Securité Réseau

Dr Toa Bi Irié Guy-Cédric,

Ph.D en Sécurité du Cloud & Expert en Cybersécurité

Securité Réseau

Module 3

01 Protocoles réseau

02 Ethernet et Protocole IP

03 Vérification de la connectivité

04 Protocole ARP

05 La couche de transport

06 Services réseau

07

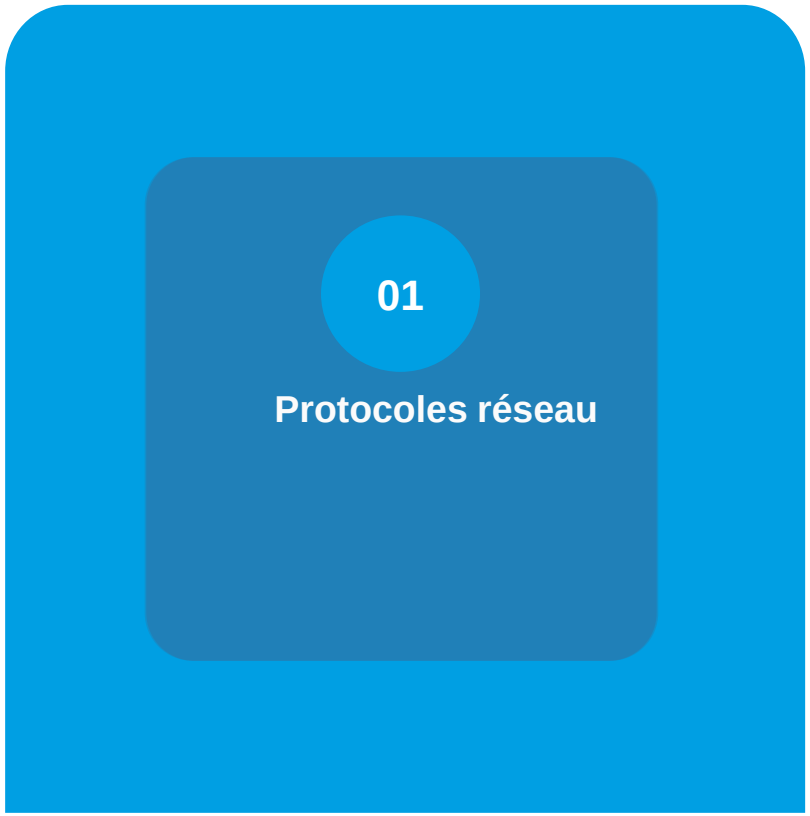
08 Lap pratiques

Objectifs du module

Titre du module: Protocoles réseau

Objectif du Module: Expliquer comment les protocoles permettent d'exploiter le réseau.

Titre du Rubrique	Objectif du Rubrique
Processus de communications réseau	Expliquer le fonctionnement de base des communications de données en réseau.
Protocoles de communication	Expliquer comment les protocoles permettent d'exploiter le réseau.
Encapsulation de données	Expliquer comment l'encapsulation de données permet la transmission des données sur le réseau.

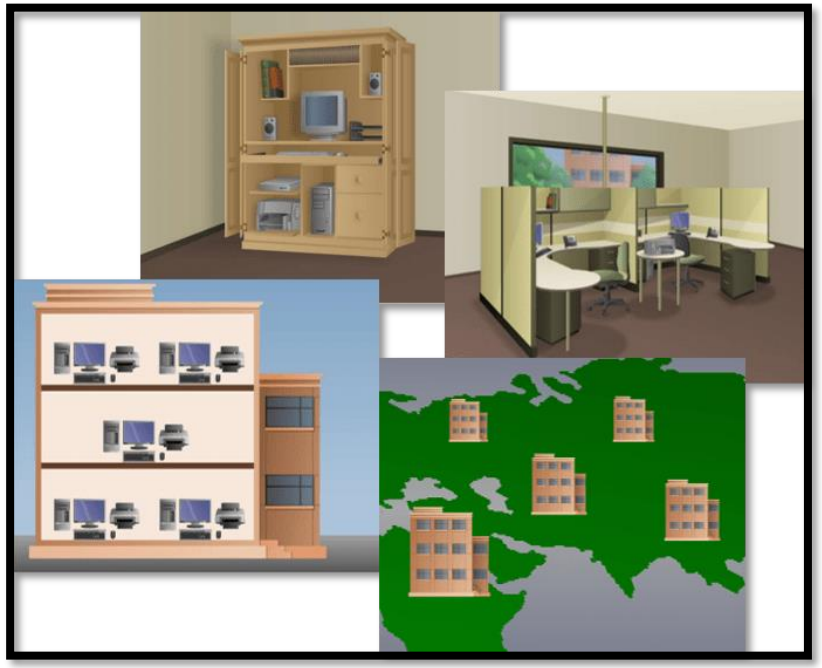


5.1 Processus de communications réseau

5.1.1 Réseaux de tailles diverses

Les **réseaux** existent dans **toutes les tailles :**

- **Les petits réseaux domestiques:** Les petits réseaux domestiques relient quelques ordinateurs entre eux et à Internet.
- **Le réseau SOHO:** Le réseau SOHO (réseau de petits bureaux/bureaux à domicile) permet de se connecter à un réseau d'entreprise.
- **Les réseaux de taille moyenne à grande**: Utilisés par les entreprises et les écoles, peuvent avoir de nombreux emplacements avec des **centaines ou des milliers** d'hôtes interconnectés.
- **Réseaux mondiaux**: **L'internet** est un réseau de réseaux qui relie des centaines de **millions d'ordinateurs** dans le monde.
- **Réseau Peer-to-Peer:** est un réseau dans lequel les ordinateurs fonctionnent à la fois comme **serveurs** et comme **clients** sur le réseau.

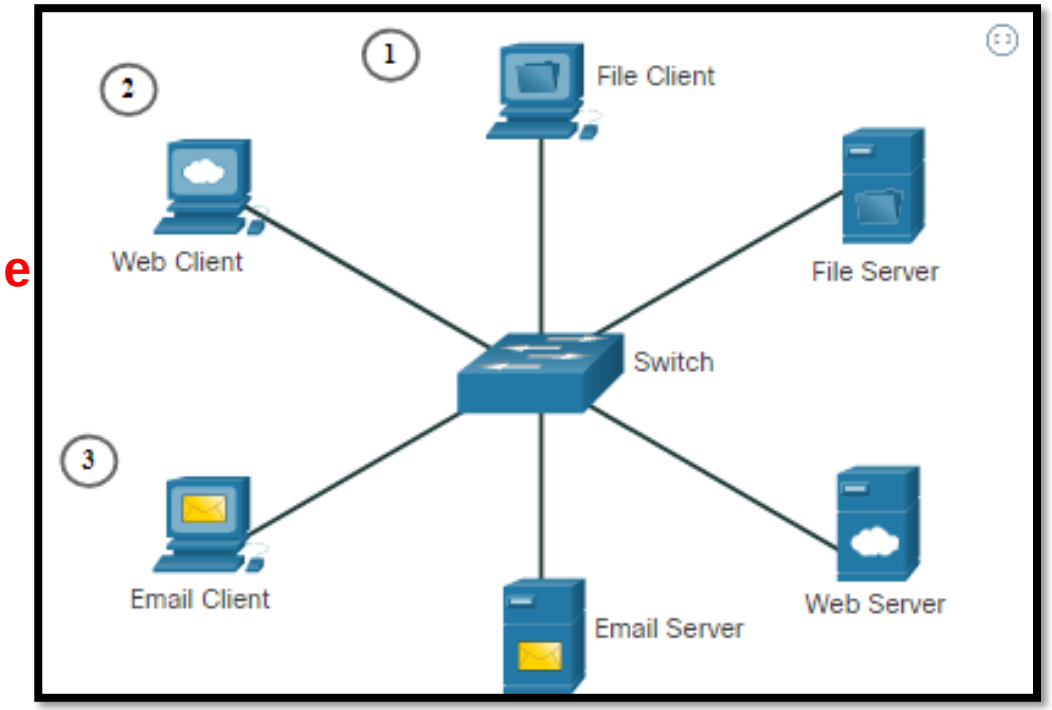


Résumé : Les **réseaux** existent dans **toutes les tailles (domestiques, SOHO, Moyen/grand réseau et réseau mondial).** Internet est le plus grand réseau existant.

Protocoles réseau

5.1.2 Communications client-serveur

- Tout appareil connecté a un réseau est un **hôte** (finaux, terminaux ou nœuds).
- Un **serveur** peut être polyvalent, c'est-à-dire qu'il offre une variété de **services**, tels que des **pages web**, la **messagerie** et les **transferts de fichiers**.
- Les c**lients** sont des ordinateurs hôtes équipés d'un logiciel qui leur permet de demander des informations auprès du serveur et de les afficher.

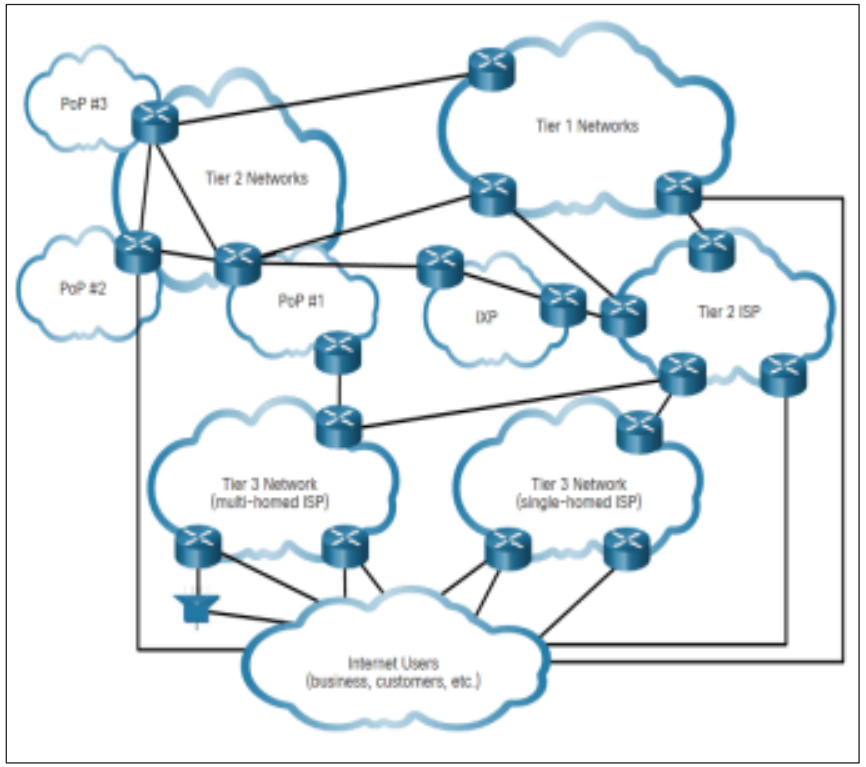


Résumé :

- ✓ Les **serveurs** sont des **ordinateurs équipés de lo**giciels leur permettant de **fournir des informations aux clients.**
- ✓ Les **clients** sont des **ordinateurs hôtes équipés d'un logiciel** qui leur **permet de demander des informations** auprès du serveur et de les afficher

5.1.4 Identifier le chemin réseau

- Le **trafic** de données est acheminé par **des câbles** en **cuivre** et à **fibre optique** qui traversent les terres et les océans. Ces connexions relient les sites de télécommunication et les fournisseurs d'accès à Internet (FAI) répartis dans le monde entier.
- Ces **FAI** mondiaux de **niveaux 1 et 2** relient certaines parties du web, généralement via un point d'échange Internet (**IXP**).
- Les réseaux de plus grande envergure se connectent aux réseaux de **niveau 2** via un **point de présence (PoP)**, qui se trouve généralement dans le bâtiment où sont établies les connexions physiques au FAI. Les **FAI** de **niveau 3** connectent les foyers et les entreprises à Internet.



