Réseaux (**CCNA**)

Olivier Roques

2017

Table des matières

Chapitre 1

Exploration du réseau

1.1 Connecté au monde entier

Tous les ordinateurs connectés à un réseau et qui participent directement aux communications transmises sur le réseau sont des hôtes. Les hôtes sont également appelés des périphériques finaux.

Clients Les clients sont des ordinateurs équipés d'un logiciel qui leur permet de demander des informations auprès du serveur et de les afficher.

Serveurs Les serveurs sont des ordinateurs équipés de logiciels leur permettant de fournir des informations, comme des messages électroniques ou des pages web, à d'autres périphériques finaux sur le réseau.

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.

1.2 LAN, WAN et Internet

1.2.1 Composants réseaux

L'infrastructure réseau comprend trois catégories de composant réseau.

Les périphériques et les supports représentent les éléments physiques ou le matériel du réseau. Le matériel correspond souvent aux composants visibles de la plate-forme 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.

Les services incluent de nombreuses applications de réseau courantes utilisées quotidiennement, comme les services d'hébergement de messagerie et les services d'hébergement web.

Périphériques finaux Un périphérique final est la source ou la destination d'un message transmis sur le réseau. Pour qu'il soit possible de distinguer les périphériques finaux, chaque périphérique final présent sur un réseau est identifié à l'aide d'une adresse. Lorsqu'un périphérique final initie une communication, il utilise l'adresse du périphérique final de destination afin de spécifier l'emplacement où le message doit être envoyé.

Périphériques intermédiaires finaux Les périphériques intermédiaires connectent les périphériques finaux individuels au réseau et peuvent connecter plusieurs réseaux individuels afin de former un interréseau. Ils fournissent la connectivité et s'assurent que les données sont transmises sur le réseau.

Les périphériques intermédiaires utilisent l'adresse du périphérique final de destination, ainsi que les informations concernant les interconnexions réseau, pour déterminer le chemin que doivent emprunter les messages à travers le réseau.

Le matériel de base Voici le matériel usuel utilisé :

- **Concentrateur (hub)** : Le concentrateur permet de relier plusieurs ordinateurs entre eux. Il reçoit des données par un port, et envoie ce qu'il reçoit aux autres.
- **Commutateur (switch)** : Le commutateur fonctionne comme le concentrateur, sauf qu'il transmet des données aux destinataires en se basant sur leurs adresses MAC (adresses physiques). Chaque machine reçoit seulement ce qui lui est adressé.
- **Routeur** : Le routeur permet d'assurer la communication entre différents réseaux pouvant être fondamentalement différents (réseau local et Internet).
- **Répéteur** : Le répéteur reçoit des données par une interface de réception et les renvoie plus fort par l'interface d'émission.

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 :

- fils métalliques réunis en câbles ;
- fibres de verre ou plastiques ;
- transmission sans fil.

Représentation du réseau Les schémas de réseau utilisent souvent des symboles, tels que ceux qui sont présentés à la figure 1.1, pour représenter les périphériques et les connexions qui composent un réseau. On appelle ce type de schéma de réseau des diagrammes de topologie.

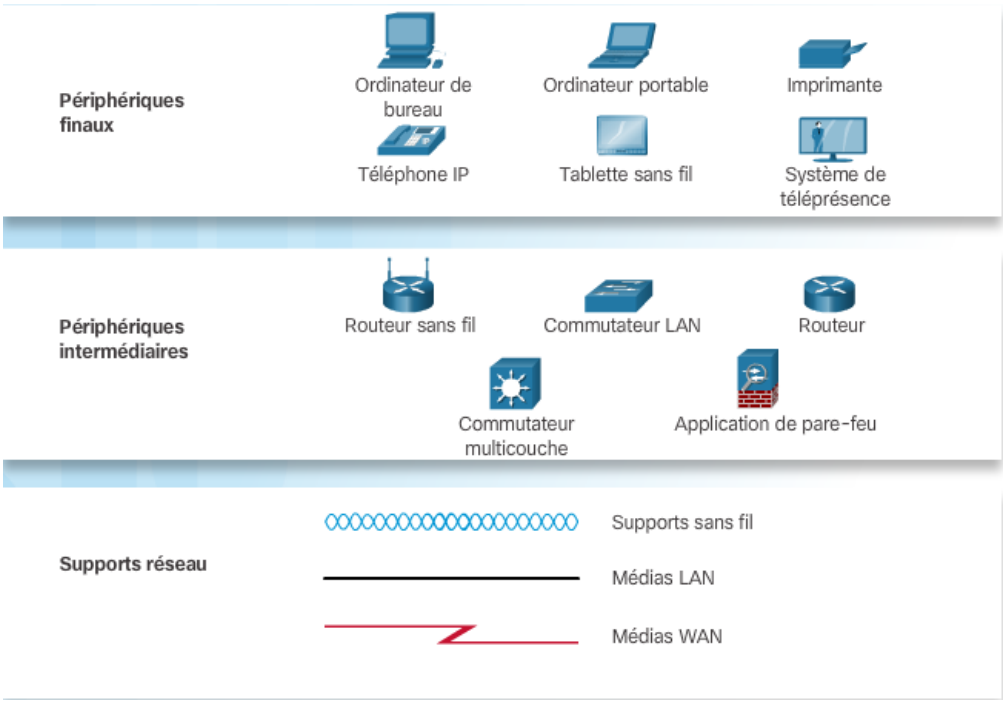


FIGURE 1.1 – Symboles des composantes d'un réseau

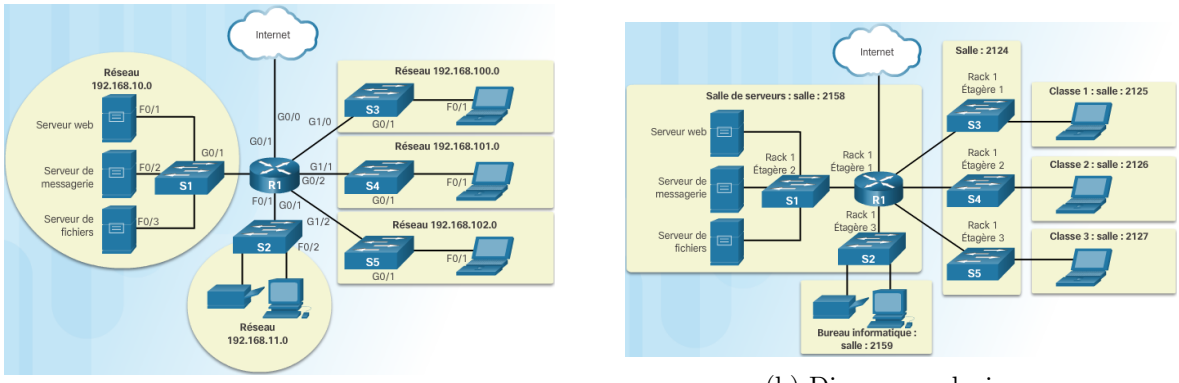
En plus de ces représentations, une terminologie spécialisée est utilisée pour étudier la manière dont ces périphériques et supports se connectent entre eux. Les termes importants dont il faut se souvenir sont les suivants :

- **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 final. 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 périphérique final ou à autre périphérique réseau.
- **Interface** : ports spécifiques sur un périphérique réseau qui se connectent à des réseaux individuels. Puisque les routeurs sont utilisés pour interconnecter des réseaux, les ports sur un routeur sont appelés des interfaces réseau.

1.2.2 Schémas de topologie

Les diagrammes de topologie 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 et des câbles (figure 1.2a).
- **Diagrammes de topologie logique** : identifient les périphériques, les ports, et le schéma d'adressage (figure 1.2b).



(a) Diagramme physique

(b) Diagramme logique

FIGURE 1.2 – Les deux types de schémas de topologie

1.2.3 LAN et WAN

Types de réseau Les infrastructures réseau peuvent considérablement varier en fonction des paramètres suivants :

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

Les deux types d'infrastructure réseau les plus courants sont :

- **LAN** (Local Area Network) ou réseau local : infrastructure réseau reliant les utilisateurs et les périphériques finaux dans une zone géographique peu étendue.
- **WAN** (Wide Area Network) ou réseau étendu : infrastructure réseau permettant d'accéder à d'autres réseaux au sein d'une zone géographique étendue.

1.2.4 Internet

Internet est un ensemble de réseaux interconnectés à l'échelle internationale (interréseaux, dont le terme Internet est une abréviation). La figure 1.3 illustre une façon de représenter l'Internet comme un ensemble de réseaux locaux et étendus interconnectés. Garantir une communication efficace sur cette infrastructure hétérogène requiert l'application de technologies et de normes cohérentes et communément reconnues, ainsi que la coopération entre de nombreux organismes gouvernementaux.

1.3 Réseau en tant que plate-forme

Les réseaux doivent prendre en charge une large gamme d'applications et de services, et fonctionner sur les nombreux et différents câbles et périphériques qui constituent l'infrastructure physique. Dans le contexte actuel, l'expression « architecture réseau » désigne aussi bien les technologies prenant en

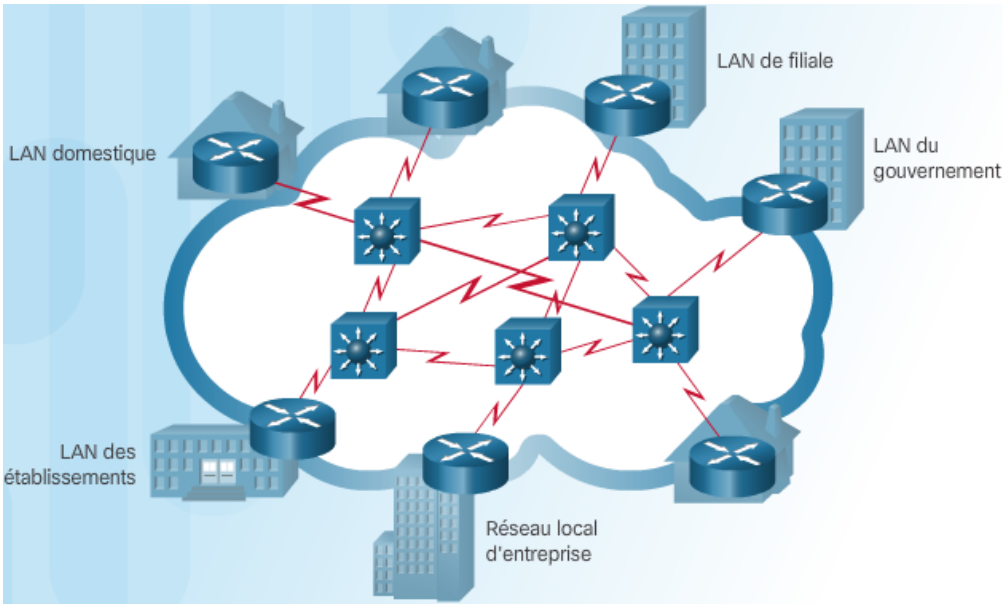


FIGURE 1.3 – Une représentation d'Internet

charge l'infrastructure que les services programmés et les règles, ou protocoles, qui font transiter les données sur le réseau.

À mesure 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 ;
- évolutivité ;
- qualité de service (QoS) ;
- sécurité.

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. 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. Le fait de disposer de plusieurs chemins vers une destination s'appelle la redondance.

L'un des moyens pour les réseaux fiables d'assurer la redondance consiste à mettre en œuvre un réseau à commutation de paquets. La commutation de paquets fractionne le trafic en paquets qui sont acheminés sur un réseau partagé. Chaque paquet comporte les informations d'adressage nécessaires de la source et de la destination du message. Les routeurs du réseau commutent les paquets en fonction de l'état du réseau à ce moment-là.

Ce n'est pas le cas dans les réseaux à commutation de circuits utilisés traditionnellement pour les communications voix. Un réseau à commutation de circuits établit un circuit dédié entre la source et

la destination de sorte que les utilisateurs puissent communiquer. Si l'appel est interrompu de façon imprévue, les utilisateurs doivent établir une nouvelle connexion.

Qualité du service La qualité de service (QoS) est également une exigence de plus en plus répandue pour les réseaux actuels.

Un encombrement survient lorsqu'une demande excessive de bande passante dépasse les capacités disponibles. La bande passante réseau est mesurée en fonction du nombre de 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, ce qui génère un encombrement du réseau.

Lorsque le volume de trafic 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.

Sécurité Deux aspects de la sécurité du réseau doivent être pris en compte : la sécurité de l'infrastructure réseau et la sécurité de l'information.

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

Sécuriser l'information consiste à protéger les informations contenues dans les paquets transmis sur le réseau, ainsi que les informations stockées sur les périphériques reliés au réseau.

Pour atteindre ces objectifs de sécurité du réseau, il faut respecter trois exigences :

- confidentialité ;
- intégrité ;
- disponibilité.

Chapitre 2

Configuration d'un système d'exploitation réseau

2.1 Formation à IOS

2.1.1 Accès à Cisco IOS

Tous les périphériques finaux et réseau requièrent un système d'exploitation (SE). La partie du SE 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 d'une interface en ligne de commande (CLI) ou d'une interface utilisateur graphique.

Un commutateur Cisco IOS peut être implémenté sans être configuré. Il effectuera tout de même la commutation des données entre les périphériques connectés. Deux PC reliés à un commutateur disposeront immédiatement d'une interconnectivité instantanée.

Même si un commutateur Cisco fonctionne toujours immédiatement, il est recommandé de configurer les paramètres initiaux. Il existe plusieurs moyens d'accéder à l'environnement CLI et de configurer le périphérique. Voici les méthodes les plus répandues :

- **Console** : il s'agit d'un port de gestion permettant un accès hors réseau à un périphérique Cisco. L'accès hors bande désigne l'accès via un canal de gestion dédié qui est utilisé uniquement pour la maintenance des périphériques.
- **Secure Shell** (**SSH**) : moyen d'établir à distance une connexion CLI sécurisée via une interface virtuelle sur un réseau. À la différence des connexions de console, les connexions SSH requièrent des services réseau actifs sur le périphérique, notamment une interface active possédant une adresse.
- **Telnet** : moyen non sécurisé d'établir une session CLI à distance via une interface virtuelle sur un réseau.

2.1.2 Naviguer dans Cisco IOS

Pour effectuer la configuration initiale d'un périphérique Cisco, une connexion console doit être établie. Une fois cette opération effectuée, le technicien réseau doit naviguer à travers différents modes de commande dans la CLI de Cisco IOS. Par mesure de sécurité, le logiciel Cisco IOS sépare l'accès à la gestion en deux modes de commande :

- **Mode d'exécution utilisateur**
- **Mode d'exécution privilégié**

Modes de commandes de configuration Pour configurer le périphérique, l'utilisateur doit passer en mode de configuration globale. Les modifications de la configuration effectuées dans l'interface en ligne de commande en mode de config. globale affectent le fonctionnement du périphérique dans son ensemble. À partir du mode de config. globale, l'utilisateur peut accéder à différents sous-modes de configuration. Chacun de ces modes permet de configurer une partie ou une fonction spéciale du périphérique IOS. Voici deux sous-modes de configuration courants :

- **Mode de configuration de ligne** : utilisé pour configurer l'accès par la console, par SSH, par Telnet, ou l'accès AUX.
- **Mode de configuration d'interface** : utilisé pour configurer l'interface réseau d'un port de commutateur ou d'un routeur.

Naviguer entre les différents modes IOS Différentes commandes sont utilisées pour entrer et sortir des invites de commandes :

- Pour passer du mode utilisateur au mode privilégié, utilisez la commande **enable**. Utilisez la commande **disable** du mode d'exécution privilégié pour retourner au mode d'exécution utilisateur.
- Pour passer en mode de configuration globale et le quitter, utilisez la commande de mode d'exécution privilégié **configure terminal**.
- Il existe de nombreux sous-modes de configuration différents. Par exemple, pour passer en sous-mode de configuration de ligne, utilisez la commande **line** suivie du type et du numéro de la ligne de gestion à laquelle vous souhaitez accéder.
- Pour passer de n'importe quel sous-mode de configuration du mode de configuration globale au mode situé un niveau plus haut dans la hiérarchie des modes, saisissez la commande **exit**.
- Pour passer de n'importe quel sous-mode de configuration au mode d'exécution privilégié, entrez la commande **end** ou utilisez la combinaison de touches **Ctrl+Z**.

2.2 Configuration des périphériques de base

2.2.1 Noms d'hôtes

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. Depuis le mode d'exécution privilégié, accédez au mode

de configuration globale. Entrez ensuite la commande **hostname** suivie du nom du commutateur. Pour supprimer le nom d'hôte configuré et renvoyer le commutateur à l'invite par défaut, utilisez la commande de config. globale **no hostname**.

2.2.2 Accès sécurisé aux périphériques

Configurer les mots de passe Cisco IOS peut être configuré pour utiliser des mots de passe de mode hiérarchique afin de permettre d'établir différents privilèges d'accès à un périphérique réseau :

- Le mot de passe le plus important à configurer est celui permettant d'accéder au mode d'exécution privilégié. Pour cela, utilisez la commande de config. globale **enable secret password**.
- Pour sécuriser l'accès au mode d'exécution utilisateur, le port de console doit être configuré. Passez en mode de configuration de console de ligne à l'aide de la commande de configuration globale **line console 0**. Le zéro sert à représenter la première (et le plus souvent, la seule) interface de console. Spécifiez ensuite le mot de passe du mode d'exécution utilisateur à l'aide de la commande de mot de passe **password psw**. Enfin, activez l'accès d'exécution utilisateur à l'aide de la commande **login**.
- Les lignes VTY (terminal virtuel) activent l'accès à distance au périphérique. Pour sécuriser les lignes VTY utilisées pour SSH et Telnet, passez en mode ligne VTY à l'aide de la commande de config. globale **line vty 0 15**. De nombreux commutateurs prennent en charge jusqu'à 16 lignes VTY, numérotées de 0 à 15. Spécifiez ensuite le mot de passe VTY à l'aide de la commande **password**. Enfin, activez l'accès VTY à l'aide de la commande **login**.

Chiffrer les mots de passe Les fichiers startup-config et running-config affichent la plupart des mots de passe en clair. Pour chiffrer les mots de passe, utilisez la commande de configuration globale **service password-encryption**. La commande 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 ; il ne s'applique pas lorsque les mots de passe sont transmis sur le réseau.

Message de bannière Pour créer une bannière MOTD (Message Of The Day) sur un périphérique réseau, utilisez la commande de config. globale du **banner motd "**. Le « " » situé dans la syntaxe de la commande est le caractère de délimitation. Il est placé avant et après le message. Vous pouvez utiliser comme délimiteur tout caractère ne figurant pas dans le message. Une fois cette commande exécutée, la bannière s'affiche lors de toutes les tentatives d'accès au périphérique jusqu'à ce que vous la supprimiez.

2.2.3 Enregistrer le fichier de configuration en cours

Deux fichiers système stockent la configuration des périphériques :

- **startup-config** : il s'agit du fichier stocké dans la mémoire vive non volatile (NVRAM) qui contient toutes les commandes qui seront utilisées par le périphérique au démarrage ou au redémarrage.

- **running-config** : il s'agit du fichier stocké dans la mémoire vive volatile (RAM) et qui reflète la configuration actuelle. Modifier une configuration en cours affecte immédiatement le fonctionnement d'un périphérique.

Vous pouvez entrer la commande du mode d'exécution privilégié **show running-config** pour afficher le fichier de configuration en cours, de même pour afficher le fichier de configuration initiale. Pour enregistrer les modifications apportées à la configuration en cours dans le fichier de configuration initiale, utilisez la commande **copy running-config startup-config** du mode d'exécution privilégié. Si le fichier running-config n'a pas encore été enregistré, vous pouvez revenir à la configuration antérieure du périphérique à l'aide de la commande **reload** du mode d'exécution privilégié afin de restaurer startup-config. Si des modifications indésirables ont été 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 à l'aide de la commande **erase startup-config**.

2.3 Schémas d'adressage

2.3.1 Ports et adresses

Adresses IP L'utilisation d'adresses IP 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.
Chaque périphérique final d'un réseau doit être configuré avec une adresse IP. La structure d'une adresse IPv4 est composée de quatre nombres décimaux compris entre 0 et 255. Les adresses IPv4 sont affectées à des périphériques individuels connectés à un réseau.
Avec une adresse IPv4, un masque de sous-réseau est également nécessaire. Un masque de sous-réseau IPv4 est une valeur 32 bits qui sépare la partie réseau de l'adresse de la partie hôte. Associé à l'adresse IPv4, le masque de sous-réseau détermine à quel sous-réseau spécifique 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.

Interfaces et ports Les communications réseau dépendent des interfaces des périphériques utilisateur final, 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.
Chaque liaison à Internet requiert un type de support réseau spécifique, ainsi qu'une technologie réseau particulière. Par exemple, 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.
Les commutateurs Cisco IOS de couche 2 sont équipés de ports physiques pour permettre à des périphériques de s'y connecter. Ces ports ne prennent pas en charge les adresses IP de couche 3. Par conséquent, les commutateurs ont une ou plusieurs interfaces de commutateur virtuelles (SVI). Ces interfaces sont 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 par défaut prête à l'emploi. L'interface SVI par défaut est l'interface VLAN1.

2.3.2 Configuration de l'interface de commutateur virtuelle

Pour accéder à distance au commutateur, une adresse IP et un masque de sous-réseau doivent être configurés sur l'interface SVI. Pour configurer une SVI, utilisez la commande de configuration globale **interface vlan 1**. Attribuez ensuite une adresse IPv4 à l'aide de la commande de configuration d'interface **ip address ipAdresse subnetMask**. Enfin, activez l'interface virtuelle à l'aide de la commande de configuration d'interface **no shutdown**.

Chapitre 3

Protocoles et communications réseau

3.1 Règles de communication

La communication commence par un message (ou des informations) qui doit être envoyé d'une source vers 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. Les protocoles doivent prendre en compte les éléments suivants :

- l'identification de l'expéditeur et du destinataire ;
- l'utilisation d'une langue et d'une syntaxe communes ;
- la vitesse et le rythme d'élocution ;
- la demande de confirmation ou d'accusé de réception.

Les protocoles informatiques courants répondent aux exigences illustrées à la figure 3.1.

FIGURE 3.1 – Caractéristiques d'un protocole

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 l'information.

Format et encapsulation des messages 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. Chaque message informatique est encapsulé dans un format spécifique, appelé trame, avant d'être transmis via le réseau. La trame fait office d'enveloppe. Elle fournit l'adresse de la destination et celle de l'hôte source, comme le montre la figure 3.2. Notez que la source et la destination sont indiquées dans la partie adressage de la trame, ainsi que dans le message encapsulé.

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.

FIGURE 3.2 – Une trame

Taille des messages La taille fait également l'objet d'une règle de communication. Lorsqu'un long message est envoyé par un hôte à un autre sur le réseau, il est nécessaire de décomposer le message en plusieurs petites parties. 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.

Synchronisation des messages Ce sont les règles de tout engagement pour la synchronisation des messages :

- **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 répondre en cas d'erreurs.
- **Contrôle de flux** : Les hôtes source et de destination utilisent des méthodes de contrôle de flux pour négocier une synchronisation correcte en vue d'établir une communication.
- **Délai d'attente de la réponse** : Les hôtes du réseau sont soumis à des règles qui spécifient le délai d'attente des réponses et l'action à entreprendre en cas de délai d'attente dépassé.

Options de remise des messages Une option de remise 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 peut être utilisée. La diffusion correspond à une option de remise de type « un à tous ». Certains protocoles utilisent un message de multidiffusion spécial qui est envoyé à tous les périphériques, le rendant largement similaire à une diffusion. De plus, les hôtes peuvent devoir accuser réception de certains messages et pas d'autres.

3.2 Normes et protocoles réseaux

3.2.1 Protocoles

Règles qui régissent les communications Un groupe de protocoles associés entre eux 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.

Protocoles réseau 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 réseau les plus courants sont le protocole **HTTP** (Hypertext Transfer Protocol), le protocole **TCP** (Transmission Control Protocol) et le protocole **IP** (Internet Protocol).

Interactions entre les protocoles La communication entre un serveur web et un client web est un exemple d'interaction entre plusieurs protocoles. Les protocoles mentionnés dans la figure 3.3 sont les suivants :

- **HTTP** : protocole d'application qui 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. Le protocole HTTP dépend d'autres protocoles pour gérer le transport des messages entre le client et le serveur.
- **TCP** : protocole de transport qui gère les conversations individuelles. 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. Le protocole TCP est également responsable du contrôle de la taille et du débit d'échange des messages entre le serveur et le client.

- **IP** : protocole responsable de la récupération des segments formatés à partir du protocole TCP, de leur encapsulation en paquets, de l'affectation des adresses appropriées et de leur remise à l'hôte de destination.
- **Ethernet** : protocole d'accès au réseau qui décrit 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 d'accès réseau prennent les paquets depuis le protocole IP et les formatent pour les transmettre via les supports.

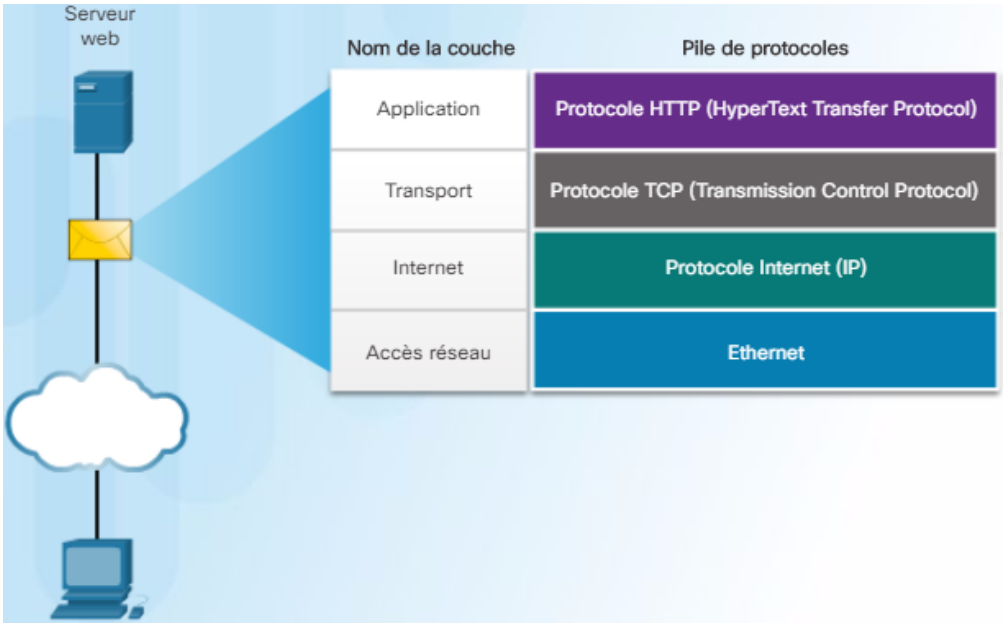


FIGURE 3.3 – Exemple d'interaction entre plusieurs protocoles

3.2.2 Suites de protocoles

Suites de protocoles et normes de l'industrie 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. Des exemples sont montrés sur la figure 3.4.

Suite de protocoles TCP/IP La suite de protocoles TCP/IP compte aujourd'hui de nombreux protocoles, comme l'indique la figure 3.5. Les différents protocoles sont organisés en couches suivant le modèle du protocole TCP/IP : couche application, couche transport, couche Internet et couche d'accès réseau. Les protocoles TCP/IP sont spécifiques aux couches application, transport et Internet. Les protocoles de la couche d'accès réseau sont responsables de la remise du paquet IP sur le support physique. Ces protocoles de couche inférieure sont développés par différents organismes de normalisation.

