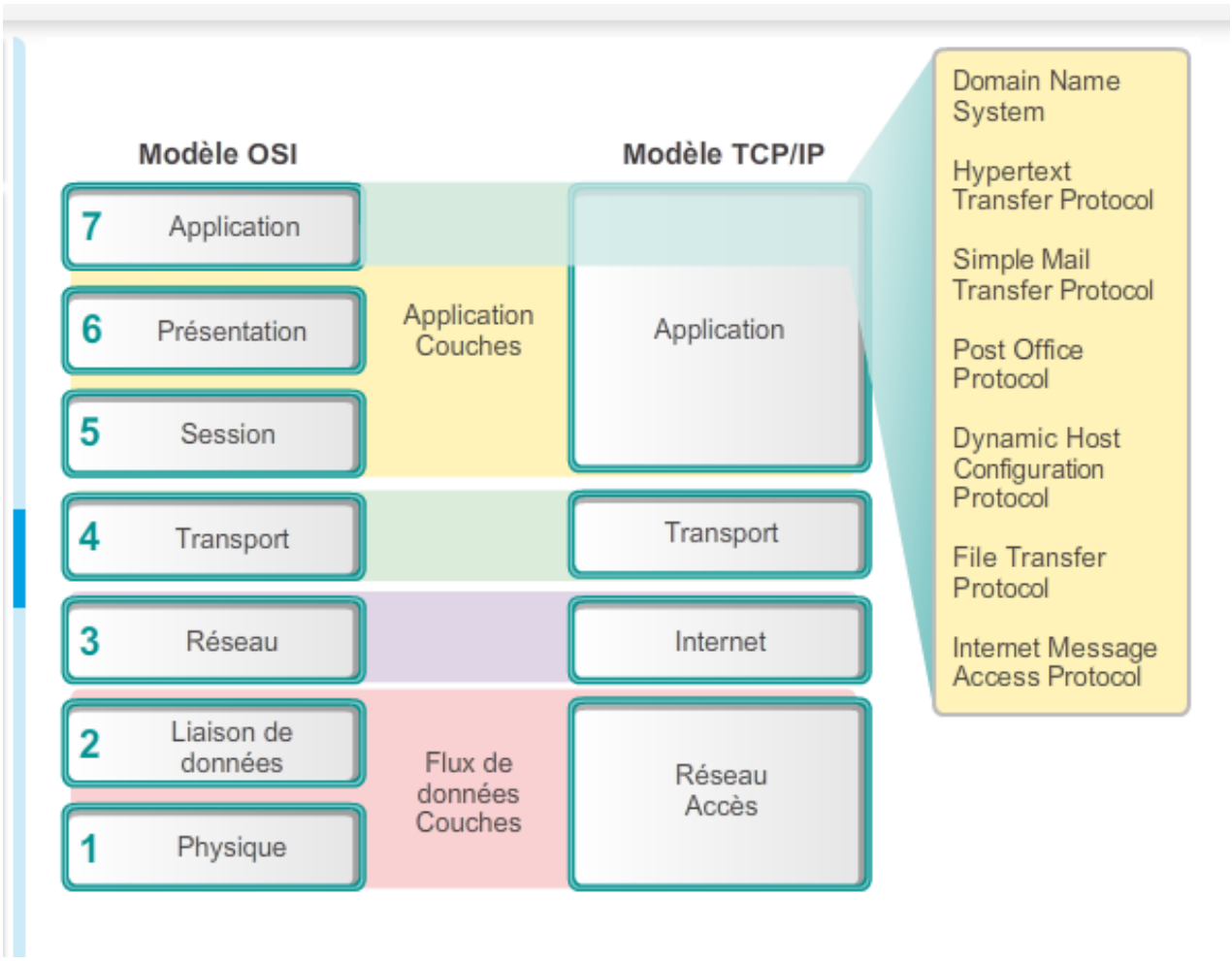
La couche application est la couche supérieure des modèles OSI et TCP/IP. La couche application TCP/IP inclut plusieurs protocoles qui fournissent des fonctionnalités spécifiques à différentes applications d'utilisateur final. Le rôle des protocoles de couche application TCP/IP correspond plus ou moins à la structure des trois couches supérieures du modèle OSI : les couches application, présentation et session. Les couches 5, 6 et 7 du modèle OSI sont utilisées en tant que références pour les développeurs et les éditeurs d'applications, afin de créer des produits tels que des navigateurs Web qui doivent accéder aux réseaux.

10.1.1.2 Couche application

La couche application

La couche application est la plus proche de l'utilisateur final. Comme le montre la figure, c'est elle qui sert d'interface entre les applications que nous utilisons pour communiquer et le réseau sous-jacent via lequel nos messages sont transmis. Les protocoles de couche application sont utilisés pour échanger des données entre les programmes s'exécutant sur les

hôtes source et de destination. Il existe déjà de nombreux protocoles de couche application et de nouveaux protocoles sont constamment développés. Les protocoles de couche application les plus connus sont notamment HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), IMAP (Internet Message Access Protocol) et DNS (Domain Name System).



10.1.1.3 Couches présentation et session

Couche présentation

La couche présentation remplit trois fonctions principales :

- Elle met en forme ou présente les données provenant du périphérique source dans un format compatible pour la réception par le périphérique de destination.
- Elle compresse les données de sorte que celles-ci puissent être décompressées par le périphérique de destination.
- chiffrement des données en vue de leur transmission et déchiffrement des données reçues par le périphérique de destination.

Comme l'illustre la figure, la couche présentation met en forme les données pour la couche application et elle définit les normes des formats de fichiers. QuickTime et MPEG (Motion Picture Experts Group) comptent parmi les normes de vidéo les plus courantes. QuickTime est une spécification informatique d'Apple pour la vidéo et l'audio, et MPEG est une norme de compression et de codage vidéo et audio.

Les formats d'images graphiques les plus connus utilisés sur les réseaux sont notamment GIF (Graphics Interchange Format), JPEG (Joint Photographic Experts Group) et PNG (Portable Network Graphics). GIF et JPEG sont des normes de compression et de codage pour les images graphiques. Le format PNG a été conçu pour pallier certaines des limitations du format GIF et pour le remplacer par la suite.

Couche session

Comme leur nom l'indique, les fonctions de la couche session créent et gèrent les dialogues entre les applications source et de destination. La couche session traite l'échange des informations pour commencer et maintenir un dialogue et pour redémarrer les sessions interrompues ou inactives pendant une longue période.

10.1.1.4 Protocoles de couche application TCP/IP

Tandis que le modèle OSI sépare les fonctions application, présentation et session, les applications TCP/IP les plus connues et les plus répandues intègrent les fonctionnalités des trois couches.

Les protocoles d'application TCP/IP spécifient les informations de format et de contrôle nécessaires à un grand nombre de fonctions courantes de communication via Internet. Voici certains de ces protocoles TCP/IP :

- **DNS (Domain Name System)** : ce protocole traduit les adresses Internet en adresses IP.

- **Telnet** : protocole utilisé pour permettre un accès distant aux serveurs et aux périphériques réseau.

- **SMTP (Simple Mail Transfer Protocol)** : ce protocole transmet les e-mails et leurs pièces jointes.

- **DHCP (Dynamic Host Configuration Protocol)** : protocole utilisé pour attribuer une adresse IP, un masque de sous-réseau, une passerelle par défaut et des adresses de serveur DNS à un hôte.

- **HTTP (Hypertext Transfer Protocol)** : ce protocole est utilisé pour transférer les fichiers qui constituent les pages du Web.

- **FTP (File Transfer Protocol)** : protocole utilisé pour le transfert interactif de fichiers entre des systèmes.

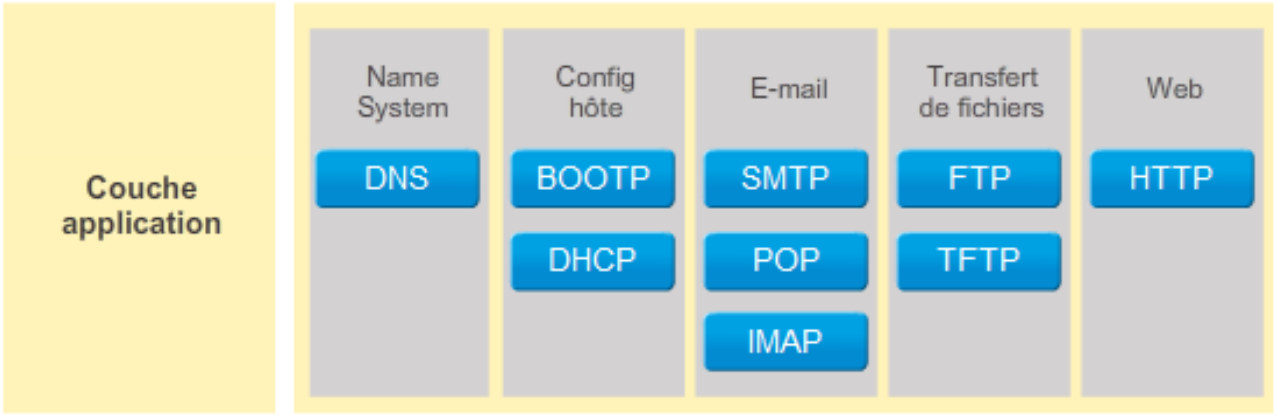
- **TFTP (Trivial File Transfer Protocol)** : ce protocole est utilisé pour le transfert actif de fichiers sans connexion.

- **BOOTP (Bootstrap Protocol)** : ce protocole est un précurseur du protocole DHCP. Il s'agit d'un protocole réseau utilisé pour obtenir des informations d'adresse IP lors du démarrage.

- **POP (Post Office Protocol)** : protocole utilisé par les clients de messagerie pour récupérer des e-mails à partir d'un serveur distant.

- **IMAP (Internet Message Access Protocol)** : autre protocole de récupération des e-mails.

Les protocoles de couche application sont utilisés par les périphériques source et de destination pendant une session de communication. Pour que les communications aboutissent, les protocoles de couche application implémentés sur les hôtes source et de destination doivent être compatibles.



Interaction des protocoles d'application avec les applications des utilisateurs finaux

10.1.2.1 Réseaux P2P

Lorsque vous accédez à des informations sur un périphérique réseau, qu'il s'agisse d'un ordinateur de bureau, d'un ordinateur portable, d'une tablette, d'un smartphone ou de tout autre périphérique connecté à un réseau, les données ne sont pas forcément stockées physiquement sur le périphérique. Si elles ne le sont pas, une requête d'accès à ces informations doit être adressée au périphérique sur lequel résident les données. Dans le modèle de réseau peer-to-peer (P2P), les données sont accessibles à partir d'un périphérique homologue (peer) sans l'intervention d'un serveur dédié.

Le modèle de réseau P2P implique deux parties : les réseaux P2P et les applications P2P. Celles-ci ont des caractéristiques similaires, mais dans les faits, elles fonctionnent très différemment.

Réseaux P2P

Dans un réseau P2P, au moins deux ordinateurs sont connectés via un réseau et peuvent partager des ressources (telles que des imprimantes et des fichiers) sans disposer de serveur dédié. Chaque périphérique final connecté (« peer » ou « homologue ») peut opérer en tant que serveur ou en tant que client. Un ordinateur peut remplir le rôle de serveur pour une transaction tout en servant simultanément de client pour un autre ordinateur. Les rôles de client et de serveur sont définis en fonction de chaque requête.

Prenons l'exemple d'un réseau domestique simple composé de deux ordinateurs, comme illustré sur la figure. Dans cet exemple, une imprimante est reliée directement à Peer2 par un câble USB. Peer2 est également configuré pour partager l'imprimante sur le réseau de sorte que Peer1 puisse imprimer sur celle-ci. Peer1 est configuré pour partager un disque dur ou un dossier sur le réseau. Cela permet à Peer2 d'accéder aux fichiers du dossier partager et de sauvegarder des fichiers dans celui-ci. Outre le partage de fichiers, un réseau comme celui-ci peut autoriser le jeu en réseau ou le partage de connexion Internet.

Les réseaux P2P décentralisent les ressources sur un réseau. Au lieu d'être stockées sur des serveurs dédiés, les données à partager peuvent se situer n'importe où et sur n'importe quel périphérique connecté. La plupart des systèmes d'exploitation actuels prennent en charge le partage des fichiers et des imprimantes sans nécessiter un logiciel serveur supplémentaire. Toutefois, les réseaux P2P n'utilisent pas de comptes utilisateurs centralisés ni de serveurs d'accès pour gérer les autorisations. Par conséquent, il est difficile d'appliquer les règles de sécurité et d'accès aux réseaux comportant un certain nombre d'ordinateurs. Les comptes et les droits d'accès utilisateur doivent être définis individuellement sur chaque périphérique homologue.

10.1.2.2 Applications peer to peer (P2P)

Une application peer-to-peer (P2P) permet à un périphérique d'agir à la fois en tant que client et serveur dans une même communication, comme le montre la figure. Dans ce modèle, chaque client est un serveur et chaque serveur un client. Les deux peuvent lancer une communication et sont considérés comme égaux dans le processus de communication. Cependant, les applications P2P nécessitent que chaque périphérique final fournisse une interface utilisateur et exécute un service en arrière-plan. Lorsque vous lancez une application P2P spécifique, le périphérique charge l'interface utilisateur et les services d'arrière-plan. Les périphériques peuvent ensuite communiquer directement.

Certaines applications P2P utilisent un système hybride dans lequel le partage des ressources est décentralisé, mais les index pointant vers l'emplacement des ressources sont stockés dans un répertoire centralisé. Dans un système hybride, chaque homologue accède à un serveur d'index pour obtenir l'emplacement d'une ressource stockée chez un autre homologue. Le serveur d'index permet également de connecter deux homologues, mais une fois ceux-ci connectés, la communication s'effectue entre les deux homologues sans autre communication vers le serveur d'index.

Les applications P2P peuvent être utilisées sur des réseaux P2P, des réseaux client/serveur et via Internet.

10.1.2.3 Applications P2P courantes

Avec les applications P2P, chaque ordinateur du réseau exécutant l'application peut servir de client ou de serveur pour les autres ordinateurs du réseau exécutant l'application. Voici certaines des applications P2P courantes :

- eDonkey
- eMule
- Shareaza
- BitTorrent
- Bitcoin
- LionShare

Certaines applications P2P sont basées sur le protocole Gnutella. Elles permettent aux utilisateurs de partager des fichiers stockés sur leurs disques durs avec d'autres personnes. Comme le montre la figure, les logiciels clients compatibles avec le protocole Gnutella permettent aux utilisateurs de se connecter aux services Gnutella via Internet et de localiser des ressources partagées par d'autres homologues Gnutella pour y accéder. De nombreuses applications clientes permettent d'accéder au réseau Gnutella, notamment BearShare, Gnucleus, LimeWire, Morpheus, WinMX et XoloX.

Le forum des développeurs Gnutella gère le protocole de base, mais les éditeurs d'applications développent souvent des extensions pour que le protocole fonctionne mieux avec leur application.

De nombreuses applications P2P n'utilisent pas de base de données centrale pour répertorier tous les fichiers disponibles sur les homologues. Au lieu de cela, chaque périphérique du réseau, lorsqu'il est interrogé, indique aux autres périphériques quels fichiers sont disponibles et utilise le protocole et les

10.1.2.5 Modèle client-serveur

Dans le modèle client-serveur, le périphérique qui demande les informations est appelé « client » et celui qui répond à la requête est appelé « serveur ». Les processus client et serveur sont considérés comme faisant partie de la couche application. Le client commence l'échange en demandant des données au serveur, qui répond en envoyant un ou plusieurs flux de données au client. Les protocoles de couche application décrivent le format des requêtes et des réponses entre clients et serveurs. Outre le transfert de données proprement dit, cet échange peut également nécessiter l'authentification de l'utilisateur et l'identification des fichiers de données à transférer.

Les services de messagerie électronique des FAI qui permettent d'envoyer, de recevoir et de stocker les e-mails sont des exemples de réseau client-serveur. Le client de messagerie sur un

ordinateur domestique envoie une requête au serveur de messagerie du FAI pour tout e-mail non lu. Le serveur répond en renvoyant au client les e-mails demandés.

Bien que les données soient généralement décrites comme étant transmises du serveur au client, certaines données sont toujours transmises du client au serveur. Le flux de données peut être égal dans les deux sens ou même plus important dans le sens client vers serveur. Par exemple, un client peut transférer un fichier vers le serveur à des fins de stockage. Comme le montre la figure, le téléchargement de données d'un client vers un serveur est dit « ascendant » et le téléchargement de données d'un serveur vers un client est dit « descendant ».

Services et protocoles de couche application courants

Protocoles de couche application courants

10.2.1.1 Révision des protocoles de couche application

Il existe des dizaines de protocoles de couche application, mais les opérations courantes font appel à seulement cinq ou six d'entre eux. Les trois protocoles de couche application suivants sont impliqués dans les tâches professionnelles ou personnelles quotidiennes :

- protocole HTTP (HyperText Transfer Protocol)
- Protocole SMTP (Simple Mail Transfer Protocol)
- Protocole POP (Post Office Protocol)

Ces protocoles de couche application permettent de parcourir le Web et d'envoyer et de recevoir des e-mails. Le protocole HTTP permet aux utilisateurs de se connecter aux sites Web sur Internet, le protocole SMTP leur permet d'envoyer des e-mails et le protocole POP de recevoir des e-mails.

Les prochaines pages se concentrent sur ces trois protocoles de couche application.

10.2.1.2 HTTP et HTML

Lorsqu'une adresse Web (ou URL pour Uniform Resource Locator) est saisie dans un navigateur Web, ce dernier établit une connexion avec le service Web s'exécutant sur le serveur à l'aide du protocole HTTP. L'URL et l'URI (Uniform Resource Identifier) sont les noms que la plupart des utilisateurs associent aux adresses Web.

L'adresse http://www.cisco.com/index.html est un exemple d'une URL qui se réfère à une ressource spécifique : une page Web nommée **index.html** sur un serveur identifié comme étant **cisco.com**. Cliquez sur chaque figure pour afficher les étapes du protocole HTTP.

Les navigateurs Web sont le type d'application cliente qu'utilise un ordinateur pour se connecter au Web et accéder aux ressources stockées sur un serveur Web. Comme avec la plupart des processus serveur, le serveur Web s'exécute en tant que service en tâche de fond et met différents types de fichiers à la disposition de l'utilisateur.

Pour accéder au contenu, les clients Web établissent des connexions au serveur et demandent les ressources voulues. Le serveur retourne les ressources et, à la réception de ces dernières, le navigateur interprète les données avant de les présenter à l'utilisateur.

Les navigateurs peuvent interpréter et présenter de nombreux types de données, tels que des données en texte clair ou HTML, le langage dans lequel sont conçues les pages Web. Cependant, d'autres types de données peuvent nécessiter un autre service ou programme, généralement nommé plug-in ou composant additionnel. Pour aider le navigateur à déterminer le type de fichier qu'il reçoit, le serveur indique le type de données que contient le fichier.

Pour mieux comprendre l'interaction entre le navigateur Web et le client Web, voyons comment une page Web s'ouvre dans un navigateur. Dans cet exemple, utilisez l'URL http://www.cisco.com/index.html.

D'abord, comme le montre la Figure 1, le navigateur interprète les trois parties de l'URL :

1. **http** (protocole ou schéma)

2. **www.cisco.com** (nom du serveur)

3. **index.html** (nom du fichier demandé)

Comme illustré à la Figure 2, le navigateur fait ensuite appel à un serveur de noms pour convertir l'adresse www.cisco.com en une adresse numérique, qu'il utilise pour se connecter au serveur. Le navigateur envoie une requête GET au serveur et demande le fichier **index.html** en se conformant à la norme HTTP. Comme le montre la Figure 3, le serveur envoie au navigateur le code HTML pour cette page Web. Enfin, comme le montre la Figure 4, le navigateur déchiffre le code HTML et met en forme la page pour la fenêtre du navigateur.

10.2.1.3 HTTP et HTTPS

Le protocole HTTP est utilisé à travers le Web pour le transfert des données et constitue l'un des protocoles d'application les plus utilisés. Au départ, il a été développé simplement pour publier et récupérer des pages HTML, mais la flexibilité de ce protocole en a fait une application indispensable dans les systèmes informatiques distribués et de collaboration.