5.1.5 – Travaux pratiques – Tracer une route

Résumé:

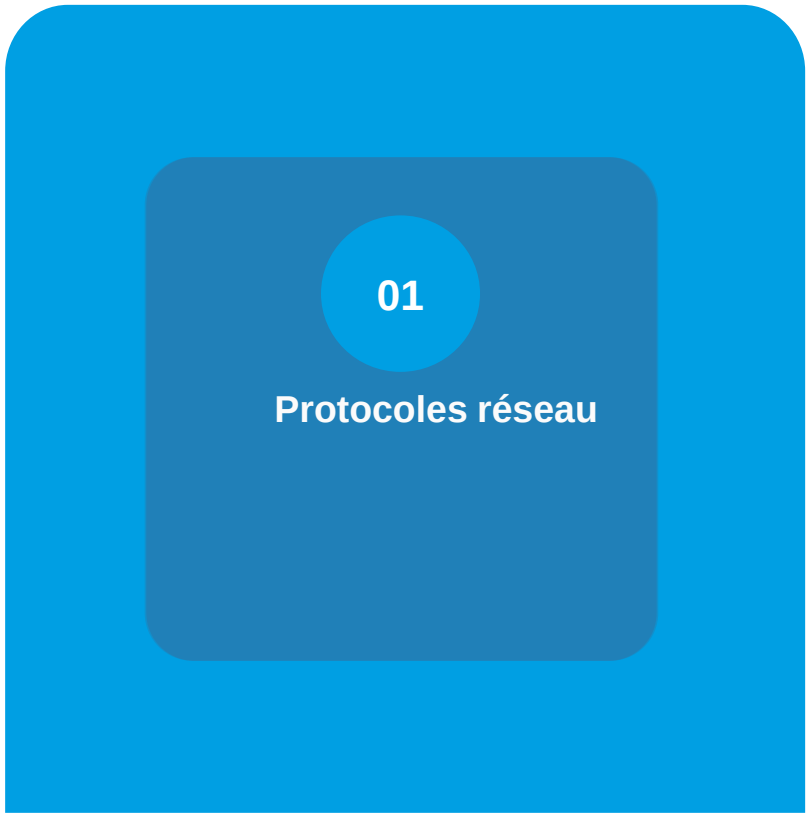
- ✓ Les **FAI** de **niveaux 1 (VERIZON) et 2 (Orange France)** sont reliés via un **point d'échange Internet** (**IXP**).
- ✓ Les **FAI** de **niveaux 2 (orange France) et 3 (Orange MALI)** sont reliés via un **point de présence** (**POP**).
- ✓ Les **FAI de niveau 3** connectent les **foyers** et les **entreprises** à l'internet

Protocoles réseau

5.1.5 Travaux pratiques – Tracer une route

Au cours de ces travaux pratiques, vous allez utiliser deux programmes de suivi de route pour examiner le chemin Internet menant aux réseaux de destination. L'objectif sera de :

- Vérifier la connectivité à un site web.
- Vous allez utiliser l'utilitaire traceroute sur la ligne de commande Linux.
- Utilisez un outil traceroute basé sur le Web.



5.2 Protocoles de communication

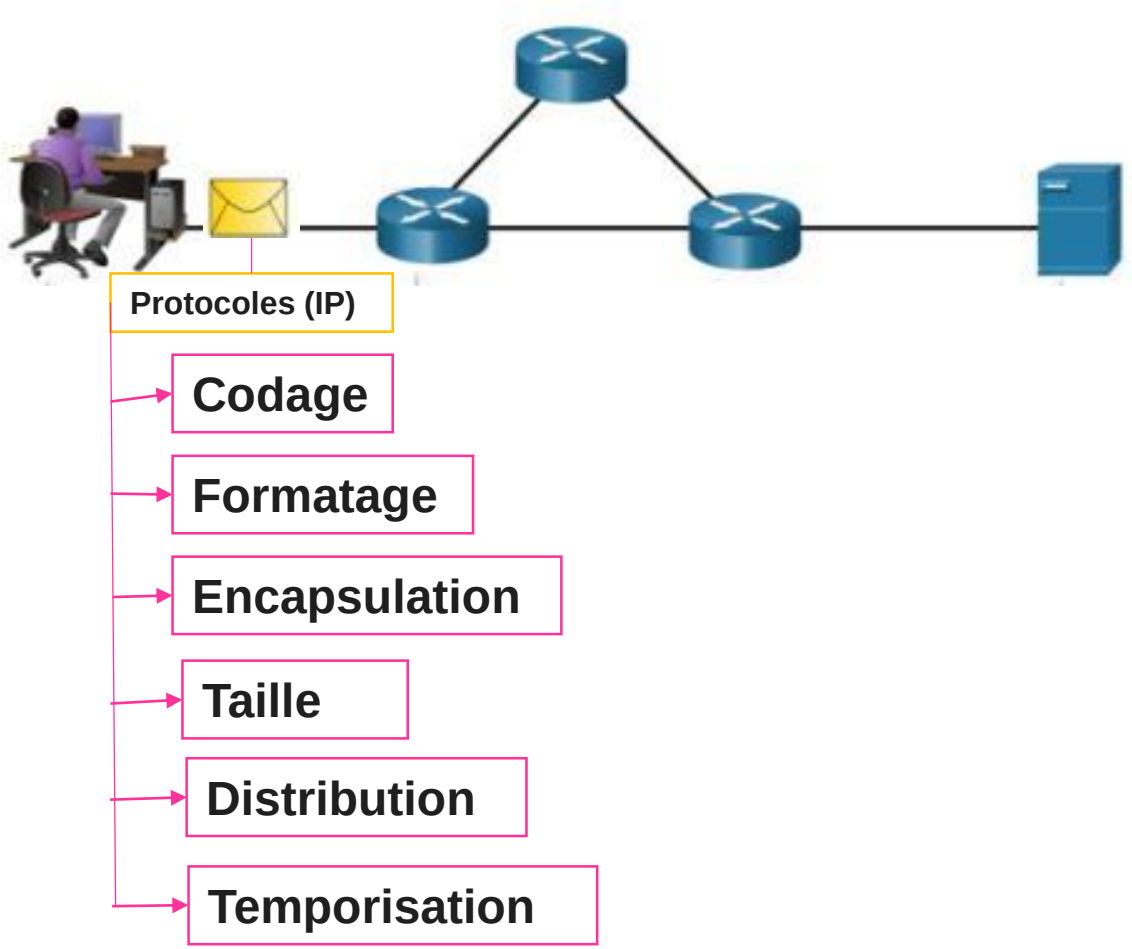
5.2.1 En quoi consistent les protocoles ?

- Une simple **connexion** physique filaire ou sans fil **ne suffit pas à établir la communication** entre deux appareils. Les périphériques doivent également savoir comment communiquer.
- Ces protocoles sont propres au mode de communication.
- Les protocoles réseau spécifient de nombreuses fonctionnalités de communication réseau.

Résumé : La **communication** est régie par des **règles** appelées **protocoles**

Protocoles de communication

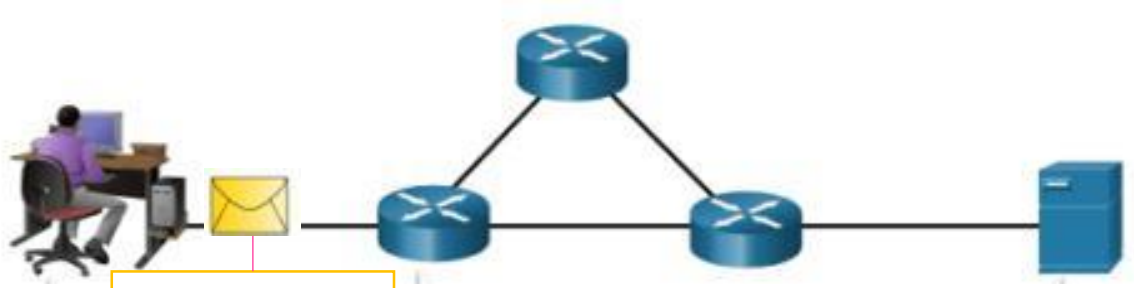
5.2.2 Protocoles réseau



- Les **protocoles réseau** permettent aux ordinateurs de **communiquer** sur les réseaux.
- 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).

Résumé : Les **protocoles réseau** définissent les paramètres de **codage**, de **formatage**, d'**encapsulation**, de **taille**, de **temporisation** et de **distribution** **des messages**.

5.2.2 Protocoles réseau



Protocoles (IP)

Structure de message

✓ spécifie comment le message est **formaté** ou **structuré**.

Le partage de chemin d'accès

✓ spécifie le processus par lequel les appareils de réseau **partagent des informations sur les chemins** d'accès avec d'autres réseaux

Le partage d'informations

✓ précise comment et quand les **messages d'erreur** et de **système** sont transmis entre les appareils.

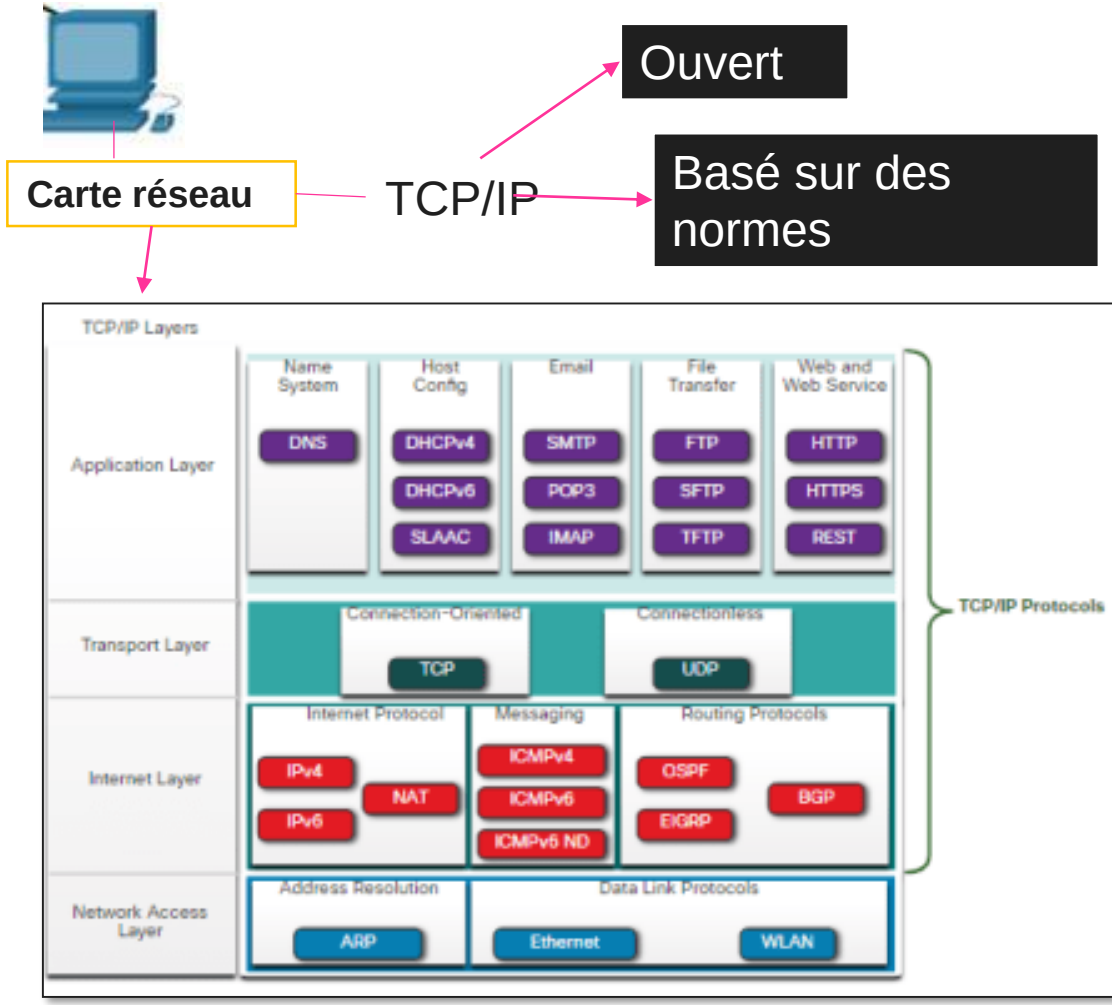
Gestion de session

- Gérer la **mise en place** et **l'arrêt des sessions** de transfert de données.