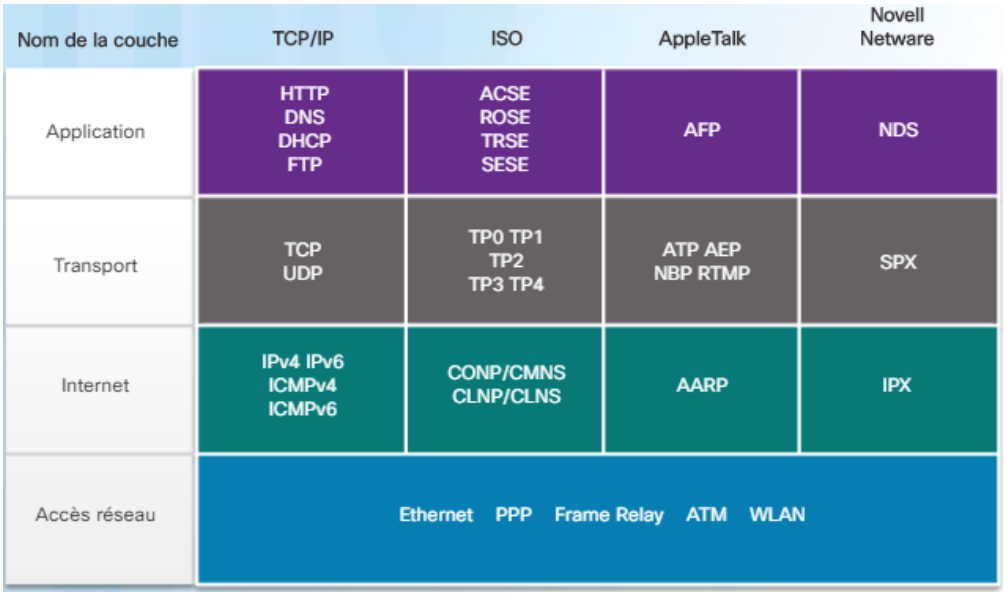


FIGURE 3.4 – Des exemples de suites de protocoles libres ou propriétaires

3.2.3 Modèles de référence

Avantages de l'utilisation d'un modèle en couches L'utilisation d'un modèle en couches pour décrire des protocoles et des opérations sur un réseau présente les avantages suivants :

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

Comme l'illustre la figure 3.6, le modèle OSI (Open Systems Interconnection) et le modèle TCP/IP sont les principaux modèles utilisés en matière de fonctionnalités réseau. Chacun représente un type basique de modèle de réseau en couches :

- Le modèle de protocole, qui suit la structure d'une suite de protocoles donnée. Le modèle TCP/IP est un modèle de protocole, car il décrit les fonctions qui interviennent à chaque couche de 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.

Le modèle de référence OSI 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. Les protocoles TCP/IP s'articulent autour des modèles OSI et TCP/IP.

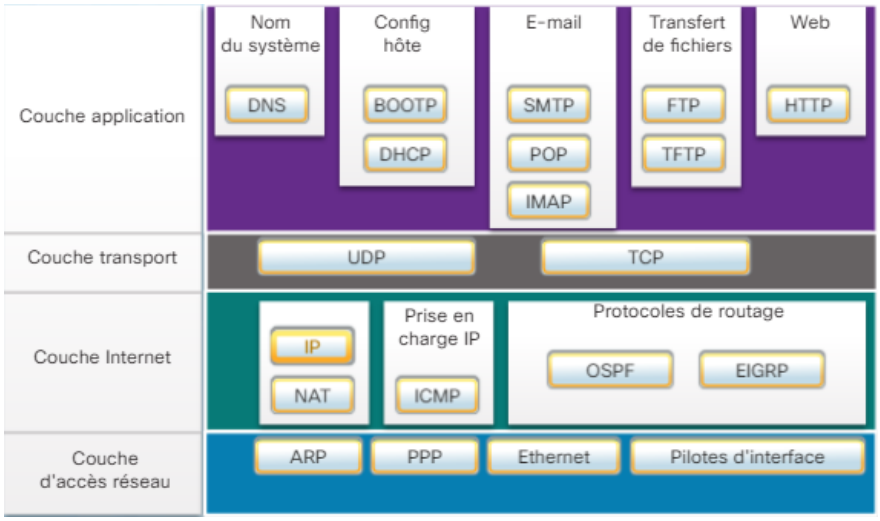


FIGURE 3.5 – La suite de protocoles TCP/IP

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 3.7, 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.

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 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 pour envoyer des données sur un réseau.

La couche OSI 3, qui correspond à la couche réseau, est directement liée à la couche Internet TCP/IP. Cette couche sert à décrire les protocoles qui traitent et dirigent les messages via l'interréseau.

La couche OSI 4, la couche transport, est directement associée à la couche transport TCP/IP. Cette couche 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.

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.

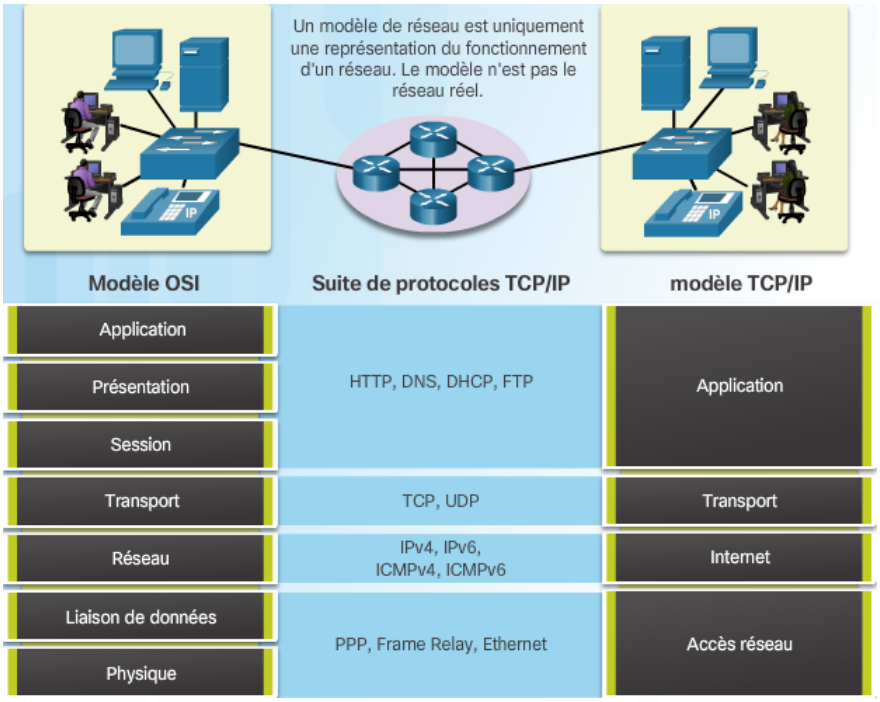


FIGURE 3.6 – Les principaux modèles de réseau

3.3 Transfert de donnéees sur le réseau

3.3.1 Encapsulation de données

Segmentation des messages La segmentation des messages 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 majeurs :

- L'envoi d'éléments individuels de plus petite taille depuis une source vers une destination permet d'entremêler de nombreuses conversations différentes sur le réseau. C'est ce que l'on appelle le multiplexage.
- La segmentation peut augmenter l'efficacité des communications réseau. Si une partie du message ne parvient pas à sa destination, en raison d'une panne réseau ou de l'encombrement du réseau, seules les parties manquantes doivent être transmises à nouveau.

Unités de données de protocole Lorsque les données d'application descendent la pile de protocoles en vue de leur transmission sur le support réseau, différentes informations de protocole sont ajoutées à chaque niveau. Il s'agit du processus d'encapsulation.

La forme qu'emprunte une donnée sur n'importe quelle couche est appelée unité de données de protocole. Au cours de l'encapsulation, chaque couche, l'une après l'autre, encapsule l'unité de données de protocole qu'elle reçoit de la couche supérieure en respectant le protocole en cours

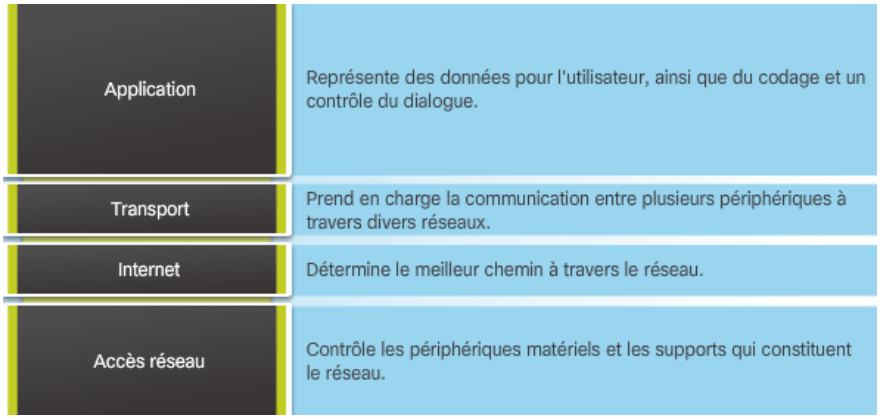


FIGURE 3.7 – Le modèle TCP/IP

d'utilisation. À chaque étape du processus, une unité de données de protocole possède un nom différent qui reflète ses nouvelles fonctions. Pour la suite TCP/IP :

- **Données** : terme générique pour 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.

3.3.2 Accès aux données

Adresses réseau Les couches réseau et liaison de données sont chargées de transmettre les données du périphérique source au périphérique de destination. Comme illustré à la figure 3.8, les protocoles de ces deux couches contiennent les adresses source et de destination, mais ils ne les utilisent pas aux mêmes fins :

- Les **adresses de couche réseau source et de destination** remettent le paquet IP de la source d'origine à la destination finale, sur le même réseau ou sur un réseau distant.
- Les **adresses de liaison de données source et de destination** transmettent la trame liaison de données d'une carte réseau à une autre, sur un même réseau.

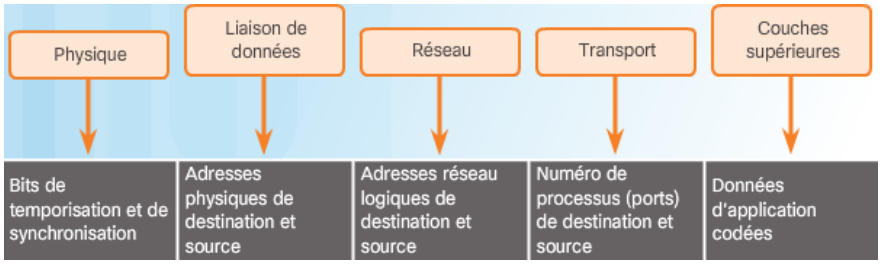
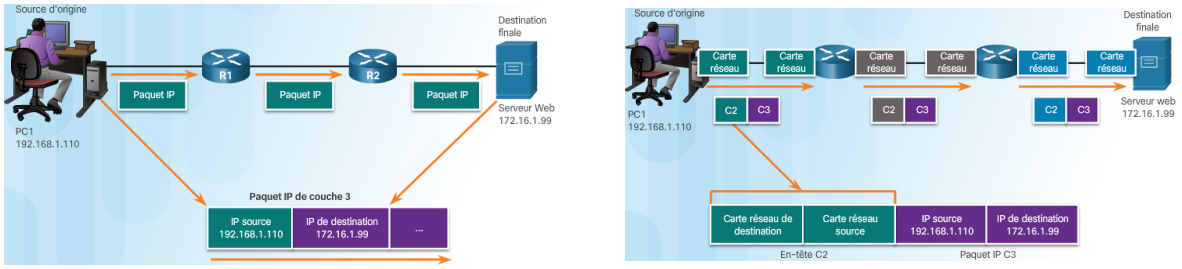


FIGURE 3.8 – Informations des couches

L'adresse IP est la couche réseau (ou couche 3), c'est-à-dire l'adresse logique utilisée pour acheminer le paquet IP de la source d'origine à la destination finale, comme illustré à la figure 3.9a. Le paquet IP contient deux adresses IP :

- **Adresse IP source** : adresse IP du périphérique expéditeur, la source d'origine du paquet.
- **Adresse IP de destination** : adresse IP du périphérique récepteur, la destination finale du paquet.

Adresses de liaison de données La couche 2, le protocole de liaison de données, sert uniquement à remettre le paquet entre les cartes réseau d'un même réseau. Le routeur supprime les informations de couche 2 dès leur réception sur une carte réseau et ajoute de nouvelles informations de liaison de données avant de les transférer vers la destination finale. Ce processus est illustré à la figure 3.9b.



(a) Adresses réseau de couche 2

(b) Adresses liaison de données de couche 2

FIGURE 3.9 – Adresses réseau et adresses de liaison de données

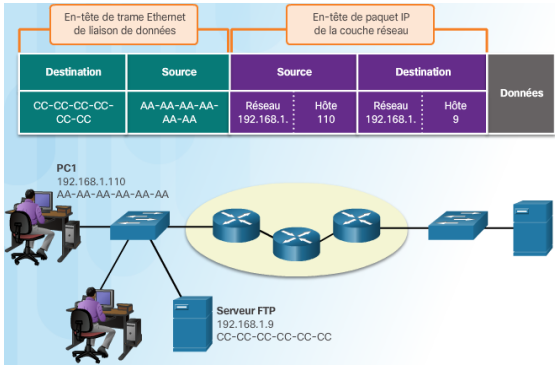
Périphériques sur le même réseau Les adresses de couche réseau ou adresses IP indiquent la source d'origine et la destination finale. Une adresse IP contient deux parties :

- **Une partie réseau** : partie située à l'extrême gauche de l'adresse qui indique à quel réseau appartient l'adresse IP.
- **Une partie hôte** : partie restante de l'adresse qui identifie un périphérique spécifique sur le réseau.

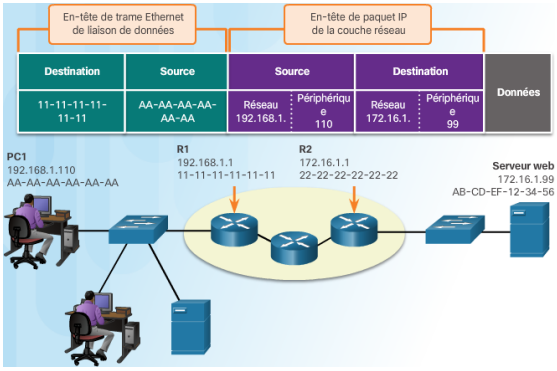
Lorsque l'expéditeur et le récepteur du paquet IP se trouvent sur le même réseau, la trame de liaison de données est envoyée directement au périphérique récepteur. Sur un réseau Ethernet, les adresses de liaison de données sont appelées adresses (MAC) Ethernet. Les adresses MAC sont physiquement incorporées dans la carte réseau Ethernet. Ce processus est illustré figure 3.10a.

Périphériques sur un réseau distant 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.

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. Ce processus est illustré figure 3.10b.



(a) Périphériqus sur le même réseau



(b) Périphériques sur des réseaux distants

FIGURE 3.10 – Communication entre périphériques

Chapitre 4

Accès réseau

4.1 Protocoles de couche physique

4.1.1 Connexion de couche physique

Types de connexions 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.

Cartes réseau Les cartes d'interface réseau ou cartes réseau (NIC en anglais) permettent de connecter 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.

4.1.2 Rôle de la couche physique

Couche physique La couche physique OSI fournit le 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 le support local. 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, illustré sur la figure 4.1 :

- 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 individuellement sur le support.
- 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.

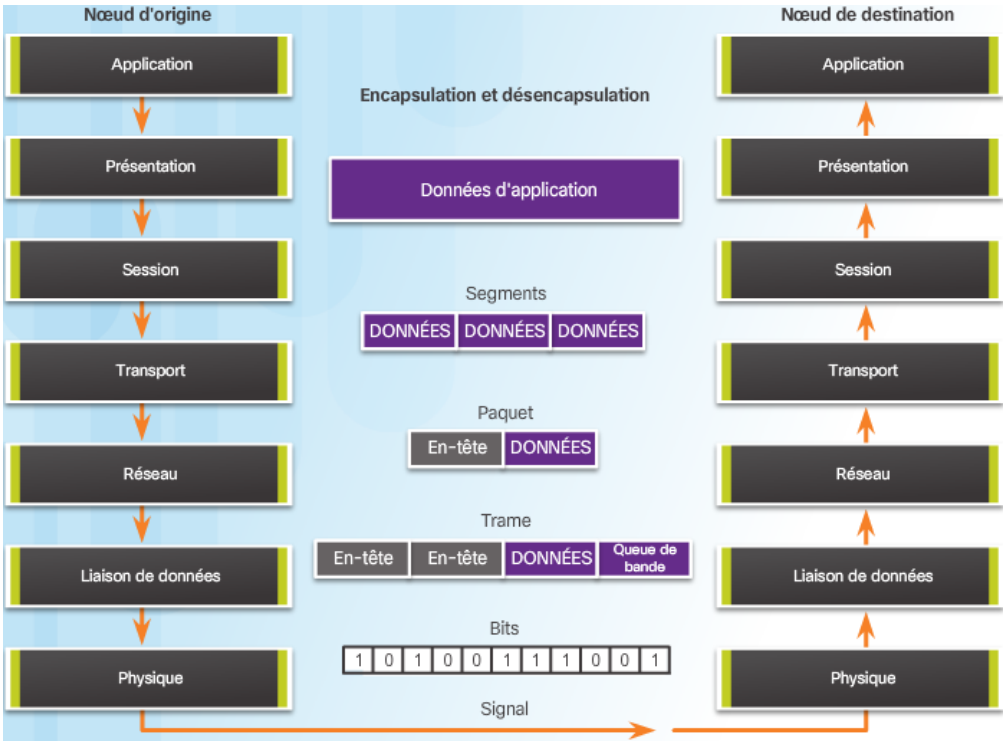


FIGURE 4.1 – Processus subi par les données

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.

4.1.3 Caractéristiques de la couche physique

Les normes de couche physique couvrent trois domaines fonctionnels :

- **Composants physiques** : Les composants physiques sont les périphériques électroniques, les supports et autres connecteurs qui transportent et transmettent les signaux qui représentent les bits.
- **Codage** : Le codage, ou codage de ligne, est une méthode permettant de convertir un flux de bits de données en un « code » prédéfini.
- **Signalisation** : La couche physique doit générer les signaux électriques, optiques ou sans fil qui représentent le 1 et le 0 sur le support. La méthode de représentation des bits est appelée méthode de signalisation.

Bande passante La bande passante est la capacité d'un support à transporter des données. La bande passante numérique mesure la quantité d'informations pouvant circuler d'un emplacement à un autre pendant une période donnée. La bande passante est habituellement exprimée en kilobits par seconde (kbit/s), en mégabits par seconde (Mbit/s) ou en gigabits par seconde (Gbit/s).

Débit Le débit est la mesure du transfert de bits sur le support pendant une période donnée. En raison d'un certain nombre de 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.

4.2 Protocoles de couche liaison de données

4.2.1 Rôle de la couche liaison de données

Couche liaison de données La couche liaison de données du modèle OSI (couche 2) a pour rôle :

- de permettre aux couches supérieures d'accéder aux supports ;
- d'accepter les paquets de couche 3 et de les encapsuler dans des trames ;
- de préparer les données du réseau pour le réseau physique ;
- de contrôler la manière dont les données sont placées et reçues sur le support ;
- d'échanger des trames entre les nœuds via le support d'un réseau physique ;
- de recevoir et d'acheminer les paquets vers un protocole de couche supérieure ;
- de détecter les erreurs.

Sous-couches liaison de données La couche liaison de données se divise en deux sous-couches :

- **Sous-couche LLC** (Logical Link Control) : cette sous-couche supérieure communique avec la 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 fournit une couche liaison de données qui traite les différentes technologies réseau et permet d'y accéder.

La figure 4.2 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.

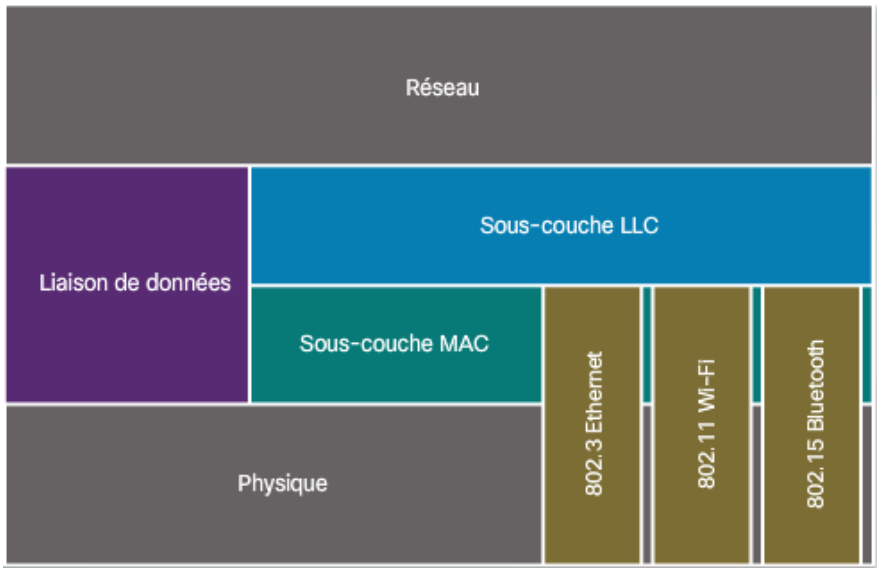


FIGURE 4.2 – Les sous-couches liaison de données

Contrôle de l'accès aux supports Les protocoles de couche 2 spécifient l'encapsulation d'un paquet en 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 est appelée 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 à fibre optique, des supports sans fil constitués de signaux électromagnétiques, à fréquences radio ou hyperfréquences, et des liaisons par satellite.

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 figurer le long d'un chemin de livraison.

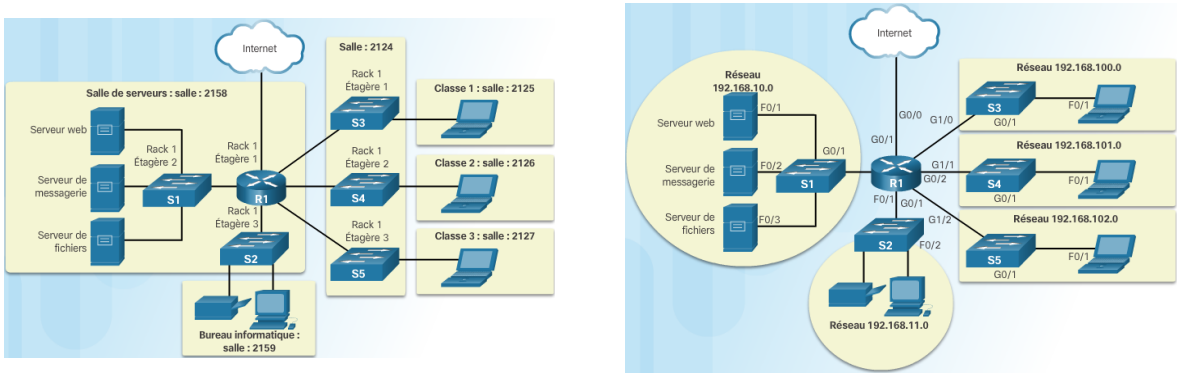
4.3 Contrôle de l'accès aux supports

4.3.1 Topologies

La topologie d'un réseau constitue l'organisation ou la relation des périphériques réseau et les interconnexions existant entre eux. Les topologies des réseau locaux et étendus 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 4.3a.
- **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 différentes. Voir la figure 4.3b.



(a) Topologie physique

(b) Topologie logique

FIGURE 4.3 – Les différentes représentations de topologies

4.3.2 Topologies de réseau étendu

Topologies physiques de réseau étendu courantes Les réseaux étendus sont généralement interconnectés selon les topologies physiques suivantes (représentées figure 4.4) :

- **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, tant administratifs que physiques, peuvent donc être élevés. Chaque liaison est simplement une liaison point à point avec l'autre nœud.

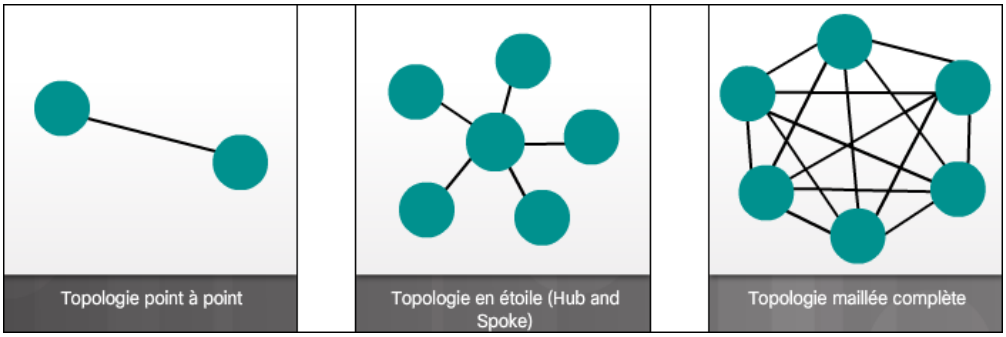


FIGURE 4.4 – Topologies physiques de réseau étendu courantes

Topologie physique point à point Les topologies point à point physiques connectent directement deux nœuds. 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 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.

4.3.3 Topologies LAN

Topologies physiques de réseau local Sur les réseaux locaux à supports partagés, les périphériques finaux peuvent être interconnectés selon les topologies physiques suivantes (voir figure 4.5) :

- **Topologie en étoile** : les périphériques finaux sont connectés à un périphérique intermédiaire central. La topologie en étoile est simple à installer, très évolutive et facile à dépanner.
- **Topologie en étoile étendue** : dans une topologie en étoile étendue, les périphériques Ethernet supplémentaires sont interconnectés avec d'autres topologies en étoile. Une topologie en étoile étendue est un exemple de topologie hybride.
- **Topologie en bus** : tous les systèmes finaux sont reliés entre eux en formant une chaîne et le réseau est terminé à chaque extrémité par un bouchon de terminaison. Les périphériques d'infrastructure tels que les commutateurs ne sont pas nécessaires pour interconnecter les périphériques finaux.
- **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.

Modes duplex intégral et semi-duplex Le terme « communications en mode duplex » désigne la direction de la transmission des données entre deux périphériques. Les communications en mode semi-duplex limitent l'échange de données dans un sens à un instant donné, tandis que les communications en mode duplex intégral permettent d'envoyer et de recevoir simultanément des données.

Méthodes de contrôle d'accès au support Certaines topologies réseau partagent un support avec plusieurs nœuds. Ce sont les réseaux à accès multiple. Les réseaux locaux Ethernet filaires et sans fil constituent des exemples de réseau à accès multiple. À tout moment, des périphériques peuvent tenter d'envoyer et de recevoir des données à l'aide des mêmes supports de réseau. Deux méthodes élémentaires de contrôle d'accès sont utilisées pour les supports partagés :

- **Accès avec gestion des conflits** : tous les nœuds fonctionnant en mode semi-duplex sont en concurrence pour utiliser le support, mais un seul périphérique à la fois peut envoyer des données. Cependant, il existe une procédure si plusieurs périphériques transmettent des données simultanément. Les réseaux locaux Ethernet filaires qui utilisent des concentrateurs et les réseaux locaux sans fil constituent des exemples de ce type de contrôle d'accès.
- **Accès contrôlé** : les nœuds utilisent le support à tour de rôle. Ces types de réseaux déterministes sont inefficaces dans la mesure où un périphérique doit attendre son tour pour accéder au support.