Le protocole HTTP est de type requête/réponse. Lorsqu'un client, généralement un navigateur Web, envoie une requête à un serveur Web, HTTP a indiqué les types de messages utilisés

pour cette communication. Les trois types de messages courants sont GET, POST et PUT (cf figure).

GET est une requête cliente pour obtenir des données. Un client (navigateur Web) envoie le message GET au serveur Web pour demander des pages HTML. Lorsque le serveur reçoit la requête GET, il renvoie une ligne décrivant l'état (par exemple, HTTP/1.1 200 OK), ainsi qu'un message propre. Le message du serveur peut inclure le fichier HTML demandé, s'il est disponible, ou il peut contenir un message d'erreur ou d'information, tel que « L'emplacement du fichier demandé a changé ».

Les messages POST et PUT servent à télécharger (upload) des fichiers de données vers le serveur Web. Par exemple, lorsque l'utilisateur saisit des données dans un formulaire intégré à une page Web (par exemple lorsqu'il passe une commande), le message POST est envoyé au serveur Web. Les données envoyées par l'utilisateur dans le formulaire sont incluses dans le message POST.

La requête PUT télécharge des ressources ou du contenu vers le serveur Web. Par exemple, si un utilisateur tente de télécharger (upload) un fichier ou une image vers un site Web, un message PUT est envoyé par le client au serveur avec le fichier ou l'image.

Le protocole HTTP est certes extrêmement flexible, mais il n'est pas sécurisé. Les messages de demande transmettent au serveur des informations en texte brut pouvant être interceptées et lues. De même, les réponses du serveur (généralement, des pages HTML) ne sont pas chiffrées.

Pour une communication sécurisée via Internet, le protocole HTTPS (HTTP Secure) est utilisé lors de l'accès aux informations du serveur Web ou de leur publication. Le protocole HTTPS peut procéder à l'authentification et au chiffrement pour sécuriser les données pendant qu'elles circulent entre le client et le serveur. Le protocole HTTPS spécifie des règles supplémentaires de transmission des données entre la couche application et la couche transport. Il utilise le même processus de demande client-réponse serveur que le protocole HTTP, à ceci près que le flux de données est chiffré avec le protocole SSL (Secure Socket Layer) avant d'être transporté sur le réseau. HTTPS crée une charge et un temps de traitement supplémentaire sur le serveur, en raison du chiffrement et du déchiffrement du trafic.

10.2.1.4 SMTP, POP et IMAP

L'un des principaux services offerts par un FAI est l'hébergement de la messagerie. Par sa simplicité et sa rapidité, l'e-mail a révolutionné la façon dont les gens communiquent. Toutefois, pour que la messagerie fonctionne sur un ordinateur ou autre périphérique final, plusieurs applications et services sont nécessaires.

L'e-mail est une méthode de stockage et de transfert qui permet d'envoyer, de stocker et de récupérer des messages électroniques à travers un réseau. Les messages sont stockés dans des bases de données sur des serveurs de messagerie. Les FAI gèrent souvent des serveurs de messagerie qui prennent en charge de nombreux comptes client différents.

Les clients de messagerie communiquent avec les serveurs de messagerie pour envoyer et recevoir des messages. Les serveurs de messagerie communiquent avec d'autres serveurs de

messagerie pour acheminer les messages d'un domaine à un autre. Un client de messagerie ne communique pas directement avec un autre client de messagerie lors de l'envoi des e-mails. En fait, les deux clients dépendent du serveur de messagerie pour transporter les messages. Cela se vérifie également lorsque les deux utilisateurs appartiennent au même domaine.

Les clients de messagerie envoient des messages au serveur de messagerie configuré dans les paramètres de l'application. Lorsque le serveur reçoit le message, il vérifie si le domaine destinataire se trouve dans sa base de données locale. Dans la négative, il envoie une requête DNS pour déterminer l'adresse IP du serveur de messagerie du domaine de destination. L'e-mail est ensuite transféré au serveur approprié.

Les e-mails font appel à trois protocoles distincts : SMTP (Simple Mail Transfer Protocol), POP (Post Office Protocol) et IMAP (Internet Message Access Protocol. Le processus de couche application qui envoie l'e-mail utilise le protocole SMTP, et ce, qu'il soit envoyé d'un client à un serveur ou d'un serveur à un autre.

Pour récupérer l'e-mail, le client fait appel à l'un des deux protocoles de couche application suivants : POP ou IMAP.

Le protocole SMTP (Simple Mail Transfer Protocol) permet de transférer les e-mails de manière fiable et efficace. Pour que les applications SMTP fonctionnent, le message doit être correctement formaté et les processus SMTP doivent être exécutés à la fois sur le client et sur le serveur.

Les formats de message SMTP exigent un en-tête et un corps de message. Si le corps du message peut contenir n'importe quelle quantité de texte, l'en-tête doit contenir une adresse de messagerie de destinataire et une adresse d'expéditeur correctement mises en forme. Toute autre information est facultative dans l'en-tête.

Lorsqu'un client envoie un e-mail, le processus SMTP client se connecte à un processus SMTP serveur sur le port réservé 25. Une fois la connexion établie, le client essaie d'envoyer l'e-mail au serveur via la connexion. Lorsque le serveur a reçu le message, il le place sur un compte local si le destinataire est local, ou le dirige à l'aide du même processus de connexion SMTP vers un autre serveur de messagerie qui devra l'acheminer.

Le serveur de messagerie de destination peut ne pas être en ligne, ou peut être occupé, lors de l'envoi des messages. Par conséquent, le protocole SMTP met le message en attente pour envoi ultérieur. Régulièrement, le serveur vérifie si des messages se trouvent dans la file d'attente et essaie de les renvoyer. À l'issue d'une durée donnée, si le message n'est toujours pas transmis, il est renvoyé à son expéditeur comme non délivrable.

Le protocole POP (Post Office Protocol) permet à un ordinateur de récupérer des e-mails à partir d'un serveur de messagerie. Avec POP, l'e-mail est téléchargé du serveur au client, puis supprimé du serveur.

Le serveur démarre le service POP en écoutant passivement les éventuelles requêtes de connexion client sur le port TCP 110. Lorsqu'un client souhaite utiliser le service, il envoie une requête d'établissement de connexion TCP au serveur. Une fois la connexion établie, le serveur POP envoie un message de bienvenue. Le client et le serveur POP échangent alors des commandes et des réponses jusqu'à ce que la connexion soit fermée ou abandonnée.

Étant donné que les messages électroniques sont téléchargés chez le client et supprimés du serveur, il n'existe pas d'emplacement centralisé de conservation des messages. Comme le protocole POP ne stocke pas les messages, il est inadapté dans une petite entreprise qui a besoin d'une solution de sauvegarde centralisée.

Le protocole POP3 convient à un FAI puisqu'il lui évite d'avoir à gérer de grandes quantités de stockage sur leurs serveurs de messagerie.

Le protocole de messagerie IMAP (Internet Message Access Protocol) décrit une autre méthode de récupération des messages électroniques. Toutefois, contrairement au protocole POP, lorsque l'utilisateur se connecte à un serveur IMAP, des copies des messages sont téléchargées vers l'application cliente. Les messages originaux sont conservés sur le serveur jusqu'à ce qu'ils soient supprimés manuellement. Les utilisateurs affichent des copies des messages dans leur logiciel de messagerie.

Ils peuvent créer une hiérarchie de fichiers sur le serveur afin d'organiser et de stocker leurs e-mails. Cette structure de fichiers est également dupliquée sur le client de messagerie. Lorsqu'un utilisateur décide de supprimer un message, le serveur synchronise cette action et supprime le message du serveur.

Pour les petites et moyennes entreprises, le protocole IMAP présente de nombreux avantages. Il permet un stockage à long terme des messages sur les serveurs de messagerie et une sauvegarde centralisée. Il permet également aux employés d'accéder aux messages depuis différents emplacements à l'aide de différents périphériques ou logiciels clients. La structure de dossiers de boîte aux lettres à laquelle est habitué l'utilisateur reste consultable quel que soit le moyen qu'il choisit pour consulter sa boîte aux lettres.

Pour un FAI, le protocole IMAP peut ne pas être le choix idéal. Il peut s'avérer coûteux à l'achat et en maintenance de l'espace disque nécessaire au stockage des messages électroniques. De plus, cette contrainte sur le FAI s'accentue si les clients paramètrent des sauvegardes régulières de leurs boîtes aux lettres.

Services d'adressage IP

10.2.2.1 Domain Name Service (service de noms de domaines)

Dans les réseaux de données, les périphériques sont identifiés par des adresses IP numériques pour l'envoi et la réception de données sur les réseaux. La plupart des gens ne retiennent pas cette adresse numérique. Pour cette raison, des noms de domaine ont été créés pour convertir les adresses numériques en noms simples et explicites.

Sur Internet, ces noms de domaine (par exemple, http://www.cisco.com) sont beaucoup plus faciles à mémoriser que leurs équivalents numériques (par exemple, 198.133.219.25 pour le serveur de Cisco). Si Cisco décide de changer l'adresse numérique www.cisco.com, l'utilisateur n'en a pas conscience, car le nom de domaine reste le même. La nouvelle adresse est simplement reliée au nom de domaine existant et la connexion est ainsi assurée. Lorsque les réseaux étaient de petite taille, il était simple de maintenir le mappage entre les noms de

domaine et les adresses qu'ils représentaient. À mesure que les réseaux se sont développés et que le nombre de périphériques a augmenté, ce système manuel est devenu impossible à gérer.

Le protocole DNS (Domain Name System) a été créé afin de permettre la résolution de nom pour ces réseaux. Le protocole DNS utilise un ensemble distribué de serveurs pour convertir les noms associés à ces adresses en numéros. Cliquez sur les boutons de la figure pour afficher les étapes de la résolution des adresses DNS.

Le protocole DNS définit un service automatisé qui associe les noms des ressources à l'adresse réseau numérique requise. Il comprend le format des demandes, des réponses et des données. Les communications via le protocole DNS utilisent un format unique nommé message. Ce format de message est utilisé pour tous les types de demandes clientes et de réponses serveur, pour les messages d'erreur et pour le transfert des informations d'enregistrement de ressource entre les serveurs.

Les figures 1 à 5 illustrent les différentes étapes de la résolution DNS.

10.2.2.2 Format du message DNS

Un serveur DNS assure la résolution des noms à l'aide du domaine *BIND (Berkeley Internet Name Domain)* ou du nom de démon, souvent appelé named (prononcer « naïme-di »). Au départ, BIND a été développé par quatre étudiants de l'université de Berkley (Californie) au début des années 1980. Comme le montre la figure, le format de message DNS utilisé par BIND est le format DNS le plus répandu sur Internet.

Le serveur DNS stocke différents types d'enregistrements de ressource utilisés pour résoudre les noms. Ces enregistrements contiennent le nom, l'adresse et le type d'enregistrement.

Certains de ces types d'enregistrements sont les suivants :

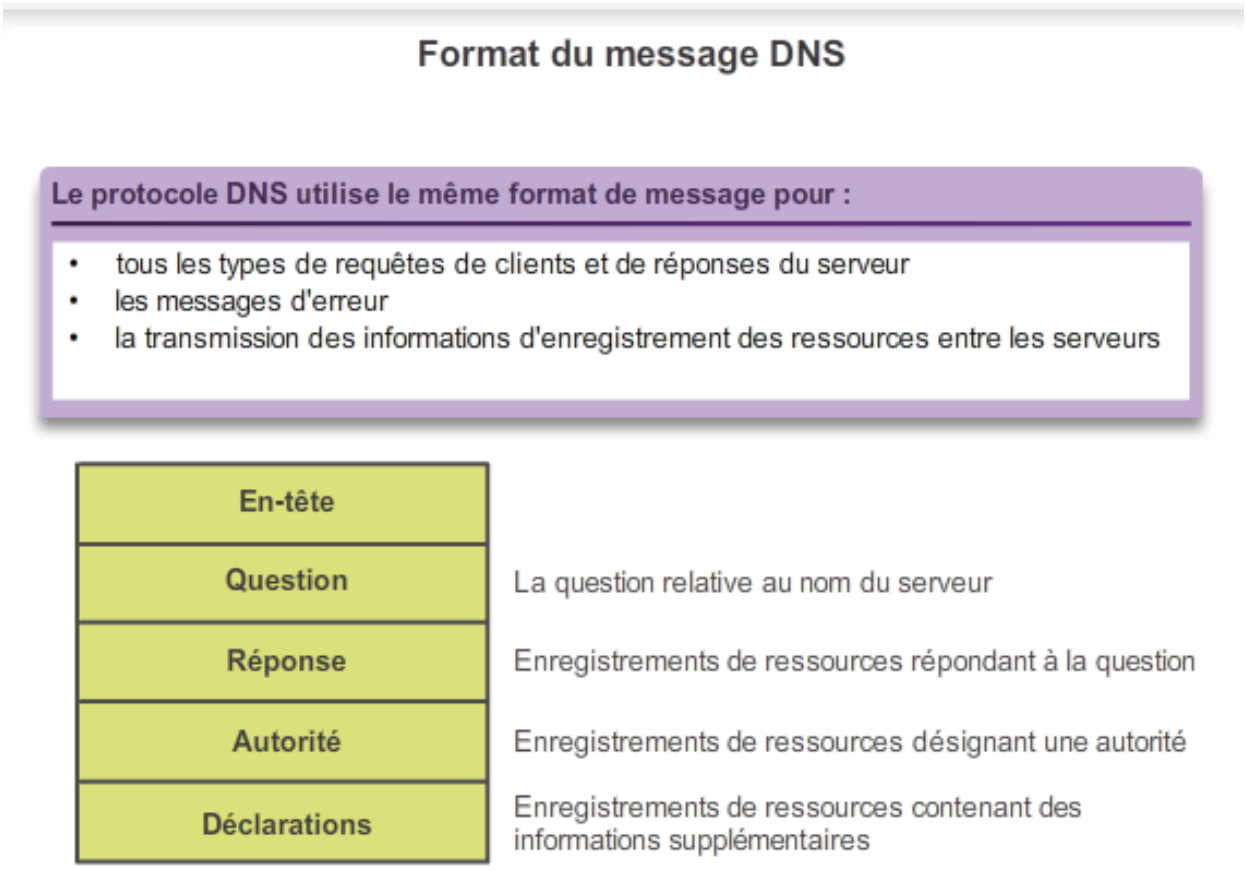
- **A** : adresse de périphérique final
- **NS** : serveur de noms faisant autorité
- **CNAME** : nom canonique (ou nom de domaine complet) d'un alias. Il est utilisé lorsque plusieurs services emploient une adresse réseau unique, mais que chaque service possède sa propre entrée dans le DNS.
- **MX** : enregistrement d'échange d'e-mails. Il associe un nom de domaine à une liste de serveurs d'échange d'e-mails pour ce domaine.

Lorsqu'un client envoie une requête, le processus BIND du serveur cherche d'abord dans ses propres enregistrements pour résoudre le nom. S'il n'est pas en mesure de résoudre le nom à l'aide de ses enregistrements stockés, il contacte d'autres serveurs.

La requête peut être transmise à plusieurs serveurs, ce qui peut nécessiter un délai supplémentaire et consommer de la bande passante. Lorsqu'une correspondance est trouvée et

retournée au serveur demandeur d'origine, le serveur stocke temporairement dans la mémoire cache l'adresse numérique correspondant au nom.

Si ce même nom est de nouveau demandé, le premier serveur peut retourner l'adresse en utilisant la valeur stockée dans son cache de noms. La mise en cache réduit le trafic réseau de données de demandes DNS et les charges de travail des serveurs situés aux niveaux supérieurs dans la hiérarchie. Le service Client DNS sur les ordinateurs Windows optimise les performances de la résolution des noms DNS en stockant également en mémoire les noms déjà résolus. La commande **ipconfig /displaydns** affiche toutes les entrées DNS mises en cache sur un système Windows.



10.2.2.3 Hiérarchie DNS

Le protocole DNS utilise un système hiérarchique pour créer une base de données assurant la résolution des noms. La hiérarchie ressemble à une arborescence inversée dont la racine se situe au sommet et les branches en dessous (cf figure). DNS utilise des noms de domaines pour élaborer sa hiérarchie.

La structure d'attribution de noms est divisée en petites zones gérables. Chaque serveur DNS tient à jour un fichier de base de données spécifique et se charge uniquement des mappages entre noms et adresses IP dans cette petite partie de la structure DNS globale. Lorsqu'un serveur DNS reçoit une demande de traduction d'un nom qui n'appartient pas à sa zone DNS,

le serveur DNS transfère la requête à un autre serveur DNS se trouvant dans la zone de traduction voulue.

Remarque : le système de noms de domaine est évolutif, car la conversion des noms d'hôte s'étend à plusieurs serveurs.

Les différents domaines de premier niveau représentent le type d'organisation ou le pays d'origine. Voici des exemples de domaines de premier niveau :

- **.au :** Australie
- **.co :** Colombie
- **.com :** entreprise ou industrie
- **.jp :** Japon
- **.org :** organisme à but non lucratif

Après les domaines de premier niveau viennent les domaines de second niveau, puis, en dessous, d'autres domaines de niveau inférieur. Chaque nom de domaine constitue un chemin qui descend dans cette arborescence inversée commençant par la racine. Par exemple, comme illustré sur la figure, le serveur DNS racine ne connait pas forcément l'emplacement exact de l'enregistrement du serveur de messagerie mail.cisco.com, mais il conserve un enregistrement pour le domaine .com dans le domaine de premier niveau. De même, les serveurs situés dans le domaine .com ne disposent pas forcément d'un enregistrement pour mail.cisco.com, mais ils disposent d'un enregistrement pour le domaine. Les serveurs du domaine cisco.com disposent d'un enregistrement (plus exactement, d'un enregistrement MX) pour mail.cisco.com.

DNS repose sur cette hiérarchie de serveurs décentralisés pour stocker et gérer ces enregistrements de ressources. Les enregistrements de ressources répertorient les noms de domaines que le serveur peut résoudre, ainsi que d'autres serveurs pouvant également traiter des requêtes. Si un serveur spécifique dispose d'enregistrements de ressources qui correspondent à son niveau dans la hiérarchie de domaines, il est qualifié de serveur d'autorité pour ces enregistrements. Par exemple, un serveur de noms dans le domaine cisco.netacad.net ne serait pas un serveur faisant autorité pour l'enregistrement mail.cisco.com, car cet enregistrement est stocké sur un serveur d'un domaine de niveau supérieur, à savoir le serveur de noms du domaine cisco.com.

10.2.2.4 nslookup

Le protocole DNS est un service client/serveur. Cependant, il diffère des autres services de ce type. Les autres services utilisent un client qui est une application (par exemple, un navigateur Web ou un client de messagerie) tandis que le client DNS s'exécute lui-même en tant que service. Le client DNS, parfois appelé résolveur DNS, prend en charge la résolution de noms pour d'autres applications réseau et d'autres services qui en ont besoin.

Lors de la configuration d'un périphérique réseau, au minimum une adresse de serveur DNS est fournie, que le client DNS peut utiliser pour la résolution de noms. Le fournisseur d'accès à Internet (FAI) fournit généralement les adresses à utiliser pour les serveurs DNS. Lorsque l'application d'un utilisateur demande à se connecter à un périphérique distant à l'aide d'un nom, le client DNS demandeur interroge l'un de ces serveurs de noms pour convertir le nom en une adresse numérique.

Le système d'exploitation des ordinateurs comprend également un utilitaire appelé nslookup qui permet à l'utilisateur d'introduire manuellement une requête auprès des serveurs de noms, afin de convertir un nom d'hôte donné. Cet utilitaire permet également de résoudre les problèmes de résolution de noms et de vérifier l'état actuel des serveurs de noms.

Comme le montre la figure, lorsque la commande **nslookup** est exécutée, le serveur DNS par défaut configuré pour votre hôte s'affiche. Dans cet exemple, le serveur DNS est dns-sj.cisco.com et possède l'adresse 171.70.168.183.

Le nom d'un hôte ou d'un domaine peut être saisi dans l'invite **nslookup**. La première requête de la figure concerne www.cisco.com. Le serveur de noms qui répond fournit l'adresse 198.133.219.25.