Protocoles de communication

5.2.3 Suite de protocoles TCP/IP

- TCP/IP a deux aspects importants pour les fournisseurs et les fabricants :
  - **Suite de protocoles standards ouverts** - Cela signifie qu'il est **librement accessible** au public et peut être utilisé par n'importe quel fournisseur sur son matériel ou dans son logiciel.
  - **Suite de protocoles basée sur des normes** - Cela signifie qu'elle a été **approuvée par le secteur des réseaux** et par un organisme de normalisation.



- **Résumé** : TCP/IP est la **suite de protocoles** utilisée par **Internet** et les **réseaux** d'aujourd'hui.
- Citer quelques protocoles de couches (**Application, Transport, Internet et accès réseau**) ?

5.2.3 La Suite de protocoles TCP/IP (Suite)

- **Couche de transport**
- **TCP** : Permet une **communication fiable** entre des processus fonctionnant sur des hôtes distincts et fournit des transmissions fiables et reconnues qui confirment le succès de la livraison.
- **UDP**: Permet à un processus s'exécutant sur un hôte d'envoyer des paquets à un processus s'exécutant sur un autre hôte.

Résumé : Les protocoles communs à la couche Transport de la suite sont :

✓ TCP : communication **fiable** et transmissions **fiables**

✓ UDP : communication **non fiable**

5.2.3 La Suite de protocoles TCP/IP (Suite)

Couche Internet

5.3.7 Travaux pratiques – Présentation de Wireshark

Protocole	Description
IPv4 (Internet Protocol version 4)	Reçoit des segments de message de la couche transport, emballe les messages en paquets et adresse les paquets pour une livraison de bout en bout sur un réseau. IPv4 utilise une adresse 32 bits.
IPv6 (IP version 6)	Similaire à IPv4 mais utilise une adresse 128 bits.
NAT (Network Address Translation)	Traduit les adresses IPv4 d'un réseau privé en adresses IPv4 publiques uniques au monde.

Résumé : Les protocoles communs à la couche Internet de la suite sont : **IPv4** (32 bits), **IPv6** (128 bits), **NAT** (traduire une IP privée en IP publique)

5.2.3 La Suite de protocoles TCP/IP (Suite)

Envoi de messages

5.3.7 Travaux pratiques – Présentation de Wireshark

Protocole	Description
ICMPv4 (Internet Control Message Protocol for IPv4)	Fournit un retour d'information d'un hôte de destination à un hôte source sur les erreurs de livraison de paquets.
ICMPv6 (ICMP pour IPv6)	Fonctionnalité similaire à ICMPv4, mais elle est utilisée pour les paquets IPv6.
ICMPv6 ND (ICMPv6 Neighbor Discovery)	Inclut quatre messages de protocole utilisés pour la résolution d'adresses et la détection d'adresses en double.

Protocoles de routage

Protocole	Description
OSPF (Open Shortest Path First)	Protocole de routage d'état de liaison qui utilise une conception hiérarchique basée sur des zones. Il s'agit d'un protocole de routage interne standard ouvert.
EIGRP (Enhanced Interior Gateway Routing Protocol)	Protocole de routage propriétaire de Cisco qui utilise une métrique composite basée sur la largeur de bande, le délai, la charge et la fiabilité.
BGP (Border Gateway Protocol)	Un protocole de routage de passerelle extérieure standard ouvert utilisé entre les fournisseurs de services Internet (ISPs).

5.2.3 La Suite de protocoles TCP/IP (Suite)

Couche accès réseau

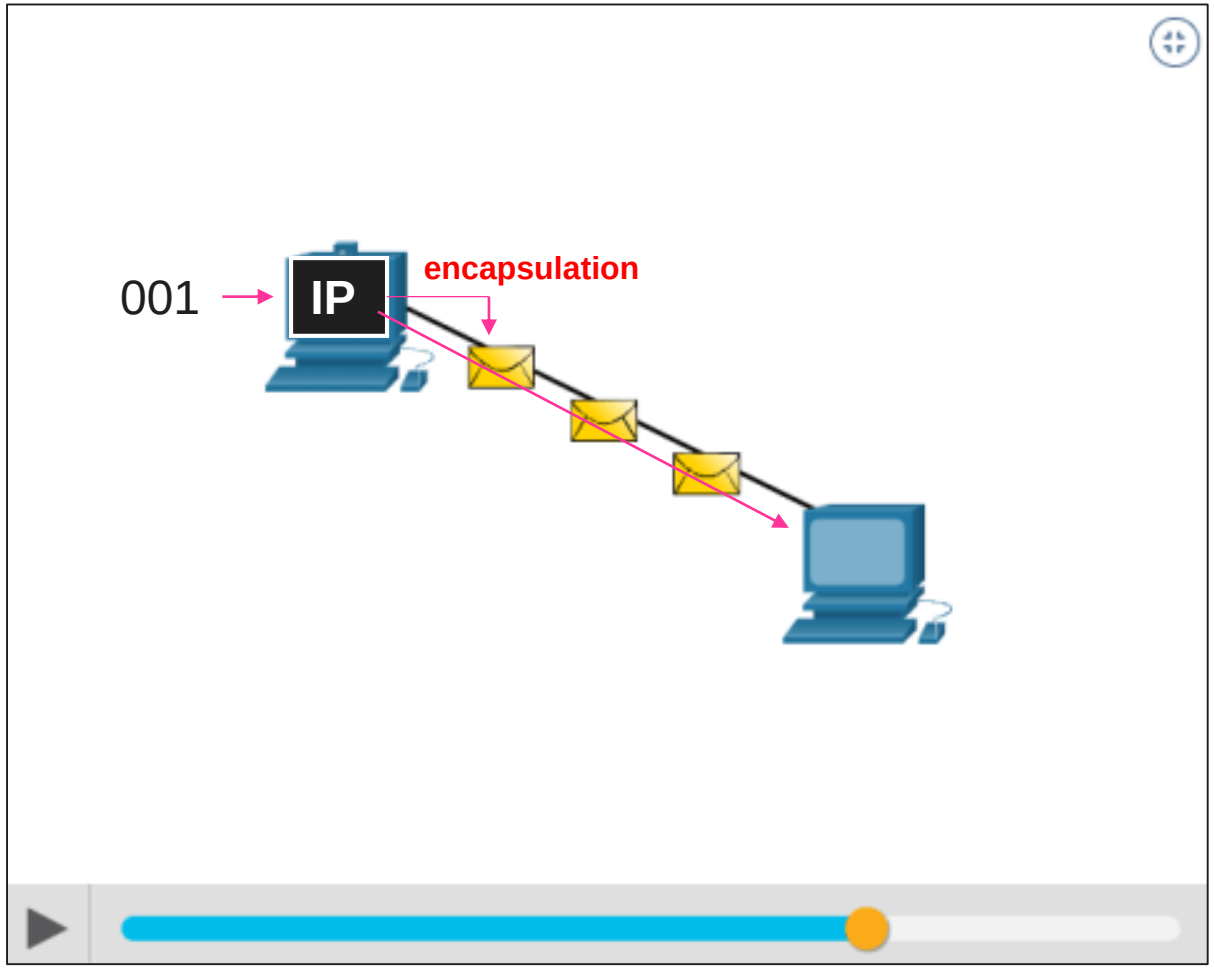
- **Le protocole ARP** (Address Resolution Protocol) assure le **mappage d'adresses dynamique** entre une adresse IP et une adresse matérielle.
- **Protocoles de Liaison de Données**
  - **Ethernet**- Définit les règles relatives aux normes de câblage et de signalisation de la couche d'accès au réseau.
  - **WLAN** (Wireless Local Area Network): Définit les règles de signalisation sans fil sur les fréquences radio 2,4 GHz et 5 GHz.

•**Résumé: Le protocole ARP** permet de déterminer l'adresse **MAC** d'un périphérique connaissant son **adresse IP**.

5.22.3 Format et encapsulation des messages

Résumé :

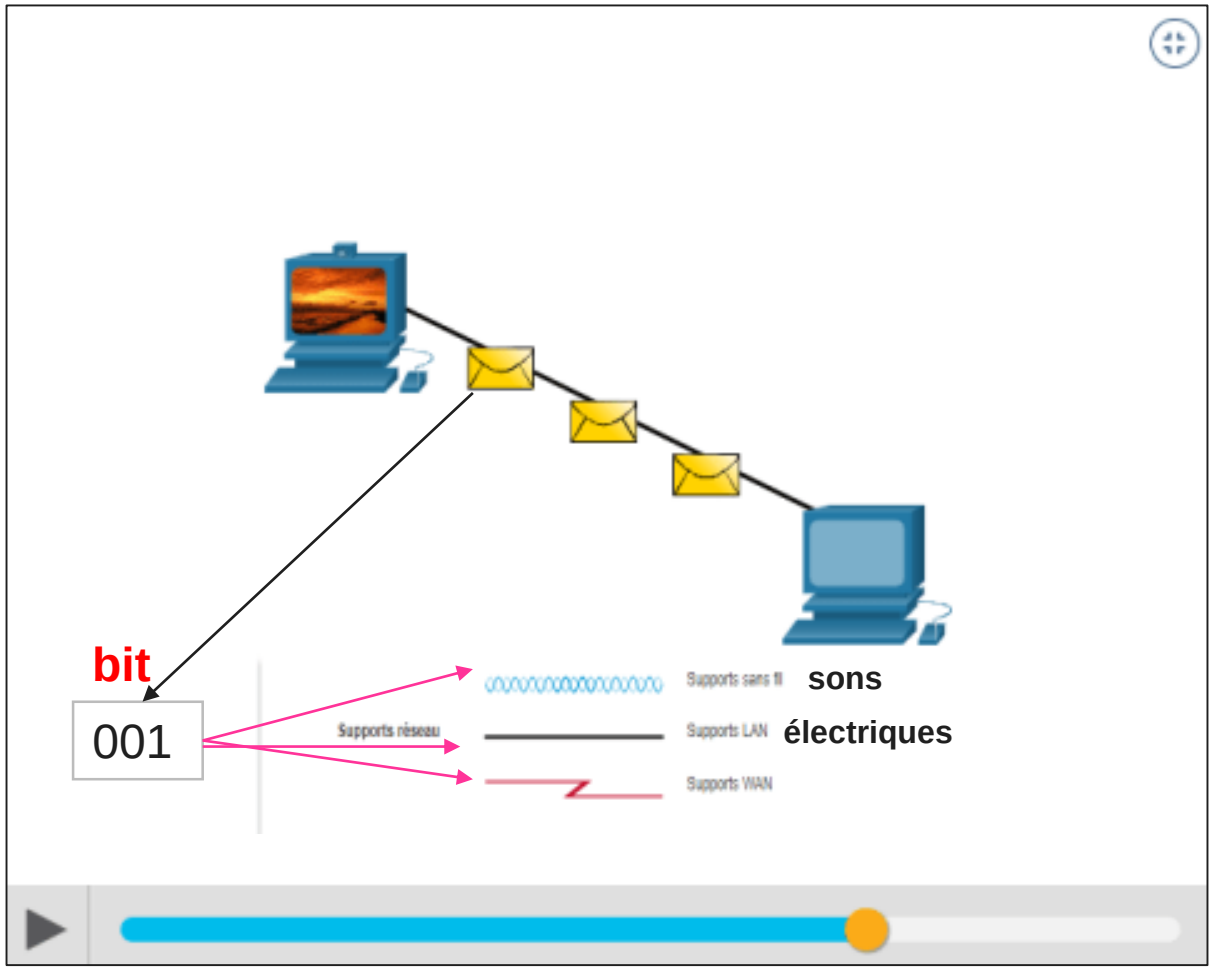
- Le **processus** consistant à placer un format de message (**la lettre**) dans un autre (**l'enveloppe**) s'appelle « **encapsulation** ».
- Une **désencapsulation** a lieu lorsque le processus est inversé par le destinataire et que la lettre est retirée de l'enveloppe.
- **IP** est **responsable de l'envoi** d'un message de la **source** du message vers la **destination** sur un ou plusieurs réseaux.