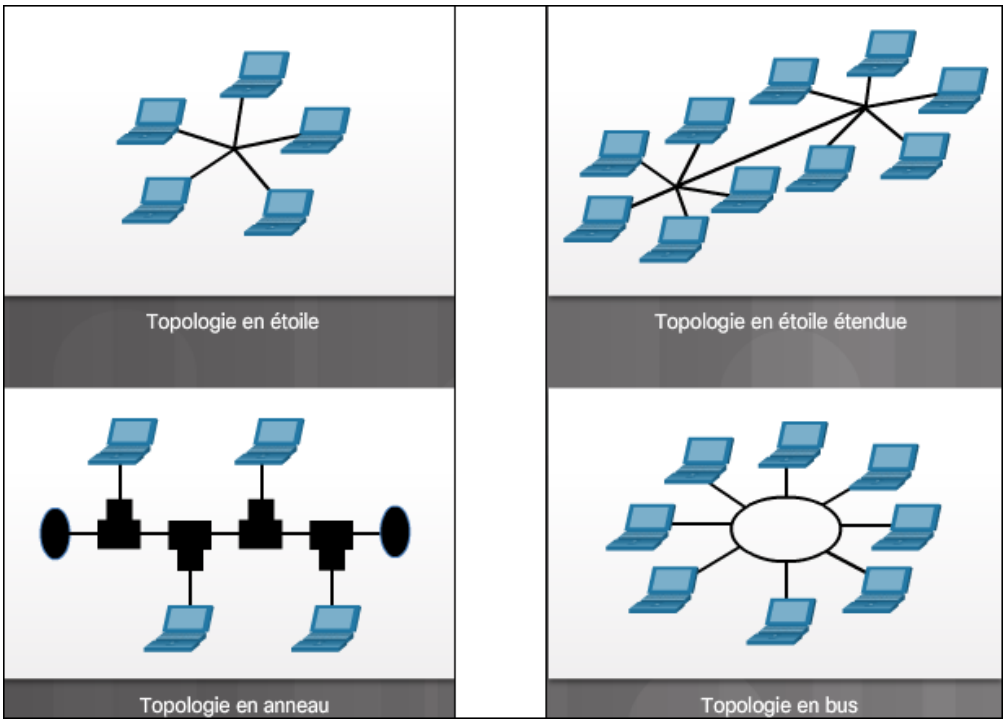


FIGURE 4.5 – Topologies physiques de réseau local courantes

Accès avec gestion des conflits – CSMA/CD Une procédure est nécessaire pour les réseaux d'accès fonctionnant en mode semi-duplex afin de déterminer à quel moment un périphérique peut envoyer des données et ce qui doit se produire lorsque plusieurs périphériques envoient des données au même moment.

Le processus d'accès multiple avec écoute de porteuse et détection de collision (CSMA/CD) est utilisé sur les réseaux locaux Ethernet en mode semi-duplex. Le processus CSMA se déroule comme suit :

1. Le PC1 a une trame Ethernet à envoyer au PC3.
2. La carte réseau du PC1 doit déterminer si une personne ne transmet pas déjà des données sur le support. Si elle ne détecte aucun signal d'opérateur, en d'autres termes, si elle ne reçoit pas de transmission de la part d'un autre périphérique, elle considère que le réseau est disponible pour effectuer un envoi.
3. La carte réseau du PC1 envoie la trame Ethernet.
4. Le concentrateur Ethernet reçoit la trame. Un concentrateur Ethernet est également appelé répéteur multiport. Tous les bits reçus sur un port entrant sont régénérés et sont envoyés à tous les autres ports.
5. Si un autre périphérique, comme le PC2, veut transmettre des données mais est en train de recevoir une trame, il doit patienter jusqu'à ce que le canal soit libre.
6. Tous les périphériques reliés au concentrateur reçoivent la trame. Étant donné que la trame possède une adresse de liaison de données de destination pour le PC3, seul ce périphérique acceptera et copiera la trame dans son ensemble. Les cartes réseau de tous les autres périphériques

ignoreront la trame.

Si deux périphériques transmettent en même temps, il se produit une collision. Les deux périphériques détectent la collision sur le réseau, constituant ce que l'on appelle une détection de collision (CD). Pour ce faire, la carte réseau compare les données transmises aux données reçues ou bien reconnaît que l'amplitude du signal est plus grande que la normale sur le support. Les données envoyées par les deux périphériques sont corrompues et doivent être envoyées de nouveau.

Accès avec gestion des conflits – CSMA/CA L'une des autres formes de processus CSMA qu'utilisent les réseaux locaux sans fil IEEE 802.11 est le processus CSMA/CA (Accès multiple avec écoute de porteuse et prévention des collisions). Le CMSA/CA utilise une méthode similaire au processus CSMA/CD pour détecter si le support est libre. Le CMSA/CA utilise aussi d'autres techniques. Il ne détecte pas les collisions, mais tente de les éviter en patientant avant d'effectuer la transmission. Chaque périphérique qui transmet des données tient compte du temps dont il a besoin pour la transmission. Tous les autres périphériques sans fil reçoivent cette information et savent combien de temps le support sera indisponible. Une fois qu'un périphérique sans fil a envoyé une trame 802.11, le récepteur renvoie un accusé de réception afin que l'expéditeur sache que la trame est arrivée.

4.3.4 Trame liaison de données

Trame La couche liaison de données prépare un paquet pour le transport à travers les supports locaux en l'encapsulant avec un en-tête et une queue de bande pour créer une trame. Chaque type de trame comprend trois éléments de base :

- un en-tête ;
- des données ;
- une queue de bande.

Champs de trame Comme l'illustre la figure 4.6, les types de champ de trame générique sont les suivants :

- **Indicateurs de début et de fin de trame**
- **Adressage** : indique les nœuds source et de destination sur les supports.
- **Type** : identifie le protocole de couche 3 dans le champ de données.
- **Contrôle** : identifie les services de contrôle de flux spéciaux comme la qualité de service (QoS). La QoS est utilisée pour donner la priorité de transfert à certains types de messages. Les trames liaison de données qui transportent des paquets en Voix sur IP (VoIP) sont normalement prioritaires, car elles sont sensibles aux retards.
- **Données** : 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 des erreurs** : ces champs sont utilisés pour la détection des erreurs et sont inclus après les données pour former la queue de bande.

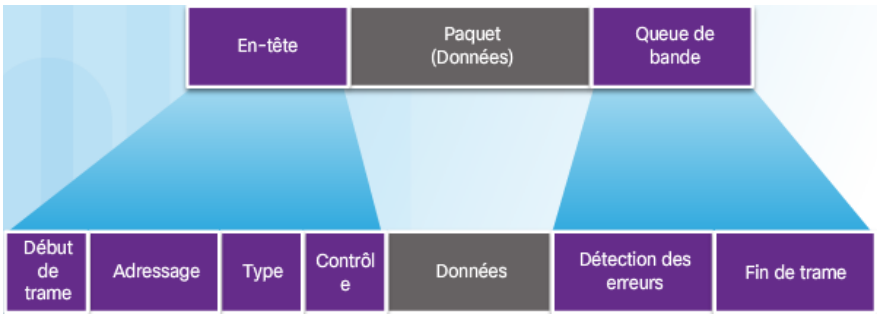


FIGURE 4.6 – Champs de trame

Chapitre 5

Ethernet

La couche physique OSI fournit le moyen de transporter les bits constituant une trame de couche liaison de données sur le support réseau.

Ethernet est désormais la technologie de réseau local prédominante dans le monde. Il 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.

5.1 Protocole Ethernet

5.1.1 Trame Ethernet

Encapsulation Ethernet Ethernet est la technologie LAN la plus répandue aujourd'hui. Il fonctionne au niveau de la couche liaison de données et de la couche physique. Ethernet est une famille de technologies de 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, comme pour toutes les normes IEEE 802, le fonctionnement d'Ethernet dépend de deux sous-couches distinctes de la couche liaison de données :

- **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 réseau 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 nœud de destination. 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.
- **La 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.

Sous-couche MAC La sous-couche MAC Ethernet a deux fonctions principales :

- **L'encapsulation de données** : L'encapsulation de données consiste à assembler les trames avant de les transmettre et à les désassembler à leur réception. Elle assure trois fonctions de base :
  - **La délimitation des trames** : le processus de tramage fournit des délimiteurs importants utilisés pour identifier un groupe de bits qui composent une trame. Ces bits de délimitation permettent la synchronisation entre les nœuds de transmission et ceux de réception.
  - **L'adressage** : l'encapsulation contient la PDU de couche 3 et fournit également un adressage pour la couche liaison de données.
  - **La détection des erreurs**
- **Contrôle de l'accès aux supports** : La deuxième fonction de la sous-couche MAC consiste à contrôler l'accès au support. Le contrôle d'accès au support gère le placement des trames sur les supports et leur suppression. 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. La méthode CSMA/CD est utilisée avec les réseaux locaux Ethernet en mode semi-duplex pour détecter et gérer les conflits. Les LAN Ethernet actuels utilisent des commutateurs en mode duplex intégral, ce qui permet à plusieurs périphériques d'envoyer et de recevoir simultanément des données sans créer de conflits.

Champs de trame Ethernet La taille minimale des trames Ethernet est de 64 octets et la taille maximale de 1 518 octets. Cela comprend tous les octets du champ Adresse MAC de destination jusqu'au champ Séquence de contrôle de trame. Le champ Préambule n'est pas inclus dans la description de la taille d'une trame.

Toute trame inférieure à 64 octets est interprétée comme un « fragment de collision » ou une « trame incomplète ». 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 traités comme étant non valides.

La figure 5.1 présente une trame Ethernet II.

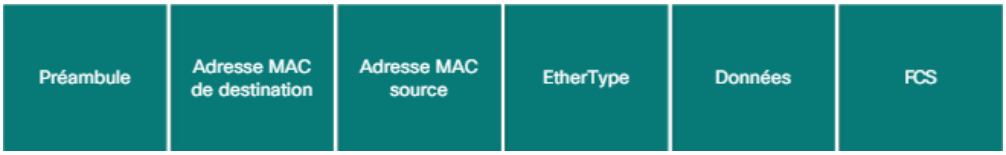


FIGURE 5.1 – Champs de trame Ethernet II

5.1.2 Adresses MAC Ethernet

Adresse MAC : identité Ethernet Dans la norme Ethernet, chaque périphérique réseau se connecte au même support partagé. À une époque, Ethernet était principalement une topologie en

mode semi-duplex utilisant un bus à accès multiple, et plus tard, des concentrateurs Ethernet. Ainsi, tous les nœuds recevaient toutes les trames transmises. Pour éviter la surcharge excessive liée au traitement de chaque trame, des adresses MAC qui identifient la source et la destination réelles ont été créées. Une adresse MAC Ethernet est une valeur binaire de 48 bits constituée de 12 chiffres hexadécimaux (4 bits par chiffre hexadécimal). L'adressage MAC fournit une méthode d'identification des périphériques au niveau inférieur du modèle OSI. L'IEEE demande aux constructeurs de respecter deux règles simples :

- 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 ayant le même identifiant OUI doivent utiliser une valeur unique dans les 3 derniers octets.

Traitement des trames L'adresse MAC est codée de manière permanente dans la puce de mémoire morte.

Lorsqu'une carte réseau reçoit une trame Ethernet, elle observe l'adresse MAC de destination pour voir si elle correspond bien à l'adresse MAC physique du périphérique. En l'absence de correspondance, la carte réseau ignore la trame. Si elle correspond, la carte réseau transmet la trame aux couches OSI, et la désencapsulation a lieu.

Une adresse MAC doit être attribuée à tout périphérique qui peut être la source ou la destination d'une trame Ethernet. Cela inclut les postes de travail, les serveurs, les imprimantes, les appareils mobiles et les routeurs.

Consultation des adresses MAC Sur un hôte Windows, la commande **ipconfig /all** permet d'identifier l'adresse MAC d'un adaptateur Ethernet. Sur les hôtes MAC ou Linux, c'est la commande **ifconfig** qui est utilisée.

Adresse MAC de monodiffusion 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 multidiffusion se voient affecter une adresse IP de groupe multidiffusion. La plage d'adresses de multidiffusion IPv4 s'étend de 224.0.0.0 à 239.255.255.255. La plage d'adresses de multidiffusion IPv6 commence par FF00 : :/8. Dans la mesure où les adresses multidiffusion représentent un groupe d'adresses (parfois appelé groupe d'hôtes), elles ne peuvent s'utiliser que dans la destination d'un paquet. La source doit toujours être une adresse de monodiffusion.

Comme avec les adresses monodiffusion et de diffusion, l'adresse IP multidiffusion nécessite une adresse MAC multidiffusion correspondante pour remettre les trames sur un réseau local. L'adresse MAC de multidiffusion associée à une adresse de multidiffusion IPv4 est une valeur spéciale commençant par 01-00-5E dans un 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. Pour une adresse IPv6, l'adresse MAC de multidiffusion commence par 33-33. Le processus est représenté figure 5.2.

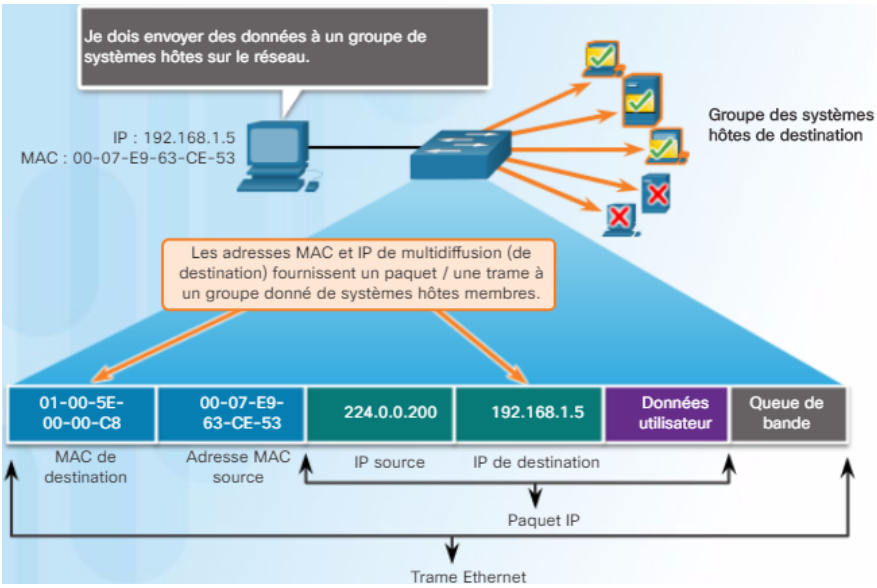


FIGURE 5.2 – Multidiffusion (multicast)

5.2 Commutateurs LAN

5.2.1 La table d'adressage MAC

Commutateurs : notions essentielles Un commutateur Ethernet de couche 2 utilise des adresses MAC pour prendre des décisions de transmission. Il ignore totalement le protocole transporté dans la partie données de la trame, tel qu'un paquet IPv4. Les décisions du commutateur concernant la transmission de données reposent uniquement sur les adresses MAC Ethernet de couche 2.

Contrairement à un concentrateur Ethernet qui répète les bits sur tous les ports sauf le port entrant, un commutateur Ethernet consulte une table d'adresses MAC pour décider de la transmission de chaque trame.

Acquérir les adresses MAC Le commutateur crée la table d'adresses MAC de manière dynamique en examinant l'adresse MAC source des trames reçues sur un port. Pour transmettre les trames, le commutateur recherche une correspondance entre l'adresse MAC de destination qui figure dans la trame et une entrée de la table d'adresses MAC.

Le processus suivant se déroule sur chaque trame Ethernet entrant dans un commutateur :

1. **Découverte - Examen de l'adresse MAC source** : Le commutateur vérifie si de nouvelles informations sont disponibles sur chacune des trames entrantes. Pour cela, il examine l'adresse MAC source de la trame et le numéro du port par lequel la trame est entrée dans le commutateur.
   - Si l'adresse MAC source n'existe pas, elle est ajoutée à la table , tout comme le numéro du port d'entrée. Sur la figure 5.3, PC-A envoie une trame Ethernet à PC-D. Le commutateur ajoute l'adresse MAC de PC-A à la table.
   - Si l'adresse MAC source existe, le commutateur réinitialise le compteur d'obsolescence de

cette entrée. Par défaut, la plupart des commutateurs Ethernet conservent les entrées dans la table pendant 5 minutes.

2. **Transfert - Examen de l'adresse MAC de destination** : Ensuite, si l'adresse MAC de destination est une adresse de monodiffusion, le commutateur recherche une correspondance entre l'adresse MAC de destination qui figure dans la trame et une entrée de sa table d'adresses MAC.
   - Si l'adresse MAC de destination se trouve dans la table, le commutateur transfère la trame par le port spécifié.
   - Si l'adresse MAC de destination ne se trouve pas dans la table, le commutateur transfère la trame sur tous les ports sauf celui d'entrée. C'est ce qu'on appelle la monodiffusion inconnue. Comme le montre la figure 5.3, la table d'adresses du commutateur ne contient pas l'adresse MAC de destination de PC-D, donc il envoie la trame sur tous les ports sauf le port 1.

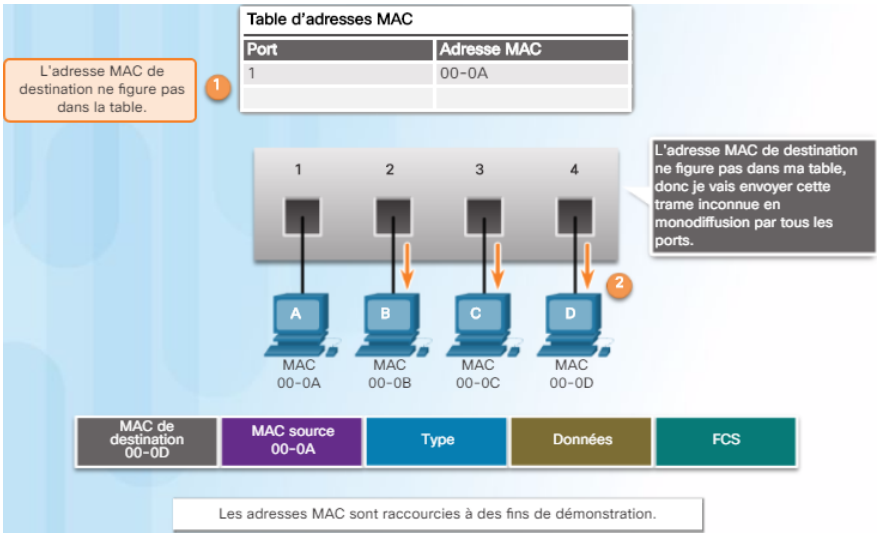


FIGURE 5.3 – Examination d'une adresse MAC source

Filtrage des trames À mesure qu'un commutateur reçoit des trames de différents périphériques, il remplit sa table d'adresses MAC en examinant l'adresse MAC source de chaque trame. Si la table d'adresses MAC du commutateur contient l'adresse MAC de destination, il peut filtrer la trame et la diffuser sur un sol port. Lorsque l'adresse IP d'un périphérique se trouve sur un réseau distant, la trame Ethernet ne peut pas être envoyée directement au périphérique de destination. Au lieu de cela, la trame Ethernet est envoyée à l'adresse MAC de la passerelle par défaut, c'est-à-dire le routeur.

5.2.2 Méthodes de transmission par commutateur

Méthodes de transmission de trames Les commutateurs utilisent l'une des méthodes suivantes de transfert des données entre des ports réseau :

- **Commutation par stockage et retransmission** (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) de l'en-queue de la trame Ethernet.
- **Commutation cut-through** : le commutateur achemine la trame avant qu'elle ne soit entièrement reçue. 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.
  - **Commutation Fragment-free** : le commutateur stocke les 64 premiers octets de la trame avant la transmission. La plupart des erreurs et des collisions sur le réseau surviennent en effet pendant ces 64 premiers octets.

Le contrôle par redondance cyclique (CRC) a recours à une formule mathématique fondée sur le nombre de bits 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 sa destination. En cas d'erreur détectée au sein de la trame, le commutateur ignore la trame.

Mise en mémoire tampon sur les commutateurs Il existe deux méthodes de mise en mémoire tampon :

- **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.
- **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.

5.3 Protocoles ARP (Adress Resolution Protocol)

5.3.1 Adresses MAC et IP

Chaque périphérique d'un réseau LAN Ethernet possède deux adresses principales :

- **L'adresse physique** (adresse MAC), qui est utilisée pour les communications entre des cartes réseau d'un même réseau.
- **L'adresse logique** (adresse IP), qui sert à envoyer le paquet de la source d'origine à la destination finale. L'adresse IP de destination peut se trouver sur le même réseau IP que la source ou sur un réseau distant.

Si l'adresse IP de destination appartient au même réseau, l'adresse MAC de destination est celle du périphérique de destination. Lorsque l'adresse IP de destination appartient à un réseau distant, l'adresse MAC de destination est celle de la passerelle par défaut de l'hôte.

5.3.2 ARP

Présentation et fonctions du protocole ARP Pour déterminer l'adresse MAC de destination, le périphérique utilise le protocole ARP. Le protocole ARP assure deux fonctions principales :

- **La résolution des adresses IPv4 en adresses MAC** : Quand un paquet est envoyé à la couche liaison de données pour être encapsulé dans une trame Ethernet, le périphérique consulte une table stockée dans sa mémoire pour connaître l'adresse MAC qui est mappée à l'adresse IPv4. Cette table est appelée table ARP ou cache ARP.
  - Si l'adresse IPv4 de destination du paquet appartient au même réseau que l'adresse IPv4 source, le périphérique recherche l'adresse IPv4 de destination dans sa table ARP.
  - Si l'adresse IPv4 de destination du paquet appartient à un autre réseau que l'adresse IPv4 source, le périphérique recherche l'adresse IPv4 de la passerelle par défaut dans sa table ARP.
- **La tenue d'une table des mappages**

Requête ARP Une requête ARP est envoyée lorsqu'un périphérique a besoin d'une adresse MAC associée à une adresse IPv4 qui ne figure pas dans sa table ARP. Les messages ARP sont encapsulés directement dans une trame Ethernet. Il n'existe pas d'en-tête IPv4. Le message de la requête ARP contient les éléments suivants :

- **l'adresse IPv4 cible**, c'est-à-dire l'adresse IPv4 dont l'adresse MAC correspondante est requise ;
- **l'adresse MAC cible**, qui n'est pas connue et n'est donc pas renseignée dans le message de la requête ARP.

La requête ARP est encapsulée dans une trame Ethernet à l'aide des informations d'en-tête suivantes :

- **L'adresse MAC de destination** : il s'agit d'une adresse de diffusion qui nécessite que toutes les cartes réseau Ethernet sur le LAN acceptent et traitent la requête ARP.
- **L'adresse MAC source** : correspond à l'adresse MAC de l'expéditeur de la requête ARP.
- **Le type** : informe la carte réseau réceptrice que la partie données de la trame doit être transmise au processus ARP.

Réponse ARP Seul le périphérique dont l'adresse IPv4 correspond à l'adresse IPv4 cible de la requête ARP envoie une réponse ARP. Le message de réponse ARP contient les éléments suivants :

- **l'adresse IPv4 de l'expéditeur**, c'est-à-dire celle du périphérique dont l'adresse MAC est requise ;
- **l'adresse MAC de l'expéditeur**, c'est-à-dire celle requise par l'expéditeur de la requête ARP.

Seul le périphérique à l'origine de la requête ARP reçoit la réponse ARP en monodiffusion. Il ajoute ensuite l'adresse IPv4 et l'adresse MAC associée à sa table ARP. Les paquets à destination de cette adresse IPv4 peuvent à présent être encapsulés dans des trames à l'aide de l'adresse MAC correspondante.

Rôle du protocole ARP dans les communications à distance L'adresse IPv4 de la passerelle par défaut est stockée dans la configuration IPv4 des hôtes. Lorsqu'un hôte crée un paquet pour une destination, il compare l'adresse IPv4 de destination à sa propre adresse IPv4 pour déterminer si celles-ci se situent sur le même réseau de couche 3. Si l'hôte de destination ne se situe pas sur le même réseau, l'hôte source cherche dans sa table ARP l'adresse IPv4 de la passerelle par défaut. Si l'entrée n'existe pas, il fait appel au processus ARP pour déterminer l'adresse MAC de la passerelle par défaut.

Chapitre 6

Couche réseau

6.1 Protocoles de couche réseau

6.1.1 Couche réseau des communications

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 :

- **L'adressage des périphériques finaux** : une adresse IP unique doit être configurée sur les périphériques finaux pour les identifier sur le réseau.
- **L'encapsulation** : la couche réseau encapsule l'unité de données de protocole (PDU) de la couche transport dans un paquet. Le processus d'encapsulation ajoute des informations d'en-tête IP, telles que l'adresse IP des hôtes source (expéditeurs) et de destination (destinataires).
- **Le 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 le meilleur chemin et 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 routeur que traverse le paquet pour atteindre l'hôte de destination est appelé un tronçon.
- **La désencapsulation** : lorsque le paquet arrive au niveau de la couche réseau de l'hôte de destination, l'hôte vérifie l'en-tête IP du paquet. 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. 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.

Il n'existe que deux protocoles de couche réseau qui sont généralement mis en œuvre :

- protocole IP version 4 (IPv4) ;
- protocole IP version 6 (IPv6).

6.1.2 Caractéristiques du protocole IP

Encapsulation IP Le protocole IP encapsule le segment de couche transport ou d'autres données 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 le même entre le moment où le paquet quitte l'hôte source et son arrivée sur l'hôte de destination.

Le processus d'encapsulation des données par couche permet aux services des différentes couches de se développer et de s'étendre sans affecter d'autres couches.

Les routeurs peuvent mettre en œuvre ces différents protocoles de couche réseau pour fonctionner simultanément sur un réseau. Le routage effectué par ces périphériques intermédiaires tient compte uniquement du contenu de l'en-tête de paquet de couche réseau. 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.

Caractéristiques du protocole IP Le protocole IP 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, si elles sont requises, sont exécutées par d'autres protocoles, sur d'autres couches, principalement TCP sur la couche 4. Les principales caractéristiques du protocole IP sont :

- Le protocole IP est **sans connexion**, ce qui signifie qu'aucune connexion de bout en bout dédiée n'est créée avant l'envoi des données.
- **Acheminement au mieux** : IP n'est pas fiable par nature, car la livraison des paquets n'est pas garantie.
- **IP indépendant vis-à-vis des supports** : Le protocole IP fonctionne indépendamment des supports acheminant les données dans les couches inférieures de la pile de protocoles. Il incombe à la couche de liaison de données OSI de prendre un paquet IP et de le préparer en vue de sa transmission sur le support de communication. Toutefois le support présente une caractéristique essentielle prise en compte par la couche réseau : il s'agit de 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 consiste à établir la taille maximale pour le paquet. La couche réseau détermine alors la taille maximale des paquets.

6.1.3 Paquet IPv4

En-tête de paquet IPv4 Un en-tête de paquet IPv4 est constitué de 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 schémas d'en-tête de protocole, lisibles de gauche à droite et de haut en bas, fournissent une référence visuelle des champs de protocole. Le schéma d'en-tête de protocole IP présenté dans la figure 6.1 identifie les champs d'un paquet IPv4.