Les demandes affichées à l'écran ne sont que de simples tests. L'utilitaire nslookup propose de nombreuses options permettant de tester et de vérifier le processus DNS de manière approfondie. Lorsque vous avez terminé, saisissez **exit** pour quitter l'utilitaire nslookup.

10.2.2.6 protocole DHCP (Dynamic Host Configuration Protocol)

Le service fourni par le protocole DHCP (Dynamic Host Configuration Protocol) permet aux périphériques d'un réseau d'obtenir d'un serveur DHCP des adresses IP et d'autres informations. Ce service automatise l'attribution des adresses IP, des masques de sous-réseau, de la passerelle et d'autres paramètres de configuration réseau IP. On parle alors d'adressage dynamique. Le contraire de l'adressage dynamique est l'adressage statique. Dans le cas de l'adressage statique, l'administrateur réseau saisit manuellement l'adresse IP sur les hôtes du réseau.

Il permet à un hôte d'obtenir une adresse IP dynamiquement lorsqu'il se connecte au réseau. Le serveur DHCP est contacté et une adresse est demandée. Le serveur DHCP choisit une adresse dans une plage d'adresses configurée (nommée pool) et attribue cette adresse à l'hôte pour une durée définie.

Sur les réseaux locaux de plus grande taille ou sur les réseaux dont les utilisateurs changent fréquemment, l'adressage par le protocole DHCP est préférable. De nouveaux utilisateurs peuvent arriver avec des ordinateurs portables et avoir besoin d'une connexion, d'autres peuvent avoir de nouveaux postes de travail qui doivent être connectés. Plutôt que de faire attribuer des adresses IP par l'administrateur réseau à chaque station de travail, il est plus efficace que les adresses IP soient attribuées automatiquement à l'aide du protocole DHCP.

Les adresses attribuées via le protocole DHCP ne sont pas affectées aux hôtes définitivement, mais uniquement pour une durée spécifique. Si l'hôte est mis hors tension ou retiré du réseau, l'adresse est retournée au pool pour être réutilisée. Ceci est particulièrement utile pour les utilisateurs mobiles qui se connectent et se déconnectent sur le réseau. Les utilisateurs peuvent librement se déplacer d'un endroit à un autre et rétablir des connexions réseau. L'hôte peut obtenir une adresse IP une fois la connexion matérielle établie, via un réseau local filaire ou sans fil.

Le protocole DHCP vous permet d'accéder à Internet via des points d'accès sans fil dans des aéroports ou des cafés. Lorsqu'un périphérique sans fil rejoint un point d'accès, le client DHCP du périphérique contacte le serveur DHCP local via une connexion sans fil, et le serveur DHCP attribue une adresse IP au périphérique.

Comme l'illustre la figure, divers types de périphériques peuvent être des serveurs DHCP lorsqu'ils exécutent des logiciels de service DHCP. Dans la plupart des réseaux de taille moyenne à grande, le serveur DHCP est généralement un serveur local dédié basé sur un ordinateur. Dans le cas des réseaux domestiques, le serveur DHCP est généralement situé sur le routeur local qui connecte le réseau domestique au FAI. Les hôtes locaux reçoivent les informations d'adresse IP directement du routeur local. Le routeur local reçoit une adresse IP du serveur DHCP chez le FAI.

Le protocole DHCP peut représenter un risque pour la sécurité car n'importe quel périphérique connecté au réseau peut recevoir une adresse. Ce risque fait de la sécurité physique un facteur déterminant en faveur de l'adressage dynamique ou manuel. L'adressage dynamique et l'adressage statique ont tous deux leur place dans la conception du réseau. De nombreux réseaux utilisent à la fois le protocole DHCP et l'adressage statique. Le protocole DHCP est utilisé pour les hôtes d'usage général (par exemple, les périphériques d'utilisateur final) et l'adressage dynamique sert aux périphériques réseau tels que les passerelles, les commutateurs, les serveurs et les imprimantes.

10.2.2.7 Fonctionnement du protocole DHCP

Sans le protocole DHCP, les utilisateurs doivent indiquer manuellement l'adresse IP, le masque de sous-réseau et d'autres paramètres réseau pour se connecter au réseau. Le serveur DHCP maintient un pool d'adresses IP et attribue temporairement une adresse à n'importe quel client DHCP lorsque celui-ci est mis sous tension. Les adresses IP étant des adresses dynamiques (temporairement attribuées) et non pas des adresses statiques (définitivement attribuées), les adresses qui ne sont plus utilisées sont automatiquement retournées au pool pour être réattribuées. Comme le montre la figure, lorsqu'un périphérique configuré pour le protocole DHCP démarre ou se connecte au réseau, le client diffuse un message de détection DHCP (DHCPDISCOVER) pour identifier les serveurs DHCP disponibles sur le réseau. Un serveur DHCP répond par un message d'offre DHCP (DHCPOFFER), qui offre un bail au client. Ce message contient l'adresse IP et le masque de sous-réseau à attribuer, l'adresse IP du serveur DNS et l'adresse IP de la passerelle par défaut. L'offre de bail indique également la durée du bail.

Le client peut recevoir plusieurs messages DHCPOFFER si le réseau local comporte plusieurs serveurs DHCP. Il doit donc effectuer un choix et envoyer une requête DHCP (DHCPREQUEST) qui identifie explicitement le serveur et l'offre de bail qu'il accepte. Un client peut également choisir de demander une adresse que le serveur lui a déjà attribuée précédemment.

En supposant que l'adresse IP demandée par le client ou offerte par le serveur est encore disponible, le serveur renvoie un message DHCP (DHCPACK) confirmant au client que le bail est conclu. Si l'offre n'est plus valide (par exemple en raison du délai d'attente ou si un autre client a pris le bail), le serveur sélectionné répond par un message d'accusé de réception DHCP négatif (DHCPNAK). Si un message DHCPNAK est retourné, le processus de sélection doit recommencer avec la transmission d'un nouveau message DHCPDISCOVER. Lorsque le client a obtenu le bail, celui-ci doit être renouvelé avant son expiration via un autre message DHCPREQUEST.

Le serveur DHCP garantit que toutes les adresses IP sont uniques (une adresse IP ne peut pas être attribuée à deux périphériques réseau différents en même temps). Le protocole DHCP permet aux administrateurs réseau de reconfigurer aisément les adresses IP des clients sans devoir apporter de modifications manuelles aux clients. La plupart des fournisseurs d'accès à Internet utilisent le protocole DHCP pour attribuer des adresses à leurs clients ne nécessitant pas d'adresse statique.

Services de partage de fichiers

10.2.3.1 File Transfer Protocol

Le protocole FTP (File Transfer Protocol) est un autre protocole de couche application couramment utilisé. Il a été développé pour permettre le transfert de données entre un client et un serveur. Un client FTP est une application s'exécutant sur un ordinateur et utilisée pour stocker des données sur un serveur exécutant un démon FTP (FTPd) et pour extraire ces données.

Comme le montre la figure, pour transférer avec succès les données, le protocole FTP nécessite deux connexions entre le client et le serveur, l'une pour les commandes et les réponses, l'autre pour le transfert de fichiers en lui-même :

- Le client établit la première connexion au serveur pour le trafic de contrôle qui se compose de commandes de clients et de réponses du serveur.

- Le client établit une seconde connexion au serveur pour le véritable transfert de données. Cette connexion est créée chaque fois que des données doivent être transférées.

Le transfert de données peut s'effectuer dans les deux directions. Le client peut télécharger (extraire) des données à partir du serveur ou le client peut télécharger (stocker) des données vers le serveur.

10.2.3.4 Server Message Block

Le protocole SMB (Server Message Block) est un protocole de partage de fichiers client/serveur développé par IBM à la fin des années 1980 pour décrire la structure des ressources réseau partagées telles que les répertoires, les fichiers, les imprimantes et les ports série. Il s'agit d'un protocole de requête-réponse.

Le protocole SMB décrit l'accès au système de fichiers et la manière dont les clients peuvent demander des fichiers. Il décrit également sa communication interprocessus. Tous les messages SMB partagent un format commun. Ce format utilise un en-tête de taille fixe, suivi d'un paramètre et d'un composant de données des tailles variables.

Les messages SMB peuvent :

- démarrer et authentifier des sessions ou y mettre fin ;
- contrôler l'accès aux fichiers et aux imprimantes ;
- permettre à une application d'envoyer ou de recevoir des messages vers ou depuis un autre périphérique.

Le partage de fichiers et les services d'impression SMB sont devenus la base des réseaux Microsoft. Avec l'introduction de la série de logiciels Windows 2000, Microsoft a modifié la structure sous-jacente pour l'utilisation du protocole SMB. Dans les versions précédentes des produits Microsoft, les services SMB utilisaient un protocole autre que TCP/IP pour implémenter la résolution de noms. Depuis Windows 2000, tous les produits Microsoft utilisent le nommage DNS qui permet aux protocoles TCP/IP de prendre en charge directement le partage des ressources SMB, comme le montre la Figure 1. Le processus d'échange de fichiers SMB entre les ordinateurs Windows est représenté à la Figure 2.

Contrairement au partage de fichiers pris en charge par le protocole FTP, les clients établissent une connexion à long terme aux serveurs. Une fois la connexion établie, l'utilisateur du client peut accéder aux ressources résidant sur le serveur comme si elles étaient situées localement sur l'hôte client.

Les systèmes d'exploitation LINUX et UNIX fournissent également une méthode de partage des ressources avec les réseaux Microsoft à l'aide d'une version de SMB nommée SAMBA. Les systèmes d'exploitation Apple Macintosh prennent en charge eux aussi le partage des ressources via le protocole SMB.

Un même message dans le monde entier

Faites passer le message !

10.3.1.1 L'Internet des objets

La couche application accède directement aux processus sous-jacents qui gèrent et permettent la communication à travers le réseau. Cette couche sert de source et de destination aux communications via les réseaux de données, quel que soit le type de réseau de données utilisé. En fait, l'évolution des réseaux à un impact direct sur le type d'applications développées.

Des tendances telles que le BYOD (Bring Your Own Device), l'accès en tout lieu, la virtualisation et les connexions machine à machine (m2m) ont ouvert la voie à une nouvelle génération d'applications. On estime qu'environ 50 milliards de périphériques seront connectés d'ici 2020. Rien qu'en 2010, plus de 350 000 applications téléchargées plus de trois millions de fois ont été développées. Tout cela donne lieu à un univers de connexions intuitives entre les personnes, les processus, les données et les objets sur le réseau.

L'utilisation de « Smart Tags » et d'une connectivité avancée pour numériser les produits non intelligents (des vélos et des bouteilles aux réfrigérateurs et aux voitures) et les connecter à Internet offrira aux particuliers et aux entreprises des possibilités d'interaction nouvelles et presque impensables. Les objets pourront collecter et recevoir des informations, et les envoyer aux utilisateurs et à d'autres objets connectés. Comme le montre la figure, cette nouvelle ère du développement d'Internet est appelée l'Internet des objets.

Aujourd'hui, plus de 100 millions de distributeurs automatiques, de véhicules, de détecteurs de fumée et d'autres périphériques partagent déjà des informations de manière automatisée. Les analystes du marché de la société Berg Insight estiment que ce chiffre s'élèvera à 360 millions d'ici 2016. Actuellement, les photocopieurs dotés d'un module machine à machine peuvent commander du tonner et du papier automatiquement ou encore avertir les techniciens lors d'une panne en précisant même les pièces à apporter.

10.3.1.2 Acheminement de messages via les réseaux

L'explosion massive des applications s'explique principalement par l'intelligence de l'approche par couches du traitement des données à travers un réseau. Plus précisément, le fait de séparer le rôle de la couche application et le rôle du transport des données permet la modification des protocoles de couche application et le développement de nouvelles applications, sans que le développeur ne doivent se soucier des mécanismes de transmission des données sur le réseau. D'autres couches et donc d'autres développeurs s'en chargent.

Comme le montre la figure, lorsqu'une application envoie une requête à une application serveur, le message est élaboré par la couche application, mais il passe ensuite par toutes les fonctionnalités des différentes couches du client en vue de son acheminement. Lorsqu'il évolue à travers la pile, chaque couche inférieure encapsule les données avec un en-tête contenant les protocoles de communication de la couche. Ces protocoles, qui sont implémentés sur les hôtes émetteurs et récepteurs, interagissent pour fournir un acheminement de bout en bout des applications sur le réseau.

Des protocoles tels que HTTP, par exemple, prennent en charge l'envoi de pages Web vers des périphériques finaux. Maintenant que nous connaissons toutes les couches et leurs rôles, nous pouvons suivre une requête client d'une page Web émise par le serveur Web pour voir le fonctionnement complet et conjoint de ces rôles indépendants.

Dans le modèle TCP/IP, le processus de communication complet se compose de six étapes :

Création des données

La première étape consiste à créer des données au niveau de la couche application du périphérique final source d'origine. Une fois que la requête du client Web, appelée HTTP GET, est établie, ces données sont ensuite codées, compressées et chiffrées si nécessaire. Cette étape relève du protocole de la couche application du modèle TCP/IP, mais elle comprend la fonctionnalité décrite par les couches application, présentation et session du modèle OSI. La couche application transmet ces données sous forme de flux vers la couche transport.

Segmentation et encapsulation initiale

L'étape suivante consiste à segmenter et encapsuler les données lorsqu'elles traversent la pile de protocoles. Au niveau de la couche transport, le message HTTP GET sera fractionné en blocs plus petits et plus faciles à gérer et un en-tête de la couche transport sera ajouté à chacun d'eux. Des indicateurs relatifs au réassemblage du message se trouvent à l'intérieur de cet en-tête, tout comme un identifiant, le numéro de port 80. Il sert à indiquer au serveur de destination que le message est destiné à son application de serveur Web. Un port source généré de manière aléatoire est également ajouté pour garantir que le client peut suivre les réponses et les transmettre à l'application cliente appropriée.

10.3.1.3 Acheminement des données jusqu'au périphérique final

Adressage

Ensuite, les identifiants d'adresse sont ajoutés aux segments, comme le montre la figure. Tout comme il existe plusieurs couches de protocoles qui préparent les données à la transmission vers leur destination, il existe plusieurs couches d'adressage pour garantir leur livraison. Le rôle de la couche réseau consiste à ajouter l'adressage qui permet la transmission des données depuis l'hôte à l'origine des données jusqu'à l'hôte qui les utilise. Pour remplir cette mission, la couche réseau encapsule chaque segment dans un en-tête de paquet IP. L'en-tête de paquet IP contient l'adresse IP des périphériques source et de destination. (L'adresse IP du périphérique de destination est généralement déterminée par un processus d'application précédent, appelé service de noms de domaine). La combinaison des adresses IP source et de destination avec les numéros des ports sources et de destination est appelée une interface de connexion (ou socket). L'interface de connexion sert à identifier le serveur et le service demandés par le client.

10.3.1.4 Acheminement des données à travers l'interréseau

Préparation au transport

Une fois que l'adressage IP est ajouté, le paquet est transmis à la couche d'accès au réseau pour la génération des données sur les supports, comme le montre la figure. Pour ce faire, la couche d'accès au réseau doit d'abord préparer le paquet à la transmission en le plaçant dans une trame comportant un en-tête et une fin. Cette trame contient l'adresse physique de l'hôte source, ainsi que l'adresse physique du tronçon suivant vers la destination finale. Cette opération correspond au rôle de la couche 2 (couche liaison de données) du modèle OSI. La couche 2 est chargée de la livraison des messages sur un réseau local unique. L'adresse de couche 2 est unique sur le réseau local et représente l'adresse du périphérique final sur le support physique. Dans un réseau local qui utilise Ethernet, cette adresse est appelée adresse MAC (Media Access Control). Une fois que la couche d'accès au réseau a préparé la trame à l'aide des adresses sources et de destination, elle convertit la trame en bits, puis en impulsions électriques ou signaux lumineux envoyés sur les supports du réseau.

Transport des données

Les données sont acheminées via l'interréseau, qui se compose de supports et de périphériques intermédiaires. Lorsque le message encapsulé est transmis sur le réseau, il peut traverser plusieurs supports et des types de réseau différents. La couche d'accès au réseau spécifie les techniques permettant de placer la trame sur chaque support et de la récupérer. Ces techniques sont des méthodes de contrôle d'accès aux supports.

Si l'hôte de destination se trouve sur le même réseau que l'hôte source, le paquet est acheminé entre les deux hôtes sur le support local sans nécessiter de routeur. Cependant, si l'hôte de destination et l'hôte source ne se trouvent pas sur le même réseau, le paquet peut être transporté sur plusieurs réseaux, sur différents types de supports et à travers plusieurs routeurs. Lors de leur acheminement sur le réseau, les informations contenues dans la trame ne sont pas modifiées.

À la limite de chaque réseau local, un périphérique réseau intermédiaire, généralement un routeur, désencapsule la trame pour lire l'adresse hôte de destination contenue dans l'en-tête du paquet. Les routeurs utilisent la partie d'identificateur de réseau de cette adresse pour déterminer le chemin à utiliser afin d'atteindre l'hôte de destination. Une fois le chemin déterminé, le routeur encapsule le paquet dans une nouvelle trame et l'envoie au tronçon suivant vers le périphérique final de destination.

10.3.1.5 Acheminement des données jusqu'à l'application adéquate

Acheminement des données jusqu'à l'application de destination adéquate

Enfin, le périphérique final de destination reçoit la trame. Celle-ci passe alors à travers la pile de protocoles qui désencapsule les données et les réassemble. Les données traversent toutes les couches : couche d'accès au réseau, puis couche réseau, puis couche transport et enfin couche application où elles peuvent être traitées. Mais comment le périphérique peut-il être sûr que le processus d'application approprié est identifié ?

Souvenez-vous qu'au niveau de la couche transport, les informations contenues dans l'en-tête de l'unité de données de protocole identifient le processus ou le service spécifique exécuté sur le périphérique hôte de destination qui traitera les données (cf figure). Les hôtes, qu'il s'agisse de clients ou de serveurs sur Internet, peuvent exécuter simultanément plusieurs applications réseau. Les personnes qui utilisent des ordinateurs de bureau exécutent souvent un client de messagerie en même temps qu'un navigateur Web, un programme de messagerie instantanée, des flux multimédias en continu et même parfois un jeu. Tous ces programmes qui s'exécutent séparément constituent des exemples de processus individuels.

L'affichage d'une page Web invoque au moins un processus réseau. Cliquer sur un lien hypertexte entraîne la communication d'un navigateur Web avec un serveur Web. Au même moment, en arrière-plan, un client de messagerie peut envoyer et recevoir un e-mail, et un collègue ou un ami peut être en train d'envoyer un message instantané.

Imaginez un ordinateur ne disposant que d'une interface réseau. Tous les flux de données créés par les applications exécutées sur l'ordinateur entrent et sortent par le biais de cette interface, mais les messages instantanés n'apparaissent pas soudainement au milieu des documents de traitement de texte et les e-mails ne s'affichent pas non plus dans l'interface d'un jeu.

La raison à cela est que les processus individuels exécutés sur les hôtes source et de destination communiquent entre eux. Chaque application ou service est représenté(e) au niveau de la couche 4 par un numéro de port. Un dialogue unique entre des périphériques est identifié par une paire de numéros de port source et de destination de la couche 4, qui représentent les deux applications qui communiquent. Lors de la réception des données sur l'hôte, le numéro de port est examiné pour déterminer quel processus ou application constitue la destination correcte des données.

10.3.1.6 Guerriers du réseau

Il existe une ressource amusante qui vous aide à visualiser les concepts de réseau : l'animation « Warriors of the Net », ou Guerriers du réseau, de TNG Media Lab. Avant de visualiser la vidéo, tenez compte des remarques suivantes. Premièrement, au regard des concepts étudiés dans ce chapitre, demandez-vous à quel moment dans la vidéo vous vous trouvez sur un réseau local, sur un réseau étendu, sur un intranet, sur Internet ; identifiez quels

sont les périphériques finaux par rapport aux périphériques intermédiaires ; comment les modèles OSI et TCP/IP s'appliquent ; quels protocoles sont impliqués.

Deuxièmement, s'il est explicitement fait référence aux numéros de port 21, 23, 25, 53 et 80 dans la vidéo, il n'est fait référence aux adresses IP qu'implicitement. Savez-vous à quel moment ? À quel moment dans la vidéo des adresses MAC sont-elles impliquées ?