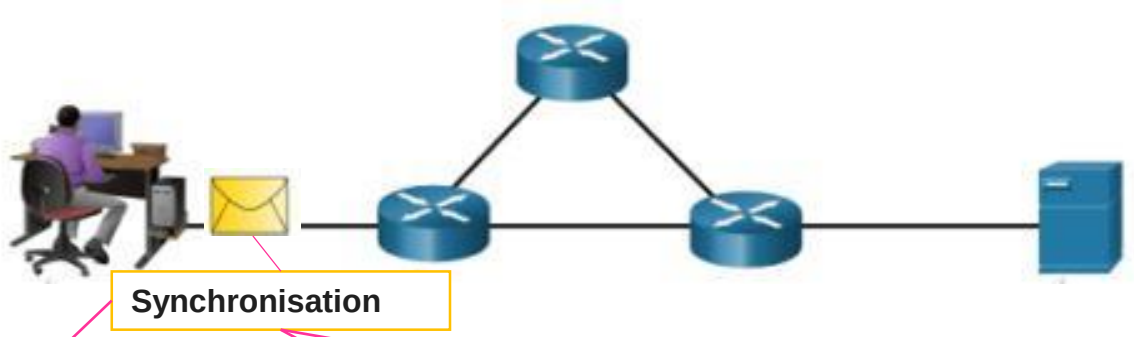
5.2.5 Taille des messages

Une autre règle de communication est la **taille** des messages.

- Le **format du codage** entre les hôtes doit être adapté au support.
- Les **messages** envoyés sur le réseau sont tout d'abord convertis en **bits**, par l'hôte émetteur.
- Chaque **bit** est codé en modèle de **sons, d'ondes lumineuses** ou **d'impulsions électriques,** selon le **support du réseau** sur lequel les bits sont transmis.
- L'hôte de destination reçoit et décode les signaux pour interpréter le message.



5.2.6 Synchronisation des messages



Contrôle du Flux

- Gère le **taux** et la **quantité** d'informations pouvant être envoyées et la **vitesse** à laquelle elles peuvent être livrées.

Délai de réponse

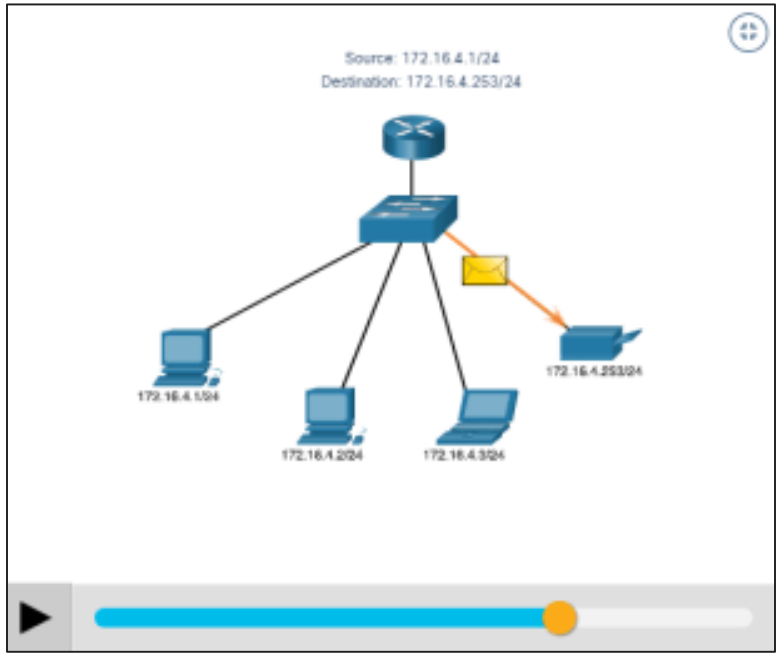
-spécifie le **délai d'attente** des réponses et l'action à entreprendre en cas de délai d'attente dépassé.

La Méthode d'Accès

-Détermine le moment où un individu peut envoyer un message.

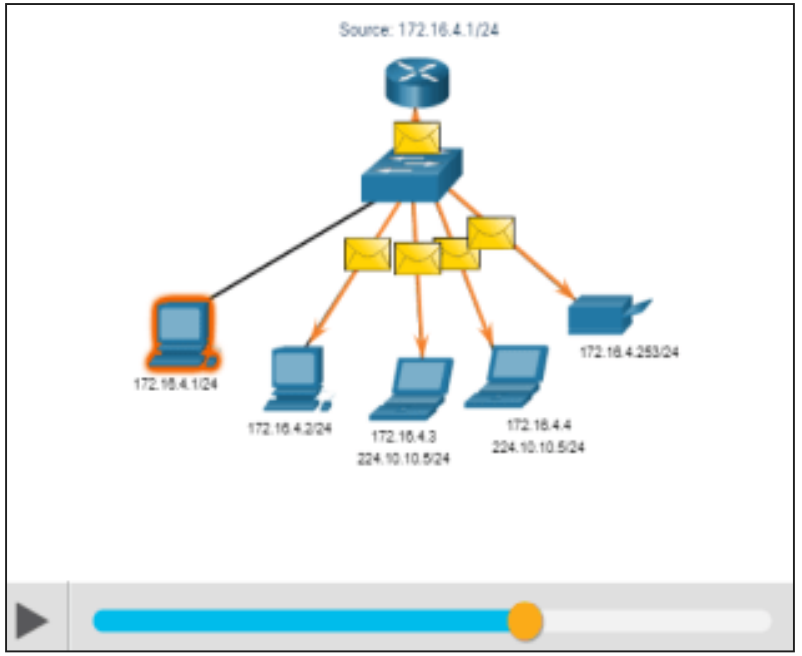
5.2.7 Monodiffusion, multidiffusion et diffusion

Monodiffusion: Une option de livraison **un à un** est appelée monodiffusion,



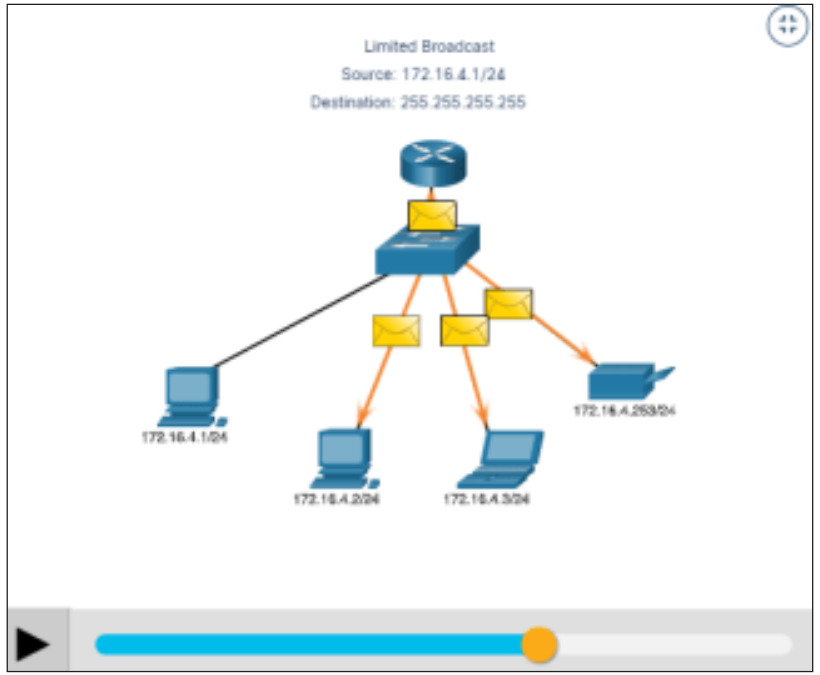
Multidiffusion:

une option de livraison de type « **un à plusieurs** ».



Diffusion:

La diffusion correspond à une option de livraison de type « **un à tous** ».



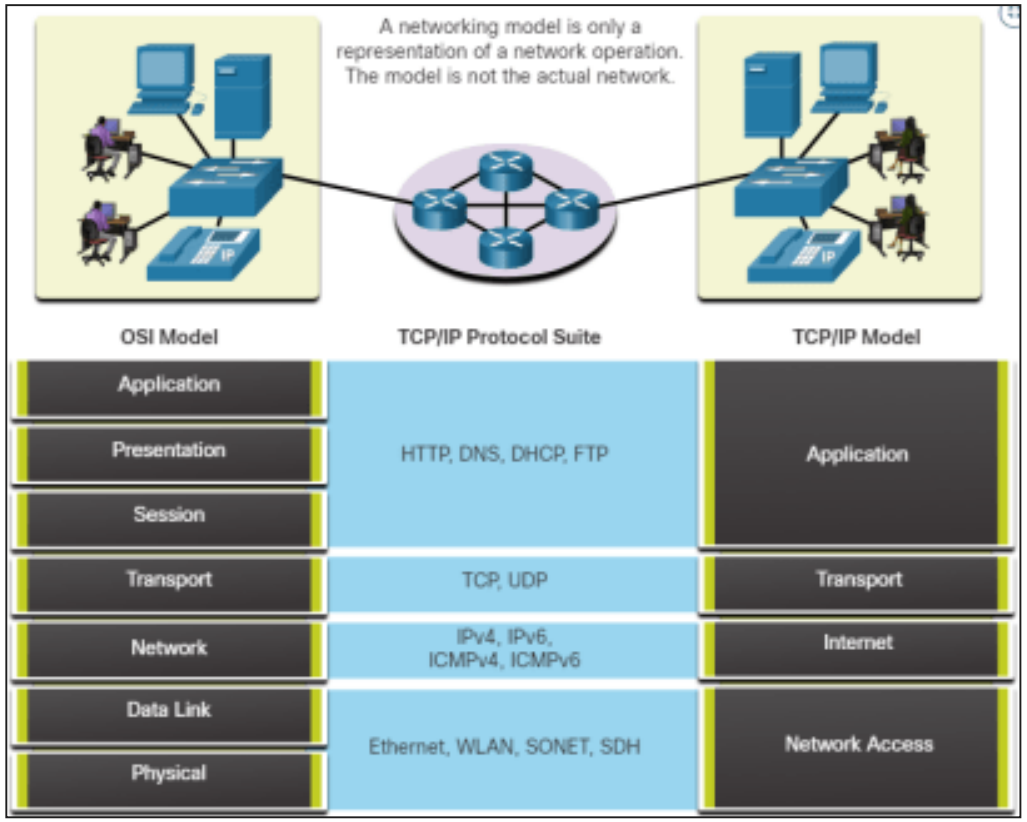
5.2.8 Avantage de l'utilisation d'un modèle en couches