Les champs importants de l'en-tête IPv4 sont les suivants :

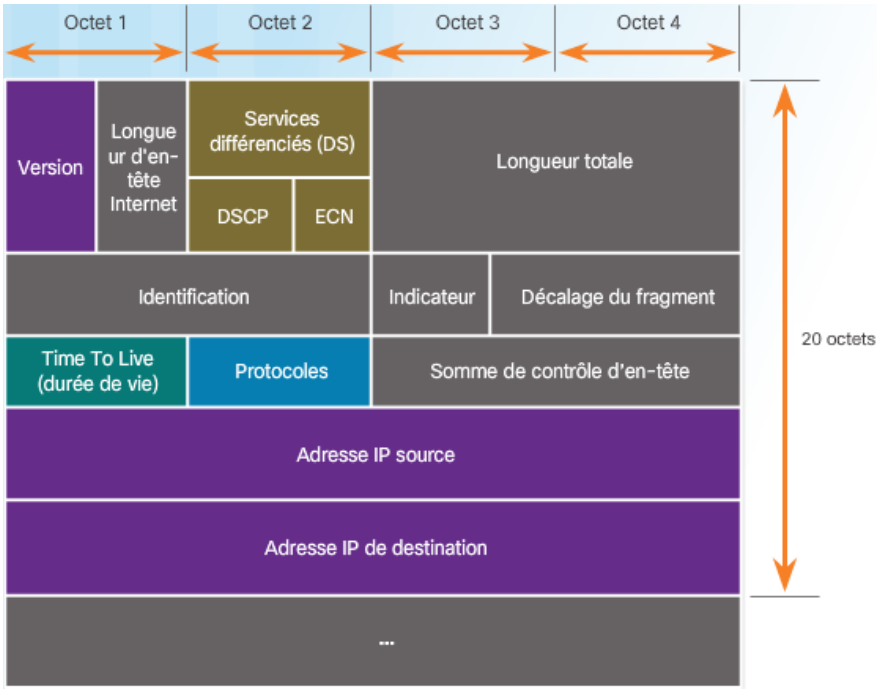


FIGURE 6.1 – Schéma d'en-tête de protocole IPv4

- **Version** : ce champ contient une valeur binaire de 4 bits définie sur 0100 indiquant qu'il s'agit d'un paquet IP version 4.
- **Services différenciés ou DiffServ (DS)** : c'est un champ de 8 bits utilisé pour définir la priorité de chaque paquet. Les six bits de poids fort du champ DiffServ sont représentés par le marquage DSCP (Differentiated Services Code Point) et les deux derniers bits sont des bits ECN (Explicit Congestion Notification).
- **Time-to-live** (durée de vie, TTL) : ce champ contient une valeur binaire de 8 bits utilisée pour limiter la durée de vie d'un paquet. L'expéditeur du paquet définit la valeur TTL initiale et celle-ci diminue d'un point chaque fois que le paquet est traité par un routeur. Si la valeur du champ TTL arrive à zéro, le routeur rejette le paquet et envoie un message de dépassement du délai ICMP (Internet Control Message Protocol) à l'adresse IP source.
- Le champ **Protocole** est utilisé pour identifier le prochain protocole de niveau. 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 les plus courantes sont notamment ICMP (1), TCP (6) et UDP (17).
- **Adresse IP source** : ce champ contient une valeur binaire de 32 bits, qui représente l'adresse IP source du paquet. L'adresse IPv4 source est toujours une adresse de mono-diffusion.
- **Adresse IP de destination** : ce champ contient une valeur binaire de 32 bits qui représente l'adresse IP de destination du paquet. L'adresse IPv4 de destination est une adresse de monodiffusion, de diffusion ou de multidiffusion.

Limites du protocole IPv4 L'IPv4 présente toujours trois problèmes majeurs :

- **La pénurie d'adresses IP**
- **La croissance de la table de routage Internet** : une table de routage est utilisée par les routeurs pour déterminer les meilleurs chemins disponibles. Le nombre de routes de réseau augmente parallèlement au nombre de serveurs connectés à Internet. Ces routes IPv4 consomment beaucoup de mémoire et de ressources processeur sur les routeurs Internet.
- **Le manque de connectivité de bout en bout** : la technologie de traduction d'adresses réseau (NAT) est généralement implémentée dans les réseaux IPv4. Elle permet à plusieurs périphériques de partager une adresse IPv4 publique unique. Cependant, étant donné que l'adresse IPv4 publique est partagée, l'adresse IPv4 d'un hôte interne du réseau est masquée, ce qui peut poser problème pour les technologies nécessitant une connectivité de bout en bout.

6.1.4 Paquet IPv6

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 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 le protocole de façon efficace, 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 (au lieu de 32 bits pour l'IPv4).
- **Traitement plus efficace des paquets** : l'en-tête IPv6 a été simplifié et comporte moins de champs.
- Traduction d'adresses réseau inutile : grâce au grand nombre d'adresses publiques IPv6, la technologie NAT n'est plus nécessaire entre une adresse privée et publique.

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 IPv6 représenté à la figure 6.2 est, quant à lui, 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).

Les champs d'en-tête de paquet IPv6 sont les suivants :

- **Version** : ce champ contient une valeur binaire de 4 bits définie sur 0110 indiquant qu'il s'agit d'un paquet IP version 6.
- **Classe de trafic** : ce champ de 8 bits est l'équivalent du champ de services différenciés pour l'IPv4.
- **Étiquetage de flux** : ce champ de 20 bits indique que tous les paquets portant la même étiquette de flux doivent être traités de la même manière par les routeurs.
- **Longueur des données utiles** : ce champ de 16 bits indique la longueur de la partie données (utiles) du paquet IPv6.
- **En-tête suivant** : ce champ de 8 bits est l'équivalent du champ de protocole de l'IPv4.
- **Limite du nombre de tronçons** : ce champ de 8 bits remplace le champ de durée de vie (TTL) de l'IPv4.

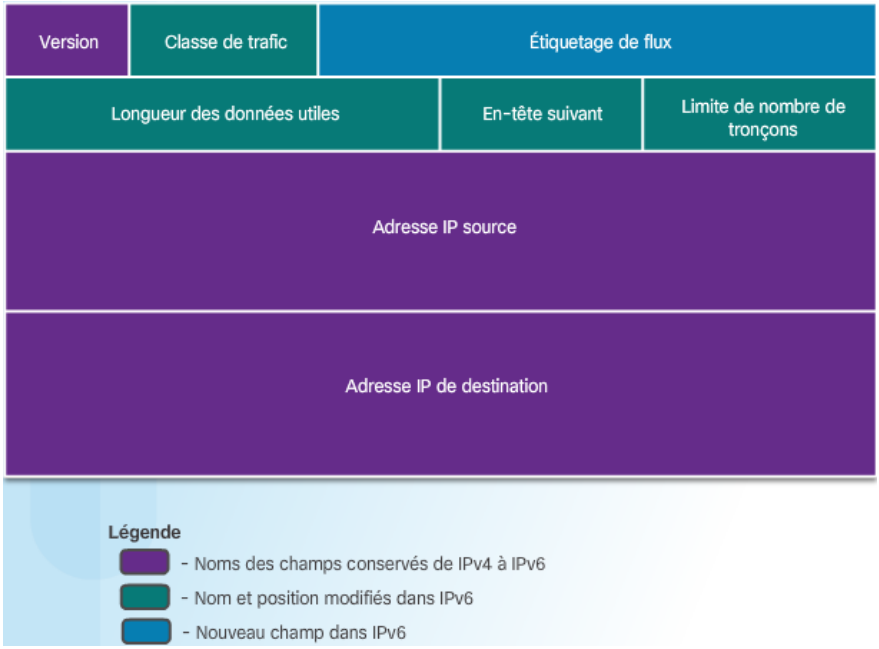


FIGURE 6.2 – Schéma d'en-tête de protocole IPv6

6.2 Routage

6.2.1 Méthode de routage des hôtes

Décisions relatives aux transmissions entre les hôtes La couche réseau est également responsable de diriger les paquets entre les hôtes. Un hôte peut envoyer un paquet à :

- **Lui-même** : un hôte peut s'envoyer une requête ping en envoyant un paquet à une adresse IPv4 spécifique, 127.0.0.1, appelée interface de bouclage. L'envoi d'une requête ping à l'interface de bouclage permet de tester la pile de protocoles TCP/IP sur l'hôte.
- **Un hôte local** : il s'agit d'un hôte sur le même réseau local 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.

Pour déterminer si le paquet est destiné à un hôte local ou à un hôte distant, la combinaison adresse IPv4/masque de sous-réseau du périphérique source (expéditeur) est comparée à la combinaison adresse IPv4/masque de sous-réseau du périphérique de destination.

Passerelle par défaut La passerelle par défaut correspond au périphérique réseau capable d'acheminer le trafic vers d'autres réseaux. C'est le routeur qui peut acheminer le trafic en dehors du réseau local. Une passerelle par défaut :

- achemine le trafic vers d'autres réseaux ;
- possède une adresse IP locale située dans la même plage d'adresses que les autres hôtes du réseau ;

- peut recevoir des données et en transmettre.

Utilisation de la passerelle par défaut Généralement, la table de routage d'un hôte inclut une passerelle par défaut. L'adresse IPv4 de la passerelle par défaut que reçoit l'hôte est configurée soit de manière dynamique à partir du protocole DHCP (Dynamic Host Configuration Protocol) soit manuellement. Lorsqu'une passerelle par défaut est configurée, une route par défaut est créée dans la table de routage du PC. La route par défaut est la route ou le chemin que votre ordinateur emprunte lorsqu'il essaie de contacter un réseau distant.

Tables de routage des hôtes Sur un hôte Windows, les commandes **route print** ou **netstat -r** permettent d'afficher la table de routage de l'hôte. Trois sections liées aux connexions réseau TCP/IP actuelles s'affichent alors :

- **Interface List** (liste des interfaces) : répertorie les adresses MAC et les numéros d'interface attribués à chaque interface réseau de l'hôte, notamment les adaptateurs Ethernet, Wi-Fi et Bluetooth.
- **IPv4 Route Table** (table de routage IPv4) : répertorie toutes les routes IPv4 connues, y compris les connexions directes, le réseau local et les routes locales par défaut.
- **IPv6 Route Table** (table de routage IPv6) : répertorie toutes les routes IPv6 connues, y compris les connexions directes, le réseau local et les routes locales par défaut.

6.2.2 Table de routage des routeurs

Décisions du routeur relatives à la transmission de paquets 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 la passerelle par défaut. Le routeur consulte alors sa table de routage pour déterminer où transmettre les paquets.La table de routage d'un routeur peut stocker 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 qu'elle est activée. Chacune des interfaces du routeur est connectée à un segment de réseau différent.
- **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 à l'aide d'un protocole de routage dynamique.
- **Route par défaut** : comme les hôtes, les routeurs utilisent une route par défaut en dernier recours s'il n'existe aucune autre route jusqu'au réseau souhaité dans la table de routage.

La figure 6.3 identifie les réseaux connectés directement et les réseaux distants du routeur R1.

Table de routage d'un routeur IPv4 Sur un routeur Cisco IOS, la commande **show ip route** peut être utilisée pour afficher la table de routage IPv4 du routeur.

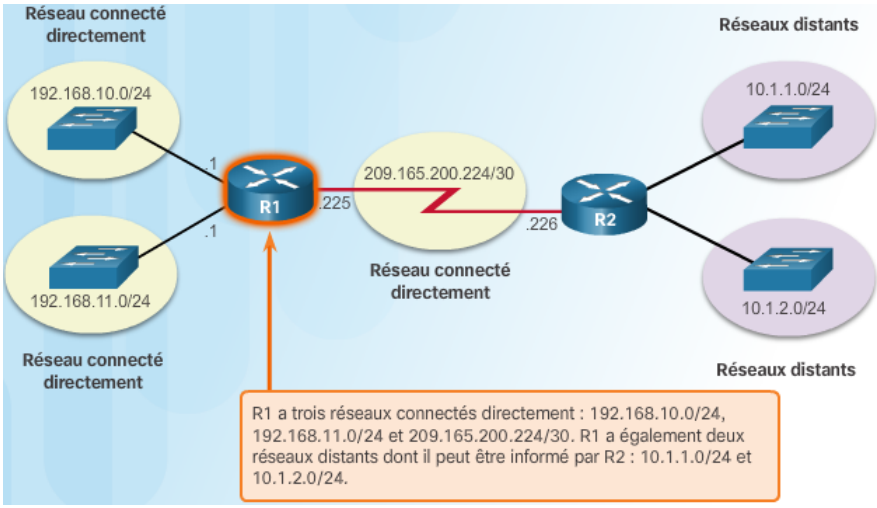


FIGURE 6.3 – Routes de réseaux connectés directement et distants

En plus des informations de routage sur les réseaux connectés directement et sur les réseaux distants, la table de routage contient également des informations sur la manière dont la route a été découverte, la fiabilité, le classement et la date de la dernière mise à jour de la route. Enfin, elle indique quelle interface utiliser pour atteindre la destination demandée

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 vers la même destination, la métrique est utilisée pour décider de la route qui apparaît dans la table de routage.

Entrées de la table de routage d'un réseau connecté directement Lorsqu'une adresse IPv4 et un masque de sous-réseau sont configurés sur une interface de routeur activée, les deux entrées suivantes sont automatiquement créées dans la table de routage :

- **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 interface locale. Cette entrée fournit l'adresse IPv4 de l'interface sur le routeur.

La figure 6.4 décrit 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.

Entrées de table de routage d'un réseau distant Plusieurs interfaces sont généralement configurées sur un routeur. La table de routage stocke des informations sur les réseaux connectés directement et distants.

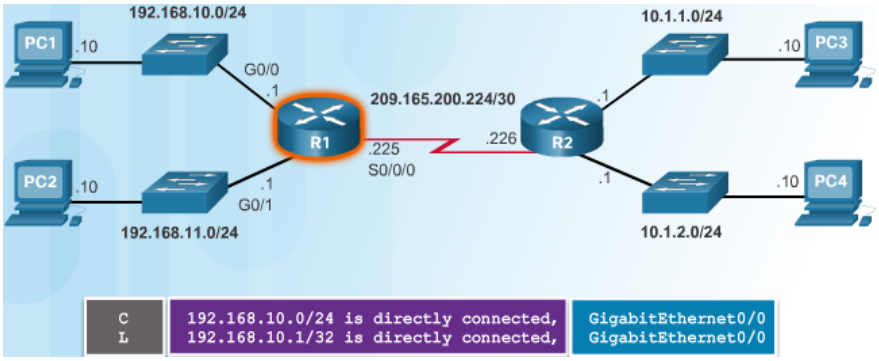


FIGURE 6.4 – Entrées de routage d'un réseau local

Adresse du tronçon 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. S'il trouve une correspondance, le routeur transfère le paquet à l'adresse du tronçon suivant à l'aide de l'interface indiquée.

Notez que les réseaux connectés directement ayant une route source C et L n'ont pas d'adresse de tronçon suivant. En effet, un routeur peut transférer des paquets directement aux hôtes sur ces réseaux via l'interface indiquée.

Il est également important de comprendre que les paquets ne peuvent pas être acheminés par le routeur s'il n'existe pas de route vers le réseau de destination dans la table de routage. Si aucune route vers le réseau de destination ne figure 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 utiliser une route statique par défaut pour créer une passerelle de dernier recours. La route par défaut peut être configurée manuellement ou être obtenue de manière dynamique.

6.3 Routeurs

6.3.1 Composants d'un routeur

Un routeur est un ordinateur 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 appareils intelligents, les routeurs nécessitent également :

- des processeurs ;
- des systèmes d'exploitation ;
- une mémoire composée de mémoire vive (RAM), de mémoire morte (ROM), de mémoire vive non volatile (NVRAM) et de mémoire Flash.

Mémoire des routeurs Les routeurs utilisent quatre types de mémoire :

- **La mémoire vive** (RAM) : il s'agit de la mémoire volatile utilisée sur les routeurs pour stocker les applications, les processus et les données requises par le processeur.

- **La mémoire morte** (ROM) : cette mémoire non volatile sert à stocker des instructions de fonctionnement essentielles et une version limitée d'IOS.
- **La mémoire vive non volatile** (NVRAM) : cette mémoire est utilisée comme stockage permanent du fichier de configuration initiale (startup-config).
- **La mémoire Flash** : il s'agit d'une mémoire non volatile d'ordinateur utilisée comme stockage permanent pour IOS et d'autres fichiers relatifs au système tels que les fichiers journaux et HTML, les fichiers de configuration vocale, les configurations de sauvegarde, etc. Lors du redémarrage d'un routeur, IOS est copié de la mémoire Flash vers la mémoire vive.

6.3.2 Démarrage du routeur

Lors du démarrage, les routeurs et les commutateurs chargent l'image IOS et le fichier de configuration initiale dans la mémoire vive, comme illustré sur la figure 6.5. La configuration en cours est modifiée lorsque l'administrateur réseau configure le périphérique. Les modifications apportées au fichier running-config doivent être enregistrées dans le fichier de configuration initiale sur la mémoire vive non volatile (NVRAM), au cas où le routeur serait redémarré ou mis hors tension.

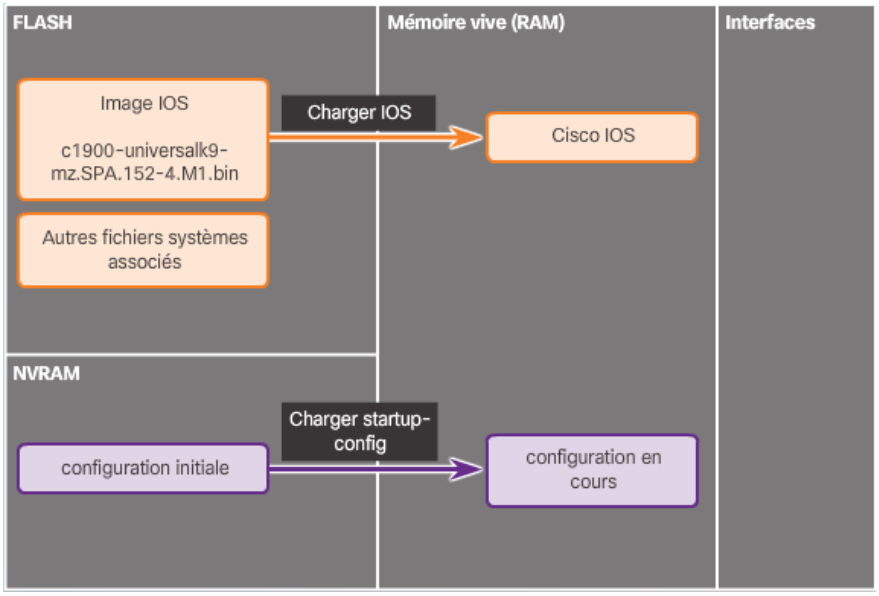


FIGURE 6.5 – Fichier copiés vers la mémoire vive lors du démarrage

6.4 Configurer un routeur

6.4.1 Configurer les paramètres initiaux

Opérations de configuration de base d'un commutateur Les tâches de configuration initiale des commutateurs sont indiquées sur la figure 6.6a.

Opérations de configuration de base d'un routeur Les tâches indiquées à la figure 6.6b doivent être traitées lors de la configuration des paramètres initiaux d'un routeur.

- **Configurer le nom du périphérique**
  - **hostname** *nom*
- **Sécuriser le mode d'exécution utilisateur**
  - **line console 0**
  - **password** *mot de passe*
  - **login**
- **Sécuriser l'accès SSH / Telnet à distance**
  - **line vty 0 15**
  - **password** *mot de passe*
  - **login**
- **Sécuriser le mode d'exécution privilégié**
  - **enable secret** *mot de passe*
- **Sécuriser tous les mots de passe dans le fichier de configuration**
  - **service password-encryption**
- **Fournir un avertissement juridique**
  - **banner motd** *délimiteur message délimiteur*
- **Configurer l'interface SVI de gestion**
  - **interface vlan 1**
  - **ip address** *adresse ip masque de sous-réseau*
  - **no shutdown**
- **Enregistrez la configuration**
  - **copy running-config startup-config**

(a) Commutateur

- **Configurer le nom du périphérique**
  - **hostname** *nom*
- **Sécuriser le mode d'exécution utilisateur**
  - **line console 0**
  - **password** *mot de passe*
  - **login**
- **Sécuriser l'accès SSH / Telnet à distance**
  - **line vty 0 15**
  - **password** *mot de passe*
  - **login**
- **Sécuriser le mode d'exécution privilégié**
  - **enable secret** *mot de passe*
- **Sécuriser tous les mots de passe dans le fichier de configuration**
  - **service password-encryption**
- **Fournir un avertissement juridique**
  - **banner motd** *délimiteur message délimiteur*
- **Enregistrez la configuration**
  - **copy running-config startup-config**

(b) Routeur

FIGURE 6.6 – Tâches de configuration

6.4.2 Configurer les interfaces

Configurer les interfaces du routeur Pour que les routeurs soient accessibles, les interfaces de routeur intrabandes doivent être configurées. Les tâches de configuration d'une interface de routeur sont énumérées à la figure 6.7. Notez qu'elles sont très similaires aux tâches de configuration d'une interface SVI sur un commutateur.

La commande **no shutdown** active l'interface, ce qui est comparable à la mise sous tension de l'interface. L'interface doit également être connectée à un autre périphérique (concentrateur, commutateur ou autre routeur) pour que la couche physique soit active.

- **Configurer l'interface**
  - **interface** *type et numéro*
  - **description** *texte descriptif*
  - **ip address** *adresse ipv4 masque de sous-réseau*
  - **no shutdown**

FIGURE 6.7 – Tâches de configuration de l'interface du routeur

Vérifier la configuration d'une interface La commande **show ip interface brief** permet de vérifier la configuration d'une interface. Le résultat généré répertorie toutes les interfaces, leur adresse IPv4 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 envoient cinq requêtes ping consécutives et mesurent les durées de transmission minimale, moyenne et maximale. Les points d'exclamation permettent de vérifier la connectivité.

Voici d'autres commandes de vérification des interfaces :

- **show ip route** - Affiche le contenu de la table de routage IPv4 stocké dans la mémoire vive.
- **show interfaces** - Affiche des statistiques pour toutes les interfaces d'un périphérique.
- **show ip interface** - Affiche des statistiques IPv4 pour toutes les interfaces d'un routeur.

6.4.3 Configurer la passerelle par défaut

Passerelle par défaut pour un hôte Pour qu'un périphérique final communique sur le réseau, les données relatives à l'adresse IP doivent être correctement configurées, notamment l'adresse de la passerelle par défaut. La passerelle par défaut est utilisée uniquement lorsque l'hôte veut transmettre un paquet à un périphérique situé sur un autre réseau. L'adresse de la passerelle par défaut est généralement celle de l'interface du routeur reliée au réseau local de l'hôte. L'adresse IP du périphérique hôte et l'adresse de l'interface du routeur doivent appartenir au même réseau.

Passerelle par défaut pour un commutateur Généralement, un commutateur de groupe de travail qui connecte entre eux des ordinateurs client est un périphérique de couche 2. En soi, un commutateur de couche 2 n'a pas besoin d'une adresse IP pour fonctionner correctement. Toutefois, si vous souhaitez vous connecter au commutateur et le gérer administrativement sur plusieurs réseaux, vous devez configurer une adresse IPv4, un masque de sous-réseau et l'adresse de la passerelle par défaut sur l'interface SVI.

L'adresse de la passerelle par défaut est généralement configurée sur tous les périphériques qui souhaitent communiquer au-delà de leur réseau local En d'autres termes, pour accéder au commutateur à distance à partir d'un autre réseau utilisant une connexion SSH ou Telnet, le commutateur doit être doté d'une interface SVI sur laquelle sont configurés une adresse IPv4, un masque de sous-réseau et l'adresse de la passerelle par défaut. Si c'est un hôte du réseau local qui accède au commutateur, alors l'adresse IPv4 de la passerelle par défaut n'est pas nécessaire.

Pour configurer une passerelle par défaut sur un commutateur, utilisez la commande de configuration globale **ip default-gateway**. L'adresse IP configurée est celle de l'interface de routeur du commutateur connecté.

Chapitre 7

Adressage IP

7.1 Adressage réseau IPv4

7.1.1 Structures de l'adresse IPv4

Parties réseau et hôte Une adresse IPv4 est une adresse hiérarchique qui se compose d'une partie réseau et d'une partie hôte. Lorsque vous déterminez la partie réseau et la partie hôte, il est nécessaire d'examiner le flux de 32 bits.

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. Si la partie réseau du flux de 32 bits est la même sur deux hôtes, ces deux hôtes résident sur le même réseau.

Masque de sous-réseau Le masque de sous-réseau sert à identifier la partie réseau et la partie hôte d'une adresse IPv4. C'est une séquence de bits 1 suivie d'une séquence de bits 0. Chaque bit du masque de sous-réseau est comparé à l'adresse IPv4, de gauche à droite, comme le montre la figure 7.1. Les 1 dans le masque de sous-réseau représentent la partie réseau, et les 0 représentent 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. Pour identifier l'adresse réseau d'un hôte IPv4, l'adresse IPv4 est soumise bit par bit à l'opération AND de manière logique avec le masque de sous-réseau.

Longueur de préfixe Il existe une méthode plus rapide d'identification du masque de sous-réseau, appelée la longueur de préfixe.

En fait, 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 », soit le signe « / » suivi du nombre de bits définis sur 1. Il suffit donc de compter le nombre de bits du masque de sous-réseau et d'y ajouter une barre oblique, comme illustré sur la figure 7.2

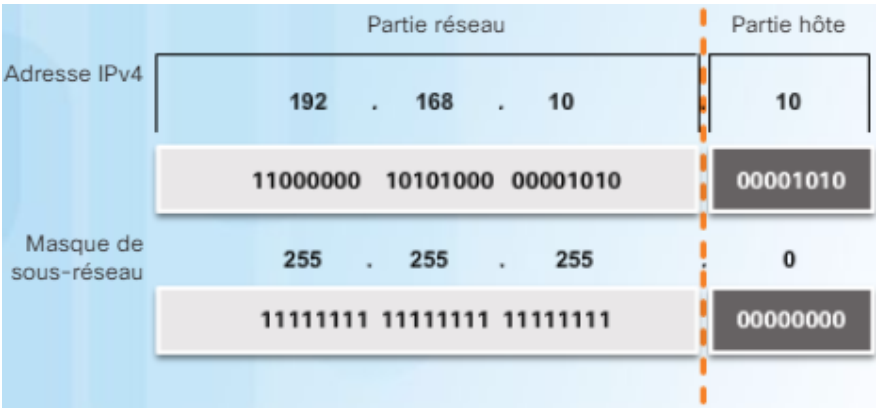


FIGURE 7.1 – Comparaison de l'adresse IP et du masque de sous-réseau

Masque de sous-réseau	Adresse 32 bits	Longueur de préfixe
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

FIGURE 7.2 – Longueur de préfixe

Adresses réseau, d'hôte et de diffusion Chaque adresse réseau contient (ou identifie) des adresses d'hôtes et une adresse de diffusion, comme décrit à la figure 7.3.

7.1.2 Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

Attribution d'une adresse IPv4 statique à un hôte Les adresses IP peuvent être attribuées aux périphériques de manière statique ou dynamique. Par exemple, les imprimantes, serveurs et périphériques réseau doivent conserver la même adresse IP. Toutefois, il serait fastidieux de saisir des adresses statiques sur chaque hôte d'un grand réseau. Il est important de tenir à jour une liste exacte des adresses IP statiques attribuées à chaque périphérique.

Attribution d'une adresse IPv4 dynamique à un hôte Sur les grands réseaux, la méthode DHCP est généralement privilégiée pour l'attribution des adresses IPv4. L'autre avantage de cette méthode réside dans le fait que les adresses ne sont pas attribuées aux hôtes de manière permanente, 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.

Communication IPv4 Un hôte connecté à un réseau peut communiquer avec les autres périphériques de trois façons :

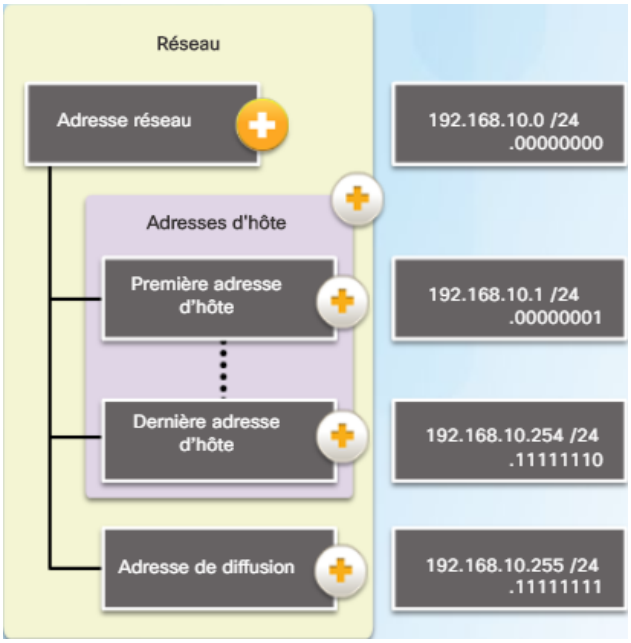


FIGURE 7.3 – Les différents types d'adresse du réseau 192.168.10.0 /24

- **La monodiffusion** : processus consistant à envoyer un paquet d'un hôte à un autre.
- **La diffusion** : processus consistant à envoyer un paquet d'un hôte à tous les autres hôtes du réseau.
- **La multidiffusion** : processus consistant à envoyer un paquet d'un hôte à un groupe d'hôtes spécifique (qui peuvent se trouver sur différents réseaux).