Enfin, même si toutes les animations comportent souvent des simplifications, la vidéo comporte une erreur évidente. Au bout de 5 minutes environ, vous entendez le commentaire suivant : « Si M. IP ne reçoit pas la confirmation que le paquet a été reçu dans les délais requis, il en envoie tout simplement une copie. » Il ne s'agit pas d'une fonction du protocole IP de couche 3, qui est « peu fiable » et achemine au mieux les paquets, mais d'une fonction du protocole TCP de la couche transport.

Téléchargez le film sur le site http://www.warriorsofthe.net.

CHAPITRE 11 : IL S'AGIT D'UN RÉSEAU

Introduction

Jusqu'à ce point du cours, nous avons considéré les services qu'un réseau de données peut fournir au réseau humain, examiné les fonctionnalités de chaque couche du modèle OSI et les opérations des protocoles TCP/IP, et observé en détail la technologie Ethernet, une technologie de réseau local universelle. L'étape suivante consiste à apprendre à assembler ces éléments dans un réseau opérationnel gérable.

Avez-vous remarqué… ?

Remarque : les étudiants peuvent effectuer cet exercice individuellement, par deux ou en classe entière.

Observez les deux réseaux représentés dans le schéma. Comparez les deux réseaux à partir de vos observations. Prenez note des périphériques utilisés dans chaque conception de réseau. Comme les périphériques sont étiquetés, vous connaissez déjà les types de périphériques finaux et intermédiaires de chaque réseau.

Mais quelles sont les différences entre les deux réseaux ? Le réseau B contient-il simplement plus de périphériques que le réseau A ?

Sélectionnez le réseau que vous utiliseriez si vous possédiez une PME. Préparez-vous à justifier choix selon les critères suivants : coût, vitesse, nombre de ports, évolutivité et simplicité de gestion.

11.1. Création et développement

11.1.1 Périphériques d'un petit réseau

11.1.1.1 Topologies de petits réseaux

La majorité des entreprises sont des petites entreprises. Il n'est donc pas étonnant que la majorité des réseaux soient de petite taille.

Leur conception est généralement simple. Le nombre et les types de périphériques du réseau sont largement réduits par rapport à un réseau plus étendu. Les topologies des réseaux de petite taille exigent généralement un seul routeur et un ou plusieurs commutateurs. Les réseaux de petite taille peuvent également comporter des points d'accès sans fil (éventuellement intégrés au routeur) et des téléphones IP. En terme de connexion à Internet, les réseaux de petite taille comportent généralement une seule connexion de réseau étendu par DSL, le câble ou une connexion Ethernet.

La gestion d'un réseau de petite taille exige la plupart des compétences requises pour la gestion d'un réseau de plus grande envergure. La maintenance et le dépannage du matériel existant, ainsi que la sécurisation des périphériques et des informations sur le réseau sont les tâches principales. La gestion d'un réseau de petite taille est confiée soit à un employé de l'entreprise soit à un sous-traitant, selon la taille et le type d'entreprise.

Un exemple de réseau classique de petite entreprise est représenté sur la figure.

11.1.1.2 Choix des périphériques d'un réseau de petite taille

Pour répondre aux besoins des utilisateurs, même les réseaux de petite taille doivent faire l'objet d'une planification et d'une conception. La planification garantit que tous les besoins, les facteurs de coûts et les options de déploiement sont pris en compte.

L'un des premiers critères à prendre en compte lors de la mise en œuvre d'un réseau de petite taille est le type de périphériques intermédiaires à utiliser pour le fonctionnement du réseau. Plusieurs facteurs déterminent le choix des périphériques intermédiaires, comme le montre la figure.

Coût

Dans les réseaux de petites entreprises, le coût est généralement l'un des aspects les plus importants. Le coût d'un commutateur ou d'un routeur dépend de sa capacité et de ses fonctionnalités. La capacité de l'équipement fait notamment référence au nombre et aux types de ports disponibles, ainsi qu'à la vitesse de fond de panier. Les autres facteurs déterminant le coût sont ses fonctions de gestion réseau, ses technologies de sécurité intégrées et ses technologies de commutation avancées en option. Le coût des câblages permettant de connecter chaque périphérique au réseau doit également être pris en compte. Enfin, la redondance du réseau a également un impact sur le coût. Elle détermine notamment les équipements, le nombre de ports par appareil et le type de câblage (cuivre ou fibre optique).

Vitesse et types de port/d'interface

Le choix du nombre et du type de ports sur un routeur ou un commutateur est décisif. Il faut notamment se poser les questions suivantes : « Allons-nous commander juste assez de ports pour répondre aux besoins actuels ou également tenir compte de la croissance potentielle ? », « Avons-nous besoin de câbles à paires torsadées non blindées de différents débits ? » et « Avons-nous besoin à la fois de ports en cuivre et à fibre optique ? »

Sur les ordinateurs récents, une carte réseau de 1 Gbit/s est intégrée. Certains ordinateurs et serveurs sont même équipés de ports 10 Gbit/s. Les équipements de couche 2 sont certes plus onéreux, mais ils peuvent gérer des débits supérieurs et permettent au réseau d'évoluer sans remplacer les périphériques centraux.

Évolutivité

Les périphériques réseau sont fournis selon les deux configurations physiques, fixes et modulaires. Les configurations fixes possèdent un nombre de ports et un type de port ou d'interface spécifiques. Les périphériques modulaires possèdent des logements d'extension qui offrent la possibilité d'ajouter de nouveaux modules à mesure que les besoins évoluent. La plupart des périphériques modulaires sont fournis avec un nombre standard de ports fixes et de logements d'extension. Les commutateurs peuvent être équipés de ports supplémentaires spéciaux pour les liaisons montantes haut débit en option. En outre, dans la mesure où les routeurs peuvent être utilisés pour connecter des quantités et des types de réseau différents, vous devez veiller à choisir les modules et les interfaces adaptés aux supports. Les questions à se poser sont notamment les suivantes : « Allons-nous commander des équipements dont les

modules sont évolutifs ? » et « Quel type d'interfaces WAN sont nécessaires sur les routeurs, le cas échéant ? »

Fonctions et services du système d'exploitation

En fonction de la version du système d'exploitation, le périphérique réseau peut prendre en charge certaines fonctions, notamment :

- Sécurité
- QS
- VoIP
- commutation de couche 3
- NAT
- DHCP

Les routeurs peuvent être coûteux en fonction des interfaces et des fonctions nécessaires. Les modules supplémentaires, notamment les modules à fibre optique augmentent le coût des périphériques réseau.

11.1.1.3 Adressage IP d'un réseau de petite taille

Lors de la mise en œuvre d'un réseau de petite taille, il est nécessaire de planifier l'espace d'adressage IP. Tous les hôtes d'un interréseau doivent avoir une adresse unique. Même sur un réseau de petite taille, l'attribution des adresses ne doit pas être aléatoire. Le schéma d'adressage IP doit être planifié, documenté et mis à jour en fonction du type de périphérique recevant l'adresse.

Exemples de différents types de périphériques qui détermineront le modèle IP :

- Périphériques finaux pour les utilisateurs
- Serveurs et périphériques
- Hôtes accessibles depuis Internet
- Périphériques intermédiaires

La planification et la documentation du schéma d'adressage IP aident l'administrateur à repérer les types de périphériques. Par exemple, si tous les serveurs obtiennent une adresse d'hôte de la plage 50 à 100, il est facile d'identifier le trafic des serveurs à l'aide de l'adresse IP. Cela peut s'avérer très utile lors de la résolution de problèmes de trafic réseau via un analyseur de protocole.

En outre, les administrateurs peuvent mieux contrôler l'accès aux ressources du réseau en fonction de l'adresse IP dans un schéma d'adressage IP déterministe. Cet aspect est particulièrement important pour les hôtes qui fournissent des ressources au réseau interne et au réseau externe. C'est notamment le cas des serveurs Web ou serveurs de commerce électronique. Si les adresses de ces ressources ne sont pas préparées et documentées, la sécurité et l'accessibilité des périphériques sont plus difficiles à contrôler. Si un serveur se voit attribuer une adresse aléatoire, le blocage de l'accès à cette adresse est quasiment impossible, et les clients risquent de ne pas être en mesure de localiser cette ressource.

Chacun de ces types de périphériques doit être alloué à un bloc d'adresses logique dans la plage d'adresses du réseau.

Cliquez sur les boutons de la figure pour afficher la méthode d'attribution.

11.1.1.4 Redondance dans un petit réseau

Un autre aspect important de la conception d'un réseau est la fiabilité. Même dans les petites entreprises, le réseau joue un rôle déterminant. La moindre panne du réseau peut coûter très cher. Pour assurer un niveau de fiabilité élevé, la redondance doit être pensée dans la conception du réseau. La redondance permet d'éliminer les points de défaillance uniques. Il existe plusieurs moyens d'assurer la redondance d'un réseau. Elle peut passer par l'installation d'équipements en double, mais elle peut également être assurée par le doublement des liaisons réseau dans les zones critiques, comme le montre la figure.

Plus la taille du réseau est réduite, moins la redondance matérielle risque d'être abordable. Par conséquent, on utilise souvent la redondance des connexions de commutateur entre plusieurs commutateurs du réseau et entre les commutateurs et les routeurs.

En outre, les serveurs disposent souvent de plusieurs ports de carte réseau qui permettent des connexions redondantes avec un ou plusieurs commutateurs. Dans un réseau de petite taille, les serveurs sont généralement déployés en tant que serveurs Web, serveurs de fichiers ou serveurs de messagerie.

Ils offrent en général un seul point de sortie vers Internet via une ou plusieurs passerelles par défaut. Lorsque la topologie comporte un seul routeur, la seule redondance des chemins de couche 3 est permise par l'utilisation de plusieurs interfaces Ethernet internes sur le routeur. Cependant, en cas de panne du routeur, c'est tout le réseau qui est déconnecté d'Internet. Par conséquent, il est conseillé aux petites entreprises de prendre une option à moindre coût chez un second fournisseur d'accès par mesure de sécurité.

11.1.1.5 Considérations liées à la conception d'un petit réseau

Les utilisateurs souhaitent accéder immédiatement à leurs e-mails et aux fichiers qu'ils partagent ou mettent à jour. Pour assurer cette disponibilité, le concepteur du réseau doit procéder ainsi :

Étape 1. S'assurer que les serveurs de messagerie et de fichiers se trouvent dans un emplacement centralisé.

Étape 2. Protéger l'emplacement contre les accès non autorisés par des mesures de sécurité physiques et logiques.

Étape 3. Créer une certaine redondance dans la batterie de serveurs qui garantit qu'en cas de défaillance de l'un des périphériques, les fichiers ne sont pas perdus.

Étape 4. Configurer des chemins d'accès redondants vers les serveurs.

En outre, les réseaux modernes utilisent souvent une forme de voix ou de vidéo sur IP pour la communication avec les clients et les partenaires commerciaux. Ce type de réseau convergent est mis en œuvre sous forme de solution intégrée ou de données brutes supplémentaires superposées sur le réseau IP. L'administrateur réseau doit tenir compte des différents types de

trafic et de leur traitement dans la conception du réseau. Dans un réseau de petite taille, les routeurs et les commutateurs doivent être configurés pour prendre en charge le trafic en temps réel, comme la voix et la vidéo, et ce, séparément du trafic des autres données. En fait, dans une conception de réseau bien pensée, le trafic est classifié de manière précise en fonction des priorités, comme le montre la figure. Les classes de trafic peuvent être aussi spécifiques que les suivantes :

- Transfert de fichiers
- E-mail
- Voix
- Vidéos
- Messagerie
- Transactionnel

En fin de compte, l'objectif de la conception du réseau, quelle que soit sa taille, est d'améliorer la productivité des employés et de réduire le temps d'indisponibilité du réseau.

11.1.2. Protocoles d'un petit réseau

11.1.2.1 Applications courantes d'un petit réseau

L'utilité du réseau dépend des applications qu'il comporte. Comme l'illustre la figure, il existe deux types de programmes ou processus dans la couche application qui permettent d'accéder au réseau : les applications réseau et les services de couche application.

Applications réseau

Les applications sont les programmes logiciels qui permettent aux utilisateurs de communiquer sur le réseau. Certaines applications destinées à l'utilisateur final sont orientées réseau, à savoir qu'elles implémentent des protocoles de couche application et sont capables de communiquer directement avec les couches inférieures de la pile de protocoles. Les clients de messagerie et les navigateurs Web sont des exemples de ce type d'application.

Services de couche application

D'autres programmes peuvent nécessiter l'assistance des services de couche application (par exemple, le transfert de fichiers ou la mise en file d'attente de tâches d'impression réseau). Bien que transparents pour les employés, ces services sont des programmes qui communiquent avec le réseau et préparent les données à transférer. Différents types de données (texte, graphique ou vidéo) nécessitent différents services réseau qui les préparent correctement à être traitées par les fonctions exécutées sur les couches inférieures du modèle OSI.

Chaque application ou service réseau utilise des protocoles qui définissent les normes et les formats de données à utiliser. Sans protocoles, le réseau de données ne disposerait d'aucune méthode commune pour formater et transmettre les données. Pour comprendre le fonctionnement des divers services réseau, il est nécessaire de connaître les protocoles sous-jacents qui régissent ces services.

11.1.2.2 Protocoles courants d'un petit réseau

Une grande partie du travail des techniciens a un rapport avec les protocoles réseau, et ce, quelle que soit la taille du réseau. Les protocoles réseau prennent en charge les services et applications utilisés par les employés d'un petit réseau. Protocoles réseau les plus courants :

- DNS
- Telnet
- IMAP, SMTP, POP (e-mail)
- DHCP
- HTTP
- FTP

Cliquez sur les serveurs de la figure pour afficher une brève description des services réseau assurés par chacun d'eux.
Ces protocoles réseau constituent la boîte à outils indispensable d'un professionnel des réseaux. Chacun des protocoles réseau définit les éléments suivants :

- Processus sur l'une des extrémités d'une session de communication
- Types de message
- Syntaxe des messages
- Signification des champs informatifs
- Comment les messages sont envoyés et la réponse attendue
- Interaction avec la couche inférieure suivante

De nombreuses entreprises ont pris le parti d'utiliser autant que possible les versions sécurisées de ces protocoles. Il s'agit des protocoles HTTPS, SFTP et SSH.

11.1.2.3 Applications en temps réel pour un petit réseau

En plus des protocoles réseau courants décrits précédemment, les entreprises modernes, même les plus petites, utilisent généralement des applications en temps réel pour la communication avec les clients et les partenaires commerciaux. Une petite entreprise ne peut pas forcément assumer le coût d'une solution Cisco Telepresence d'entreprise, mais d'autres applications en temps réel sont abordables et se justifient dans les PME (cf Figure 1). Les applications en temps réel exigent une plus grande planification et des services dédiés (par rapport à d'autres types de données) pour garantir l'acheminement prioritaire du trafic voix et vidéo. Cela signifie que l'administrateur réseau doit s'assurer que l'équipement approprié est installé dans le réseau et que les périphériques réseau sont configurés pour assurer un acheminement prioritaire. La Figure 2 représente les éléments d'un réseau de petite taille prenant en charge les applications en temps réel.

Infrastructure

Pour prendre en charge les applications en temps réel existantes et prévues, l'infrastructure doit être compatible avec les caractéristiques de chaque type de trafic. Le concepteur du réseau doit déterminer si le câblage et les commutateurs existants peuvent prendre en charge le trafic ajouté au réseau. Un câblage pouvant prendre en charge des transmissions gigabit doit pouvoir acheminer le trafic généré, sans nécessiter de changement d'infrastructure. Les commutateurs plus anciens ne prennent pas toujours en charge la technologie Power over

Ethernet (PoE). Un câblage obsolète peut ne pas prendre en charge les besoins en matière de bande passante. Les commutateurs et le câblage nécessiteraient une mise à niveau pour la prise en charge de ces applications.

VoIP

La voix sur IP (VoIP) est mise en œuvre dans les entreprises qui utilisent encore des téléphones traditionnels. La VoIP fait appel à des routeurs compatibles avec les services de voix. Ces routeurs convertissent la voix analogique provenant des signaux téléphoniques traditionnels en paquets IP. Une fois que les signaux sont convertis en paquets IP, le routeur achemine ces paquets entre les emplacements correspondants. La VoIP est beaucoup moins onéreuse que les solutions intégrées de téléphonie IP, mais la qualité des communications ne répond pas aux mêmes normes. Les solutions de voix et vidéo sur IP pour les petites entreprises peuvent par exemple faire appel à Skype et à des versions non professionnelles de Cisco WebEx.

Téléphonie IP

Dans le cas de la téléphonie IP, le téléphone IP effectue lui-même la conversion voix à IP. Dans les réseaux équipés d'une solution intégrée de téléphonie IP, aucun routeur compatible avec les services de voix n'est nécessaire. Les téléphones IP utilisent un serveur dédié pour le contrôle des appels et la signalisation. De nombreux constructeurs proposent désormais des solutions de téléphonie IP dédiées pour les réseaux de petite entreprise.

Applications en temps réel

Pour transporter efficacement des flux multimédias en continu, le réseau doit être en mesure de prendre en charge les applications sensibles aux retards d'acheminement. Les protocoles RTP (Real-Time Transport Protocol) et RTCP (Real-Time Transport Control Protocol) répondent tous deux à cette exigence. Les protocoles RTP et RTCP permettent le contrôle et l'extensibilité des ressources réseau en autorisant l'incorporation des mécanismes de qualité de service (QS). Ces mécanismes QS offrent de précieux outils pour la réduction des problèmes de latence des applications RTSP,

11.1.3 Croissance en de plus grands réseaux

11.1.3.1 Évolutivité d'un petit réseau

La plupart des petites entreprises se développent naturellement et leurs réseaux doivent suivre cette évolution. L'administrateur d'un réseau de petite taille adoptera soit une approche réactive soit une approche proactive selon les dirigeants de la société dont il fait souvent partie. Dans l'idéal, l'administrateur réseau a suffisamment de temps pour prendre des décisions réfléchies concernant l'expansion du réseau en fonction de la croissance de l'entreprise.

Pour faire évoluer un réseau, plusieurs éléments sont nécessaires :

- **Documentation réseau** : topologie physique et logique
- **Inventaire des équipements** : liste des périphériques qui utilisent ou constituent le réseau

- **Budget** : budget informatique détaillé comprenant le budget annuel alloué à l'achat du matériel
- **Analyse du trafic** : les protocoles, les applications et les services, ainsi que leurs exigences respectives en termes de trafic doivent être documentés

Ces éléments servent à éclairer la prise de décision qui accompagne l'évolution d'un petit réseau.

11.1.3.2 Analyse des protocoles d'un petit réseau

La prise en charge et le développement d'un petit réseau requièrent une bonne connaissance des protocoles et des applications réseau exécutés sur le réseau concerné. Même si l'administrateur réseau d'un environnement de petite taille a plus de temps pour analyser l'utilisation réseau de chaque périphérique connecté, il est recommandé d'adopter une approche plus globale faisant appel à un analyseur de protocoles logiciel ou matériel.

Comme le montre la figure, les analyseurs de protocoles permettent à un professionnel des réseaux de compiler rapidement des données statistiques à propos des flux de trafic sur un réseau.

Au moment de déterminer comment gérer le trafic réseau, en particulier s'il se développe, il est important de connaître le type de trafic acheminé sur le réseau, ainsi que le flux de trafic actuel. Si les types de trafic sont inconnus, l'analyseur de protocoles permet d'identifier le trafic et sa source.

Pour déterminer des modèles de flux de trafic, il est recommandé d'observer les points suivants :

- capturer le trafic pendant les périodes de pointe pour obtenir une représentation juste des différents types de trafic ;
- effectuer la capture sur différents segments du réseau, car certaines parties du trafic peuvent être locales sur un segment spécifique.

Les informations collectées par l'analyseur de protocole sont analysées en fonction de la source et la destination du trafic, ainsi que du type de trafic envoyé. L'analyse peut ensuite être utilisée pour déterminer comment améliorer la gestion du trafic. Pour ce faire, il peut être nécessaire de réduire les flux de trafic superflus, voire même de modifier les modèles de flux en déplaçant un serveur, par exemple.