Les avantages de l'utilisation d'un modèle à plusieurs niveaux :

- Aide à la **conception de protocoles**
- Stimule la **concurrence.**
- **Prévention des changements technologiques** ou de capacités
- Fournir un **langage commun**

Deux **modèles en couches** décrivent les opérations réseau:

- Modèle de référence pour l'interconnexion des systèmes ouverts (**OSI**)
- Modèle de Référence **TCP/IP**



Résumé : Le modèle OSI comporte **sept couches.** Le modèle TCP/IP comporte **quatre couches**

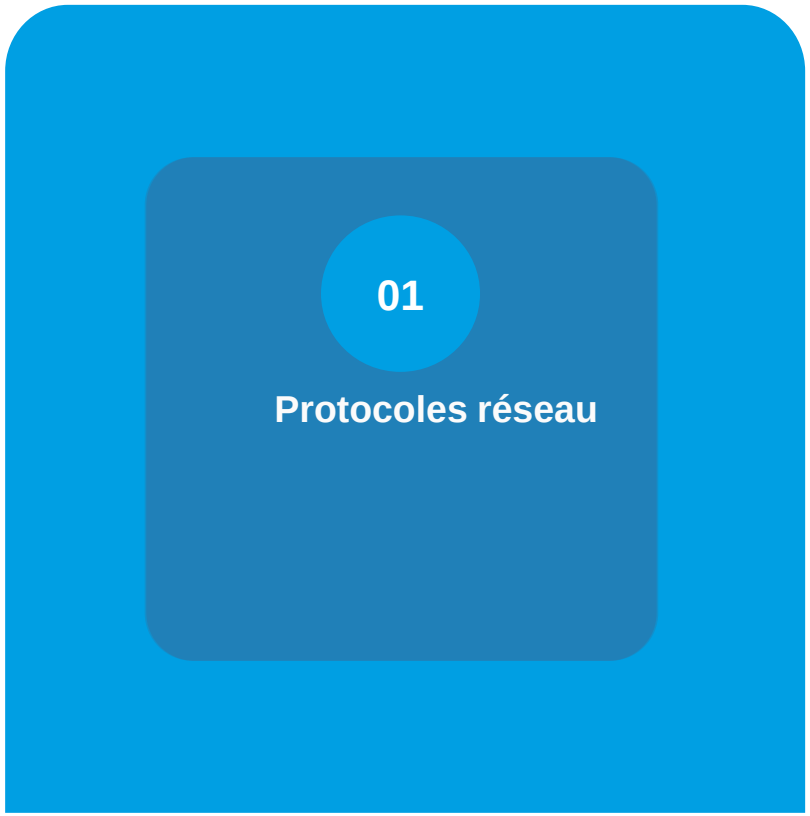
5.2.9 Modèle de référence OSI (Suite)

Couche du Modèle OSI	Description
7 - Application	Détention des protocoles utilisés pour les communications de processus à processus
6 - Présentation	Permet une représentation commune des données transférées entre les services de la couche application.
5 - Session	fournit des services à la couche de présentation pour organiser son dialogue et qui gère les échanges de données.
4 - Transport	Définit les services permettant de segmenter, transférer et ré-assembler les données pour les communications individuelles entre les périphériques finaux.
3 - Réseau	Fournit des services permettant d'échanger des données individuelles sur le réseau.
2 - Liaison de Données	Décrivent des méthodes d'échange de trames de données entre des périphériques sur un support commun.
1 - Physique	Décrivent les moyens mécaniques, électriques, fonctionnels et méthodologiques permettant d'activer, de gérer et de désactiver des connexions physiques pour la transmission de bits vers et depuis un périphérique réseau.

5.2.10 Le modèle de référence TCP/IP

- Le modèle de protocole TCP/IP est couramment appelé **modèle Internet**.

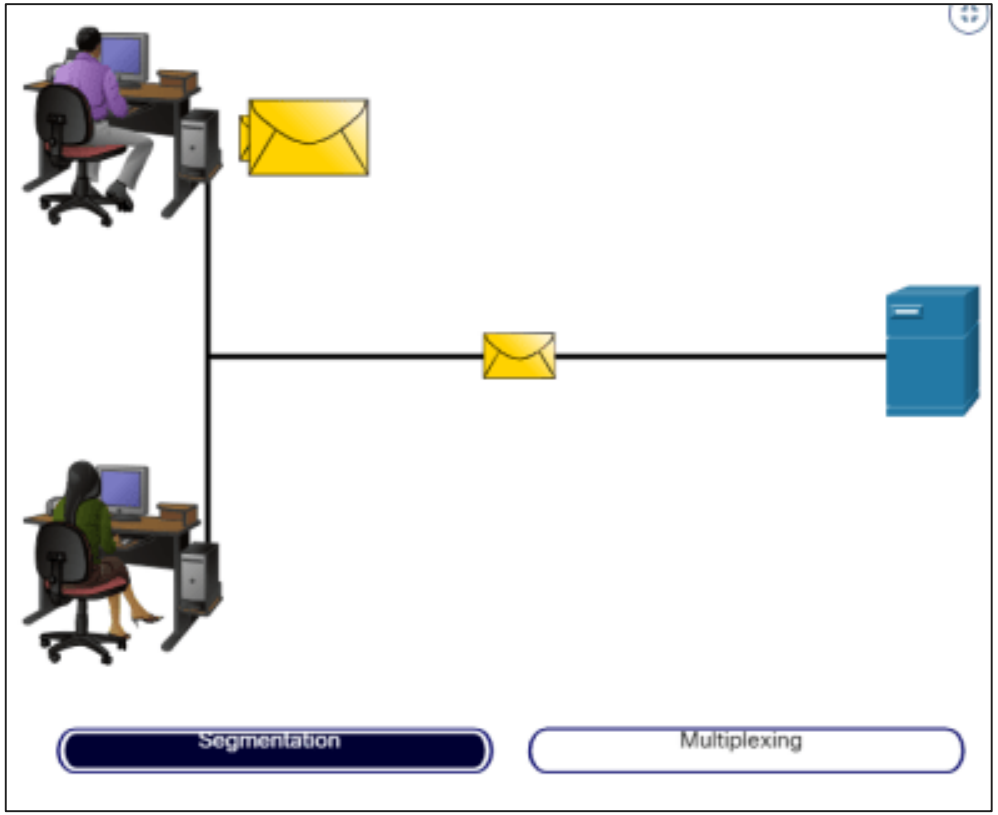
Couche du Modèle TCP/IP	Description
4 - Application	Représente des données pour l'utilisateur, ainsi que du codage et un contrôle du dialogue.
3 - Transport	prend en charge la communication entre les appareils sur divers réseaux
2 - Internet	Détermine le meilleur chemin à travers le réseau
1 - Accès réseau	Contrôle les périphériques matériels et les supports qui constituent le réseau.



5.3 L'encapsulation des données

5.3.1 Segmentation des messages

- La segmentation est nécessaire car les réseaux de données utilisent la suite de protocoles TCP/IP pour envoyer des données dans des paquets IP individuels.
- Les paquets contenant des segments pour la même destination peuvent être envoyés sur des chemins différents.



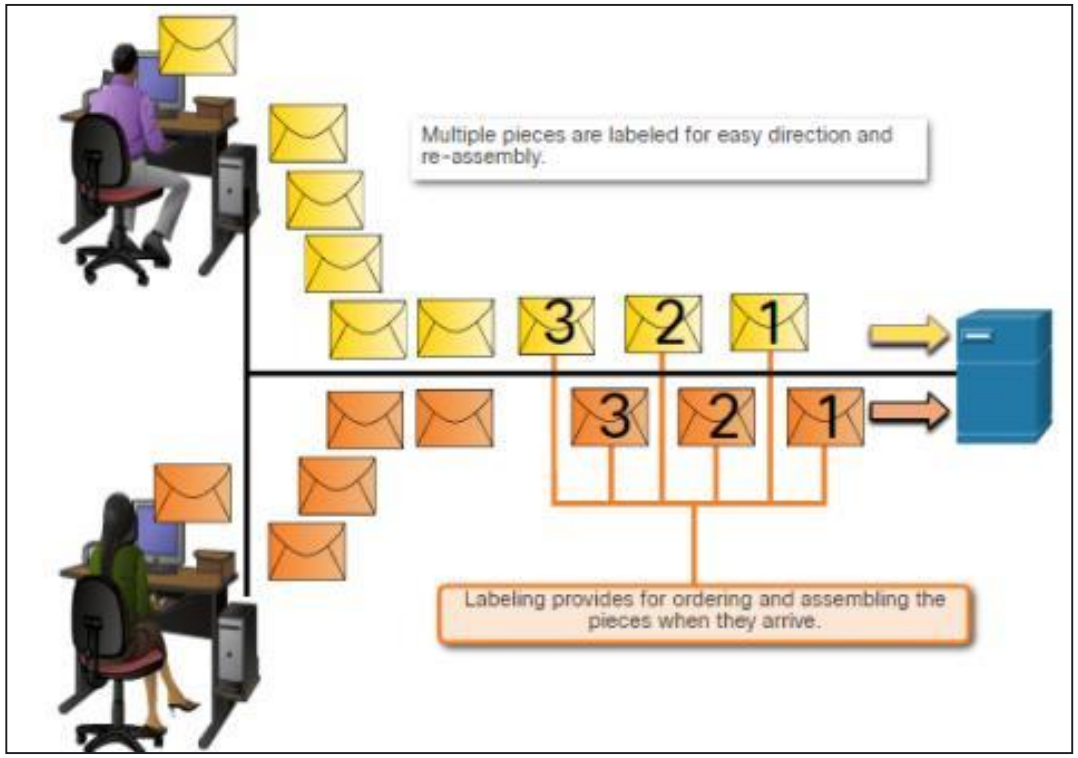
•**Résumé** : La **segmentation** est le processus consistant à **diviser un flux de données en unités plus petites** pour les transmissions sur le réseau.