Dans les trois cas, l'adresse IPv4 de l'hôte émetteur est placée dans l'en-tête du paquet comme adresse source.

Transmission 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 l'adresse du périphérique de destination comme adresse de destination et peuvent être acheminés sur un interréseau.

Dans un réseau IPv4, l'adresse monodiffusion appliquée à un périphérique final est désignée sous le nom d'adresse d'hôte. Dans une monodiffusion, les adresses attribuées aux deux périphériques finaux sont utilisées comme adresses IPv4 source et de destination.

Transmission de diffusion En diffusion, le paquet contient une adresse IPv4 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.

Transmission multidiffusion La transmission multidiffusion réduit le volume du trafic en permettant à un hôte d'envoyer un seul paquet à un groupe d'hôtes désigné inscrits à un groupe de

multidiffusion.

IPv4 a réservé les adresses 224.0.0.0 à 239.255.255.255 comme plage de multidiffusion. Les adresses de multidiffusion IPv4 du bloc 224.0.0.0 à 224.0.0.255 sont réservées à la multidiffusion sur le réseau local uniquement. Les adresses de multidiffusion de réseau local réservées s'appliquent principalement aux protocoles de routage qui utilisent la transmission multidiffusion pour échanger des informations de routage.

7.1.3 Types d'adresses IPv4

Adresses IPv4 publiques et privées Les adresses IPv4 publiques sont acheminées de manière globale entre les routeurs des FAI (fournisseurs d'accès à Internet). Toutefois, toutes les adresses IPv4 disponibles ne peuvent pas être utilisées sur Internet. Certains blocs d'adresses appelés adresses privées sont utilisés par la plupart des entreprises pour attribuer des adresses IPv4 aux hôtes internes.

Les adresses IPv4 privées ont été créées au milieu des années 1990 en raison de la pénurie d'espace d'adresses IPv4. Les adresses IPv4 privées ne sont pas uniques et peuvent être utilisées par un réseau interne.

Les blocs d'adresses privées sont les suivants :

- 10.0.0.0 /8 ou 10.0.0.0 à 10.255.255.255 ;
- 172.16.0.0 /12 ou 172.16.0.0 à 172.31.255.255 ;
- 192.168.0.0 /16 ou 192.168.0.0 à 192.168.255.255.

Il est important de savoir que les adresses appartenant à ces blocs ne sont pas autorisées sur Internet et doivent être filtrées (rejetées) par les routeurs Internet.

Adresses IPv4 d'utilisateurs spéciaux Certaines adresses, telles que l'adresse réseau et l'adresse de diffusion ne peuvent pas être attribuées à des hôtes. Il existe également des adresse spéciales qui peuvent être attribuées aux hôtes, mais des restrictions s'appliquent sur les interactions de ces hôtes sur le réseau.

- **Adresses de bouclage** (127.0.0.0 /8 ou 127.0.0.1 à 127.255.255.254) : couramment appelées 127.0.0.1, ces adresses spéciales sont utilisées par des hôtes pour diriger le trafic vers eux-mêmes. Par exemple, elles peuvent être utilisées sur un hôte pour vérifier si la configuration TCP/IP est opérationnelle.
- **Adresses locales-liens** (169.254.0.0 /16 ou 169.254.0.1 à 169.254.255.254) : plus connues sous le nom d'adresses APIPA (adressage IP privé automatique), elles sont utilisées par un client DHCP Windows pour se configurer automatiquement si aucun serveur DHCP n'est disponible. Elles sont utiles dans une connexion peer-to-peer.
- **Adresses TEST-NET** (192.0.2.0/24 ou 192.0.2.0 à 192.0.2.255) : ces adresses sont réservées à des fins pédagogiques et utilisées dans la documentation et dans des exemples de réseau.

Attribution des adresses IP Pour que les entreprises ou organisations puissent prendre en charge les hôtes réseau (par exemple les serveurs web) accessibles depuis Internet, elles 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. Elles sont gérées par l'Internet Assigned Numbers Authority (IANA).

7.2 Adressage réseau IPv6

7.2.1 Nécessité du protocole IPv6

Le protocole 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 34.10^{37} d'adresses disponibles. Toutefois, l'IPv6 ne se limite pas à la multiplication des adresses. 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 inexistantes dans le protocole ICMP pour l'IPv4 (ICMPv4).

7.2.2 Adressage 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. Le format privilégié pour noter une adresse IPv6 est x :x :x :x :x :x :x :x, où chaque « x » est constitué de quatre valeurs hexadécimales. Il existe deux règles permettant de réduire le nombre de chiffres requis pour représenter une adresse IPv6 :

- **Omettre les zéros en début de segment**
- **Omettre les séquences composées uniquement de zéros** : Une suite de deux fois deux points (: :) peut remplacer toute chaîne unique et contiguë d'un ou plusieurs segments de 16 bits composés uniquement de 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.

7.2.3 Types d'adressage IPv6

Types d'adresses IPv6 Il existe trois types d'adresses IPv6 :

- **monodiffusion** ;
- **multidiffusion** ;
- **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.

Contrairement à l'IPv4, l'IPv6 n'a pas d'adresse de diffusion. Cependant, il existe une adresse de multidiffusion destinée à tous les nœuds IPv6 et qui offre globalement les mêmes résultats.

Longueur de préfixe IPv6 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 être comprise entre 0 et 128. La longueur de préfixe IPv6 standard pour les réseaux locaux et la plupart des autres types de réseau est /64.

Adresses de monodiffusion 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. L'adresse IPv6 de destination peut, quant à elle, être une adresse de monodiffusion ou de multidiffusion.

Les types d'adresses de diffusion IPv6 les plus courants sont les adresses de diffusion globale et les adresses de monodiffusion link-local.

- **Monodiffusion globale** : Une adresse de diffusion globale est similaire à une adresse IPv4 publique. Ces adresses sont uniques au monde et routables sur Internet. Les adresses de diffusion globale peuvent être configurées de manière statique ou attribuées dynamiquement.
- **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 routables au-delà de la liaison. En d'autres termes, les routeurs ne transmettent aucun paquet avec une adresse source ou de destination link-local.
- **Adresse locale unique** : L'adresse de monodiffusion locale unique est un autre type d'adresse de monodiffusion. 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 et ne doivent pas être traduites en adresses IPv6 globales. Les adresses locales uniques sont comprises entre FC00 : :/7 et FDFF : :/7.

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 link-local source ou de destination ne peuvent pas être acheminés au-delà de leur liaison d'origine.

L'adresse de diffusion globale n'est pas obligatoire. Toutefois, 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.

7.2.4 Adresses de monodiffusion IPv6

Structure d'une adresse de diffusion globale IPv6 Les adresses de diffusion globale IPv6 sont uniques au monde et routables (Internet IPv6). L'ICANN (Internet Committee for Assigned Names and Numbers) attribue des blocs d'adresses IPv6 aux cinq organismes d'enregistrement

Internet locaux. Actuellement, seules des adresses de diffusion globale dont les trois premiers bits sont 001 ou 2000 : :/3 sont attribuées. En d'autres termes, le premier chiffre hexadécimal d'une adresse de diffusion globale commence par 2 ou par 3. 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.

Une adresse de diffusion globale se compose de trois parties, comme illustré sur la figure 7.4 :

- **Préfixe de routage global** : C'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. Généralement, les RIR attribuent le préfixe global de routage /48 aux clients, à savoir tous les clients potentiels, des réseaux d'entreprise aux réseaux particuliers.
- **ID de sous-réseau** : L'ID de sous-réseau est utilisé par une entreprise pour identifier les sous-réseaux au sein de son site. Plus l'ID de sous-réseau est un nombre important, plus il y a de sous-réseaux disponibles.
- **ID d'interface** : Un hôte unique peut avoir plusieurs interfaces, chacune dotée d'une ou de plusieurs adresses IPv6. Dans la plupart des cas, il est fortement recommandé d'utiliser des sous-réseaux /64, c'est-à-dire un ID d'interface 64 bits

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 attribuée, 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.

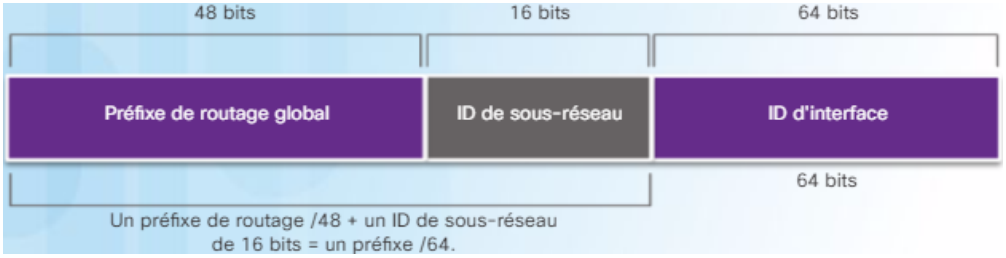


FIGURE 7.4 – Préfixe de routage global IPv6 /48

Configuration statique d'une adresse de diffusion globale La plupart des commandes de configuration et de vérification IPv6 sont semblables à celles 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 permettant de configurer une adresse de monodiffusion globale IPv6 sur une interface est **ipv6 address** *adresse IPv6/longueur du préfixe*.

La configuration manuelle de l'adresse IPv6 sur un hôte est similaire à celle d'une adresse IPv4.

Un périphérique peut obtenir automatiquement une adresse de diffusion globale IPv6 de deux façons :

- La configuration automatique des adresses sans état (SLAAC)
- DHCPv6 avec état

Configuration dynamique - SLAAC La configuration automatique des adresses sans état (SLAAC) est une méthode permettant à un périphérique d'obtenir son préfixe, la longueur de préfixe, l'adresse de la passerelle par défaut et d'autres informations auprès d'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 des messages d'annonce de routeur ICMPv6 toutes les 200 secondes à tous les périphériques IPv6 du réseau. Un message d'annonce de routeur est également envoyé en réponse à un hôte qui envoie un message de sollicitation 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.

Le message d'annonce de routeur contient les éléments suivants :

- **le préfixe de réseau et la longueur de préfixe**, qui indiquent au périphérique le réseau auquel il appartient ;
- **l'adresse de la passerelle par défaut**, qui est une adresse link-local et l'adresse IPv6 source du message d'annonce de routeur ;
- **les adresses DNS et le nom de domaine**, c'est-à-dire les adresses des serveurs DNS et un nom de domaine.

Il existe trois options de messages d'annonce de routeur :

- **SLAAC**.
- **SLAAC avec un serveur DHCPv6 sans état** : le message d'annonce de routeur suggère aux périphériques d'utiliser :
  - SLAAC pour créer sa propre adresse de diffusion globale IPv6 ;
  - l'adresse link-local du routeur, l'adresse IPv6 source du message d'annonce de routeur comme adresse de la passerelle par défaut ;
  - un serveur DHCPv6 sans état pour obtenir d'autres informations telles que l'adresse d'un serveur DNS et un nom de domaine.
- DHCPv6 avec état (pas de SLAAC) : similaire à DHCP pour IPv4.

Adresses link-local Tous les périphériques IPv6 doivent avoir une adresse link-local IPV6. Une adresse link-local peut être établie dynamiquement ou configurée manuellement comme adresse link-local statique.

7.2.5 Adresses de multidiffusion IPv6

Adresses de multidiffusion IPv6 attribuées Les adresses de multidiffusion IPv6 ont le préfixe FF00 : :/8. Il existe deux types d'adresses de multidiffusion IPv6 :

- **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 rejoindre. Cette opération a le même effet qu'une adresse de diffusion IPv4.
- **Groupe de multidiffusion à tous les routeurs** FF02 : :2 : il s'agit d'un groupe de multidiffusion que peuvent rejoindre tous les routeurs IPv6.

- **Les adresses de multidiffusion de nœud sollicité** : Une adresse de multidiffusion de nœud sollicité est comparable à une adresse de multidiffusion à tous les nœuds. Elle offre l'avantage d'être mappée à une adresse de multidiffusion Ethernet spéciale. Cela permet à la carte réseau Ethernet de filtrer la trame en examinant l'adresse MAC de destination sans l'envoyer au processus IPv6 pour voir si le périphérique est la cible prévue du paquet IPV6.

7.3 Vérification de la connectivité

ICMPv4 et ICMPv6 Bien que le protocole IP tâche de réaliser ses promesses, 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. Le protocole ICMP est disponible pour IPv4 et IPv6. Les messages ICMP communs à ICMPv4 et à ICMPv6 sont les suivants :

- **Host confirmation** : Un message ICMP Echo permet de déterminer si un hôte est fonctionnel.
- **Destination or Service Unreachable** : Lorsqu'un hôte ou une passerelle ne peut pas acheminer un paquet reçu, 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.
- **Time exceeded** : 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.
- **Route redirection**

Messages de sollicitation et d'annonce de routeur ICMPv6 L'ICMPv6 offre de nouvelles fonctions et fonctionnalités avancées qui n'existent pas dans l'ICMPv4. Les messages ICMPv6 sont encapsulés dans l'IPv6. ICMPv6 offre quatre nouveaux protocoles dans le cadre du protocole NDP (Neighbor Discovery Protocol) ou ND :

1. Messages envoyés entre un routeur IPv6 et un périphérique IPv6 :
   - Message de sollicitation de routeur (RS) :
   - Message d'annonce de routeur (RA) :
2. Messages envoyés entre des périphériques IPv6. Ils sont utilisés pour la résolution d'adresse et la détection d'adresse dupliquée.
   - Message de sollicitation de voisin
   - Messages d'annonce de voisin

Chapitre 8

Segmentation des réseaux IP en sous-réseaux

8.1 Segmenter un sous-réseau IPv4 en sous-réseau

8.1.1 Segmentation du réseau

Domaines de diffusion Dans un réseau LAN Ethernet, les périphériques utilisent des diffusions pour localiser les éléments suivants :

- **Les autres périphériques** : les périphériques utilisent le protocole ARP qui envoie des diffusions de couche 2 à une adresse IPv4 connue du réseau local pour connaître son adresse MAC.
- **Les services** : en règle générale, les configurations d'adresse IPv4 des hôtes sont définies via le protocole DHCP, qui envoie des messages de diffusion sur le réseau local afin de localiser un serveur DHCP.

Les commutateurs diffusent les messages de diffusion sur toutes les interfaces, sauf celle d'où les messages proviennent. Les routeurs ne diffusent pas les messages de diffusion. Chaque interface du routeur est connectée à un domaine de diffusion et les messages de diffusion sont uniquement diffusés au sein de son domaine.

Pourquoi créer des sous-réseaux ? La segmentation en sous-réseaux réduit le trafic global et améliore les performances réseau. Elle permet également aux administrateurs de mettre en œuvre des politiques de sécurité, notamment pour définir si les différents sous-réseaux sont autorisés ou non à communiquer entre eux.

8.1.2 Segmenter un réseau IPv4 en sous-réseaux

Limites d'octet Pour créer des sous-réseaux IPv4, on utilise un ou plusieurs bits d'hôte en tant que bits réseau. Pour cela, il faut étendre le masque de sous-réseau pour emprunter quelques bits de la portion 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. Le plus simple est de segmenter les réseaux à la limite d'octet de /8, /16 et /24.

Création de sous-réseaux au niveau de la limite d'octet Pour comprendre l'intérêt de créer des sous-réseaux à la limite d'octet, prenons l'exemple qui suit. Supposons qu'une entreprise ait choisi comme adresse réseau interne l'adresse privée 10.0.0.0/8. Cette adresse réseau permet de connecter 16 777 214 hôtes dans un seul domaine de diffusion. Évidemment, ce n'est pas idéal.

Une solution consiste à segmenter le réseau à la limite d'octet /24, comme illustré à la figure 8.1. Cela lui permettrait de définir 65 536 sous-réseaux capables chacun de connecter 254 hôtes. La limite /24 est la plus utilisée pour la segmentation en sous-réseaux, car elle est pratique et permet de définir un nombre raisonnable d'hôtes.

Adresse des sous-réseaux (65 536 sous-réseaux possibles)	Plage d'hôtes (254 hôtes possibles par sous-réseau)	Diffusion
10.0.0.0/24	10.0.0.1 - 10.0.0.254	10.0.0.255
10.0.1.0/24	10.0.1.1 - 10.0.1.254	10.0.1.255
10.0.2.0/24	10.0.2.1 - 10.0.2.254	10.0.1.255
...	...	...
10.0.255.0/24	10.0.255.1 - 10.0.255.254	10.0.255.255
10.1.0.0/24	10.1.0.1 - 10.1.0.254	10.1.0.255
10.1.1.0/24	10.1.1.1 - 10.1.1.254	1.1.1.0.255
10.1.2.0/24	10.1.2.1 - 10.1.2.254	10.1.2.0.255
...	...	...
10.100.0.0/24	10.100.0.1 - 10.100.0.254	10.100.0.255
...	...	...
10.255.255.0/24	10.255.255.1 - 10.255.255.254	10.255.255.255

FIGURE 8.1 – Segmentation du réseau 10.x.x.0/24

Sous-réseaux sans classe Dans les exemples que nous avons vus jusqu'à présent, des bits d'hôte étaient empruntés aux préfixes de réseau courants /8, /16 et /24. Toutefois, les sous-réseaux peuvent emprunter des bits d'hôte de n'importe quelle position pour créer d'autres masques.

Par exemple, la segmentation d'une adresse réseau /24 implique souvent l'utilisation de préfixes plus longs qui empruntent des bits au quatrième octet. L'administrateur dispose ainsi d'une plus grande flexibilité lorsqu'il attribue les adresses réseau à un nombre réduit de périphériques finaux. Un exemple est présenté 8.2.

8.1.3 Segmentation du réseau pour répondre aux besoins

Deux considérations sont à prendre en compte lors de la planification de sous-réseaux :

- le nombre d'adresses d'hôtes requis pour chaque réseau ;
- le nombre de sous-réseaux individuels requis.

Le tableau de la figure 8.3 indique les détails de la segmentation d'un réseau /24. Plus le nombre de bits empruntés pour créer des sous-réseaux est élevé, moins il y a d'hôtes disponibles.

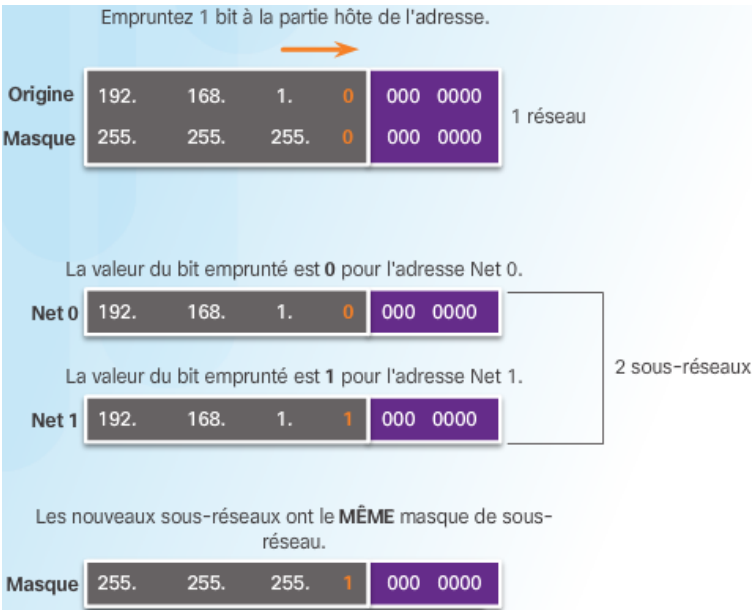


FIGURE 8.2 – Réseau 192.168.1.0/25

Longueur du préfixe	Masque de sous-réseau	Masque de sous-réseau (binaire) (n = réseau, h = hôte)	Nombre de sous-réseaux	Nombre d'hôtes
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	64	2

FIGURE 8.3 – Segmentation d'un réseau /24

8.1.4 Avantages du masquage de sous-réseau de longueur variable

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 intéressante. Mais, bien souvent, ce n'est pas le cas, comme illusté sur la figure 8.4.

Masques de sous-réseau de longueur variable 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

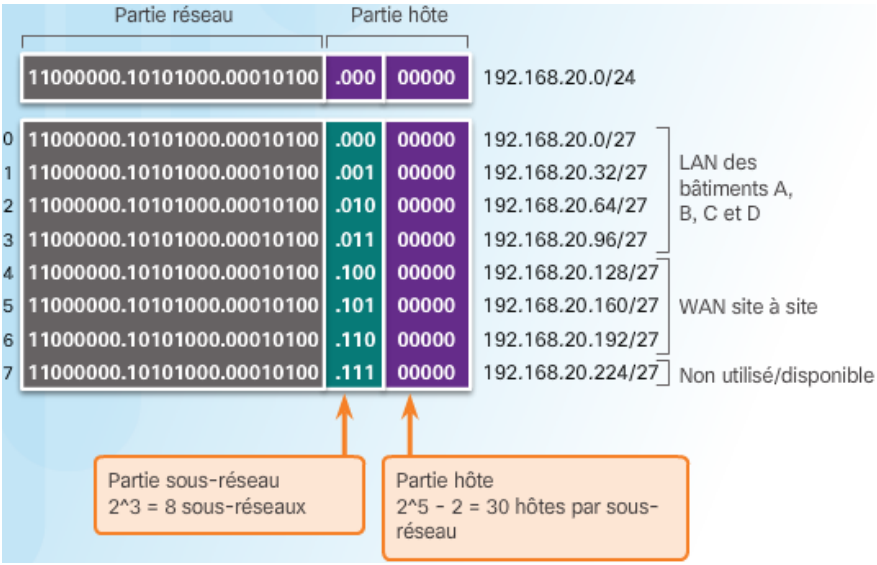


FIGURE 8.4 – Schéma de sous-réseaux de base

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.

VLSM de base Pour mieux comprendre le processus VLSM, revenez à l'exemple précédent présenté à la figure 8.4. Le réseau 192.168.20.0/24 a été divisé en huit sous-réseaux de même taille. Sept des huit 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. 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 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. Dans cet exemple, le dernier sous-réseau, 192.168.20.224/27, est encore subdivisé. Pour obtenir deux adresses utilisables, 2 bits d'hôte doivent rester dans la partie hôte. Étant donné que l'espace d'adresses segmenté 192.168.20.224/27 comporte 5 bits d'hôte, 3 bits supplémentaires peuvent être empruntés, ce qui laisse 2 bits dans la partie hôte.

Le schéma de segmentation VLSM permet de réduire suffisamment le nombre d'adresses par sous-réseau pour les liaisons WAN. 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 5 sous-réseaux supplémentaires disponibles pour les réseaux étendus.

Diagramme VLSM Un diagramme VLSM peut être utilisé pour 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.

Afin d'utiliser plus efficacement l'espace d'adressage, des sous-réseaux /30 sont créés pour les liaisons de réseau étendu, comme le montre le diagramme VLSM de la figure 8.5. Pour conserver ensemble les blocs d'adresses contiguës inutilisées, le dernier sous-réseau /27 a été subdivisé une nouvelle fois pour créer les sous-réseaux /30. Les 3 premiers sous-réseaux ont été affectés aux liaisons de réseau étendu.

	Réseau /27	Hôtes
Bât. A	.0	.1 - .30
Bât. B	.32	.33 - .62
Bât. C	.64	.65 - .94
Bât. D	.96	.97 - .126
Capacités	.128	.129 - .158
Capacités	.160	.161 - .190
Capacités	.192	.193 - .222
	.224	.225 - .254

	Réseau /30	Hôtes
WAN R1–R2	.224	.225 - .226
WAN R2–R3	.228	.229 - .230
WAN R3–R4	.232	.233 - .234
Capacités	.236	.237 - .238
Capacités	.240	.241 - .242
Capacités	.244	.245 - .246
Capacités	.248	.249 - .250
Capacités	.252	.253 - .254

FIGURE 8.5 – Segmentation en sous-réseaux VLSM de 192.168.20.0/24

8.2 Schémas d'adressage

Préparation de l'adressage d'un réseau Il y a trois critères principaux 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.
- **La surveillance de la sécurité et des performances des hôtes** : le trafic réseau est examiné, à la recherche d'adresses IP source qui génèrent ou reçoivent un nombre trop important de paquets. Lorsque l'adressage réseau est planifié et documenté correctement, les périphériques réseau posant problème doivent être facilement identifiés.

Attribution d'adresses à des périphériques Dans un réseau, il existe différents types d'appareils nécessitant des adresses, à savoir :

- **Les clients d'utilisateurs finaux** : la plupart des réseaux attribuent des adresses de manière dynamique à l'aide du protocole DHCP. Cela réduit la charge de travail des techniciens réseau et élimine les erreurs de saisie. Par ailleurs, les adresses ne sont affectées que pendant une certaine durée. En cas de modification du schéma de segmentation en sous-réseaux, le serveur DHCP doit être reconfiguré et les clients doivent renouveler leurs adresses IP. Les clients IPv6 peuvent obtenir des informations d'adressage avec DHCPv6 ou SLAAC.
- **Les serveurs et les périphériques**, qui doivent avoir une adresse IP statique prévisible. Utilisez un système de numérotation cohérent pour ces appareils.
- **Les serveurs qui sont accessibles via Internet** doivent également être disponibles pour les utilisateurs distants dans la plupart des réseaux. En général, des adresses privées sont attribuées en interne à ces serveurs, et le routeur ou le pare-feu situé en périphérie du réseau doit être configuré de manière à traduire les adresses internes en adresses publiques.
- **Les périphériques intermédiaires** : des adresses sont attribuées à ces périphériques pour la gestion, la surveillance et la sécurité du réseau. Puisque nous devons savoir comment communiquer avec les périphériques intermédiaires, ils doivent avoir des adresses statiques prévisibles.
- **La passerelle** : une adresse IP est attribuée à chacune des interfaces des routeurs et pare-feu servant 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.

8.3 Critères de conception à prendre en compte pour les réseaux IPv6

Adresse de monodiffusion globale IPv6 La segmentation en sous-réseaux IPv6 exige une approche différente de celle des sous-réseaux IPv4. En effet, en raison du grand nombre d'adresses IPv6, le problème du maintien des adresses ne se pose plus. Le schéma d'adresse IPv6 peut se concentrer sur la meilleure approche hiérarchique afin de gérer et d'attribuer les sous-réseaux IPv6.

Souvenez-vous qu'il existe deux types d'adresses IPv6 attribuables. Les adresses link-local IPv6 ne sont jamais segmentées en sous-réseaux, car elles n'existent que sur la liaison locale. En revanche, les adresses de monodiffusion globale IPv6 peuvent être segmentées en sous-réseau.

L'adresse de monodiffusion globale IPv6 comporte généralement un préfixe de routage global /48, un ID de sous-réseau de 16 bits et un ID d'interface de 64 bits.

Segmentation du réseau en sous-réseaux à l'aide d'ID de sous-réseau Les entreprises peuvent utiliser la partie ID de sous-réseau de 16 bits de l'adresse de monodiffusion globale IPv6 pour créer des sous-réseaux internes.

L'ID de sous-réseau fournit plus de sous-réseaux et prend en charge plus d'hôtes que nécessaire. Par exemple, la partie de 16 bits permet de :

- créer jusqu'à 65 536 sous-réseaux /64, sans même avoir à emprunter des bits à l'ID d'interface de l'adresse ;
- prendre en charge jusqu'à 18.10^{18} d'adresses IPv6 d'hôte par sous-réseau.