Parfois, le simple fait de déplacer un serveur ou un service vers un autre segment de réseau améliore les performances réseau et répond aux besoins croissants de trafic. D'autres fois en revanche, une intervention plus radicale sera nécessaire, qui peut se traduire par un remodelage du réseau.

11.1.3.3 Évolution des exigences liées aux protocoles

L'administrateur réseau doit non seulement connaître l'évolution des tendances du trafic, mais également l'évolution de l'utilisation du réseau. Comme le montre la figure, l'administrateur réseau d'un petit réseau a la possibilité d'obtenir des « instantanées » informatiques en personne de l'utilisation des applications par la plupart des employés au fil du temps. Ces instantanées comportent généralement les informations suivantes :

- Système d'exploitation + version du système d'exploitation
- Applications non réseau
- Applications réseau
- Utilisation de l'UC
- Utilisation du disque dur
- Utilisation de la RAM

Dans un petit réseau, la documentation des instantanés des employés au fil du temps contribuera largement à informer l'administrateur réseau sur l'évolution des besoins de protocole et sur les flux de trafic associés. Par exemple, il se peut que certains employés utilisent des ressources hors site tels que des réseaux sociaux pour mieux faire la promotion de l'entreprise. Lorsqu'ils ont commencé à travailler dans l'entreprise, ces employés étaient peut-être moins orientés sur la publicité sur Internet. Cette évolution dans l'utilisation des ressources peut obliger l'administrateur réseau à adapter l'allocation des ressources.

L'administrateur réseau est responsable de suivre les besoins d'utilisation du réseau et de flux de trafic, et d'apporter des modifications au réseau afin d'optimiser la productivité des employés lorsque le réseau et l'entreprise se développent.

11.2 Évaluation de la sécurité des périphériques réseau

11.2.1 Évaluation de la sécurité des périphériques réseau

11.2.1.1 Les catégories de menaces à la sécurité du réseau

Qu'ils soient filaires ou sans fil, les réseaux informatiques jouent un rôle essentiel dans la vie quotidienne. Les particuliers comme les entreprises sont dépendants de leurs ordinateurs et de leurs réseaux. Une intrusion par une personne non autorisée peut causer des pannes de réseau et des pertes de productivité coûteuses. Les attaques sur un réseau peuvent être dévastatrices et résulter en une perte de temps et d'argent, parce que des informations ou des ressources importantes sont endommagées ou volées.

Les intrus peuvent accéder à un réseau en exploitant les failles logicielles, en lançant des attaques matérielles ou en devinant l'identifiant et le mot de passe d'un utilisateur. Les intrus qui modifient le logiciel ou tirent profit de vulnérabilités logicielles pour accéder au réseau sont souvent appelés des pirates informatiques.

Une fois que le pirate a accédé au réseau, il existe quatre types de menaces :

- Vol d'informations
- Usurpation d'identité
- Perte / manipulation de données
- Interruption de service

Cliquez sur les images de la figure pour afficher plus d'informations.

Même dans les réseaux de petite taille, il est nécessaire de tenir compte des menaces et des failles de sécurité lors la planification d'une configuration réseau.

11.2.1.2 Sécurité physique

Lorsque vous pensez à la sécurité du réseau ou même à la sécurité des ordinateurs, vous vous représentez peut-être des pirates qui exploitent des vulnérabilités logicielles. Pourtant, la sécurité physique des périphériques peut présenter les mêmes failles, comme le montre la figure. Un pirate peut empêcher l'utilisation de ressources réseau si celles-ci sont physiquement compromises.

Les quatre catégories de menaces physiques sont les suivantes :

- **Menaces matérielles** : dommages physiques aux serveurs, routeurs, commutateurs, installations de câblage et postes de travail.
- **Menaces environnementales** : dues aux températures ou aux taux d'humidité extrêmes.
- **Menaces électriques** : pointes de tension, tension d'alimentation insuffisante (chutes de tension), alimentation non contrôlée (bruit) et coupure totale de l'alimentation.
- **Menaces liées à la maintenance** : mauvaise manipulation des composants électroniques principaux (décharges électrostatiques), absence de pièces de rechange essentielles, câblage de mauvaise qualité et étiquetage peu efficace.

Certains de ces problèmes doivent être traités par une stratégie d'entreprise. D'autres dépendent d'une bonne gestion au sein de l'organisation.

11.2.1.3 Types de faille de sécurité

Les trois principaux risques pour la sécurité du réseau sont les failles, les menaces et les attaques.

Les failles correspondent au degré de vulnérabilité inhérent à tout réseau ou périphérique. Cela concerne les routeurs, les commutateurs, les ordinateurs de bureau, les serveurs et même les périphériques de sécurité.

Les menaces viennent d'individus qui cherchent à exploiter les failles de sécurité et sont capables d'y parvenir. Il est prévisible que de tels individus continueront à rechercher de nouvelles faiblesses et de nouveaux exploits.

Ces menaces sont mises en œuvre à l'aide de différents outils, de scripts et de programmes permettant de lancer des attaques contre des réseaux et leurs périphériques. En général, les périphériques réseau attaqués sont des points d'extrémité tels que des serveurs et des ordinateurs de bureau.

Les vulnérabilités ou faiblesses interviennent principalement sur trois niveaux :

- La technologique

Vulnérabilités - technologie

1 2 3

Faiblesses de sécurité des réseaux :

Faiblesse des protocolesTCP/IP

- Les protocoles HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol (FTP) et ICMP (Internet Control Message Protocol) ne sont pas sécurisés.
- Les protocoles SNMP (Simple Network Management Protocol) et SMTP (Simple Mail Transfer Protocol) sont liés à la structure intrinsèquement non sécurisée sur laquelle le protocole TCP a été conçu.

Faiblesses du système d'exploitation

- Chaque système d'exploitation présente des problèmes de sécurité qui doivent être résolus.
- UNIX, Linux, MacOS, MacOSX, Windows Server2012, Windows7, Windows8
- Ils sont documentés dans les archives de la CERT (Computer Emergency réponse Team) à l'adresse http://www.cert.org.

Faiblesse des équipements réseau

Différents types d'équipement réseau tels que les routeurs, les pare-feu et les commutateurs présentent des failles de sécurité qui doivent être identifiées et protégées. Ces faiblesses concernent la protection des mots de passe, le manque d'authentification, les protocoles de routage et les ouvertures dans les pare-feu.

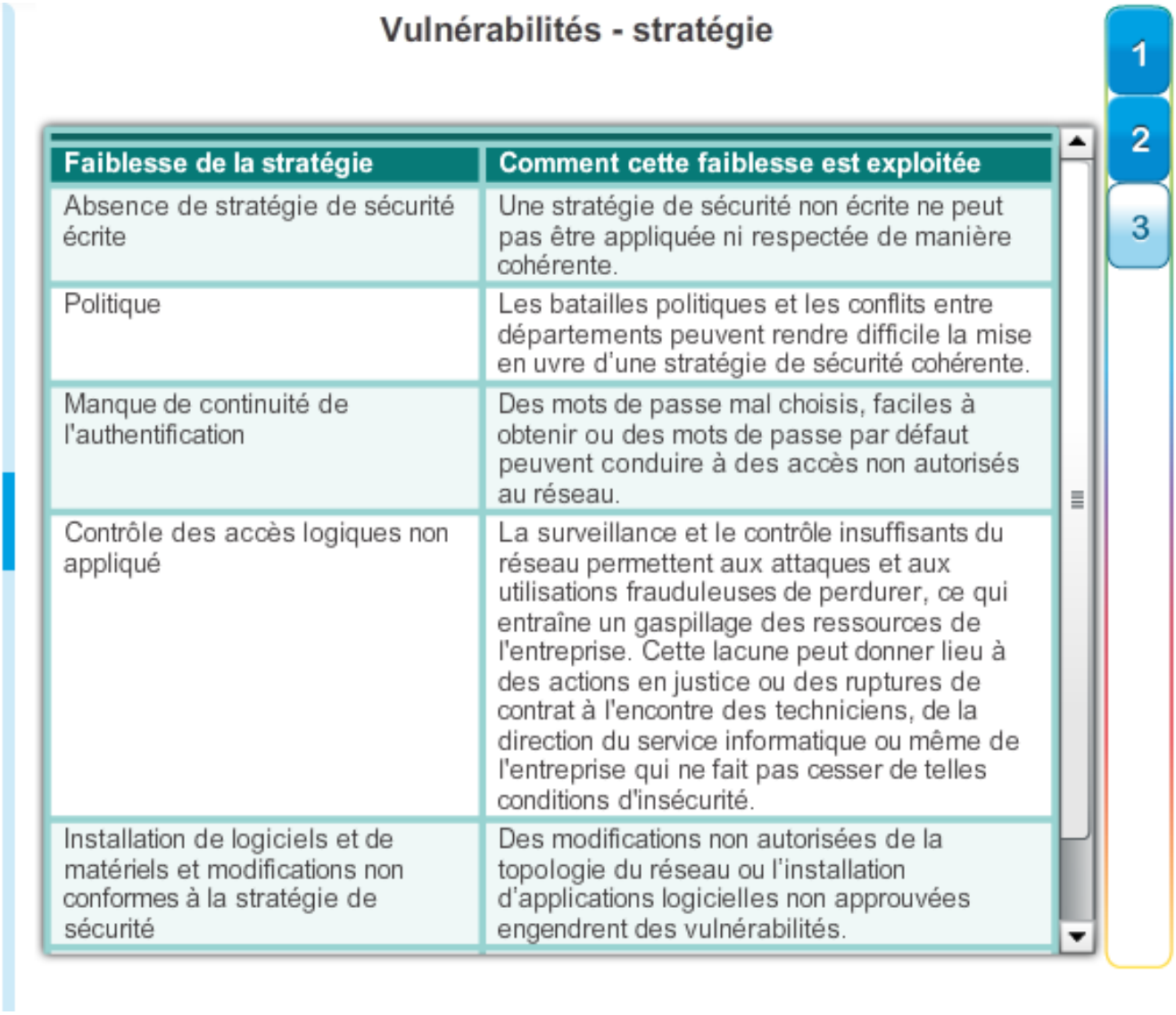
- La configuration

Vulnérabilités - configuration

1 2 3

Faiblesse de la configuration	Comment cette faiblesse est exploitée
Comptes utilisateurs non sécurisés	Les données des comptes utilisateurs peuvent être transmises de manière non sécurisée dans le réseau, ce qui expose les noms d'utilisateur et les mots de passe aux logiciels espions.
Comptes système avec mots de passe faciles à deviner	Ce problème fréquent résulte de mots de passe utilisateur choisis de manière maladroite et qui sont dès lors faciles à deviner.
Services Internet mal configurés	Problème courant: le recours à JavaScript dans les navigateurs Web, qui permet des attaques par des scripts malveillants lors de l'accès à des sites non fiables. Les protocoles IIS, FTP et les services de terminal posent également problème.
Paramètres par défaut non sécurisés dans les produits logiciels	Un grand nombre de produits logiciels ont des paramètres de configuration par défaut qui génèrent des failles de sécurité.
Équipement réseau mal configuré	Les erreurs de configuration du matériel peuvent entraîner d'importants problèmes en matière de sécurité. Par exemple, des listes d'accès, des protocoles de routage ou des chaînes de communauté SNMP mal configurés peuvent ouvrir de larges failles

- La stratégie de sécurité



Vulnérabilités - stratégie

Faiblesse de la stratégie	Comment cette faiblesse est exploitée
Absence de stratégie de sécurité écrite	Une stratégie de sécurité non écrite ne peut pas être appliquée ni respectée de manière cohérente.
Politique	Les batailles politiques et les conflits entre départements peuvent rendre difficile la mise en uvre d'une stratégie de sécurité cohérente.
Manque de continuité de l'authentification	Des mots de passe mal choisis, faciles à obtenir ou des mots de passe par défaut peuvent conduire à des accès non autorisés au réseau.
Contrôle des accès logiques non appliqué	La surveillance et le contrôle insuffisants du réseau permettent aux attaques et aux utilisations frauduleuses de perdurer, ce qui entraîne un gaspillage des ressources de l'entreprise. Cette lacune peut donner lieu à des actions en justice ou des ruptures de contrat à l'encontre des techniciens, de la direction du service informatique ou même de l'entreprise qui ne fait pas cesser de telles conditions d'insécurité.
Installation de logiciels et de matériels et modifications non conformes à la stratégie de sécurité	Des modifications non autorisées de la topologie du réseau ou l'installation d'applications logicielles non approuvées engendrent des vulnérabilités.

1 2 3

Ces trois vulnérabilités ou faiblesses peuvent donner lieu à différentes attaques, notamment des attaques de programmes malveillants et des attaques de réseau.

Garantie de la sécurité du réseau

11.2.2 Failles et attaques du réseau

11.2.2.1 Virus, vers et chevaux de Troie

Les attaques de programmes malveillants peuvent provenir de différents types de programmes informatiques créés dans le but d'entraîner l'endommagement ou la perte de données. Les trois principaux types d'attaques de programmes malveillants sont les virus, les chevaux de Troie et les vers.

Un virus est un logiciel malveillant intégré à un autre programme pour exécuter une fonction indésirable spécifique sur l'ordinateur de l'utilisateur. Par exemple, il peut s'agir d'un programme intégré à command.com (interpréteur de commandes principal des systèmes Windows) qui supprime certains fichiers et infecte toute autre version de command.com qu'il détecte.

Un cheval de Troie se distingue uniquement par le fait qu'il a été entièrement conçu pour ressembler à une application normale, alors qu'il s'agit d'un outil malveillant. Une application logicielle qui exécute un programme de jeu sur un ordinateur peut être un exemple de cheval de Troie. Pendant que l'utilisateur est occupé à jouer, le cheval de Troie envoie une copie de lui-même à tous les contacts du carnet d'adresses de l'utilisateur. Les destinataires reçoivent le jeu et y jouent, ce qui propage le cheval de Troie à toutes les adresses de leur propre carnet.

En principe, un virus a besoin d'un mécanisme de transmission (un vecteur), comme un fichier .zip ou un autre fichier exécutable joint à un e-mail, pour transmettre son code d'un système à l'autre. Le virus informatique se distingue fondamentalement du ver par le fait qu'une interaction humaine est nécessaire pour le propager.

Les vers sont des programmes autonomes qui attaquent un système en tentant d'exploiter une faille spécifique. Lorsque l'exploitation de la vulnérabilité réussit, le ver recopie son programme de l'hôte assaillant vers les systèmes nouvellement exploités et le cycle recommence. Les différentes phases de l'attaque d'un ver sont les suivantes :

- **Activation de la vulnérabilité** : un ver s'installe en exploitant les vulnérabilités connues d'un système, comme des utilisateurs naïfs qui exécutent sans vérification un fichier exécutable joint à un e-mail.

- **Mécanisme de propagation** : l'accès à l'hôte étant acquis, le ver s'y reproduit, puis choisit d'autres cibles.

- **Charge** : une fois l'hôte infecté par un ver, le pirate peut y accéder et bien souvent en tant qu'utilisateur privilégié. Les assaillants peuvent utiliser une faille locale pour augmenter leur niveau de privilèges jusqu'à celui d'administrateur.

11.2.2.2 Attaques de reconnaissance

En plus des attaques de programmes malveillants, les réseaux peuvent également être la proie de différentes attaques de réseau. Les attaques de réseau peuvent être classées en trois catégories principales :

- **Attaques de reconnaissance** : découverte et mappage non autorisés de systèmes, services ou vulnérabilités ;

- **Attaques par accès** : manipulation non autorisée des données, des accès aux systèmes ou des privilèges utilisateur ;

- **Attaques par déni de service** : désactivation ou corruption de réseaux, de systèmes ou de services.

Attaques de reconnaissance

Des pirates externes peuvent utiliser des outils Internet, comme les utilitaires nslookup et whois, pour découvrir facilement les adresses IP attribuées à une entreprise ou à une entité donnée. Une fois ces adresses IP connues, l'assaillant peut lancer des requêtes ping vers les adresses publiquement accessibles pour déterminer celles qui sont actives. Pour automatiser cette étape, l'assaillant peut utiliser un outil de balayage comme fping ou gping, qui envoie systématiquement des requêtes ping à une plage d'adresses ou à toutes les adresses d'un sous-réseau. Cette approche est similaire à celle qui consiste à utiliser un annuaire téléphonique et à appeler tous les numéros pour savoir qui répond.

Cliquez sur chaque type d'outil d'attaque de reconnaissance regarder une animation.

11.2.2.3 Attaques par accès

Attaques par accès

Ces attaques exploitent les vulnérabilités connues des services d'authentification, services FTP et services Web pour accéder à des comptes Web, des bases de données confidentielles et d'autres informations sensibles. Une attaque par accès permet à une personne d'obtenir un accès non autorisé à des informations qu'elle n'a pas le droit de consulter. Il existe quatre types d'attaques par accès. L'un des plus courants est l'attaque de mot de passe. Les attaques de mots de passe peuvent utiliser un analyseur de paquets qui récupère les comptes utilisateur et les mots de passe transmis en clair. Les attaques de mot de passe peuvent également faire référence aux tentatives de connexion répétées à une ressource partagée, comme un serveur ou un routeur, afin d'identifier un compte utilisateur, un mot de passe ou les deux. Ces tentatives répétées sont appelées attaques par dictionnaire ou attaques en force.

Cliquez sur les boutons de la figure pour afficher des exemples d'attaques par accès.

11.2.2.4 Attaques DoS

Déni de service (DoS)

Les attaques par déni de service sont les plus médiatisées, mais également très difficiles à éliminer. Dans la communauté des pirates, ce type d'attaque est même considéré comme trivial et est peu prisé, car son exécution demande peu d'efforts. Toutefois, la facilité de mise en œuvre des attaques DoS et leurs dégâts potentiellement importants doivent retenir toute l'attention des administrateurs de la sécurité.

Les attaques DoS peuvent prendre de nombreuses formes. Elles empêchent l'utilisation d'un service par les personnes autorisées en épuisant les ressources du système.

Cliquez sur les boutons de la figure pour afficher des exemples d'attaques DoS et DDoS.

La limitation des attaques de réseau

11.2.3.1 Sauvegarde, mise à jour, mise à niveau et correctif

Les logiciels antivirus peuvent détecter la plupart des virus et des chevaux de Troie et les empêcher de se propager dans le réseau. Ils peuvent être déployés au niveau de l'utilisateur et au niveau du réseau.

La mise à jour de ces logiciels en fonction des nouveaux développements de virus et chevaux de Troie permet également de se prémunir plus efficacement contre les attaques. De nouvelles attaques de ce type apparaissent sans cesse, c'est pourquoi les entreprises doivent toujours disposer de la version la plus récente de leur logiciel antivirus.

La lutte contre les attaques de vers demande une certaine rigueur du personnel d'administration des systèmes et du réseau. Voici la procédure recommandée pour limiter les attaques de vers :

- **Confinement** : contenir la propagation du ver au sein du réseau en cloisonnant les parties non infectées.

- **Inoculation** : appliquer les correctifs à tous les systèmes, si possible, en recherchant les systèmes vulnérables.

- **Quarantaine** : dépister toutes les machines infectées au sein du réseau. Déconnecter, retirer ou bloquer les machines infectées du réseau.

- **Traitement** : nettoyer tous les systèmes infectés et y appliquer des correctifs. Certains vers peuvent nécessiter une réinstallation complète du système pour le nettoyer.

La meilleure façon de limiter les risques d'attaque de ver est de télécharger les mises à jour de sécurité du fournisseur du système d'exploitation et d'appliquer des correctifs sur tous les systèmes vulnérables. Cette opération est difficile si des systèmes utilisateur non contrôlés se trouvent sur le réseau local. L'administration d'un grand nombre de systèmes implique la création d'une image logicielle standard (système d'exploitation et applications accréditées dont l'utilisation est autorisée sur les systèmes clients) déployée sur les systèmes nouveaux ou mis à niveau. Toutefois, les exigences de sécurité évoluent et il sera peut-être nécessaire d'installer des correctifs de sécurité mis à jour sur les systèmes déjà déployés.

Pour faciliter la gestion des correctifs critiques, il est possible de les centraliser sur un serveur de correctifs auquel tous les systèmes doivent se connecter périodiquement, comme le montre la figure. Tout correctif qui n'est pas encore appliqué à un hôte est alors automatiquement téléchargé depuis le serveur et installé sans intervention de l'utilisateur.