5.3.1 Segmentation des messages (Suite)

Résumé :

Avantages de segmentation des Messages:

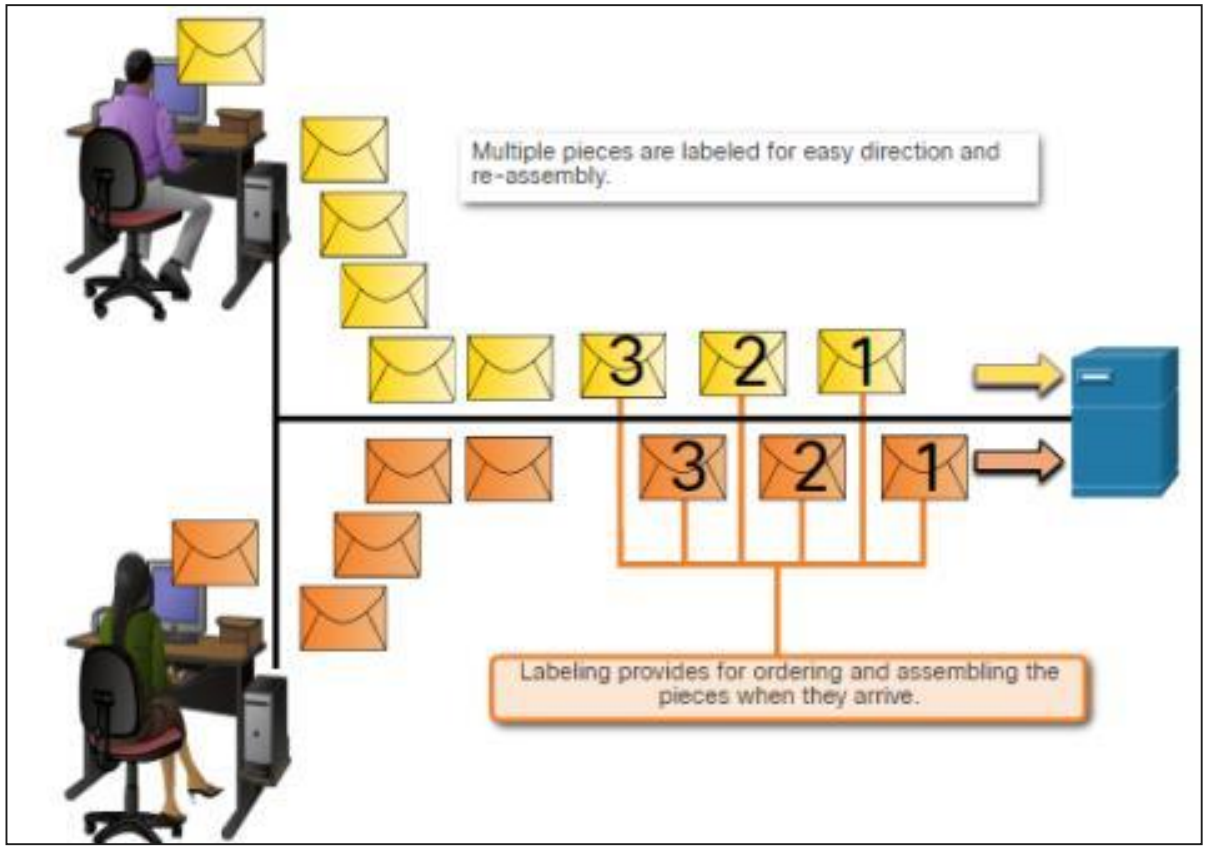
- **Augmente la vitesse-** Permet à de nombreuses conversations différentes d'être entrelacées sur le réseau appelé **multiplexage.**
- **Augmente l'efficacité-** Si un segment ne parvient pas à atteindre sa destination, **seul ce segment doit être retransmis** au lieu de renvoyer l'intégralité du flux de données.



Encapsulation de données

5.3.2 Séquençage

- Lors de la transmission de messages en utilisant la segmentation et le multiplexage, il est possible que les données atteignent la destination dans un **ordre réduit**.
- Chaque segment du message doit passer par un processus similaire pour s'assurer qu'il arrive à la bonne destination et peut être réassemblé dans le contenu du message original.

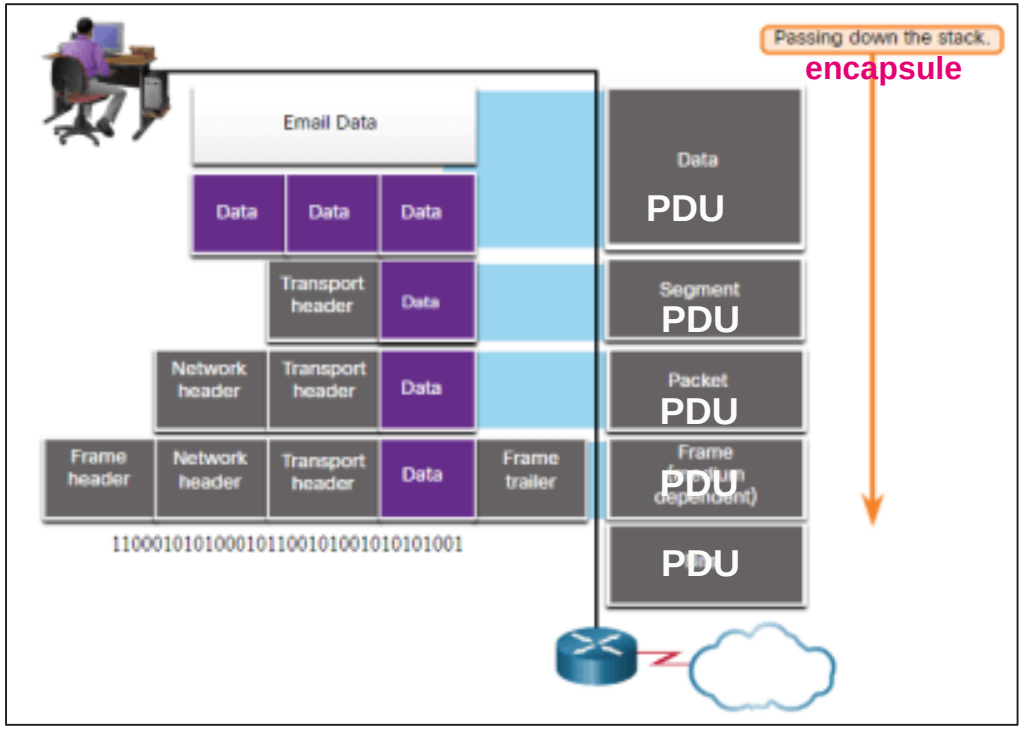


Résume : **TCP** est responsable du **séquençage des segments** individuels

Encapsulation de Données

5.3.3 Unités de Données du 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 d'utilisation.
- À chaque étape du processus, une unité de données de protocole possède un nom différent qui reflète ses nouvelles fonctions.

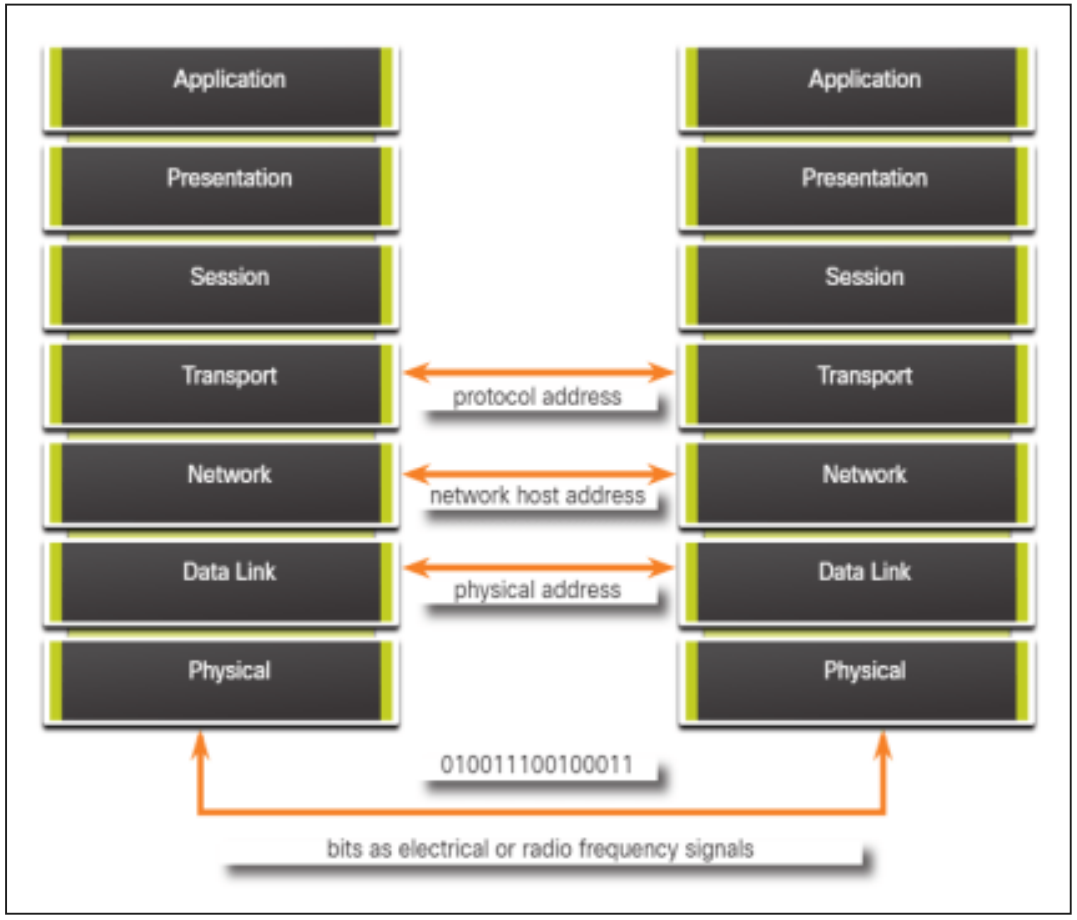


***Remarque**: Bien que la PDU UDP soit appelée datagramme, les paquets IP sont parfois également appelés datagrammes IP.*

Résumé : La forme que prend un élément de données à **n'importe quelle couche** est appelée **unité de données de protocole** (PDU)

5.3.4 Trois adresses

- La couche Transport utilise des adresses de protocole sous la forme de **numéros de port** pour **identifier les applications** du réseau .
- La couche Réseau spécifie les adresses **qui identifient les réseaux** auxquels sont connectés les clients et les serveurs.
- La **couche Liaison de données** spécifie les appareils du réseau local chargés de traiter les **trames de données.**



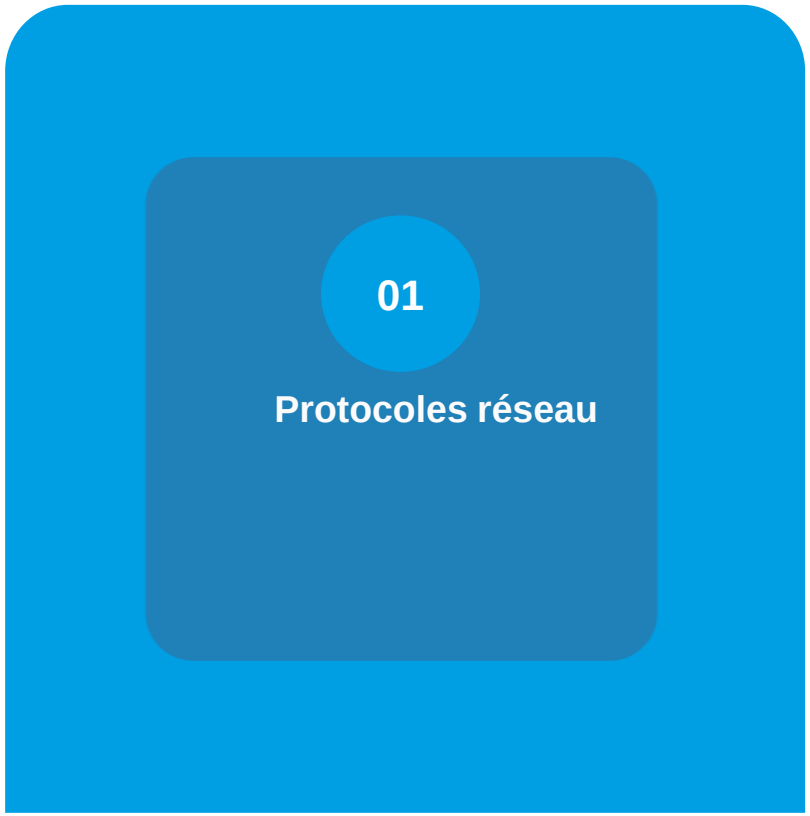
Résumé : Pour assurer la communication sur le réseau, les protocoles réseau utilisent trois adresses: **Adresse de port, Adresse IP et Adresse MAC**

Exemple de dés-encapsulation

5.3.7 Travaux pratiques – Présentation de Wireshark

Wireshark est un analyseur de protocoles (analyseur de paquets) utilisé pour dépanner les réseaux, effectuer des analyses, développer des logiciels et des protocoles et s'informer.