La mise en œuvre des sous-réseaux IPv6 est également plus simple que celle des sous-réseaux IPV4, puisqu'aucune conversion en binaire n'est requise. Pour déterminer le sous-réseau disponible suivant, il suffit de compter en hexadécimal.

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 8.6, 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. Un sous-réseau /64 est attribué à chaque segment LAN et à la liaison WAN.

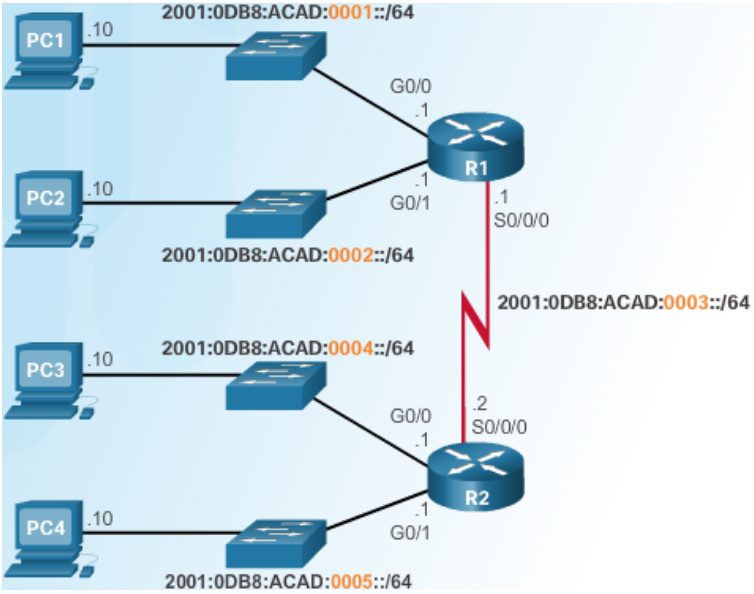


FIGURE 8.6 – Bloc d'adresses : 2001 :0DB8 :ACAD : :/48

Chapitre 9

Couche transport

9.1 Protocoles de couche transport

9.1.1 Transport des données

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 des données qui sont envoyées d'une application située sur un hôte source à une autre application située sur un hôte de destination. Et ce, sans se soucier du type de l'hôte de destination, du type de support que les données doivent emprunter, du chemin suivi par ces données, de l'encombrement de la liaison ni de la taille du réseau. Comme le montre la figure 9.1, la couche transport constitue la liaison entre la couche application et les couches inférieures chargées de la transmission sur le réseau.

Responsabilités de la couche transport

- **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. 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 taille appropriée. Il s'agit notamment de l'encapsulation devant s'appliquer à chaque bloc de données. Par ailleurs, 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 et utilisable par 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 servent

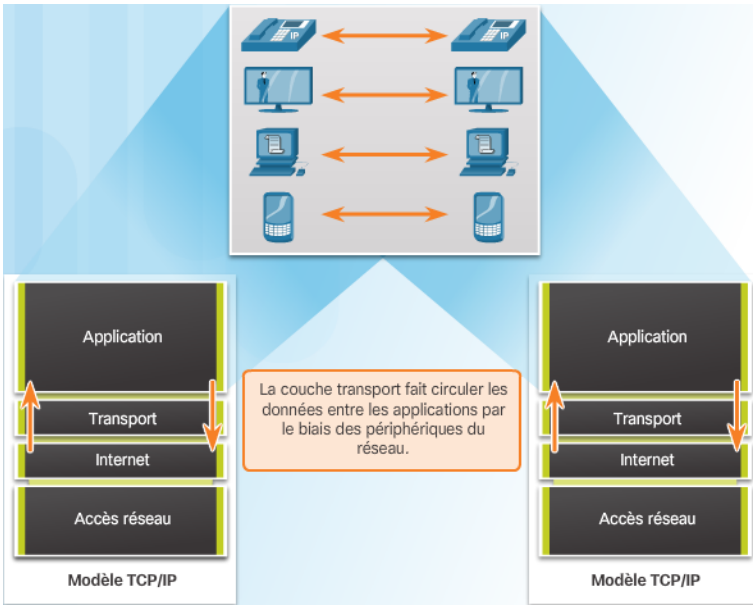


FIGURE 9.1 – Activation de la communication des applications sur les périphériques

à réassembler les blocs de données en flux qui seront transmis à la couche application.

- **Identification des applications** : Pour que les flux de données atteignent les applications auxquelles ils sont destinés, la couche transport doit identifier l'application cible. Pour cela, la couche transport affecte un identificateur à chaque application, appelé numéro de port. Chaque processus logiciel ayant besoin d'accéder au réseau se voit affecter un numéro de port unique sur son hôte.

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 nécessiter d'utiliser toute la bande passante disponible. De fait, cela empêche d'autres communications d'avoir lieu en même temps. En outre, cela rend également difficiles la reprise sur erreur et la retransmission des données endommagées.

La figure 9.2 montre que la segmentation des données en éléments plus petits permet à plusieurs communications différentes, provenant de nombreux utilisateurs, d'être imbriquées (multiplexées) sur le même réseau.

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.

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 9.3. Le protocole IP utilise ces protocoles de transport pour permettre aux hôtes de communiquer et de transmettre des données.

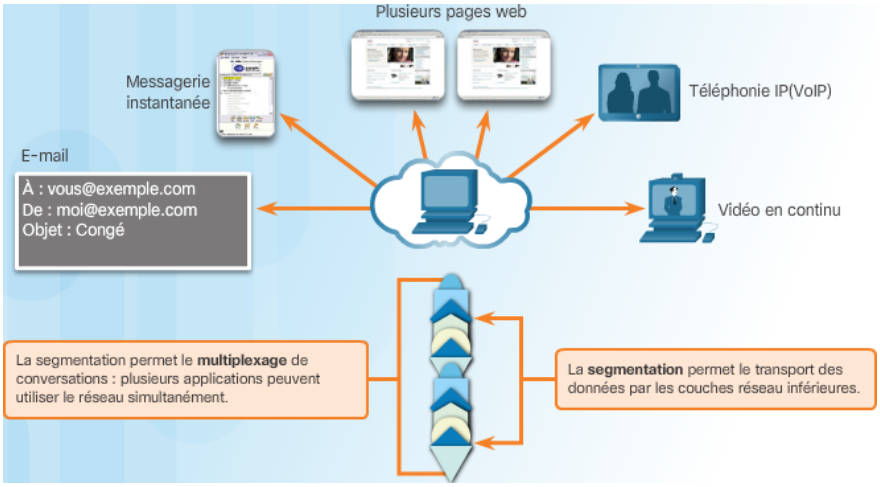


FIGURE 9.2 – Services de la couche transport

Le protocole TCP est un protocole de couche transport fiable et complet, qui garantit que toutes les données arrivent à destination. Toutefois, cela nécessite des champs supplémentaires dans l'en-tête TCP, ce qui augmente la taille du paquet et engendre des retards. En revanche, le protocole UDP est un protocole de couche transport plus simple, qui ne permet pas de garantir la fiabilité du transport. Il compte donc moins de zones et s'avère plus rapide que le protocole TCP. Le choix d'un protocole de couche transport le mieux adapté à une application donnée se fait à partir des caractéristiques de ces protocoles, illustrées figure 9.4.

Protocole TCP Avec le protocole TCP, les trois fonctions de fiabilité de base sont :

- numérotation et suivi des segments de données transmis à un hôte donné à partir d'une application spécifique ;
- accusé de réception des données reçues ;
- retransmission des données pour lesquelles aucun accusé de réception n'a été reçu, après un certain temps.

Protocole UDP Le protocole UDP fournit des fonctions de base permettant d'acheminer des segments de données entre les applications appropriées tout en ne nécessitant que très 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.

9.1.2 Présentation des protocoles TCP et UDP

Fonctions 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 conversations.

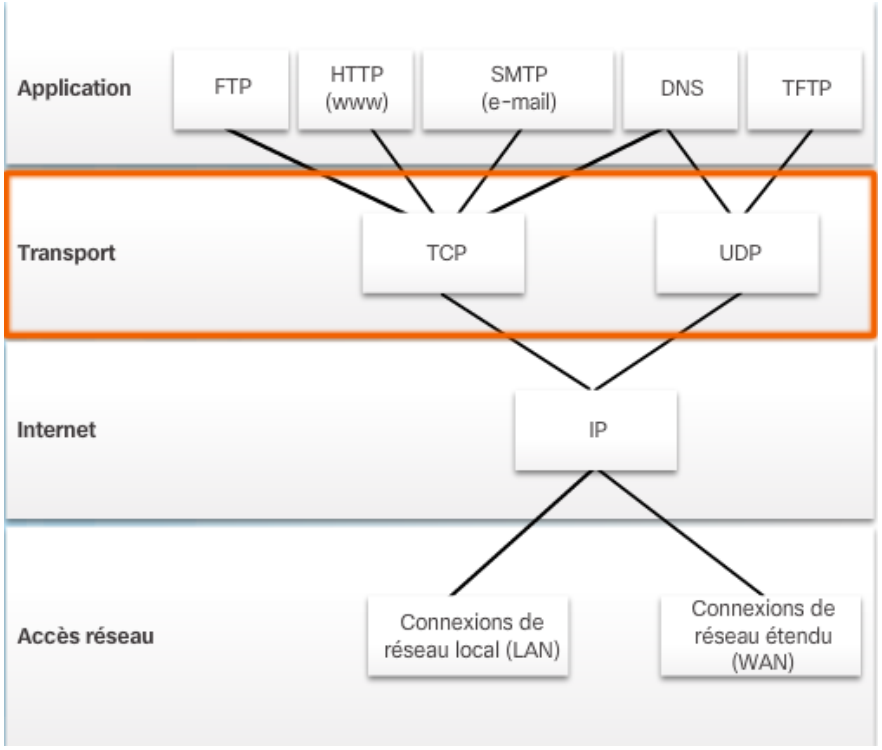


FIGURE 9.3 – Les couches transport et réseau

- **Établissement d'une 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. 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.
- **Acheminement fiable** : Dans le contexte des réseaux, la fiabilité consiste à veiller à ce que chaque segment envoyé par la source parvienne à destination.
- **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 puissance de traitement. 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 rendre inutile la retransmission des données lorsque les ressources de l'hôte de réception sont saturées.

En-tête TCP Le protocole TCP est un protocole avec état. Un protocole avec état est un protocole qui contrôle l'état de la session de communication. Pour suivre l'état d'une session, le protocole TCP

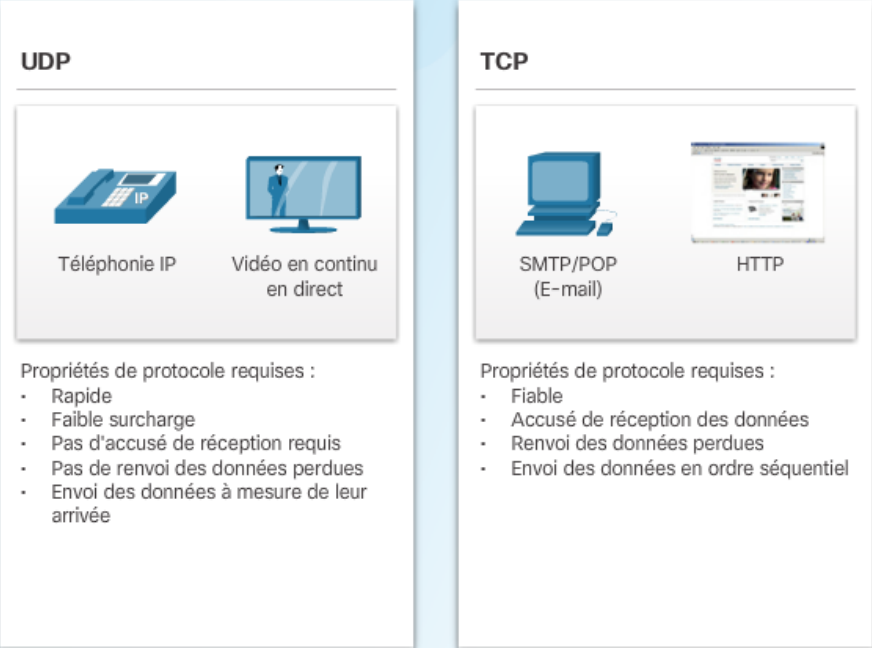


FIGURE 9.4 – Les caractéristiques des protocoles UDP et TCP

enregistre les informations qu'il a envoyées et les informations qu'il a reçues. La session avec état commence avec l'établissement de la session et se termine lorsque la session est interrompue.

Comme l'illustre la figure 9.5, chaque segment TCP utilise 20 octets de surcharge dans l'en-tête pour encapsuler les données de la couche application :

- **Port source (16 bits) et port de destination (16 bits)** : utilisés pour identifier l'application.
- **Numéro d'ordre (32 bits)** : utilisé pour réorganiser les données.
- **Numéro d'accusé de réception (32 bits)** : indique les données qui ont été reçues.
- **Longueur d'en-tête (4 bits)** : connue sous le nom de « décalage de données ». Indique la longueur de l'en-tête du segment TCP.
- **Réservé (6 bits)** : champ réservé pour les futures évolutions.
- **Bits de contrôle (6 bits)** : comprennent des codes de bits, ou indicateurs, indiquant l'objectif et la fonction du segment TCP.
- **Taille de fenêtre (16 bits)** : indique le nombre de segments pouvant être acceptés en même temps.
- **Somme de contrôle (16 bits)** : utilisée pour le contrôle des erreurs dans l'en-tête et les données de segment.
- **Urgent (16 bits)** : indique si les données sont urgentes.

Fonctionnalités du protocole UDP Les fonctionnalités du protocole UDP sont :

- les données sont reconstituées selon l'ordre de réception ;

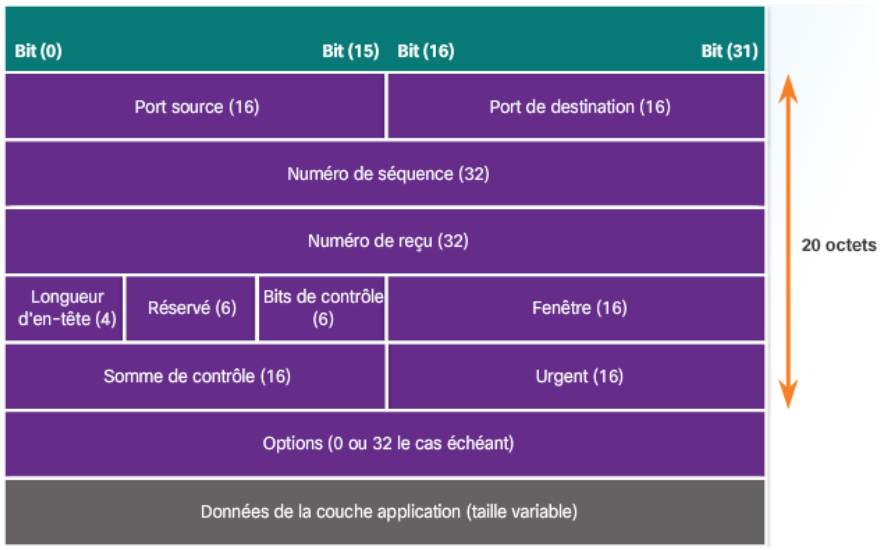


FIGURE 9.5 – Segment TCP

- les segments perdus ne sont pas renvoyés ;
- pas d'établissement de session ;
- l'expéditeur n'est pas informé de la disponibilité des ressources.

En-tête UDP Les blocs de communications utilisés dans le protocole UDP sont appelés des datagrammes, comme le montre la figure 9.6. Ces datagrammes sont envoyés « au mieux » par le protocole de couche transport. Le protocole UDP présente une surcharge faible de 8 octets.

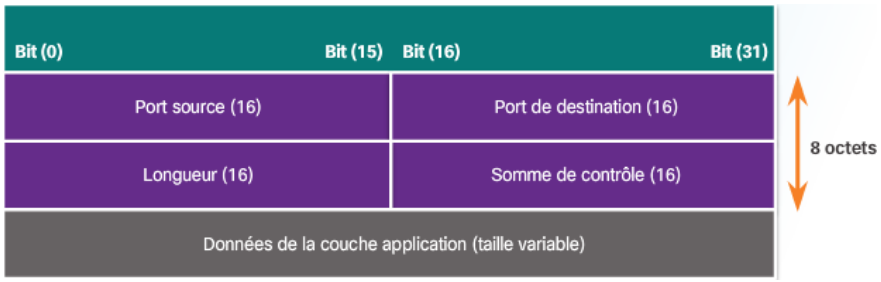


FIGURE 9.6 – Segment UDP

Plusieurs conversations simultanées La couche transport doit pouvoir segmenter et gérer plusieurs communications ayant des exigences différentes en matière de transport. Les utilisateurs s'attendent à pouvoir recevoir et envoyer simultanément des e-mails et des messages instantanés, afficher des sites web et passer un appel téléphonique par voix sur IP (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 téléphonique ne sont pas dirigées vers le navigateur web et le texte des messages instantanés n'apparaît pas dans un e-mail.

Les protocoles TCP et UDP gèrent ces conversations simultanées multiples au moyen de champs d'en-tête identifiant ces applications de façon unique. Ces identificateurs uniques sont les numéros de port.

Numéros de port Le numéro du port source est associé à l'application d'origine sur l'hôte local. Le numéro du port de destination est associé à l'application de destination sur l'hôte distant.

- **Port source** : Le numéro du port source est généré de manière dynamique par le périphérique émetteur pour identifier une conversation entre deux périphériques. Ainsi, plusieurs conversations peuvent s'effectuer simultanément. Un périphérique peut ainsi envoyer plusieurs requêtes de service HTTP à un serveur web en même temps. Un suivi des différentes conversations HTTP est effectué sur la base des ports sources.
- **Port de destination** : Le client place un numéro de port de destination dans le segment pour informer le serveur de destination du service demandé, comme le montre la figure 9.7.

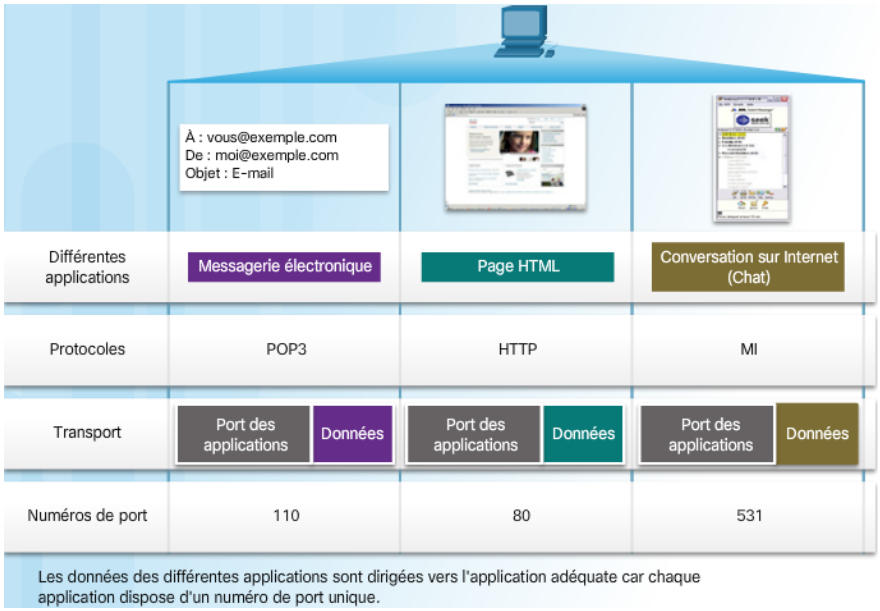


FIGURE 9.7 – Adressage de ports

Paires d'interfaces de connexion 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 de l'adresse IP source et du numéro de port source, ou de l'adresse IP de destination et du numéro de port de destination, est appelée interface de connexion. L'interface de connexion sert à identifier le serveur et le service demandés par le client. Une interface de connexion cliente peut se présenter comme suit, 1099 représentant le numéro du port source : 192.168.1.5 :1099. Un exemple est illustré 9.8.

Les interfaces de connexion 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 numéro de port source 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.

Sous Windows, la commande **netstat** permet d'afficher les protocoles utilisés, l'adresse et les numéros de port locaux, l'adresse et les numéros de port distants, et l'état de la connexion.

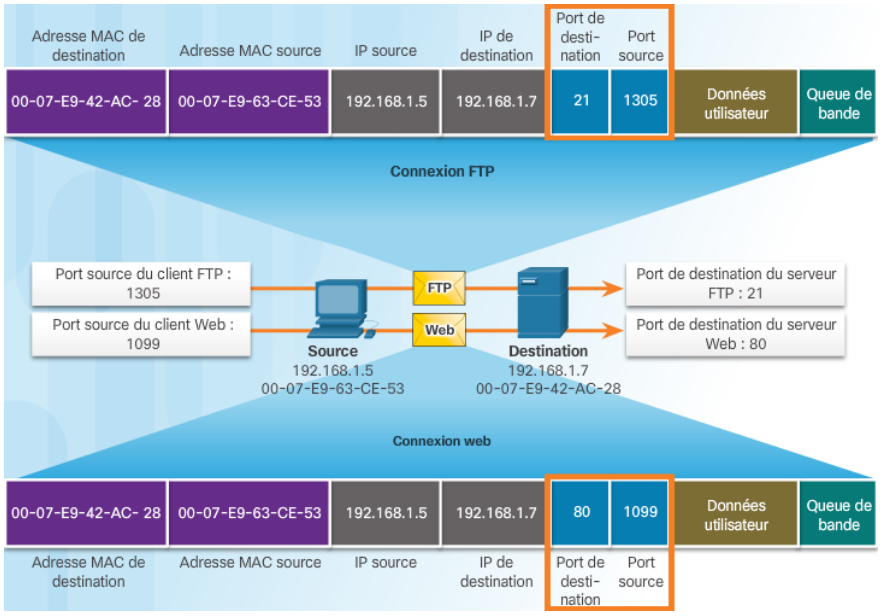


FIGURE 9.8 – Paires d'interfaces de connexion

Groupes de numéros de port Il existe différents types de numéros de port :

- **Ports réservés (numéros 0 à 1023)** : ces numéros sont réservés à des services et des applications. Ils sont généralement utilisés pour des applications de type navigateur web, client de messagerie et client d'accès à distance. 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 enregistrés (numéros 1024 à 49151)** : ces numéros de port sont affectés par l'IANA à une entité demandeuse pour une utilisation avec des processus ou des applications spécifiques. Ces processus sont essentiellement des applications particulières qu'un utilisateur a choisi d'installer plutôt que des applications courantes qui recevraient un port réservé.
- **Ports privés ou dynamiques (numéros 49152 à 65535)** : également appelés ports éphémères, ces ports sont généralement affectés de façon dynamique par le système d'exploitation du client lorsqu'une connexion à un service est initiée. Le port dynamique est ensuite utilisé pour identifier l'application cliente durant la communication.

9.2 TCP et UDP

9.2.1 Processus de communication TCP

Processus serveur TCP 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 particulier au sein des mêmes services de la couche transport.

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 demande entrante d'un client qui est adressée à l'interface de connexion correcte 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.

Établissement d'une connexion TCP Une connexion TCP s'établit en trois étapes (*Three-way handshake*) :

1. **SYN**, le client demande l'établissement d'une session de communication client-serveur avec le serveur : le client qui désire établir une connexion avec un serveur va envoyer un premier paquet SYN (synchronized) au serveur. Le numéro de séquence de ce paquet est un nombre aléatoire A.
2. **SYN-ACK**, le serveur accuse réception de la session de communication client-serveur et demande l'établissement d'une session de communication serveur-client : le serveur va répondre au client à l'aide d'un paquet SYN-ACK (synchronize, acknowledge). Le numéro du ACK est égal au numéro de séquence du paquet précédent (SYN) incrémenté de un ($A + 1$) tandis que le numéro de séquence du paquet SYN-ACK est un nombre aléatoire B.
3. **ACK**, le client accuse réception de la session de communication serveur-client : le client va envoyer un paquet ACK au serveur qui va servir d'accusé de réception. Le numéro de séquence de ce paquet est défini selon la valeur de l'acquittement reçu précédemment (par exemple $A + 1$) et le numéro du ACK est égal au numéro de séquence du paquet précédent (SYN-ACK) incrémenté de un ($B + 1$).

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 duplex intégral, où chaque connexion représente deux flux de communication unidirectionnelle, ou sessions. Ce sont les bits de contrôle de l'en-tête TCP qui indiquent la progression et l'état de la connexion.

Une fois la communication terminée, les sessions sont fermées et il est mis fin à la connexion. Ce sont ces mécanismes de connexion et de sessions qui garantissent la fiabilité du protocole TCP.

Fermeture 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. Pour mettre fin à une seule conversation TCP, quatre échanges sont nécessaires pour mettre fin aux deux sessions.

1. quand le client n'a plus de données à envoyer dans le flux, il envoie un segment dont l'indicateur FIN est défini ;
2. le serveur envoie un segment ACK pour indiquer la bonne réception du segment FIN afin de fermer la session du client au serveur ;
3. le serveur envoie un segment FIN au client pour mettre fin à la session du serveur au client ;
4. le client répond à l'aide d'un segment ACK pour accuser réception du segment FIN envoyé par le serveur.

9.2.2 Fiabilité et contrôle de flux

Fiabilité du protocole TCP - Livraison ordonnée Il se peut que les segments TCP parviennent à leur 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. Le numéro d'ordre représente le premier octet de données du segment TCP.

Lors de la configuration de la session, un numéro d'ordre initial, ou ISN, est défini. Cet ISN représente la valeur de départ 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.

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.

Perte de données et retransmission 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 pour les données sans accusé de réception.

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.

Taille de fenêtre et accusés de réception Le protocole TCP offre également des mécanismes relatifs au contrôle de flux, à la quantité de données que la destination peut recevoir et à la fiabilité du processus. 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. Pour cela, l'en-tête TCP inclut un champ de 16 bits appelé taille de fenêtre.

La figure illustre un exemple de taille de fenêtre et d'accusés de réception. La taille de fenêtre est le nombre d'octets que le périphérique de destination d'une session TCP peut accepter et traiter en une fois. Dans cet exemple, la taille de fenêtre initiale du PC-B pour la session TCP est définie à 10 000 octets. En commençant par le premier octet, à savoir l'octet numéro 1, le dernier octet que le

PC-A peut envoyer sans recevoir d'accusé de réception est l'octet 10 000. C'est ce qu'on appelle la fenêtre d'envoi du PC-A. La taille de fenêtre est incluse dans chaque segment TCP de telle sorte que la destination peut la modifier à tout moment en fonction de la disponibilité de la mémoire tampon.