11.2.3.2 Autentification, autorisation et gestion des comptes

Les services de sécurité réseau d'authentification, d'autorisation et de gestion des comptes fournissent la structure principale permettant de mettre en place un contrôle d'accès sur un périphérique réseau. Ces services permettent de contrôler les utilisateurs autorisés à accéder à un réseau (authentification), ce que ces derniers peuvent faire lorsqu'ils sont connectés (autorisation) et les actions qu'ils exécutent lors de l'accès au réseau (gestion des comptes). Les services d'authentification, d'autorisation et de gestion des comptes offrent une évolutivité supérieure à celle des commandes d'authentification AUX, VTY et mode d'exécution privilégiée seules de la console.

Authentification

Les utilisateurs et les administrateurs doivent prouver leur identité. L'authentification peut être implémentée à l'aide de combinaisons de nom d'utilisateur et de mot de passe, de questions d'authentification, de jetons et d'autres méthodes. Par exemple : « Je suis un utilisateur « étudiant ». Je connais le mot de passe qui prouve que je suis un utilisateur « étudiant ». »

Dans un réseau de petite taille, l'authentification locale est souvent utilisée. Dans ce cas, chaque périphérique met à jour sa propre base de données de combinaisons identifiant/mot de passe. Cependant, lorsqu'il existe un certain nombre de comptes d'utilisateur dans une base de données du périphérique local, leur gestion devient complexe. En outre, à mesure que le réseau se développe et davantage de périphériques y sont ajoutés, l'authentification locale devient difficile à maintenir à jour et n'offre pas d'évolutivité. Par exemple, s'il existe 100 périphériques réseau, tous les comptes d'utilisateur doivent être ajoutés sur chacun des 100 périphériques.

Dans les réseaux de plus grande envergure, l'authentification externe est une solution plus évolutive. Celle-ci permet à tous les utilisateurs d'être authentifiés par le biais d'un serveur réseau externe. Les deux options les plus utilisées pour l'authentification externe des utilisateurs sont RADIUS et TACACS+ :

- RADIUS est une norme ouverte qui utilise peu de ressources de processeur et peu de mémoire. Cette méthode est utilisée par un large éventail de périphériques réseau, tels que des commutateurs, des routeurs et des périphériques sans fil.

- TACACS+ est un mécanisme de sécurité qui active des services d'authentification, d'autorisation et de gestion des comptes modulaires. Il fait appel à un démon TACACS+ exécuté sur un serveur de sécurité.

Autorisation

Une fois que l'utilisateur est authentifié, les services d'autorisation déterminent les ressources auxquelles l'utilisateur peut accéder et les opérations qu'il est autorisé à effectuer. Exemple : « L'utilisateur « étudiant » peut accéder au serveur hôte XYZ via Telnet uniquement. »

Accounting

Les services de gestion des comptes consignent les actions de l'utilisateur, notamment les ressources auxquelles il accède et pendant combien de temps, et toutes les modifications apportées. Ces services permettent de contrôler la manière dont les ressources réseau sont utilisées. Exemple : « L'utilisateur « étudiant » a accédé au serveur hôte XYZ via Telnet pendant 15 minutes. »

Le concept des services d'authentification, d'autorisation et de gestion des comptes est similaire à l'utilisation d'une carte de crédit. La carte de crédit identifie qui est autorisé à l'utiliser, combien cet utilisateur peut dépenser et consigne les achats de l'utilisateur (cf figure).

11.2.3.3 Pare-feu

Il est important de protéger les ordinateurs individuels et les serveurs reliés au réseau, mais il convient également de contrôler le trafic en direction et en provenance du réseau.

Le pare-feu est l'un des outils de sécurité les plus efficaces pour protéger les utilisateurs internes du réseau des menaces externes. Un pare-feu se trouve entre deux réseaux, ou plus, et contrôle le trafic entre eux tout en contribuant à éviter les accès non autorisés. Les pare-feu emploient diverses techniques pour déterminer les accès autorisés à un réseau ou les accès à interdire. Ces techniques sont les suivantes :

- **Filtrage des paquets** : interdit ou autorise l'accès selon les adresses IP ou MAC.
- **Filtrage des applications** : interdit ou autorise l'accès à des types d'applications spécifiques en fonction des numéros de ports.
- **Filtrage d'URL** : interdit ou autorise l'accès à des sites Web en fonction d'URL ou de mots clés spécifiques.
- **Inspection dynamique de paquets (SPI)** : les paquets entrants doivent constituer des réponses légitimes aux requêtes d'hôtes internes. Les paquets non sollicités sont bloqués, sauf s'ils sont expressément autorisés. L'inspection SPI peut éventuellement reconnaître et filtrer des types d'attaques spécifiques telles que le déni de service.

Les pare-feu peuvent prendre en charge une ou plusieurs possibilités de filtrage, parmi celles décrites. En outre, les pare-feu effectuent souvent une traduction d'adresses réseau (NAT). Ce mécanisme consiste à traduire (ou convertir) une adresse IP ou un groupe d'adresses IP internes en une adresse IP publique externe envoyée sur le réseau. Cela permet de dissimuler les adresses IP internes aux utilisateurs externes.

Les pare-feu sont disponibles sous plusieurs formes, comme l'illustre la figure.

- **Pare-feu matériel** - Un pare-feu matériel est intégré à un périphérique matériel dédié appelé appareil de sécurité.
- **Pare-feu basé sur un serveur** : un pare-feu basé sur un serveur est constitué d'une application de pare-feu qui s'exécute sur un système d'exploitation réseau tel qu'UNIX ou Windows.
- **Pare-feu intégré** : un pare-feu intégré est mis en œuvre par l'ajout d'une fonction de pare-feu à un périphérique existant, comme un routeur.
- **Pare-feu personnel** - Un pare-feu personnel se trouve sur un ordinateur hôte et n'est pas conçu pour une mise en œuvre sur un réseau local. Il peut être disponible par défaut dans le système d'exploitation ou obtenu auprès d'un vendeur externe.

11.2.3.4 Sécurité des terminaux

Un réseau sécurisé est aussi robuste que sa liaison la plus faible. Les menaces sophistiquées les plus médiatisées sont les menaces externes, telles que les vers Internet et les attaques par déni de service. Pourtant, la sécurisation du réseau interne est aussi importante que la sécurisation du périmètre d'un réseau. Le réseau interne est composé de points de terminaison du réseau, dont certains sont représentés sur la figure. Un point de terminaison, ou hôte, est un système informatique ou un périphérique qui a un rôle de client réseau. Les terminaux courants sont les ordinateurs portables, les ordinateurs de bureau, les serveurs, les smartphones ou encore les tablettes. Si les utilisateurs n'assurent pas la sécurité de leurs points de terminaison, aucune mesure de sécurité ne permettra de garantir la sécurité du réseau.

La sécurisation des points de terminaison est l'une des tâches les plus difficiles d'un administrateur réseau, car elle implique la participation d'humains. L'entreprise doit mettre en place des stratégies bien documentées et les employés doivent en être informés. Ils doivent également être formés sur l'utilisation appropriée du réseau. Les stratégies incluent souvent l'utilisation de logiciels antivirus et la prévention des intrusions sur les hôtes. Des solutions plus complètes de sécurité des points de terminaison reposent sur le contrôle d'accès au réseau.

La sécurité des terminaux nécessite également la sécurisation des périphériques de couche 2 dans l'infrastructure réseau pour empêcher les attaques sur cette couche, notamment les usurpations d'adresse MAC, la saturation de la table d'adresses MAC et l'inondation du réseau local. C'est ce qu'on appelle la limitation des attaques.

Sécurisation des périphériques

11.2.4.1 Initiation à la sécurisation des périphériques

La sécurité du réseau passe par la protection des périphériques réels, y compris les périphériques finaux et intermédiaires, tels que les périphériques réseau.

Lorsqu'un nouveau système d'exploitation est installé sur un périphérique, les paramètres de sécurité sont définis à l'aide des valeurs par défaut. Dans la plupart des cas, le niveau de sécurité correspondant n'est pas suffisant. Sur les routeurs Cisco, la fonction Cisco AutoSecure permet de sécuriser le système, comme décrit sur la figure. Voici quelques étapes simples qu'il convient d'effectuer sur la plupart des systèmes d'exploitation :

- Changement immédiat des noms d'utilisateur et des mots de passe par défaut.
- Accès aux ressources du système limité strictement aux personnes autorisées à utiliser ces ressources.
- Désactivation des services et applications qui ne sont pas nécessaires et désinstallation dans la mesure du possible.

Les correctifs de sécurité doivent être appliqués à tous les périphériques dès leur mise à disposition. Souvent, les périphériques expédiés par les fabricants ont été entreposés pendant un certain temps et ne disposent pas des correctifs les plus récents. Avant leur mise en œuvre,

il est donc important de mettre à jour tous les logiciels et d'installer tous les correctifs de sécurité.

11.2.4.2 Mots de passe

Pour protéger les périphériques réseau, il est important d'utiliser des mots de passe forts. Voici quelques recommandations classiques à suivre :

- Utilisez un mot de passe d'au moins 8 caractères et de préférence au moins 10 caractères. Plus le mot de passe est long, plus il est fort.

- Choisissez des mots de passe complexes. Utilisez une combinaison de lettres majuscules et minuscules, de chiffres, de symboles et d'espaces si elles sont autorisées.

- Évitez la répétition d'un même mot, l'utilisation de mots communs du dictionnaire, les lettres ou les chiffres consécutifs, les noms d'utilisateur, les noms de parents ou d'animaux domestiques, les informations biographiques telles que la date de naissance, les numéros d'identification, les noms d'ancêtre et toute autre information facilement identifiable.

- Faites volontairement des fautes d'orthographe. Par exemple, Smith = Smyth = 5mYth ou Sécurité = 5ecur1te.

- Modifiez régulièrement votre mot de passe. Si un mot de passe devient obsolète sans que le pirate en soit conscient, son champ d'action est limité.

- Ne notez pas les mots de passe sur des bouts de papier conservés à des endroits visibles sur votre bureau ou sur votre écran.

La figure présente des exemples de mots de passe forts et faibles.

Sur les routeurs Cisco, les espaces en début de mot de passe sont ignorés, mais celles situées après le premier caractère sont prises en compte. Par conséquent, vous pouvez utiliser la barre d'espace pour créer un mot de passe fort composé d'une expression de plusieurs mots. C'est ce qu'on appelle une phrase secrète. Il est souvent plus facile de mémoriser une phrase secrète qu'un seul mot. Elle est également plus longue et plus difficile à deviner.

Les administrateurs doivent s'assurer que des mots de passe forts sont utilisés sur le réseau. Pour vérifier la force des mots de passe, ils peuvent utiliser les mêmes outils d'attaque en force que les pirates.

11.2.4.3 Principes de sécurité de base

Lors de la mise en œuvre des périphériques, il est important de respecter toutes les consignes de sécurité définies par l'entreprise. Cela implique que les noms des périphériques permettent une documentation et un suivi faciles, mais assurent également la sécurité. Il n'est pas judicieux de fournir trop d'informations sur l'utilisation du périphérique dans le nom d'hôte. D'autres mesures de sécurité de base doivent également être prises.

Sécurité supplémentaire des mots de passe

Les mots de passe forts sont efficaces uniquement s'ils sont secrets. Plusieurs mesures permettent de s'assurer de leur confidentialité. Tout d'abord, la commande de configuration globale **service password-encryption** empêche les personnes non autorisées de consulter les mots de passe en clair dans le fichier de configuration, comme le montre la figure. Cette commande génère le chiffrement de tous les mots de passe en clair.

En outre, pour garantir la longueur minimale de tous les mots de passe configurés, utilisez la commande **security passwords min-length** en mode de configuration globale.

Les pirates peuvent également obtenir les mots de passe simplement par une attaque en force, en essayant plusieurs mots de passe jusqu'à ce que l'un d'eux fonctionne. Il est possible d'empêcher ce type d'attaque en bloquant les tentatives de connexion au périphérique si un nombre défini d'échecs survient sur une période donnée.

Router(config)# **login block-for 120 attempts 3 within 60**

Cette commande bloque les tentatives de connexion pendant 120 secondes après trois échecs de connexion en l'espace de 60 secondes.

Bannières

Un message de bannière est l'équivalent d'un panneau Entrée interdite. Ces messages sont indispensables pour permettre l'assignation au tribunal de quiconque accède au système de façon inappropriée. Assurez-vous que les messages de bannière sont conformes aux stratégies de sécurité de l'entreprise.

Router(config)# **banner motd #message#**

Exec Timeout

Il est également recommandé de définir des délais d'exécution. Vous indiquez ainsi au périphérique Cisco de déconnecter automatiquement tout utilisateur en ligne en cas d'inactivité pendant le délai défini. Les délais d'exécution peuvent être configurés sur la console, l'interface vty et les ports auxiliaires.

Router(config)# **line vty 0 4**

Router(config-vty)# **exec-timeout 10**

Cette commande déconnecte les utilisateurs au bout de 10 minutes.

```
Router(config)#service password-encryption
Router(config)#security password min-length 8
Router(config)#login block-for 120 attempts 3 within 60
Router(config)#line vty 0 4
Router(config-vty)#exec-timeout 10
Router(config-vty)#end
Router#show running-config
-more-
!
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 exec-timeout 10
 login
```

11.2.4.4 Activer SSH

Accès distant via SSH

L'ancien protocole de gestion à distance des périphériques est Telnet. Ce protocole n'est pas sécurisé. Les données contenues dans un paquet Telnet sont transmises en clair. Un outil comme Wireshark permet d'« analyser » une session Telnet et d'obtenir ainsi les mots de passe. Par conséquent, il est vivement recommandé d'activer SSH sur les périphériques pour assurer la sécurité des accès à distance. Il est possible de configurer un périphérique Cisco de sorte qu'il prenne en charge le protocole SSH, en quatre étapes décrites sur la figure.

Étape 1. Assurez-vous que le routeur dispose d'un nom d'hôte unique, puis spécifiez le nom de domaine IP du réseau à l'aide de la commande **ip domain-name** *domain-name* en mode de configuration globale.

Étape 2. Des clés secrètes unidirectionnelles doivent être générées pour qu'un routeur chiffre le trafic SSH. La clé est l'élément qui permet concrètement de chiffrer et de déchiffrer les données. Pour créer une clé de chiffrement, utilisez la commande **crypto key generate rsa general-keys modulus** *modulus-size* en mode de configuration globale. La signification précise des différentes parties de cette commande est complexe et ne rentre pas dans le cadre du cours, mais pour l'instant, notez simplement que le module détermine la taille de la clé, de 360 à 2 048 bits. Plus le module est grand, plus la clé est sécurisée, mais plus le chiffrement et le déchiffrage des informations sont longs. Il est recommandé d'utiliser un module d'au moins 1 024 bits.

Router(config)# **crypto key generate rsa general-keys modulus 1024**

Étape 3. Créez une entrée de nom d'utilisateur dans la base de données locale à l'aide de la commande **username** *name* **secret** *secret* en mode de configuration globale.

Étape 4. Activez les sessions SSH entrantes à l'aide des commandes de ligne vty **login local** et **transport input ssh**.

Le service SSH du routeur est désormais accessible à l'aide d'un logiciel client SSH.

Performances réseau de base

Les commandes

11.3.1.1 Interprétation des résultats de requête ping

Une fois que le réseau a été mis en œuvre, l'administrateur doit pouvoir tester sa connectivité pour s'assurer qu'il fonctionne correctement. En outre, il est judicieux que l'administrateur documente le réseau.

Les commandes Ping

L'utilisation de la commande **ping** constitue un moyen efficace de tester la connectivité. Cette vérification est souvent appelée « test de la pile de protocoles », puisque la commande **ping** passe de la couche 3 du modèle OSI à la couche 2, puis à la couche 1. La commande ping emploie le protocole ICMP pour vérifier la connectivité.

Bien qu'elle ne permette pas toujours de diagnostiquer précisément la nature du problème, la commande **ping** peut contribuer à l'identification de la cause du problème, ce qui constitue une première étape importante dans le dépannage d'un réseau.

La commande **ping** permet de vérifier la pile de protocoles et la configuration des adresses IPv4 sur un hôte, mais également de tester la connectivité aux hôtes de destination locaux ou distants, comme le montre la figure. D'autres outils susceptibles de fournir davantage d'informations que **ping**, par exemple Telnet ou les commandes de trace, seront expliqués plus en détail plus loin dans ce chapitre.

Indicateurs IOS de la commande ping

Une commande ping émise par l'IOS génère une indication pour chaque écho ICMP envoyé. Les indicateurs employés le plus souvent par IOS sont les suivants :

- **!** – indique la réception d'une réponse d'écho ICMP.
- **.** - indique l'expiration du délai pendant l'attente d'une réponse d'écho ICMP.
- **U** - indique la réception d'un message ICMP d'inaccessibilité.

Le point d'exclamation (**!**) indique que la commande ping a réussi et vérifié la connectivité de la couche 3.

Le point (**.**) peut dénoter des problèmes dans la communication. Il peut par exemple indiquer qu'un problème de connectivité a été rencontré sur le chemin parcouru. Il peut aussi signifier

qu'un routeur situé sur le chemin ne possède pas de route vers la destination et n'a pas envoyé de message ICMP de destination inaccessible. Enfin, il indique parfois que la commande ping a été tout simplement bloquée par la sécurité d'un périphérique.

La lettre **U** indique qu'un routeur situé sur le chemin ne possédait pas de route vers l'adresse de destination ou que la requête ping a été bloquée, et que le routeur a répondu par un message ICMP d'inaccessibilité.

Test de la boucle

La commande **ping** permet de vérifier la configuration IP interne sur l'hôte local. Souvenez-vous que ce test s'effectue en exécutant la commande **ping** sur une adresse réservée appelée adresse de bouclage (127.0.0.1). Ceci permet de vérifier le bon fonctionnement de la pile de protocoles, de la couche réseau à la couche physique (et en sens inverse), sans pour autant envoyer de signal sur les supports.

Les commandes Ping sont saisies sur une ligne de commande.

Utilisez la syntaxe ci-dessous pour envoyer une requête ping à la boucle :

C:\> **ping 127.0.0.1**

Vous obtenez une réponse de ce type :

Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=128

Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=128

Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=128

Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 127.0.0.1 :

Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),

Durée approximative des boucles en millisecondes :

Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms

Le résultat indique que quatre paquets de test de 32 octets ont été envoyés, et ont été renvoyés par l'hôte 127.0.0.1 en moins de 1 ms. TTL est l'abréviation de Time to Live (durée de vie) et définit le nombre de sauts que le paquet ping peut encore effectuer avant d'être abandonné

11.3.1.2 Extensions de la commande ping

Cisco IOS propose un mode « étendu » de la commande ping. Pour entrer dans ce mode, saisissez ping en mode d'exécution privilégié sans spécifier l'adresse IP de destination. Une série d'invites apparaît alors, comme le montre l'exemple suivant. Il suffit d'appuyer sur Entrée pour accepter les valeurs par défaut indiquées. L'exemple ci-dessous montre comment

forcer une requête ping à utiliser 10.1.1.1 comme adresse source (voir R2 sur la figure). L'adresse source d'une requête ping standard serait 209.165.200.226. Ainsi, l'administrateur réseau peut contrôler à distance (à partir de R2) que R1 dispose de la route 10.1.1.0/24 dans sa table de routage.

R2# **ping**

Protocol [ip]:

Target IP address: **192.168.10.1**

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: **y**

Source address or interface: **10.1.1.1**

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 36/97/132 ms

Vous pouvez détecter d'éventuels problèmes de latence en entrant à l'invite un délai d'attente plus long que celui utilisé par défaut. Si l'allongement du délai d'attente de la requête ping permet d'obtenir une réponse, vous pouvez en conclure qu'une connexion existe entre les hôtes, mais que la latence réseau risque de poser problème.

Remarque : si vous saisissez « y » à l'invite « Extended commands », vous obtiendrez davantage d'options utiles au dépannage.