Au cours de ces travaux pratiques, vous allez utiliser Wireshark pour capturer et analyser le trafic réseau.



5.4 Récapitulation des protocoles du réseau

Qu'est-ce que j'ai appris dans ce module?

- Les réseaux existent dans toutes les tailles et peuvent être trouvés dans les maisons, les entreprises et d'autres organisations. Internet est le plus grand réseau existant.
- Les serveurs sont des hôtes qui utilisent des logiciels spécialisés pour leur permettre de répondre aux demandes de différents types de données émanant des clients.
- Les clients sont des hôtes qui utilisent des applications logicielles telles que des navigateurs Web, des clients de messagerie ou des applications de transfert de fichiers pour demander des données aux serveurs.
- Les grandes entreprises peuvent se connecter à des FSI de niveau 2 par l'intermédiaire d'un point de présence (POP).
- Les FAI de niveau 3 connectent les foyers et les entreprises à l'internet.
- Les protocoles réseau spécifient de nombreuses fonctionnalités de communication réseau telles que l'encodage des messages, la mise en forme et l'encapsulation des messages et les options de remise.
- Les protocoles spécifient la structure des messages et la façon dont les périphériques réseau partagent des informations sur les chemins d'accès à d'autres réseaux.

Qu'est-ce que j'ai appris dans ce module? (suite)

- Les protocoles communs à la couche d'application de la suite sont DNS, DHCP, POP3 et HTTPS.
- Le modèle OSI comporte sept couches. Le modèle TCP/IP comporte quatre couches.
- Les données sont divisées en une série de petites pièces et envoyées sur le réseau. C'est ce qu'on appelle la segmentation.
- Une vitesse accrue est gagnée parce que de nombreuses conversations de données peuvent se produire en même temps sur le réseau. Ce processus est appelé multiplexage.
- Lorsque les données sont transmises à la pile de protocole à envoyer, différentes informations sont ajoutées par chaque couche. Ce processus est appelé encapsulation.
- La forme que prend un élément de données à n'importe quelle couche est appelée unité de données de protocole (PDU).
- La **désencapsulation** est le processus utilisé par un périphérique récepteur pour supprimer une ou plusieurs des en-têtes de protocole.

Securité Réseau

Module 3

01 Protocoles réseau

02 Ethernet et Protocole IP

03 Vérification de la connectivité

04 Protocole ARP

05 La couche de transport

06 Services réseau

07

08 Lap pratiques

Objectifs du module

Titre du module: Ethernet et Protocole IP

Objectif du Module: Expliquer comment l'Ethernet et les protocoles IP assurent la communication réseau.

Titre du Rubrique	Objectif du Rubrique
Ethernet	Expliquer comment Ethernet prend en charge la communication réseau.
IPv4	Expliquer comment le protocole IPv4 prend en charge la communication réseau.
Notions de base sur l'adressage IP	Expliquer comment les adresses IP assurent la communication réseau.
Les types d'adresses IPv4	Présenter les types d'adresses IPv4 qui permettent la communication réseau.
La passerelle par défaut	Expliquer comment la passerelle par défaut assure la communication réseau.
IPv6	Expliquer comment le protocole IPv6 assure la communication réseau.

02

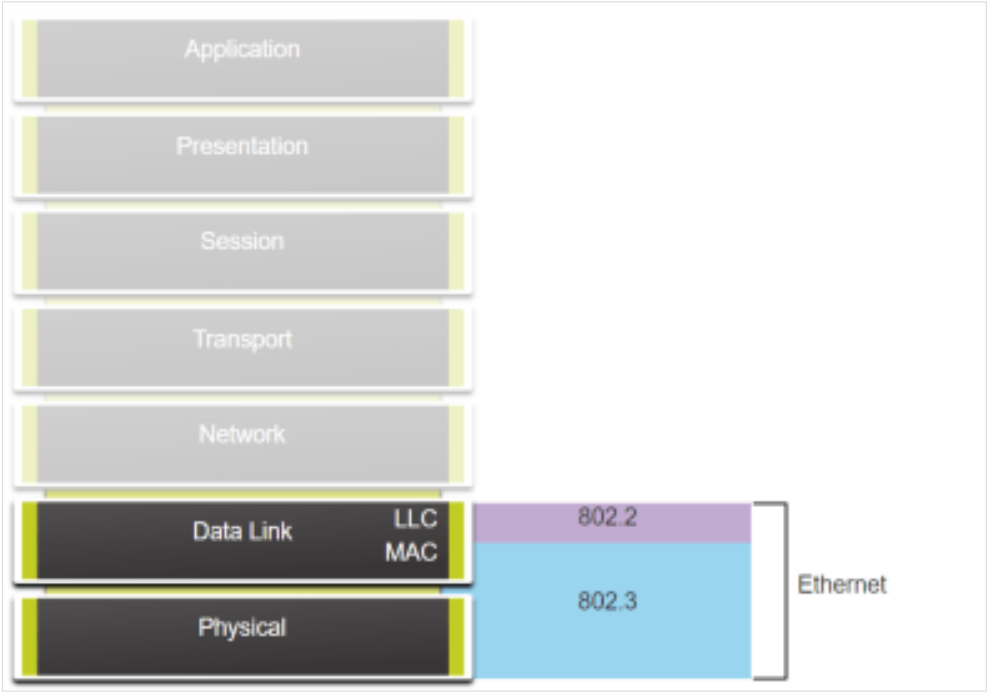
Ethernet et Protocole IP

6.1 Ethernet

6.1.1 Encapsulation Ethernet

- Ethernet prend en charge les **bandes passantes** de données de **10 Mbit/s à 100,000 Mbit/s** (100 Gbit/s)
- Comme illustré à la figure, les normes Ethernet définissent à la fois les protocoles de la couche 2 et les technologies de la couche 1.

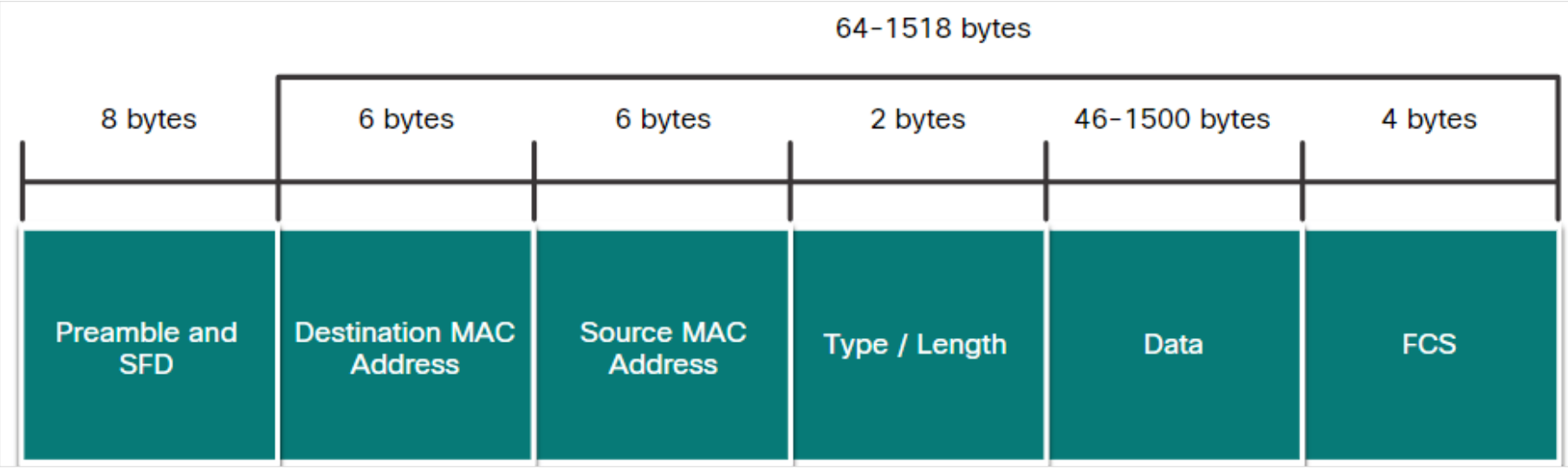
Ethernet et le modèle OSI



- **Résumé** : Les réseaux **LAN Ethernet** et **sans fil** (WLAN) sont les **deux technologies LAN** les plus populaires. Il fonctionne sur les **couches physiques** et **de liaison de données du modèle OSI** et est défini dans les normes **IEEE 802.2** et **802.3**.

6.1.2 Champs de trame Ethernet

- Toute **trame inférieure à 64 octets** est interprétée comme un «**fragment de collision**» ou une «**trame incomplète**» et est automatiquement **rejetée** par les périphériques récepteurs.
- Les **trames** de **plus de 1500 octets** de données sont considérées comme des trames «**jumbo» (géantes) ou «baby giant frames**» (légèrement géantes).

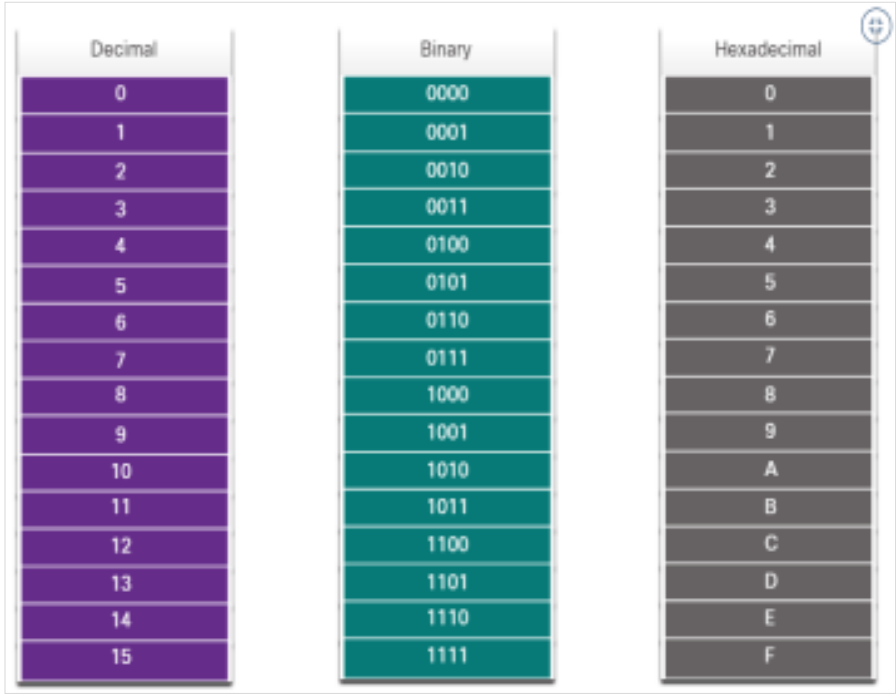


Champs de trame Ethernet

Résumé : La **taille minimale** des trames Ethernet est de **64 octets** et la **taille maximale** de **1518 octets**. Le champ SFD n'est pas utilisé dans le calcule de la taille.