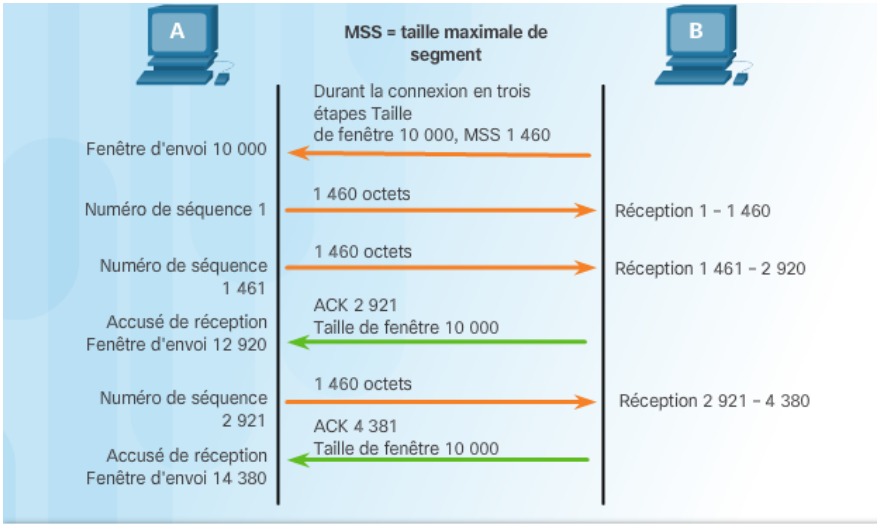


FIGURE 9.9 – Exemple de taille de fenêtre TCP

La taille de fenêtre initiale est déterminée lors de l'établissement de la session TCP par l'intermédiaire de la connexion en trois étapes. Le périphérique source doit limiter le nombre d'octets envoyés au périphérique de destination en fonction de la taille de fenêtre de la destination. Une fois que le périphérique source a reçu un accusé de réception l'informant que les octets ont été reçus, il peut continuer à envoyer plus de données pour la session. D'une manière générale, la destination n'attend pas que tous les octets de sa taille de fenêtre aient été reçus avant de répondre par un accusé de réception. Une fois que tous les octets ont été reçus et traités, la destination envoie des accusés de réception afin d'informer la source qu'elle peut continuer à envoyer des octets supplémentaires.

En règle générale, le PC-B n'attendra pas d'avoir reçu la totalité des 10 000 octets avant d'envoyer un accusé de réception. Cela signifie que le PC-A peut ajuster sa fenêtre d'envoi en fonction des accusés de réception reçus du PC-B. Comme le montre la figure, quand le PC-A reçoit un accusé de réception avec le numéro 2921, la fenêtre d'envoi du PC-A se voit incrémentée de 10 000 octets supplémentaires, à savoir la taille actuelle de fenêtre du PC-B, pour atteindre 12 920 octets. Le PC-A peut maintenant continuer à envoyer jusqu'à 10.000 nouveaux octets au PC-B, pour autant qu'il ne dépasse pas sa nouvelle fenêtre d'envoi de 12.920 octets.

Le processus d'envoi d'accusés de réception par la destination en fonction du traitement des octets reçus et d'ajustement continu de la fenêtre d'envoi de la source porte le nom de « fenêtres glissantes ».

Si l'espace libre dans la mémoire tampon de la destination diminue, cette dernière peut réduire sa taille de fenêtre afin de demander à la source de diminuer le nombre d'octets envoyés avant de

recevoir un accusé de réception.

Prévention des encombrements En cas d'encombrement sur un réseau, des paquets sont mis au rebut par le routeur surchargé. Lorsque des paquets contenant des segments TCP ne parviennent pas à leur destination, ils sont considérés comme étant non reçus. En déterminant la vitesse à laquelle les segments TCP sont envoyés, mais non reçus, la source peut estimer le niveau d'encombrement du réseau.

Chaque fois qu'il y a encombrement, les segments TCP perdus sont retransmis par la source. Si la retransmission n'est pas correctement contrôlée, une retransmission supplémentaire des segments TCP peut aggraver encore le niveau d'encombrement du réseau. Non seulement de nouveaux paquets contenant des segments TCP sont introduits sur le réseau, mais l'effet de rétroaction des segments TCP perdus et retransmis encombre encore davantage le réseau. Afin d'éviter et de contrôler l'encombrement du réseau, le protocole TCP utilise divers mécanismes, minuteurs et algorithmes de gestion des encombrements.

Si la source détermine que les segments TCP n'ont pas été reçus ou qu'ils n'ont pas été reçus à temps, elle peut diminuer le nombre d'octets à envoyer avant la réception d'un accusé de réception. Notez que c'est la source qui diminue le nombre d'octets non reçus à envoyer et non la taille de fenêtre déterminée par la destination.

9.2.3 Communication UDP

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).

Réassemblage de datagrammes UDP Le protocole UDP n'effectue pas le suivi des numéros d'ordre comme le fait le protocole TCP. Le protocole UDP ne peut donc pas réassembler les datagrammes dans leur ordre de transmission.

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.

Processus et requêtes des serveurs UDP Comme pour les applications basées sur le protocole TCP, des numéros de ports réservés sont affectés aux applications serveur basées sur le protocole UDP. Lorsque ces applications ou processus s'exécutent sur un serveur, elles ou ils 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.

Processus des clients UDP Comme c'est le cas avec le protocole TCP, la communication entre le client et le serveur est initiée par une application cliente qui demande des données à un processus serveur. Le processus client UDP sélectionne dynamiquement un numéro de port dans une plage de numéros de ports et il l'utilise en tant que port source pour la conversation. Le port de destination est généralement le numéro de port réservé affecté au processus serveur.

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.

9.2.4 TCP ou UDP

Applications utilisant le protocole TCP Le protocole TCP illustre parfaitement les rôles spécifiques des différentes couches de la pile de protocoles TCP/IP. Le protocole TCP gère toutes les tâches associées à la division du flux de données en segments, offrant ainsi à la fois fiabilité, contrôle du flux de données et réorganisation des segments. Le protocole TCP libère l'application de la gestion de l'ensemble de ces tâches. Les applications, telles que celles illustrées dans la figure 9.10, peuvent simplement envoyer le flux de données à la couche transport et utiliser les services du protocole TCP.

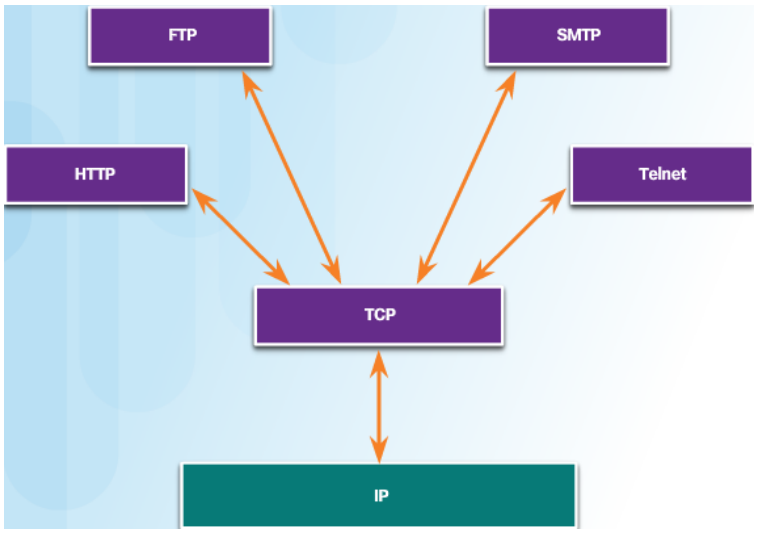


FIGURE 9.10 – Applications utilisant le protocole TCP

Applications utilisant le protocole UDP Il existe trois types d'application plus adaptés au protocole UDP :

- **Applications multimédia et de streaming vidéo** : applications pouvant tolérer certaines pertes de données, mais peu ou pas de retard. La voix sur IP et le streaming vidéo en sont de bons exemples.
- **Simples applications de requête et de réponse** : applications dont les transactions sont

simples et pour lesquelles un hôte envoie une requête à laquelle il recevra ou non une réponse (DNS et DHCP par exemple).

- **Applications gérant elles-mêmes la fiabilité** : communications unidirectionnelles pour lesquelles le contrôle de flux, la détection des erreurs, les accusés de réception et la reprise sur erreur ne sont pas nécessaires ou peuvent être gérés par l'application elle-même (SNMP et TFTP par exemple).

Chapitre 10

Couche application

10.1 Protocoles de couche application

10.1.1 Application, présentation et session

Couche application La couche application est la plus proche de l'utilisateur final. Comme le montre la figure 10.1a, c'est elle qui sert d'interface entre les applications que nous utilisons pour communiquer et le réseau sous-jacent via lequel les 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.

Les trois couches supérieures du modèle OSI (application, présentation et session) définissent les fonctions de la couche application TCP/IP unique.

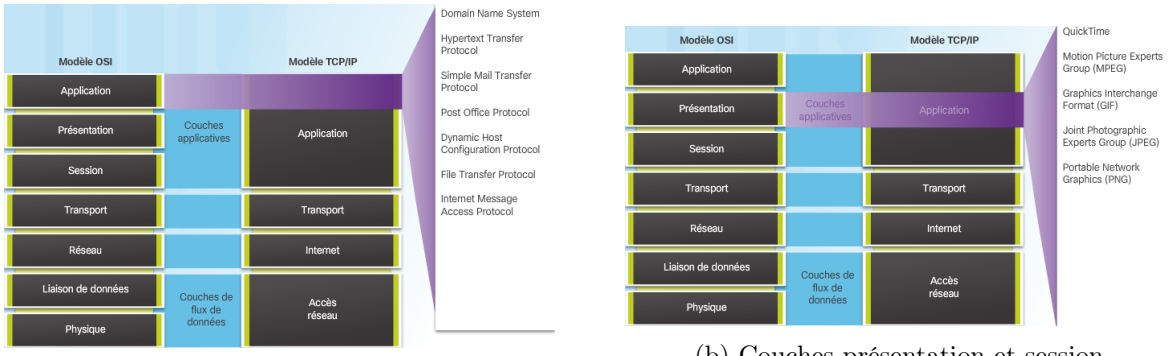
Couches présentation et session La couche présentation remplit trois fonctions principales :

- mettre en forme ou présenter les données provenant du périphérique source dans un format compatible pour la réception par le périphérique de destination ;
- compresser les données de sorte que celles-ci puissent être décompressées par le périphérique de destination ;
- chiffrer les données pour la transmission et les déchiffrer à la réception.

Comme l'illustre la figure 10.1b, la couche présentation met en forme les données pour la couche application et définit les normes des formats de fichiers.

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.

Protocoles de couche application TCP/IP 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. Les protocoles de couche application sont utilisés par les périphériques



(a) Couche application

(b) Couches présentation et session

FIGURE 10.1 – Application, présentation et session

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.

10.1.2 Interaction des protocoles d'application avec les applications des utilisateurs finaux

Modèle client/serveur Dans le modèle client/serveur, le périphérique qui demande les informations est nommé client et celui qui répond à la requête est nommé 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 effectif, cet échange peut également nécessiter l'authentification de l'utilisateur et l'identification d'un fichier 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. 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 ».

Réseaux peer to peer 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.

Dans un réseau peer to peer, deux ordinateurs au moins sont connectés via un réseau et peuvent partager des ressources (par exemple, des imprimantes et des fichiers) sans disposer de serveur dédié. Chaque périphérique terminal connecté (ou « homologue ») peut opérer à la fois en tant que serveur et 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.

Applications peer to peer 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. Dans ce modèle, chaque client est un serveur et chaque serveur un client. Les applications P2P nécessitent que chaque périphérique terminal fournisse une interface utilisateur et exécute un service en arrière-plan.

Certaines applications peer to peer 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.

10.2 Services et protocoles de couche application courants

10.2.1 Protocoles web et messagerie électronique

HTTP (Hypertext Transfer Protocol) et HTML (Hypertext Markup Language) Lorsqu'une adresse web (ou URL) est tapée dans un navigateur web, ce dernier établit une connexion au 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. Dans un premier temps, le navigateur interprète les trois parties de l'URL (ici http ://www.cisco.com/index.html) :

- **http** : protocole ou schéma ;
- **www.cisco.com** : nom du serveur ;
- **index.html** : nom du fichier demandé.

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. Puis le serveur envoie au navigateur le code HTML pour cette page web. Enfin, le navigateur déchiffre le code HTML et met en forme la page pour la fenêtre du navigateur.

HTTP et HTTPS Le protocole HTTP est de type requête/réponse. Lorsqu'un client, généralement un navigateur web, envoie une requête à un serveur web, HTTP spécifie les types de messages utilisés pour cette communication. Les trois types de messages courants sont GET, POST et PUT :

- **GET** est une requête cliente visant à obtenir des données. Un client (navigateur web) envoie le message GET au serveur web pour demander des pages HTML.
- **POST** télécharge des fichiers de données vers le serveur web, comme des données de formulaires.
- **PUT** télécharge des ressources ou du contenu vers le serveur web, comme une 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. 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. HTTPS utilise l'authentification et le chiffrement pour sécuriser les données pendant leur transfert entre le client et le serveur. HTTPS 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.

Protocoles de messagerie électronique L'un des principaux services offerts par un FAI est l'hébergement de la messagerie. Pour qu'elle fonctionne sur un ordinateur ou un autre périphérique terminal, plusieurs applications et services sont nécessaires, comme le montre la figure 10.2. Le courriel 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 électroniques sont stockés dans des bases de données sur des serveurs de messagerie.

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 de courriel. En fait, les deux clients dépendent du serveur de messagerie pour transporter les messages.

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 les e-mails utilise le protocole SMTP. Pour les récupérer, le client fait appel à l'un des deux protocoles de couche application suivants : POP ou IMAP.

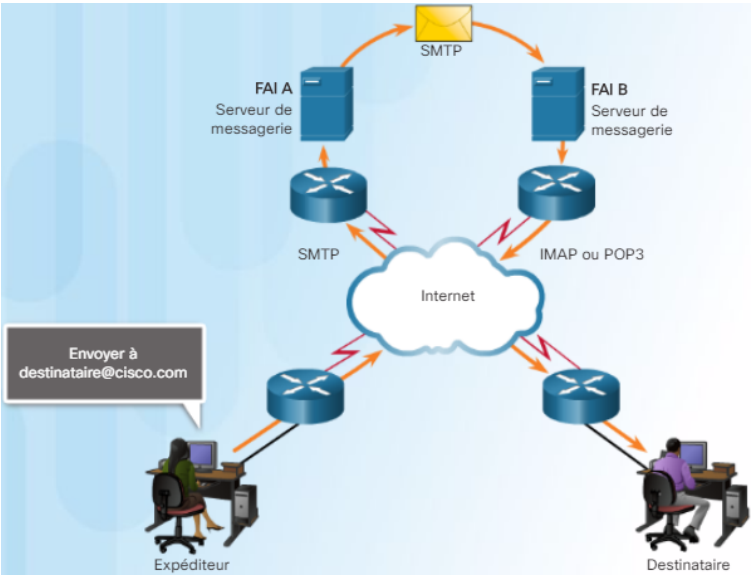


FIGURE 10.2 – Émission et réception d'un e-mail

Fonctionnement du protocole SMTP 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.

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 reçoit le message, il place celui-ci dans un compte local, si le destinataire est local, ou transfère le message vers un autre serveur de messagerie, comme le montre la figure 10.3.

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. Après une durée donnée, si le message n'est toujours pas transmis, il est renvoyé à son expéditeur comme non délivrable.

Fonctionnement du protocole POP Le protocole POP (Post Office Protocol) est utilisé par une application pour récupérer le courrier électronique à partir d'un serveur de messagerie. Avec POP, le courriel est téléchargé du serveur au client, puis supprimé du serveur. Le protocole POP fonctionne par défaut de cette façon.

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. Ceci est illustré figure 10.3.

Avec POP, 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.

Fonctionnement du protocole IMAP Le protocole de messagerie IMAP (Internet Message Access Protocol) décrit une autre méthode de récupération des messages électroniques. 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 leur courriel. 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.

10.2.2 Services d'adressage IP

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

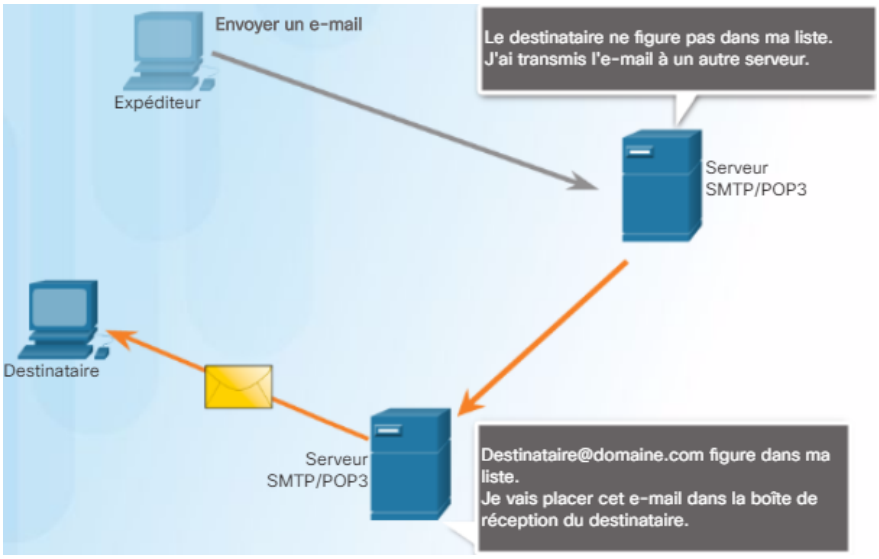


FIGURE 10.3 – SMTP et POP3

sur les réseaux. Des noms de domaine ont été créés pour convertir les adresses numériques en noms simples et explicites.

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.

Format du message DNS Le serveur DNS stocke différents types d'enregistrements de ressource utilisés pour résoudre des noms. Ces enregistrements contiennent le nom, l'adresse et le type d'enregistrement. Certains de ces types d'enregistrements sont les suivants :

- **A** : une adresse IPv4 de périphérique terminal ;
- **NS** : un serveur de noms autorisé ;
- **AAAA** : une adresse IPv6 de périphérique terminal ;
- **MX** : un enregistrement d'échange de courrier électronique.

Lorsqu'un client envoie une requête, le processus DNS du serveur cherche d'abord dans ses propres enregistrements pour résoudre le nom. S'il ne peut pas résoudre le nom à l'aide de ses enregistrements stockés, il contacte d'autres serveurs pour résoudre le nom. Lorsqu'une correspondance est trouvée et retournée au serveur demandeur d'origine, le serveur stocke provisoirement l'adresse numérotée pour le cas où le même nom serait à nouveau demandé.

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 (voir la figure 10.4). 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 de nom qui n'appartient pas à cette zone DNS, le serveur DNS transfère la requête à un autre serveur DNS se trouvant dans la zone de traduction correcte.

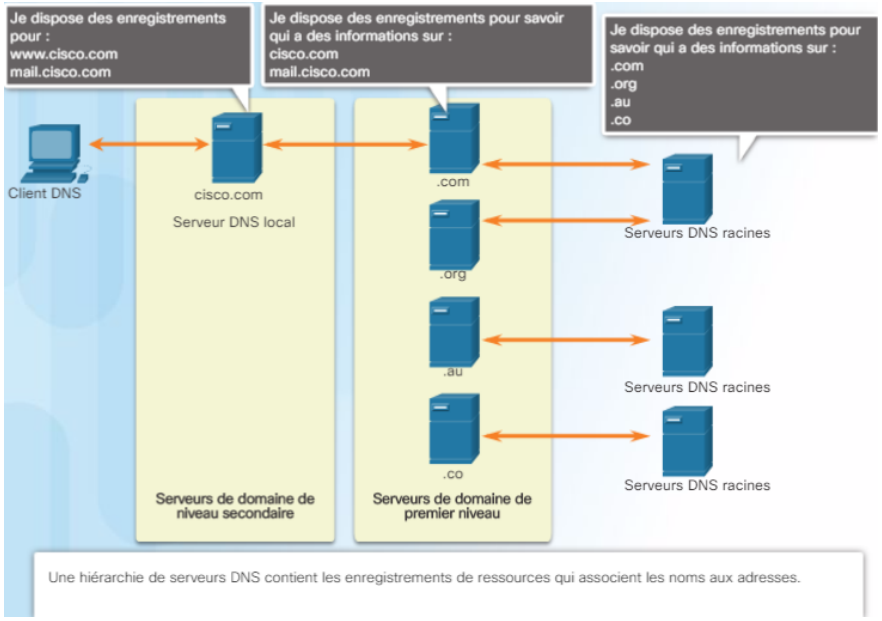


FIGURE 10.4 – Hiérarchie DNS

Commande nslookup Lors de la configuration d'un périphérique réseau, une ou plusieurs adresses de serveur DNS sont fournies, 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 le serveur de noms pour convertir le nom en une adresse numérique.

Le système d'exploitation des ordinateurs (Linux ou Windows) comprend également un utilitaire nommé **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.

Protocole DHCP (Dynamic Host Configuration Protocol) Le protocole DHCP pour IPv4 automatise l'affectation des adresses IPv4, des masques de sous-réseau, des passerelles et d'autres paramètres réseau IPv4. 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.

Lorsqu'un hôte 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 affecte

cette adresse à l'hôte pour une durée définie.

Les adresses DHCP distribuées sont affectées pour une période de temps définie. Une fois ce délai expiré et si l'hôte est mis hors tension ou retiré du réseau, l'adresse est renvoyée au pool d'adresses afin d'être réutilisée. Les utilisateurs peuvent librement se déplacer d'un endroit à un autre et rétablir aisément des connexions réseau au moyen de DHCP.

Comme l'illustre la figure 10.5, divers types de périphériques peuvent être des serveurs DHCP. Dans la plupart des réseaux de taille moyenne à grande, le serveur DHCP est généralement un serveur local dédié basé sur un PC. Dans le cas des réseaux domestiques, le serveur DHCP est généralement situé sur le routeur local qui connecte le réseau domestique au FAI.

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, comme les périphériques des utilisateurs finaux. L'adressage statique est utilisé pour les périphériques réseau tels que les passerelles, les commutateurs, les serveurs et les imprimantes.

Le protocole DHCPv6 (DHCP pour IPv6) offre des services similaires aux clients IPv6. Une différence importante est que DHCPv6 ne fournit pas d'adresse de passerelle par défaut. Celle-ci ne peut être obtenue dynamiquement qu'à partir du message d'annonce du routeur.

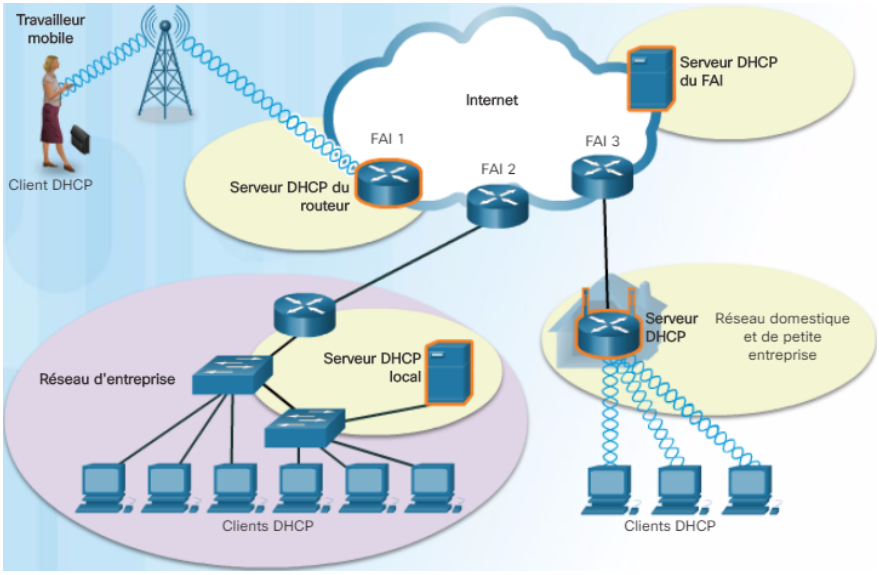


FIGURE 10.5 – Protocole DHCP

Fonctionnement du protocole DHCP Comme le montre la figure 10.6, lorsqu'un périphérique IPv4 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 IPv4 et le masque de sous-réseau à attribuer, l'adresse IPv4 du serveur DNS et l'adresse IPv4 de la passerelle par défaut. L'offre de bail indique également la durée du bail.

Le client peut recevoir plusieurs messages DHCP OFFER 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 choisir de demander une adresse que le serveur lui a déjà attribuée précédemment.

En supposant que l'adresse IPv4 demandée par le client ou offerte par le serveur est encore disponible, le serveur renvoie un message d'accusé de réception DHCP (DHCPACK) confirmant au client que le bail est conclu. Si l'offre n'est plus valide, le serveur sélectionné répond par un message d'accusé de réception DHCP négatif (DHCPNAK). Si un message DHCPNAK est renvoyé, le processus de sélection doit recommencer avec un nouveau message DHCPDISCOVER transmis. Une fois que le client obtient le bail, celui-ci doit être renouvelé avant son expiration via un autre message DHCPREQUEST.

Le serveur DHCP s'assure que toutes les adresses IP sont uniques (une même adresse IP ne peut pas être attribuée à deux périphériques réseau différents en même temps). La plupart des fournisseurs Internet utilisent le protocole DHCP pour attribuer des adresses à leurs clients.

Le protocole DHCPv6 possède un ensemble de messages similaires à ceux illustrés dans la figure et relatifs à DHCP pour IPv4. Les messages DHCPv6 sont SOLICIT, ADVERTISE, INFORMATION REQUEST et REPLY.

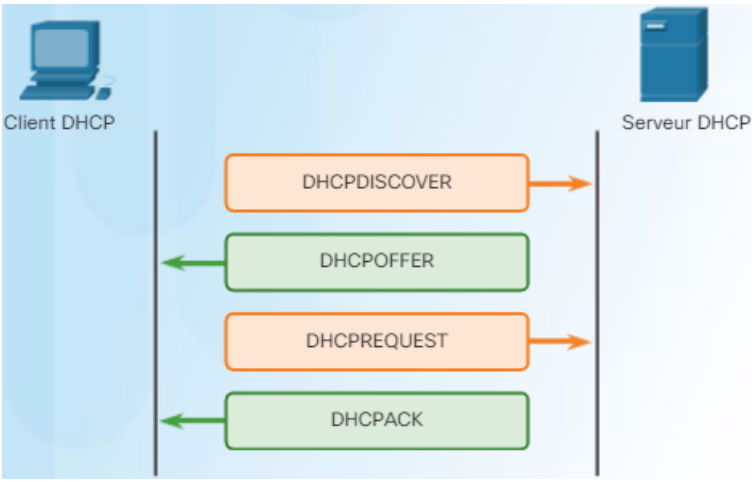


FIGURE 10.6 – Fonctionnement du protocole DHCP

10.2.3 Services de partage de fichiers

File Transfer Protocol Le protocole FTP (File Transfer Protocol) est un autre protocole de couche d'application couramment utilisé. Il a été développé en vue de permettre le transfert de données entre un client et un serveur. Un FTP est une application s'exécutant sur un ordinateur client. Il sert à envoyer et à extraire des données d'un serveur FTP.

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 sur le port TCP 21.

Cette première connexion se compose de commandes de clients et de réponses du serveur.

- Le client établit la seconde connexion au serveur pour le transfert de données proprement dit sur le port TCP 20. Cette connexion est créée chaque fois que des données doivent être transférées.

Le transfert de fichiers peut s'effectuer dans les deux sens. Le client peut télécharger (extraire) des données à partir du serveur ou le client peut télécharger (stocker) des données vers le serveur.

Server Message Block Le protocole SMB (Server Message Block) est un protocole de partage de fichiers client/serveur 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. 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 de taille variable. 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.

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.

Chapitre 11

Conception d'un réseau de petite taille

11.1 Conception de réseaux

11.1.1 Périphériques d'un petit réseau

Topologies des petits réseaux La conception de petits réseaux est généralement simple. Le nombre et les types de périphériques inclus sont largement réduits par rapport à un réseau plus étendu. Les topologies des réseaux 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 termes 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 de l'entreprise.

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 inter-réseau doivent avoir une adresse unique. 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.

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.

Les petits réseaux offrent en général un seul point de sortie vers Internet via une ou plusieurs passerelles par défaut. 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 un second fournisseur d'accès par mesure de sécurité.

Gestion du trafic 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. 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 Applications et protocoles des réseaux de petite taille

Applications courantes L'utilité du réseau dépend des applications qu'il comporte. Il existe deux types de programmes ou processus logiciels permettant d'accéder au réseau :

- **Applications réseau** : Les applications sont des 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 les 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 un employé, ces services constituent les programmes qui établissent l'interface avec le réseau et préparent les données à transférer. Différents types de données (texte, graphique ou vidéo) nécessitent différents services réseau pour être correctement préparés afin d'être traités par les fonctions s'exécutant au niveau des 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.