11.3.1.3 Performances de référence du réseau

L'un des moyens les plus efficaces pour surveiller les performances d'un réseau et le dépanner consiste à établir une ligne de base du réseau. Un étalon est un processus permettant d'étudier le réseau à intervalles réguliers pour s'assurer qu'il fonctionne comme prévu. Les performances de référence d'un réseau représentent bien plus qu'un simple rapport détaillant l'état du réseau à un moment donné. La création d'un étalon efficace pour les performances du réseau prend un certain temps. En effet, pour obtenir une image fidèle des performances globales d'un réseau, il convient de mesurer les performances à des moments et des niveaux d'activité variés (Figures 1 et 2).

Les résultats fournis par certaines commandes réseau permettent de recueillir des données qui feront partie de la ligne de base du réseau.

Pour commencer à élaborer un étalon, vous pouvez copier et coller dans un fichier texte les résultats d'une commande telle que ping, traceroute ou tracert. Il est possible d'horodater ces fichiers texte et de les enregistrer dans une archive en vue d'une extraction ultérieure.

Une utilisation efficace de ces informations stockées consiste à comparer les résultats dans le temps (Figure 3). Parmi les éléments dont il faut tenir compte, les messages d'erreur et les temps de réponse d'un hôte à l'autre fournissent des indications précieuses. Par exemple, un accroissement considérable des temps de réponse peut dénoter un problème de latence.

On ne soulignera jamais assez l'importance de la création d'une documentation. La vérification de la connectivité d'hôte à hôte, la détection de problèmes de latence et la résolution des problèmes identifiés sont autant d'expériences susceptibles d'aider un administrateur à faire fonctionner un réseau aussi efficacement que possible.

Les réseaux des entreprises doivent disposer de lignes de base si détaillées qu'elles dépassent largement le cadre de ce cours. Il existe toutefois des outils logiciels de qualité professionnelle pour collecter et gérer les informations d'étalon. Dans ce cours, nous nous limitons à traiter quelques techniques fondamentales et à expliquer le but des étalons.

Les meilleures pratiques en matière d'établissement des étalons sont disponibles ici.

Il est également possible d'obtenir le résultat de la commande **ping** à partir de l'invite IOS, comme le montre Figure 4.

11.3.2.1 Interprétation des messages tracert

Cette commande renvoie une liste des sauts effectués par un paquet acheminé à travers un réseau. La forme de cette commande dépend de l'endroit où elle est soumise. Sur un ordinateur Windows, utilisez **tracert**. À partir de l'interface en ligne de commande d'un routeur, utilisez **traceroute**, comme le montre la Figure 1.

De même que les commandes **ping**, les commandes **trace** sont saisies sur la ligne de commande et admettent une adresse IP comme argument.

Dans l'hypothèse où la commande est envoyée à partir d'un ordinateur Windows, nous employons la forme **tracert** suivante :

C:\> **tracert 10.1.0.2**

Tracing route to 10.1.0.2 over a maximum of 30 hops

1 2 ms 2 ms 2 ms 10.0.0.254

2 * * * Request timed out.

3 * * * Request timed out.

4 ^C

La seule réponse positive reçue a été émise par la passerelle sur le Routeur A. Les requêtes de trace vers le tronçon suivant ont dépassé le délai d'attente, ce qui signifie que le routeur du tronçon suivant n'a pas répondu. Les résultats de la commande trace indiquent donc que le défaut se trouve dans l'interréseau au-delà du réseau local.

Vous pouvez également obtenir le résultat de traceroute à partir de l'invite du routeur, comme le montre la Figure 2.

Commandes Show

11.3.3.1 Révision des commandes show courantes

Les comandes **show** de l'interface de ligne de commande Cisco IOS permettent d'afficher des informations utiles sur la configuration et le fonctionnement du périphérique.

Les techniciens réseau utilisent fréquemment ces commandes **show** pour afficher les fichiers de configuration, vérifier l'état des interfaces et des processus des périphériques et consulter l'état de fonctionnement du périphérique. Les commandes **show** sont disponibles que le périphérique ait été configuré à l'aide de l'interface de ligne de commande ou de Cisco Configuration Professional.

Vous pouvez afficher l'état de presque tous les processus ou fonctions du routeur à l'aide des commandes **show**. Les commandes show les plus couramment utilisées sont notamment :

- **show running-config** (Figure 1)
- **show interfaces** (Figure 2)
- **show arp** (Figure 3)
- **show ip route** (Figure 4)
- **show protocols** (Figure 5)

- **show version** (Figure 6)

Cliquez sur les boutons de la figure pour afficher plus d'informations sur les commandes **show**.

11.3.3.2 Affichage des paramètres du routeur grâce à la commande show version

Une fois le fichier de configuration initiale chargé et le routeur démarré correctement, vous pouvez utiliser la commande **show version** pour vérifier et dépanner certains composants matériels et logiciels de base utilisés au cours du processus de démarrage. Le résultat de la commande **show version** comprend les éléments suivants :

- la version du logiciel Cisco IOS utilisé ;
- la version du logiciel de démarrage système (bootstrap) stocké dans la mémoire vive qui a été utilisé pour démarrer le routeur ;
- le nom de fichier complet de l'image Cisco IOS et l'emplacement auquel le programme d'amorçage l'a recherchée ;
- le type de processeur utilisé sur le routeur et la taille de la mémoire vive. Vous devrez peut-être mettre à niveau la taille de la mémoire vive lors de la mise à niveau du logiciel Cisco IOS ;
- le nombre et le type d'interfaces physiques sur le routeur ;
- la taille de la mémoire vive non volatile (NVRAM). La mémoire vive non volatile sert à stocker le fichier de configuration initiale.
- la taille de la mémoire flash du routeur. Vous devrez peut-être mettre à niveau la taille de la mémoire flash lors de la mise à niveau du logiciel Cisco IOS ;
- la valeur configurée actuellement du registre de configuration du logiciel, au format hexadécimal.

Cliquez sur le bouton Lecture de la figure pour regarder une animation sur l'identification de ces fonctions du résultat de la commande show version.

Le registre de configuration indique au routeur comment démarrer. Par exemple, le paramètre d'usine par défaut pour le registre de configuration est 0x2102. Cette valeur indique que le routeur tente de charger une image du logiciel Cisco IOS à partir de la mémoire flash et essaie de charger le fichier de configuration initiale à partir de la mémoire vive non volatile. Il est possible de modifier le registre de configuration et, par conséquent, de modifier l'emplacement auquel le routeur recherche l'image Cisco IOS et le fichier de configuration initiale au cours du processus de démarrage. S'il existe une deuxième valeur entre parenthèses, celle-ci indique la valeur du registre de configuration à utiliser au cours du prochain rechargement du routeur.

Cliquez sur l'icône Remarque dans le coin inférieur droit de la figure pour obtenir plus d'informations sur le registre de configuration.

11.3.3.3 Affichage des paramètres du commutateur grâce à la commande show version

Sur un commutateur, la commande **show version** affiche des informations sur la version du logiciel actuellement chargée, ainsi que sur le matériel et les périphériques. Cette commande affiche notamment les informations suivantes :

- **Version du logiciel** : version d'IOS
- **Version du bootstrap** : version du programme de démarrage
- **Durée de l'activité du système** - Temps écoulé depuis le dernier redémarrage
- **Informations sur le redémarrage du système** - Méthode de redémarrage (par exemple le cycle d'alimentation ou un incident)
- **Nom de l'image du logiciel** : nom du fichier IOS
- **Type de commutateur et type de processeur** : numéro de modèle et type de processeur
- **Type de mémoire (partagée/principale)** : mémoire vive principale du processeur et mémoire partagée servant de tampon pour les paquets d'E/S
- **Interfaces matérielles** : interfaces disponibles sur le commutateur
- **Registre de configuration** : définit les spécifications du démarrage, la vitesse de la console et des paramètres connexes.

La figure montre un exemple de résultat **show version** classique affiché par un commutateur.

Commandes hôtes et IOS

11.3.4.1 Options de commande ipconfig

Comme le montre la Figure 1, vous pouvez afficher l'adresse IP de la passerelle par défaut d'un hôte en exécutant la commande **ipconfig** sur la ligne de commande d'un ordinateur Windows.

Pour visualiser l'adresse MAC de votre ordinateur, utilisez la commande **ipconfig /all**. Remarque : sur la Figure 2, l'adresse MAC de l'ordinateur est maintenant affichée et accompagnée d'informations sur l'adressage de couche 3 du périphérique. Essayez d'utiliser cette commande.

En outre, le fabricant de l'interface réseau sur l'ordinateur peut être identifié par la partie OUI de l'adresse MAC, qui peut ensuite être recherchée sur Internet.

Le service client DNS sur les PC Windows optimise les performances de la résolution de noms DNS en stockant également en mémoire les noms déjà résolus. La commande **ipconfig /displaydns** affiche toutes les entrées DNS mises en cache sur un système Windows.

11.3.4.2 Options de commande arp

La commande **arp** permet la création, la modification et l'affichage des mappages des adresses physiques aux adresses IPv4 connues. La commande **arp** est exécutée à partir de l'invite de commande Windows.

Pour exécuter une commande **arp**, à l'invite de commande d'un hôte, saisissez la séquence suivante :

C:\host1> **arp -a**

Comme le montre la figure, la commande **arp –a** fournit la liste de tous les périphériques actuellement présents dans le cache ARP de l'hôte, en précisant leur adresse IPv4, leur adresse physique et leur type d'adressage (statique/dynamique).

Pour mettre à jour les informations stockées dans le cache du routeur, l'administrateur réseau peut effacer le cache à l'aide de la commande **arp -d**.

Remarque : le cache ARP ne contient que les informations des périphériques auxquels des utilisateurs ont accédé récemment. Pour être sûr que le cache ARP contient des informations sur un périphérique donné dans sa table ARP, envoyez une requête ping à ce périphérique.

11.3.4.3 Options de commande show cdp neighbors

Examinez le résultat des commandes **show cdp neighbors** sur la Figure 1 avec la topologie de la Figure 2. Notez que R3 a collecté certaines informations détaillées sur R2 et sur le commutateur connecté à l'interface FastEthernet sur R3.

CDP est un protocole propriétaire de Cisco qui s'exécute au niveau de la couche liaison de données. Puisque le protocole CDP fonctionne au niveau de la couche liaison de données, deux périphériques réseau Cisco ou plus, tels que des routeurs prenant en charge différents protocoles de couche réseau, peuvent échanger des informations même si la connectivité de couche 3 n'existe pas.

Lorsqu'un périphérique Cisco démarre, le protocole CDP démarre par défaut. Le protocole CDP détecte automatiquement les périphériques Cisco voisins qui l'exécutent, quels que soient le protocole ou les suites de couche 3 en cours d'exécution. Le protocole CDP échange des informations sur les périphériques matériels et logiciels avec ses voisins CDP connectés directement.

Le protocole CDP fournit les informations suivantes concernant chaque périphérique CDP voisin :

- **Identificateurs de périphériques** : par exemple, le nom d'hôte configuré d'un commutateur.

- **Liste d'adresses** : une adresse de couche réseau maximum pour chaque protocole pris en charge.

- **Identificateur de port** : le nom du port local et distant (sous la forme d'une chaîne de caractères ASCII, comme ethernet0).

- **Liste de capacités** : par exemple, pour savoir si ce périphérique est un routeur ou un commutateur.

- **Plateforme** : plateforme matérielle du périphérique, par exemple, un routeur Cisco série 1841.

La commande **show cdp neighbors detail** indique l'adresse IP d'un périphérique voisin. Le protocole CDP révèle l'adresse IP du voisin, que vous puissiez lui envoyer ou non une requête ping. Cette commande est très utile lorsque deux routeurs Cisco ne peuvent pas router via leur liaison de données partagée. La commande **show cdp neighbors detail** permet de déterminer si l'un des voisins CDP présente une erreur de configuration IP.

Pour les situations de détection réseau, connaître l'adresse IP du voisin CDP suffit souvent pour établir une connexion Telnet avec ce périphérique.

Pour des raisons évidentes, le protocole CDP représente un risque pour la sécurité. Certaines versions d'IOS envoyant des annonces CDP par défaut, il est important de savoir comment désactiver le protocole CDP.

Pour désactiver le protocole CDP globalement, utilisez la commande de configuration globale **no cdp run**. Pour désactiver le protocole CDP sur une interface, utilisez la commande d'interface **no cdp enable.**

11.3.4.4 Utilisation de la commande show ip interface brief

De la même manière que les commandes et les utilitaires sont utilisés pour vérifier la configuration d'un hôte, les commandes peuvent être utilisées pour vérifier les interfaces des périphériques intermédiaires. Cisco IOS fournit plusieurs commandes permettant de vérifier le fonctionnement des interfaces de routeur et de commutateur.

Vérification des interfaces de routeur

Pour vérifier les interfaces d'un routeur, la commande **show ip interface brief** est le plus souvent préférée à la commande **show ip interface**, car ses résultats sont plus abrégés. Elle fournit un résumé des informations clés pour toutes les interfaces réseau d'un routeur.

La Figure 1 présente la topologie utilisée dans cet exemple.

Sur la Figure 2, cliquez sur le bouton R1. Le résultat de la commande **show ip interface brief** affiche toutes les interfaces du routeur, l'adresse IP attribuée à chaque interface et, le cas échéant, l'état opérationnel de l'interface.

D'après le résultat, l'interface FastEthernet 0/0 possède l'adresse IP 192.168.254.254. Les deux dernières colonnes de cette ligne indiquent l'état des couches 1 et 2 de cette interface. La

mention **up** dans la colonne Status indique que cette interface est opérationnelle sur la couche 1. La mention **up** dans la colonne Protocol indique que le protocole de couche 2 est lui aussi opérationnel.

Notez également que l'interface Serial 0/0/1 n'a pas été activée puisque son état indiqué dans la colonne Status est **administratively down**.

De même que dans le cas d'un périphérique final, vous pouvez vérifier la connectivité de couche 3 du routeur avec les commandes **ping** et **traceroute**. Dans cet exemple, les commandes **ping** et **trace** affichent une connectivité fonctionnelle.

Vérification des interfaces de commutateur

Sur la Figure 2, cliquez sur le bouton S1. La commande **show ip interface brief** peut également servir à vérifier l'état des interfaces du commutateur. L'adresse IP du commutateur est appliquée à une interface de réseau local virtuel. Dans ce cas, l'interface Vlan1 obtient l'adresse IP 192.168.254.250, elle a été activée et est opérationnelle.

Le résultat indique également que l'interface FastEthernet0/1 est désactivée. Cela signifie soit qu'aucun périphérique n'est connecté à l'interface soit que l'interface réseau du périphérique connecté à cette interface n'est pas opérationnelle.

En revanche, les résultats affichés pour FastEthernet0/2 et FastEthernet0/3 montrent que ces interfaces sont opérationnelles. Cet état est indiqué par la mention **up** dans les deux colonnes Status et Protocol.

Le commutateur peut aussi tester sa connectivité de couche 3 à l'aide des commandes **show ip interface brief** et **traceroute**. Dans cet exemple, les commandes **ping** et **trace** affichent une connectivité fonctionnelle.

Il est important de garder à l'esprit qu'un commutateur ne doit pas forcément disposer d'une adresse IP pour effectuer son travail de transmission de trame sur la couche 2. L'adresse IP est nécessaire seulement si le commutateur est prévu pour être géré en réseau à l'aide de Telnet ou de SSH. Si l'administrateur réseau a l'intention de se connecter à distance au commutateur à partir d'un emplacement extérieur au réseau local, alors une passerelle par défaut doit également être configurée.

Gestion des fichiers de configuration IOS

Systèmes de fichiers du routeur et du commutateur

11.4.1.1 Systèmes de fichiers du routeur

L'administrateur réseau est non seulement chargé de mettre en œuvre et de sécuriser le réseau de petite taille, mais il doit également gérer les fichiers de configuration. La gestion des fichiers de configuration est importante pour la sauvegarde et la récupération en cas de défaillance d'un périphérique.

Cisco IFS (système de fichiers Cisco IOS) offre une interface unique à tous les systèmes de fichiers utilisés par un routeur, notamment :

- Les systèmes de fichiers de la mémoire Flash
- Les systèmes de fichiers réseau (TFTP et FTP)
- Tout autre terminal permettant la lecture ou l'écriture de données (tel que la mémoire vive non volatile, la configuration en cours, la mémoire morte, etc.)

Avec Cisco IFS, tous les fichiers peuvent être affichés et classés (image, fichier texte, etc.) y compris ceux situés sur des serveurs distants. Par exemple, il est possible d'afficher un fichier de configuration situé sur un serveur distant pour vérifier qu'il s'agit du bon fichier avant de le charger sur le routeur.

Cisco IFS permet à l'administrateur de naviguer dans différents répertoires et d'établir la liste des fichiers d'un répertoire, mais également de créer des sous-répertoires dans la mémoire Flash ou sur un disque. Les répertoires disponibles dépendent du périphérique.

La Figure 1 présente le résultat de la commande **show file systems**, qui répertorie tous les systèmes de fichiers disponibles sur un routeur, le modèle Cisco 1941 dans cet exemple. Cette commande fournit des informations utiles comme la quantité de mémoire disponible, le type de système de fichiers et les autorisations appliquées. Les autorisations sont indiquées dans la colonne Flags du résultat de la commande. Elles peuvent être la lecture seule (ro pour « read only ») ou la lecture et l'écriture (rw pour « read and write »).

Bien que plusieurs systèmes de fichiers soient répertoriés, seuls les systèmes de fichiers TFTP, Flash et NVRAM nous intéressent.

Notez l'astérisque devant le système de fichiers Flash. Il indique qu'il s'agit du système de fichiers par défaut actuel. L'IOS amorçable se trouve dans la mémoire Flash. Par conséquent, le symbole dièse (#) est ajouté à la liste Flash pour indiquer qu'il s'agit d'un disque amorçable.

Le système de fichiers Flash

La Figure 2 présente le contenu du système de fichiers par défaut actuel. Dans le cas présent, il s'agit de la mémoire Flash comme l'indique l'astérisque en début de ligne dans la figure précédente. Plusieurs fichiers se trouvent dans la mémoire Flash, mais seule la dernière liste nous intéresse. Il s'agit du nom de l'image en cours des fichiers Cisco IOS qui s'exécute dans la mémoire vive.

Le système de fichiers NVRAM

Pour afficher le contenu de la mémoire vive non volatile (NVRAM), vous devez modifier le système de fichiers par défaut à l'aide de la commande **cd** (« change directory », changer de répertoire), comme le montre la Figure 3. La commande **pwd** (« present working directory », répertoire courant) confirme que nous consultons le répertoire NVRAM. Enfin, la commande **dir** (« directory », répertoire) affiche la liste du contenu de la mémoire NVRAM. Parmi les différents fichiers affichés, le seul qui présente un intérêt pour nous est le fichier nommé « startup-configuration » qui définit la configuration de démarrage

11.4.1.2 Systèmes de fichiers du commutateur

Avec le système de fichiers Flash du commutateur Cisco 2960, vous pouvez copier les fichiers de configuration et archiver (télécharger) des images logicielles.

La commande permettant d'afficher les systèmes de fichiers sur un commutateur Catalyst est la même que sur les routeurs Cisco : **show file systems**, comme le montre la figure.

De nombreuses commandes de base d'UNIX sont prises en charge sur les commutateurs et les routeurs Cisco : **cd** pour changer de système de fichiers ou de répertoire, **dir** pour afficher les répertoires d'un système de fichiers, et **pwd** pour afficher le répertoire courant

Fichiers de sauvegarde et de restauration de la configuration

Sauvegarde des configurations par capture de texte (Tera Term)

11.4.2.1 Sauvegarde et restauration à l'aide de fichiers texte

Vous pouvez également utiliser Tera Term pour enregistrer/archiver les fichiers de configuration dans un document texte.

Comme le montre la figure, la procédure est la suivante :

Étape 1. Dans le menu File, cliquez sur **Log**.

Étape 2. Choisissez l'emplacement où vous souhaitez enregistrer le fichier. Tera Term commence à capturer le texte.

Étape 3. Après avoir démarré la capture, exécutez la commande **show running-config** ou **show startup-config** à l'invite du mode d'exécution privilégié. Le texte affiché dans la fenêtre du terminal est alors placé dans le fichier choisi.

Étape 4. Une fois la capture terminée, sélectionnez **Close** dans la fenêtre Tera Term:Log.

Étape 5. Affichez le fichier pour vérifier qu'aucun problème n'est survenu.