Protocoles courants 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.

Ces protocoles réseau constituent la boîte à outils indispensable d'un professionnel des réseaux. Chacun des protocoles réseau définit les éléments suivants :

- les processus sur l'une des extrémités d'une session de communication ;
- les types de messages ;
- la syntaxe des messages ;
- la signification des champs informatifs ;
- la manière dont les messages sont envoyés et la réponse attendue ;
- l'interaction avec la couche du niveau juste en dessous.

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.

Croissance d'un petit réseau La plupart des petites entreprises se développent naturellement et leurs réseaux doivent suivre cette évolution. 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** : documentation des protocoles, applications et services, avec leurs besoins respectifs quant au trafic

Ces éléments servent à éclairer la prise de décision qui accompagne l'évolution d'un petit réseau.

11.2 Sécurité du réseau

11.2.1 Attaques de réseau

Types de programmes malveillants Un « malware » désigne un programme malveillant. Il s'agit de code ou d'un logiciel spécialement conçu pour endommager, perturber ou effectuer une action illégitime sur des données, des hôtes ou des réseaux. Les virus, les vers et les chevaux de Troie sont des types de logiciels malveillants.

- **Virus** : Un virus informatique est un type de programme malveillant qui se propage en insérant une copie de lui-même dans un autre programme. Les virus se propagent lorsque le logiciel ou le document auquel ils sont attachés est transféré d'un ordinateur à un autre par le biais d'un réseau, d'un disque, d'un partage de fichiers ou de pièces jointes infectées.
- **Vers** : Les vers informatiques sont semblables aux virus en ce sens qu'ils reproduisent des copies fonctionnelles d'eux-mêmes et peuvent provoquer le même type de dommages. Contrairement aux virus, qui nécessitent la diffusion d'un fichier hôte infecté, les vers sont des logiciels autonomes et ne requièrent pas de programme d'accueil ou d'intervention humaine pour se propager. Les vers utilisent les fonctionnalités du système pour voyager sans assistance à travers le réseau.
- **Chevaux de Troie** : Il s'agit d'une partie de code qui présente une apparence tout à fait légitime. Les utilisateurs sont généralement trompés en les chargeant et en les exécutant sur leurs systèmes. Contrairement aux virus et aux vers, les chevaux de Troie ne se reproduisent pas en infectant d'autres fichiers et ils sont incapables de se répliquer automatiquement.

Types d'attaques de réseau 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 Dans les attaques de reconnaissance, des assaillants 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.

Attaques par accès Les attaques par accès 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.

Attaques par déni de service Les attaques par déni de service sont les plus médiatisées, mais constituent également l'une des formes d'attaque les plus difficiles à éliminer. 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.

11.2.2 Réduction du risque d'attaque du réseau

Sauvegarde, mise à jour, mise à niveau et correctif Pour se protéger efficacement des attaques réseau, il faut s'informer en continu sur les menaces. Au fur et à mesure que de nouveaux programmes malveillants apparaissent, les entreprises doivent acquérir la version la plus récente de leur logiciel antivirus.

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. 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.

Authentification, 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).

Pare-feu Un pare-feu est l'un des outils de sécurité disponibles les plus efficaces pour protéger les utilisateurs contre les menaces externes. Un pare-feu se trouve entre deux réseaux, ou plus, et contrôle le trafic entre eux tout en contribuant à interdire les accès non autorisés. Des pare-feu basés sur les hôtes ou des pare-feu personnels sont installés sur les systèmes terminaux. 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.
- **Filtrage 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 (DoS).

Sécurité des points de terminaison Un point de terminaison, ou hôte, est un système informatique ou un périphérique qui tient lieu de client réseau. La sécurisation des points de terminaison est l'une des tâches les plus difficiles pour un administrateur réseau, car elle implique de prendre en compte le facteur humain. 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.

11.2.3 Sécurité des appareils

Présentation de la sécurité des appareils 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. 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.

Souvent, les périphériques expédiés par les fabricants ont été entreposés pendant un certain temps et ne disposent pas des correctifs les plus récents. Il est important de mettre à jour les logiciels et d'installer les correctifs de sécurité avant toute mise en œuvre.

Principes de sécurité de base 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 avec la commande de configuration globale **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.

Il est également recommandé de définir des délais d'exécution. Vous indiquez ainsi au périphérique 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 au moyen de la commande **exec-timeout** dans le mode de configuration de ligne.

Activer SSH Le protocole Telnet n'est pas sécurisé. Les données contenues dans un paquet Telnet sont transmises en clair. 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 de sorte qu'il prenne en charge le protocole SSH, à l'aide du processus en quatre étapes indiqué dans la figure 11.1.

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** en mode de configuration globale.
2. Des clés secrètes unidirectionnelles doivent être générées pour qu'un routeur chiffre le trafic SSH. Pour générer la clé SSH, utilisez la commande **crypto key generate rsa general-keys** en mode de configuration globale. Le module détermine la taille de la clé et qu'il peut être configuré à partir de 360 bits jusqu'à 2048 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.
3. Créez une entrée de nom d'utilisateur dans la base de données locale à l'aide de la commande de configuration globale **username**.
4. Activez les sessions SSH entrantes à l'aide des commandes de ligne VTY **login local** et **transport input ssh**.

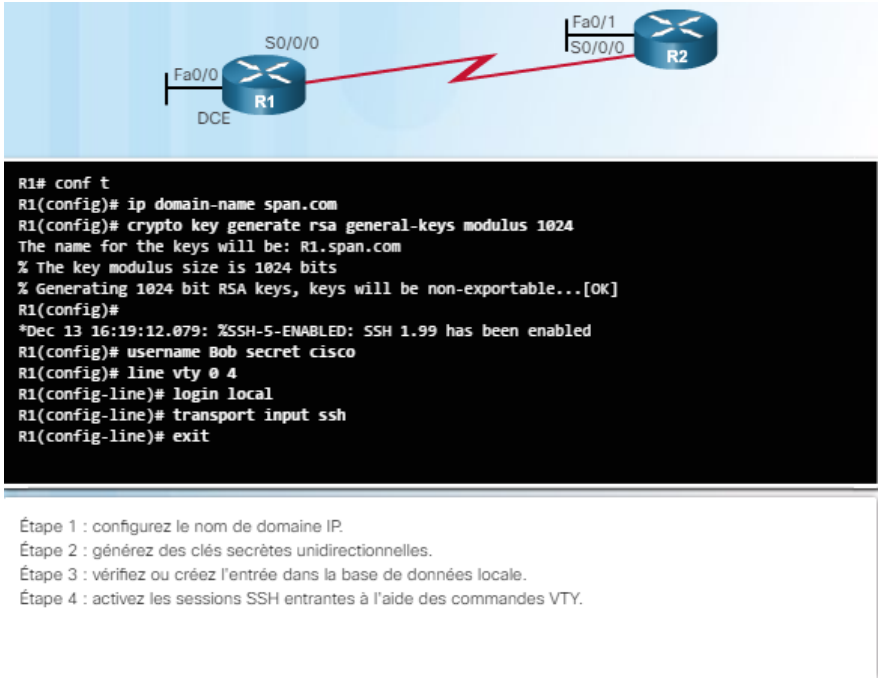


FIGURE 11.1 – Activer SSH

11.3 Performances réseau de base

11.3.1 Commande ping

Interprétation des résultats de requête ping L'utilisation de la commande ping constitue un moyen efficace de tester la connectivité. La commande ping utilise le protocole ICMP (Internet Control Message Protocol) et vérifie la connectivité de couche 3. Bien qu'elle ne permette pas toujours de diagnostiquer précisément la nature du problème, la commande ping peut aider à en identifier la cause, ce qui constitue une première étape importante dans le dépannage d'un réseau.

Une commande ping 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, comme le montre la figure 11.2.
- **.** - Indique l'expiration du délai d'attente d'une réponse d'écho ICMP.
- **U** - indique la réception d'un message ICMP d'inaccessibilité.

Le caractère « . » (point) 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 qu'il 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. Lors de l'envoi d'une requête ping sur un réseau local Ethernet, il est courant que le délai d'attente de la première requête d'écho expire si le processus ARP est requis.

La lettre « U » indique qu'un routeur situé sur le chemin et ne possédant pas de route vers l'adresse de destination a répondu par un message ICMP d'inaccessibilité. Le routeur ne possède pas de route vers l'adresse de destination ou la requête ping a été bloquée.

La commande ping peut également être utilisée pour vérifier la configuration IP interne sur l'hôte local en envoyant une requête à l'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.

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 un profil de référence du réseau. La création d'un profil de référence 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.

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 profil de référence, vous pouvez copier et coller dans un fichier texte les résultats d'une commande telle que **ping**, **trace** ou autre. Il est possible d'horodater ces fichiers texte et de les enregistrer dans une archive en vue d'une extraction et d'une comparaison ultérieures. 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.

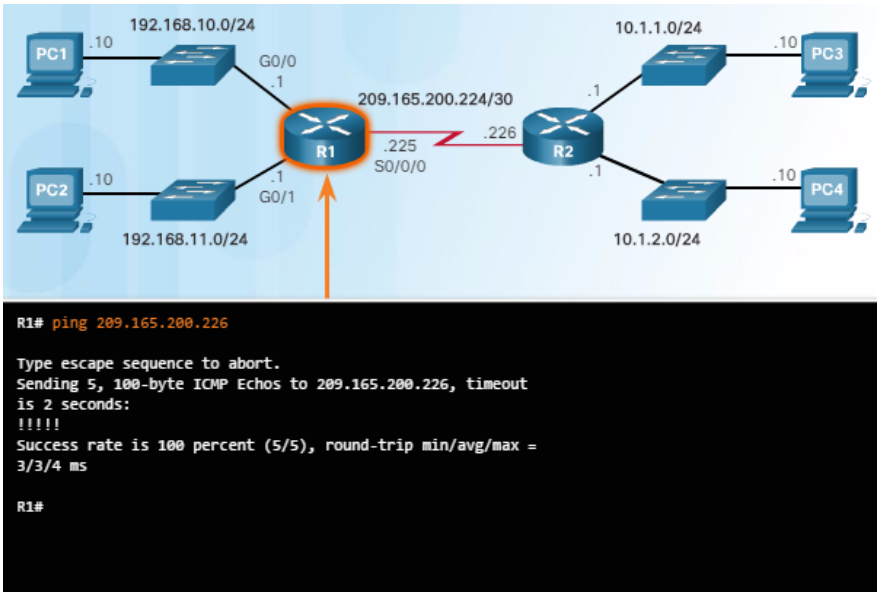


FIGURE 11.2 – Indicateurs de la commande **ping**

11.3.2 Commande traceroute et tracert

La commande **trace** 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. Avec un ordinateur Windows, utilisez **tracert**. À partir de l'interface en ligne de commande d'un routeur, utilisez traceroute, comme le montre la figure 11.3a.

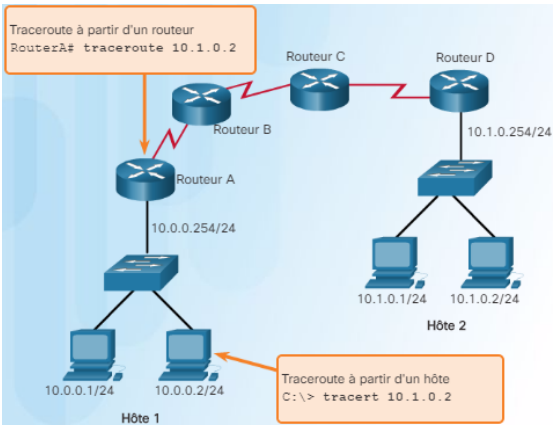
La figure 11.3b illustre un exemple de résultat de la commande **tracert** exécutée sur l'hôte 1 afin de suivre l'itinéraire du trafic vers l'hôte 2. La seule réponse reçue provient de la passerelle située sur le routeur A. Les requêtes trace vers le tronçon suivant ont dépassé le délai d'attente, ce qui signifie que le routeur de tronçon suivant n'a pas répondu. Les résultats indiquent soit une défaillance dans l'inter-réseau situé au-delà du réseau local soit que ces routeurs n'ont pas été configurés de manière à répondre aux requêtes d'écho utilisées dans la commande **trace**.

11.3.3 Commandes show

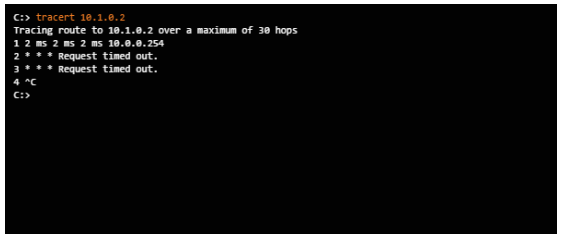
L'interface en ligne de commande Cisco IOS comprend des commandes **show** permettant d'afficher les informations appropriées sur la configuration et le fonctionnement du périphérique.

Les techniciens réseau utilisent fréquemment les commandes **show** pour afficher les fichiers de configuration, vérifier l'état des interfaces et des processus des périphériques et confirmer l'état de fonctionnement du périphérique. 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 les suivantes :

- **show running-config**
- **show interfaces**



(a) Test du chemin vers un hôte distant



(b) Traceroute de l'hôte 1 à l'hôte 2

FIGURE 11.3 – Interprétation des messages **trace**

- **show arp**
- **show ip route**
- **show protocols**
- **show version**

11.3.4 Commandes hôtes et IOS

Utilisation de la commande ipconfig Comme le montre la figure 11.4, 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.

Utilisez la commande **ipconfig /all** pour afficher l'adresse MAC ainsi que les informations sur l'adressage de couche 3 de l'équipement. La commande **ipconfig /displaydns** affiche toutes les entrées DNS mises en cache sur un système Windows.

Commande arp 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, l'administrateur réseau peut effacer le cache à l'aide de la commande **arp -d***.

Utilisation de la commande show cdp neighbors CDP (Cisco Discovery Protocol) 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.

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.

FIGURE 11.4 – **ipconfig**

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 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**.

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.

Pour vérifier les interfaces d'un routeur, la commande **show ip interface brief** est l'une des plus utilisées. Elle fournit un résumé des informations clés pour toutes les interfaces réseau d'un routeur. La commande **show ip interface brief** peut également servir à vérifier l'état des interfaces du commutateur.

11.3.5 Débogage

Commande debug Les processus, protocoles, mécanismes et événements IOS génèrent des messages pour communiquer leur état. Ces messages peuvent fournir des informations utiles lors du dépannage ou de la vérification du fonctionnement du système. La commande **debug** d'IOS permet à l'administrateur d'afficher ces messages en temps réel pour analyse. Toutes les commandes debug sont entrées en mode d'exécution privilégié.

Commande terminal monitor Les connexions octroyant l'accès à l'interface de ligne de commande IOS peuvent être établies localement ou à distance.

Les connexions locales requièrent un accès physique au routeur ou au commutateur ; une connexion

par câble est donc requise. Ce genre de connexion s'établit généralement en connectant un ordinateur au routeur ou au port de console du commutateur à l'aide d'un câble de renversement. Lorsque nous parlons de connexion de console, nous faisons référence à une connexion locale.

Les connexions à distance sont établies sur le réseau et, par conséquent, nécessitent un protocole réseau tel que le protocole IP. Aucun accès physique direct n'est requis pour les sessions distantes. SSH et Telnet sont deux protocoles de connexion couramment utilisés pour les sessions à distance. Lorsque nous parlons de connexion à distance, nous faisons référence aux protocoles Telnet ou SSH.

Si les messages de journal IOS sont envoyés par défaut à la console, ils ne sont pas envoyés aux lignes virtuelles. Étant donné que les messages de débogage sont des messages de journal, ce comportement empêche l'affichage des messages de débogage sur les lignes VTY.

Pour afficher les messages de journal sur un terminal (console virtuelle), utilisez la commande d'exécution privilégiée **terminal monitor**. Pour désactiver la journalisation des messages sur un terminal, utilisez la commande d'exécution privilégiée **terminal no monitor**.

11.4 Dépannage du réseau

11.4.1 Méthodologies de dépannage

Les problèmes de réseau peuvent résulter d'une combinaison de problèmes matériels, logiciels et de connectivité de différente envergure. Les techniciens doivent être capables d'analyser le problème et d'en déterminer la cause afin de résoudre le problème du réseau. Cela s'appelle le dépannage.

Une procédure de dépannage couramment utilisée et efficace repose sur une approche scientifique et comprend six étapes clés, comme l'indique l'illustration 11.5.

Pour déterminer la complexité d'un problème, vous devez savoir combien de périphériques du réseau sont concernés. Si le problème concerne un seul périphérique, commencez la procédure de dépannage sur celui-ci. S'il concerne l'ensemble des périphériques du réseau, commencez le dépannage sur le périphérique contenant toutes les connexions.

Vérification et surveillance de la solution Cisco IOS inclut des outils puissants de vérification et de dépannage. Lorsqu'un problème a été résolu et une solution mise en œuvre, il est important de vérifier le fonctionnement du système. Les outils de vérification incluent les commandes **ping**, **traceroute** et **show**.

La commande **ping** sert à tester la connectivité réseau. Si elle aboutit, on peut aisément conclure que les paquets sont acheminés de la source à la destination.

La commande **traceroute** permet d'afficher le chemin emprunté par les paquets pour atteindre une destination. Tandis que le résultat d'une commande **ping** indique si un paquet est arrivé à destination, celui d'une commande **traceroute** indique le chemin emprunté pour arriver à cette destination ou l'endroit exact où le paquet a été bloqué.

Les commandes **show** comptent parmi les outils de dépannage et de vérification les plus utiles. Tirant parti d'une grande variété d'options et de sous-options, la commande **show** peut être utilisée pour filtrer ou afficher des informations concernant la quasi-totalité des aspects d'IOS.

Étape	Titre	Description
1	Identification du problème	La première étape de la procédure de dépannage consiste à identifier le problème. Si des outils peuvent être utilisés à cette étape, une conversation avec l'utilisateur est souvent très utile.
2	Élaboration d'une théorie des causes probables	Après avoir discuté avec l'utilisateur et identifié le problème, vous pouvez établir une théorie des causes probables. Cette étape fait généralement naître plusieurs causes probables.
3	Test de la théorie en vue de déterminer la cause	En fonction des causes probables, testez vos théories afin de dégager la véritable cause du problème. Un technicien peut alors appliquer une rapide procédure et voir si cela permet de résoudre le problème. Sinon, vous devrez peut-être effectuer des recherches complémentaires en vue de déterminer la cause exacte.
4	Élaboration d'un plan d'action visant à résoudre le problème et à implémenter la solution	Après avoir déterminé la cause exacte du problème, établissez un plan d'action en vue de le résoudre en implémentant la solution.
5	Vérification du fonctionnement de l'ensemble du système et implémentation des mesures préventives	Après avoir résolu le problème, vous devez vérifier le fonctionnement de l'ensemble du système et s'il y a lieu, implémenter des mesures préventives.
6	Documentation des résultats des recherches et des actions entreprises	Au cours de la dernière étape du processus de dépannage, vous devez documenter les résultats de vos recherches ainsi que les actions entreprises. Cette étape est très importante pour référence ultérieure.

FIGURE 11.5 – Les six étapes de la procédure de dépannage

11.4.2 Scénario de dépannage

Problèmes d'adressage IP sur périphériques IOS Les problèmes liés aux adresses IP empêchent généralement les périphériques réseau distants de communiquer. Les adresses IP respectant une certaine hiérarchie, toute adresse IP attribuée à un périphérique réseau doit être conforme à la plage d'adresses de ce réseau. Toute adresse IP mal attribuée génère un grand nombre de problèmes, y compris des conflits d'adressage IP et des problèmes de routage.

Parmi les causes les plus courantes d'attribution IPv4 incorrecte, notons les erreurs d'attribution manuelle ou les problèmes DHCP.

Les administrateurs réseau doivent souvent affecter manuellement des adresses IP à des périphériques tels que des serveurs et des routeurs. Si une erreur est commise au moment de l'affectation, il y a de fortes chances que cela génère des problèmes de communication avec le périphérique.

Sur un équipement Cisco IOS, utilisez les commandes **show ip interface** ou **show ip interface brief** pour vérifier que les adresses IPv4 ont été attribuées aux interfaces réseau. La figure 11.6 présente le résultat de la commande **show ip interface** exécutée sur R1. Notez que le résultat affiche des données IPv4 (couche 3 OSI), tandis que la commande **show interfaces** précédemment mentionnée affiche les données physiques et de liaison de données d'une interface.

Problèmes d'adressage IP sur des périphériques finaux Sous Windows, lorsque le périphérique ne parvient pas à contacter un serveur DHCP, Windows attribue automatiquement une adresse appartenant à la plage 169.254.0.0/16. Ce processus est conçu pour faciliter la communication sur le réseau local. Un ordinateur avec l'adresse 169.254.0.0/16 n'est généralement pas en mesure de communiquer avec d'autres périphériques du réseau, car il y a de fortes chances que ces périphériques n'appartiennent pas au réseau 169.254.0.0/16. Cette situation traduit un problème d'attribution automatique d'adresse IPv4 qui doit être résolu. Pour vérifier les adresses IP attribuées à un ordinateur Windows, utilisez la commande **ipconfig**.

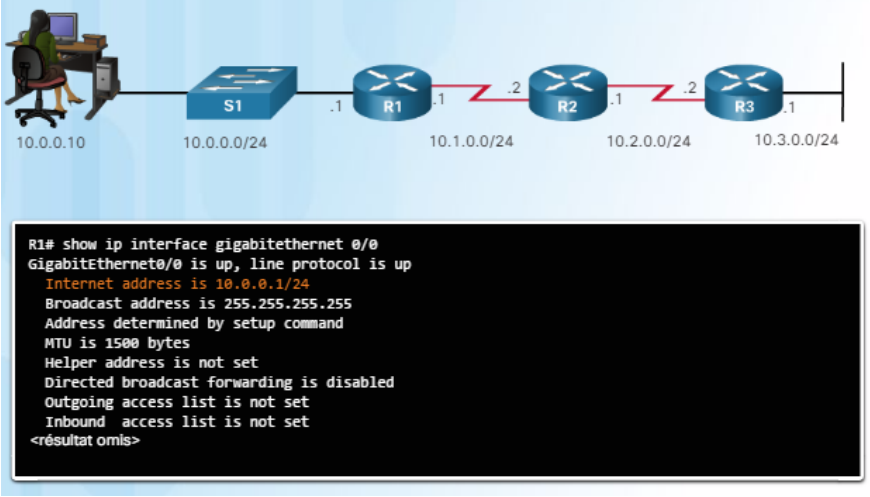


FIGURE 11.6 – Commande **show ip interface**

Problèmes de passerelle par défaut La passerelle par défaut pour un périphérique final est le périphérique réseau le plus proche capable d'acheminer le trafic vers d'autres réseaux. Si un périphérique possède une adresse de passerelle par défaut incorrecte ou inexistante, il ne pourra pas communiquer avec les périphériques de réseaux distants. Comme la passerelle par défaut est le chemin d'accès aux réseaux distants, son adresse doit appartenir au même réseau que le périphérique final.

L'adresse de la passerelle par défaut peut être configurée manuellement ou obtenue auprès d'un serveur DHCP. Tout comme les problèmes IPv4, les problèmes de passerelle par défaut peuvent être liés à une mauvaise configuration (en cas d'attribution manuelle) ou à des problèmes DHCP (en cas d'attribution automatique).

Pour résoudre les problèmes de passerelle par défaut mal configurée, assurez-vous d'abord que la passerelle par défaut du périphérique est correctement configurée. Si l'adresse par défaut a été manuellement définie mais n'est pas valide, remplacez-la tout simplement par l'adresse appropriée. Si l'adresse de la passerelle par défaut a été définie automatiquement, assurez-vous que le périphérique communique correctement avec le serveur DHCP. Il est également important de vérifier que l'adresse IPv4 et le masque de sous-réseau appropriés ont été configurés sur l'interface du routeur et que l'interface est active.

Pour vérifier la passerelle par défaut sur un ordinateur Windows, utilisez la commande **ipconfig**. Sur un routeur, utilisez la commande **show ip route** pour afficher la table de routage et vérifier que la passerelle par défaut, appelée « route par défaut », a été définie. Cette route est utilisée lorsque l'adresse de destination du paquet ne correspond à aucune autre route dans sa table de routage. La figure 11.7 indique que R2 est la route par défaut pour R1, et le résultat de la commande **show ip route** montre que la passerelle par défaut a été définie avec la route par défaut 10.1.0.2.

Résolution des problèmes DNS DNS (Domain Name Service) fait référence à un service automatisé permettant de mettre en correspondance des noms, comme www.cisco.com, avec des adresses IP. Bien que la résolution DNS ne soit pas indispensable à la communication des périphériques,

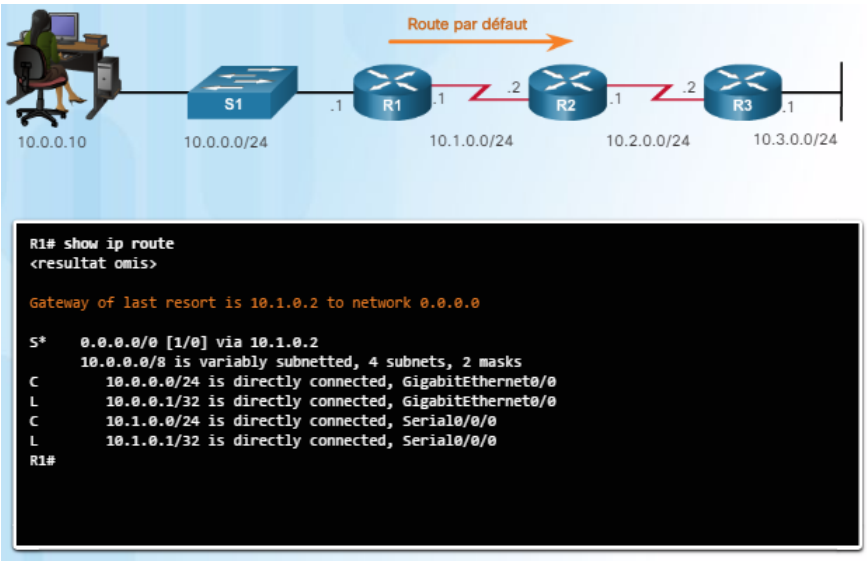


FIGURE 11.7 – Vérification de la route par défaut d'un routeur

elle est très importante pour l'utilisateur final.

Il n'est pas rare qu'un utilisateur confonde le fonctionnement d'un lien Internet avec la disponibilité du service DNS. Lorsqu'un utilisateur se plaint d'une panne de réseau ou d'Internet, il y a de fortes chances pour que cela soit dû à l'inaccessibilité d'un serveur DNS. Bien que le routage des paquets et tous les autres services réseau soient toujours opérationnels, les échecs DNS font croire à un problème de connexion. Si l'utilisateur entre un nom de domaine tel que www.cisco.com dans un navigateur Web, mais que le serveur DNS est inaccessible, le nom n'est pas traduit en adresse IP et le site Web ne s'affiche pas.

Les adresses du serveur DNS peuvent être attribuées manuellement ou automatiquement. Les administrateurs réseau sont souvent responsables de l'attribution manuelle des adresses du serveur DNS sur les serveurs et autres périphériques, tandis que le protocole DHCP est utilisé pour attribuer automatiquement des adresses de serveur DNS aux clients.

Utilisez la commande **ipconfig /all** pour déterminer le serveur DNS utilisé par l'ordinateur Windows. La commande **nslookup** est un autre outil de dépannage DNS utile pour les ordinateurs. Elle permet à l'utilisateur de lancer manuellement des requêtes DNS et d'analyser la réponse DNS.