Restauration des configurations sauvegardées dans un document texte

Il est possible de copier une configuration à partir d'un fichier vers un périphérique. Lorsque vous avez copié la configuration depuis un fichier texte et que vous l'avez collée dans une fenêtre de terminal, IOS exécute chaque ligne de texte de la configuration comme une commande. Il est donc nécessaire de modifier le fichier pour s'assurer que les mots de passe chiffrés apparaissent en clair et supprimer le texte ne correspondant pas à des commandes, par exemple « --More-- » et les messages IOS. Ce processus est expliqué dans les travaux pratiques.

En outre, dans la CLI, le périphérique doit être placé en mode de configuration globale pour recevoir les commandes du fichier texte copié dans la fenêtre de terminal.

Avec Tera Term, la procédure est la suivante :

Étape 1. Dans le menu File, cliquez sur **Send**.

Étape 2. Recherchez le fichier à copier sur le périphérique et cliquez sur **Open**.

Étape 3. Tera Term colle alors le fichier dans le périphérique.

Le texte contenu dans le fichier est appliqué sous forme de commandes dans l'interface en ligne de commande et devient la configuration en cours du périphérique. Cette méthode s'avère pratique pour configurer manuellement un routeur.

11.4.2.2 Sauvegarde et restauration via TFTP

Sauvegarde des configurations via TFTP

Les copies des fichiers de configuration doivent être stockées en tant que fichiers de sauvegarde pour parer à toute éventualité. Les fichiers de configuration peuvent être stockés sur un serveur TFTP (Trivial File Transfer Protocol) ou sur un périphérique de stockage USB. Vous devez également inclure un fichier de configuration dans la documentation du réseau.

Pour enregistrer la configuration en cours ou la configuration de démarrage sur un serveur TFTP, utilisez soit la commande **copy running-config tftp** soit la commande **copy startup-config tftp**, comme le montre la figure. Procédez comme suit pour sauvegarder la configuration en cours sur un serveur TFTP :

Étape 1. Saisissez la commande **copy running-config tftp**.

Étape 2. Entrez l'adresse IP de l'hôte sur lequel le fichier de configuration sera stocké.

Étape 3. Entrez le nom à attribuer au fichier de configuration.

Étape 4. Appuyez sur Entrée pour confirmer chaque choix.

Restauration des configurations via TFTP

Pour restaurer la configuration en cours ou la configuration de démarrage à partir d'un serveur TFTP, utilisez soit la commande **copy tftp running-config** soit la commande **copy tftp startup-config**. Procédez comme suit pour restaurer la configuration en cours à partir d'un serveur TFTP :

Étape 1. Saisissez la commande **copy tftp running-config**.

Étape 2. Saisissez l'adresse IP de l'hôte sur lequel le fichier de configuration est stocké.

Étape 3. Entrez le nom à attribuer au fichier de configuration.

Étape 4. Appuyez sur Entrée pour confirmer chaque choix.

La fonction de stockage USB (Universal Serial Bus) permet à certains modèles de routeurs Cisco de prendre en charge les disques Flash USB. La fonction Flash USB fournit une capacité de stockage secondaire en option et un périphérique d'amorçage supplémentaire. Les images, les configurations et d'autres fichiers peuvent être copiés vers ou depuis une mémoire Flash USB Cisco avec la même fiabilité qu'en utilisant la carte mémoire CompactFlash. En outre, les routeurs à services intégrés modulaires peuvent démarrer n'importe quelle image du logiciel Cisco IOS stockée sur la mémoire Flash USB.

11.4.2.3 Utilisation des ports USB d'un routeur Cisco

Les modules de mémoire Flash USB Cisco sont disponibles en versions 64 Mo, 128 Mo et 256 Mo.

Pour qu'il soit compatible avec un routeur Cisco, un disque Flash USB doit être formaté pour le système de fichiers FAT16. Si ce n'est pas le cas, la commande show file systems affiche une erreur indiquant un système de fichiers incompatible.

Voici un exemple d'utilisation de la commande dir sur un système de fichiers USB :

Router# dir usbflash0:

Directory of usbflash0:/

1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00 c3825-entservicesk9-mz.123-14.T

63158272 bytes total (33033216 bytes free)

La mémoire Flash USB présente l'avantage de pouvoir contenir plusieurs copies de Cisco IOS et plusieurs configurations de routeur. Elle permet à un administrateur de déplacer et de copier facilement les fichiers IOS et les configurations d'un routeur à un autre et bien souvent, le processus de copie est largement plus rapide qu'il ne le serait sur un réseau local ou étendu. Notez qu'IOS n'identifie pas forcément la capacité de la mémoire Flash USB, mais cela ne signifie pas nécessairement que cette mémoire n'est pas prise en charge. En outre, la version des ports USB d'un routeur est généralement USB 2.0, comme sur la figure.

11.4.2.4 Sauvegarde et restauration par USB

Sauvegarde des configurations à l'aide d'un disque Flash USB

Lorsque vous effectuez une sauvegarde vers un port USB, il est recommandé d'exécuter la commande **show file systems** pour vérifier que le disque USB est connecté et pour confirmer son nom, comme à la Figure 1.

Ensuite, utilisez la commande **copy run usbflash0:/** pour copier le fichier de configuration vers le disque Flash USB. Veillez à utiliser le nom du disque Flash tel qu'il apparait dans le système de fichiers. La barre oblique est facultative et indique le répertoire racine du disque Flash USB.

IOS vous invite à indiquer le nom du fichier. Si le fichier existe déjà sur le périphérique USB, le routeur demande s'il peut le remplacer, comme le montre la Figure 2.

Utilisez la commande **dir** pour afficher le fichier sur le disque USB et la commande **more** pour voir le contenu, comme l'illustre la Figure 3.

Restauration des configurations à l'aide d'un disque Flash USB

Afin de pouvoir copier à nouveau le fichier, vous devrez modifier le fichier USB R1-Config dans un éditeur de texte pour en faire un fichier de configuration valide. Si vous omettez cette étape, de nombreuses entrées seront des commandes non valides et aucune interface ne sera affichée.

R1# **copy usbflash0:/R1-Config running-config**

Destination filename [running-config]?

Services de routage intégrés

Routeur intégré

11.5.1.1 Périphérique multifonction

L'utilisation des réseaux n'est pas limitée aux entreprises.

Les particuliers tirent eux aussi de plus en plus profit des technologies réseau. Les réseaux domestiques sont utilisés pour assurer la connectivité et le partage d'Internet entre plusieurs ordinateurs de bureau et portables personnels dans une habitation. Ils permettent également aux particuliers de profiter de différents services tels que le partage d'une imprimante réseau ou le stockage centralisé de photos, de musiques et de films sur un appareil de stockage en réseau (NAS). Ils offrent également un accès à Internet à d'autres périphériques d'utilisateur final, tels que les tablettes, les smartphones et même des appareils domestiques tels que les téléviseurs.

Un réseau domestique est très similaire à un réseau de petite entreprise. Cependant, la plupart des réseaux domestiques et de nombreux réseaux de petites entreprises n'exigent aucun périphérique de grande envergure tels que des routeurs et des commutateurs dédiés. Les périphériques de plus petite envergure sont suffisants tant qu'ils intègrent les mêmes fonctions de routage et de commutation. De ce fait, de nombreux réseaux domestiques et de petites entreprises utilisent un périphérique multifonction.

Pour les besoins de ce cours, les périphériques multifonctions seront désignés sous le nom de « routeurs intégrés ».

L'utilisation d'un routeur intégré revient en quelque sorte à disposer de plusieurs périphériques interconnectés. Par exemple, la connexion entre le commutateur et le routeur est mise en œuvre, mais de manière interne. Lorsqu'un paquet est transmis d'un périphérique à un autre sur le même réseau local, le commutateur intégré transmet automatiquement le paquet au

périphérique de destination. Toutefois, si un paquet est transmis à un périphérique sur un réseau distant, le commutateur intégré transmet ensuite le paquet à la connexion interne du routeur. Le routeur interne détermine alors le meilleur chemin et achemine le paquet en conséquence.

La plupart des routeurs intégrés proposent à la fois une commutation filaire et une connexion sans fil. Ils servent alors de point d'accès (AP) au réseau sans fil, comme le montre la Figure 1. La connexion sans fil est un moyen répandu, flexible et économique de fournir des services réseau aux périphériques finaux pour les particuliers comme les entreprises.

Les Figures 2 et 3 présentent les principaux avantages et considérations liés à l'utilisation de connexions sans fil.

Outre le routage, la commutation et la connexion sans fil, un routeur intégré peut proposer de nombreuses fonctionnalités, notamment : le service DHCP, un pare-feu et même des services de stockage en réseau.

11.5.1.2 Types de routeur intégré

La gamme des routeurs intégrés s'étend des petits périphériques adaptés à des environnements informatiques de particuliers et de petites entreprises aux périphériques plus puissants, qui prennent en charge des succursales de grosses sociétés.

Le routeur sans fil Linksys est un exemple de routeur intégré illustré par la figure. Il s'agit d'un routeur intégré de conception simple et n'est généralement pas équipé de composants séparés, ce qui réduit le coût du périphérique. Toutefois, en cas de panne, il est impossible de remplacer uniquement le composant défectueux. De ce fait, les routeurs intégrés créent un point de défaillance unique et ne sont pas optimisés pour toutes les fonctions.

Le routeur de services intégré ISR de Cisco est un autre exemple de routeur intégré. La gamme ISR de Cisco est complète et offre des produits conçus aussi bien pour les environnements informatiques de particuliers et de petites entreprises que pour les plus grands réseaux. De nombreux routeurs ISR sont modulables et ont des composants distincts pour chaque fonction, par exemple un commutateur et un routeur. Cela permet d'ajouter, de remplacer et de mettre à niveau les composants séparément.

Tous les routeurs intégrés offrent des paramètres de configuration de base, tels que les mots de passe, les adresses IP et les paramètres DHCP. Ceux-ci sont identiques, que le périphérique soit utilisé pour une connexion filaire ou sans fil des hôtes. Cependant, si vous utilisez la fonctionnalité sans fil, des paramètres de configuration supplémentaires sont nécessaires, notamment le réglage du mode sans fil, du SSID et du canal sans fil.

11.5.1.3 Fonctionnalités sans fil

Mode sans fil

Le mode sans fil consiste à définir la norme sans fil IEEE 802.11 qui sera utilisée par le réseau. Quatre amendements ont été apportés à la norme IEEE 802.11 et décrivent différentes

caractéristiques des communications sans fil. Il s'agit de 802.11a, 802.11b, 802.11g et 802.11n. La Figure 1 fournit davantage d'informations sur chaque norme.

La plupart des routeurs sans fil intégrés prennent en charge les normes 802.11b, 802.11g et 802.11n. Ces trois technologies sont compatibles, mais tous les périphériques du réseau doivent utiliser la même norme. Par exemple, si un routeur 802.11n est relié à un ordinateur portable selon la norme 802.11n, le réseau fonctionne conformément à la norme 802.11n. Ajoutons maintenant une imprimante sans fil 802.11b au réseau. Le routeur et l'ordinateur portable repasseront à la norme 802.11b moins rapide pour toutes les communications. Par conséquent, si des périphériques sans fil d'ancienne génération restent connectés au réseau, l'intégralité du réseau sera ralentie. Il est important de garder cela à l'esprit lorsque vous prenez la décision de garder ou non des périphériques sans fil anciens.

SSID

De nombreux autres réseaux sans fil peuvent être disponibles dans la zone où vous vous trouvez. Il est important que les périphériques sans fil se connectent au réseau local sans fil approprié. Pour ce faire, un identifiant SSID (Service Set Identifier, identifiant de l'ensemble de services) est utilisé.

Le SSID est un nom alphanumérique sensible à la casse attribué à votre réseau sans fil domestique. Le nom peut contenir jusqu'à 32 caractères. Le SSID est utilisé pour indiquer aux périphériques sans fil à quel réseau local sans fil ils appartiennent et avec quels autres périphériques ils peuvent communiquer. Quel que soit le type d'installation WLAN utilisée, tous les périphériques sans fil du réseau local sans fil doivent être configurés avec le même SSID pour pouvoir communiquer entre eux.

Canal sans fil

Pour créer des canaux, il suffit de diviser en différentes sections le spectre des radiofréquences disponible. Chaque canal peut transmettre une conversation différente. Ce fonctionnement est similaire à celui d'une télévision, où les différentes chaînes sont diffusées via un support unique. Plusieurs points d'accès peuvent fonctionner à proximité les uns des autres, dans la mesure où ils utilisent différents canaux de communication.

11.5.1.4 Sécurité sans fil de base

Avant de connecter le point d'accès au réseau ou au FAI, vous devez prévoir et configurer des mesures de sécurité.

Comme le montre la Figure 1, il existe des mesures de sécurité de base, notamment :

- Modification de la valeur par défaut des SSID, des identifiants et des mots de passe
- Désactivation de la diffusion SSID
- Configuration du chiffrement WEP ou WPA

Le chiffrement est un processus consistant à transformer les données afin qu'elles soient inutilisables si elles sont interceptées.

WEP (Wired Equivalency Protocol)

Le protocole WEP est une fonction de sécurité sophistiquée qui permet de chiffrer le trafic réseau lors de sa transmission aérienne. Le WEP utilise des clés préconfigurées pour chiffrer et déchiffrer les données, comme le montre la Figure 2.

La clé WEP saisie est une chaîne alphanumérique, généralement d'une longueur de 64 ou 128 bits. Dans certains cas, le protocole WEP prend également en charge les clés 256 bits. Pour simplifier la création et la saisie de ces clés, de nombreux périphériques proposent une option Phrase de passe. La phrase de passe est un moyen simple pour mémoriser le mot ou la phrase utilisé(e) pour générer automatiquement une clé.

Pour pouvoir utiliser la fonction WEP, la même clé WEP doit avoir été saisie pour le point d'accès et tout périphérique sans fil autorisé à accéder au réseau. Sans cette clé, les périphériques ne pourront pas comprendre les transmissions sans fil.

Cependant, cette fonction présente quelques inconvénients, notamment le fait d'utiliser une clé statique sur tous les périphériques compatibles WEP. Il existe des applications qui permettent aux pirates de découvrir la clé WEP. Ces applications se trouvent facilement sur Internet. Une fois que le pirate a extrait la clé, il dispose d'un accès complet aux données transmises.

Il convient donc de changer de clé fréquemment pour mieux se protéger. Il est également possible d'utiliser un mode de chiffrement plus sophistiqué et plus sûr, appelé WPA (Wi-Fi Protected Access).

Fonction WPA (Wi-Fi Protected Access)

La fonction WPA utilise également des clés de chiffrement entre 64 et 256 bits. Cependant, contrairement au protocole WEP, le WPA génère de nouvelles clés dynamiques à chaque fois qu'un client tente d'établir une connexion au point d'accès. C'est pourquoi la fonction WPA, beaucoup plus difficile à pirater, est jugée plus sûre que le protocole WEP.

Plusieurs autres mesures de sécurité peuvent être configurées sur un point d'accès sans fil, notamment le filtrage des adresses MAC, l'authentification et le filtrage du trafic. Cependant, celles-ci sortent du cadre de ce cours.

Configuration du routeur intégré

11.5.2.1 Configuration du routeur intégré

Les routeurs sans fil Linksys sont des périphériques répandus à la fois dans les réseaux des particuliers et des petites entreprises. Nous nous servirons donc de l'un d'eux dans ce cours pour montrer les configurations de base d'un routeur intégré. En général, les appareils Linksys sont équipés de quatre ports Ethernet pour les liaisons filaires, et servent également de point d'accès sans fil. Ils remplissent également les fonctions d'un serveur DHCP et d'un mini serveur Web prenant en charge une interface graphique utilisateur (GUI) Web.

Accès à un routeur Linksys et configuration

Pour commencer, accédez au routeur à l'aide d'un câble reliant un ordinateur à l'un des ports Ethernet du réseau local du routeur, comme l'illustre la figure. Une fois câblé, l'ordinateur connecté obtiendra automatiquement des informations d'adressage IP de la part du routeur intégré, notamment l'adresse de la passerelle par défaut. Celle-ci correspond à l'adresse IP du périphérique Linksys. Vérifiez les paramètres réseau de l'ordinateur à l'aide de la commande **ipconfig /all** pour obtenir cette adresse. Vous pouvez maintenant saisir cette adresse IP dans un navigateur Web sur l'ordinateur pour accéder à l'interface utilisateur Web de configuration.

Une configuration par défaut est définie sur le périphérique Linksys et permet l'utilisation de services de routage et de commutation de base. Par défaut, l'appareil est également configuré pour remplir les fonctions d'un serveur DHCP. Les tâches de configuration de base, telles que modifier l'identifiant et le mot de passe par défaut, modifier l'adresse IP par défaut de l'appareil Linksys ou même les plages d'adresses IP DHCP par défaut doivent être effectuées avant la connexion du point d'accès au réseau actif

11.5.2.2 Activation de la connectivité sans fil

Pour activer la connectivité sans fil, le mode sans fil, le SSID, le canal de transmission et un dispositif de chiffrement doivent être configurés.

Tout d'abord, sélectionnez le mode sans fil voulu, comme le montre la figure. Chaque mode ou norme sans fil est associé à une certaine surcharge. Si tous les périphériques du réseau utilisent la même norme, le fait de sélectionner le mode associé à cette norme limite la surcharge occasionnée. Cela permet également de renforcer la sécurité dans la mesure où les périphériques utilisant des normes différentes ne seront pas autorisés à se connecter. Toutefois, si des périphériques utilisant des normes différentes doivent accéder au réseau, il convient de choisir le mode mixte. Les performances du réseau seront diminuées en raison de la surcharge induite par la prise en charge de tous les modes.

Ensuite, définissez le SSID. Tous les périphériques qui souhaitent participer au réseau local sans fil doivent utiliser le même SSID. Pour des raisons de sécurité, le SSID par défaut doit être modifié. Pour faciliter la détection du réseau étendu par les clients, le SSID est diffusé par défaut. Il est toutefois possible de désactiver la fonction de diffusion du SSID. Si le SSID n'est pas diffusé, cette valeur devra être configurée manuellement sur les clients sans fil.

Le choix du canal de transmission du routeur intégré doit être effectué par rapport aux autres réseaux sans fil à proximité.

Les réseaux sans fil adjacents doivent faire appel à des canaux indépendants (qui ne se chevauchent pas) pour optimiser le débit. La plupart des points d'accès proposent désormais plusieurs canaux pour permettre au routeur de détecter automatiquement le canal le moins encombré.

Enfin, sélectionnez le mécanisme de chiffrement de votre choix et saisissez une clé ou une phrase secrète.

11.5.2.3 Configuration d'un client sans fil

Configuration d'un client sans fil

Un hôte sans fil, ou client correspond à tout périphérique contenant une carte réseau sans fil et un logiciel client sans fil. Ce logiciel client permet au périphérique matériel de participer au réseau local sans fil. Les périphériques peuvent être des smartphones, des ordinateurs portables, des ordinateurs de bureau, des imprimantes, des téléviseurs, des consoles de jeu et des tablettes.

Pour qu'un client sans fil puisse se connecter au réseau étendu sans fil, les paramètres de configuration du client doivent correspondre à ceux du routeur sans fil, notamment au SSID, aux paramètres de sécurité et aux informations du canal (si celui-ci a été configuré manuellement). Ces paramètres sont spécifiés dans le logiciel client.

Le logiciel client sans fil utilisé peut être intégré au système d'exploitation du périphérique, ou il peut s'agir d'un logiciel utilitaire sans fil autonome et téléchargeable, spécifiquement conçu pour l'interaction avec les cartes réseau sans fil.

Une fois le logiciel client configuré, vérifiez la liaison entre le client et le point d'accès.

Ouvrez la fenêtre contenant les informations sur la liaison sans fil, qui indique notamment le débit de données, l'état de la connexion et le canal sans fil utilisé, comme l'illustre la figure. La fonction d'informations sur la liaison, si disponible, affiche en temps réel la puissance et la qualité du signal sans fil.

Outre l'état de la connexion sans fil, vous pouvez également vérifier que les données sont correctement transmises. L'un des principaux tests permettant de vérifier la bonne transmission des données est le test ping. Si le ping réussit, la transmission des données est possible.