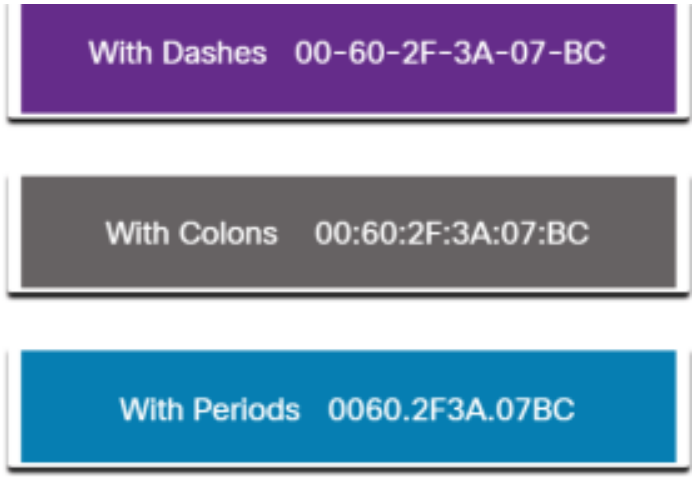
6.1.4 Format des adresses MAC

- Les chiffres hexadécimaux utilisent les chiffres 0 à 9 et les lettres A à F.
- On utilise généralement le format hexadécimal pour représenter des données binaires.



Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Équivalents **décimaux et binaires** des caractères hexadécimaux **0 à F**



Différentes **représentations** des adresses MAC

Résumé: Une **adresse MAC Ethernet** est une valeur binaire de **48 bits** exprimées sur **12 chiffres hexadécimaux.**

02

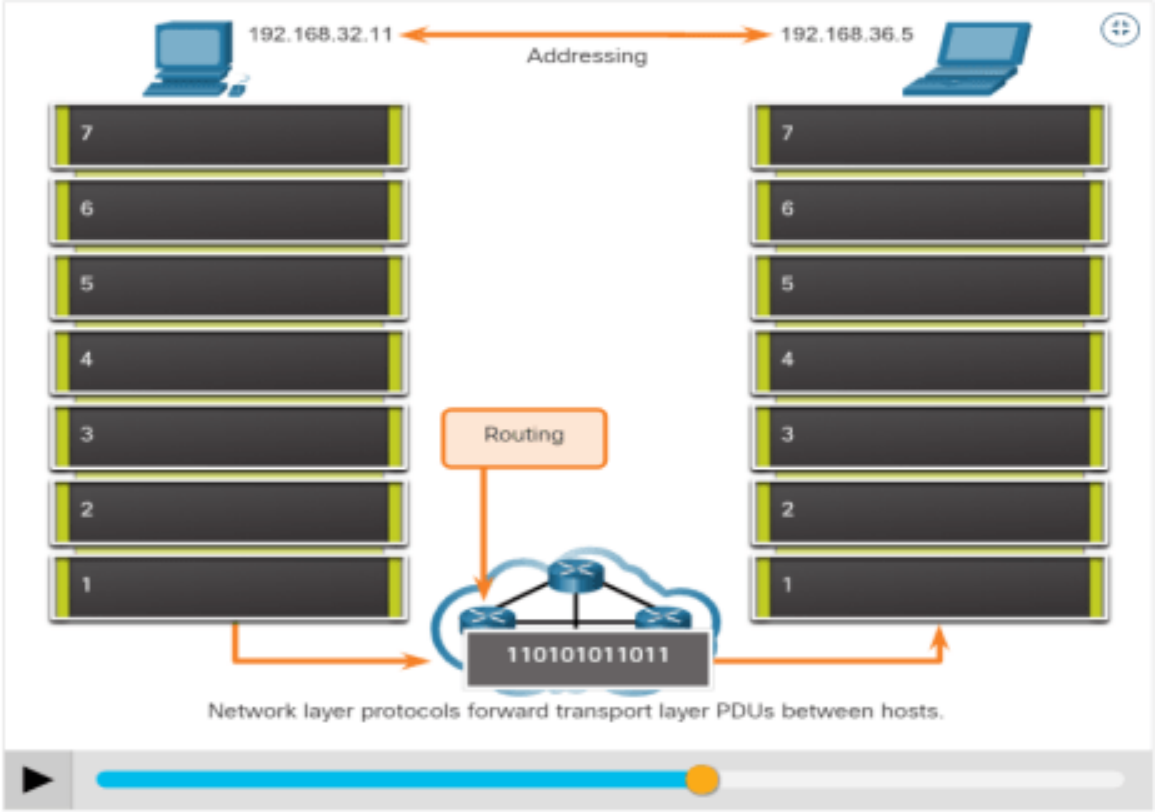
Ethernet et Protocole IP

6.2 IPv4

IPv4
6.2.1 Couche réseau

Opérations de base du protocole de couche réseau:

- **Adressage des terminaux** - Configurés avec une adresse IP unique pour l'identification sur le réseau
- **Encapsulation** - Encapsule l'unité de données de protocole (PDU) de la couche transport dans un paquet.
- **Routage** - Sélectionnez le meilleur chemin d'accès et dirigez les paquets vers l'hôte de destination.
- **De-encapsulation** - Effectué par l'hôte de destination du paquet IP.

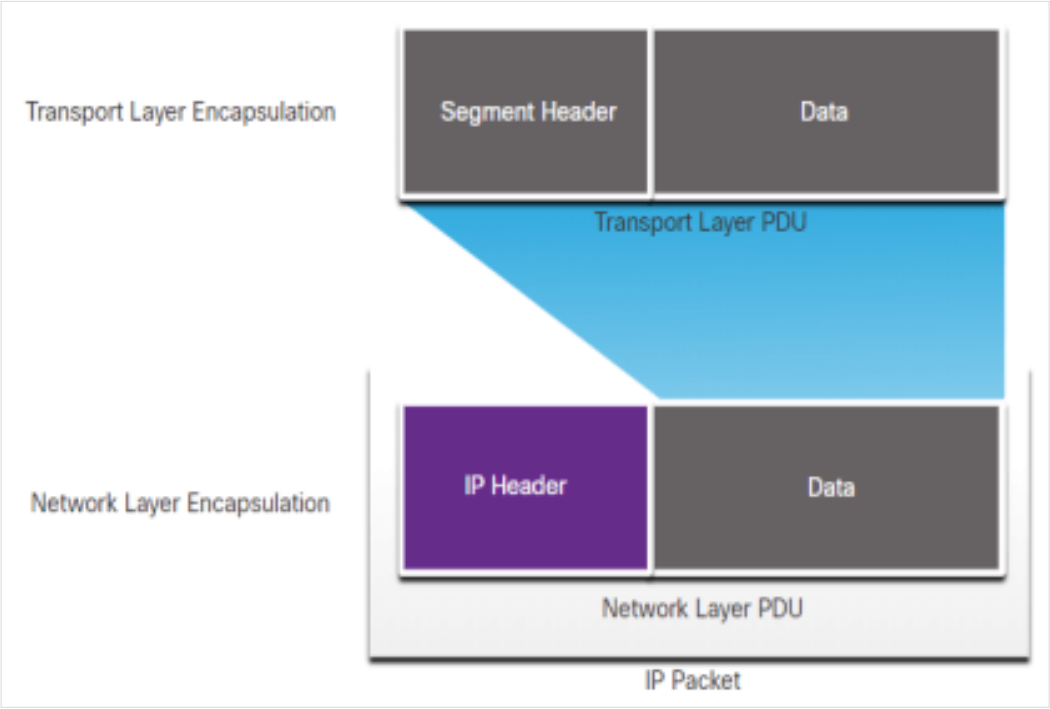


Résumé : IP **version 4** (IPv4) et IP **version 6** (IPv6) sont les principaux protocoles de communication de couche réseau. La couche réseau a 4 fonctions: **Adressage, Encapsulation, Routage, De-encapsulation**

IPv4

6.2.2 Encapsulation IP

- 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 **informations d'adressage IP** restent **les mêmes depuis le moment où le paquet quitte l'hôte source jusqu'à ce qu'il arrive à l'hôte de destination,** sauf lorsqu'elles sont traduites par le périphérique effectuant la traduction d'adresses réseau (NAT) pour IPv4.

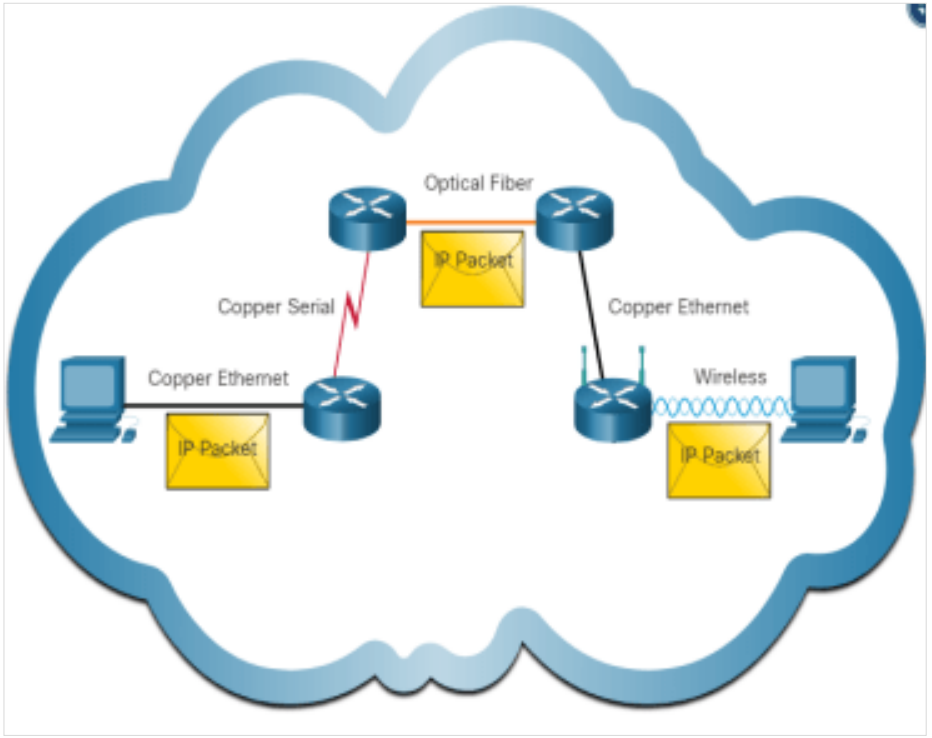


Résumé: Le **protocole IP** encapsule le **segment** de couche transport ou d'autres données en **ajoutant un en-tête IP**.

6.2.3 Caractéristiques du protocole IP

Les caractéristiques de base de l'IP**:**

- **Sans connexion** - Il n'y a pas de connexion avec la destination établie avant l'envoi des paquets de données.
- **Remise au mieux (Best effort)** - L'IP est intrinsèquement peu fiable car la livraison des paquets n'est pas garantie.
- **Indépendant vis-à-vis des supports** - L'opération est indépendante du support (par ex. cuivre, fibre optique ou sans fil) qui transporte les données.

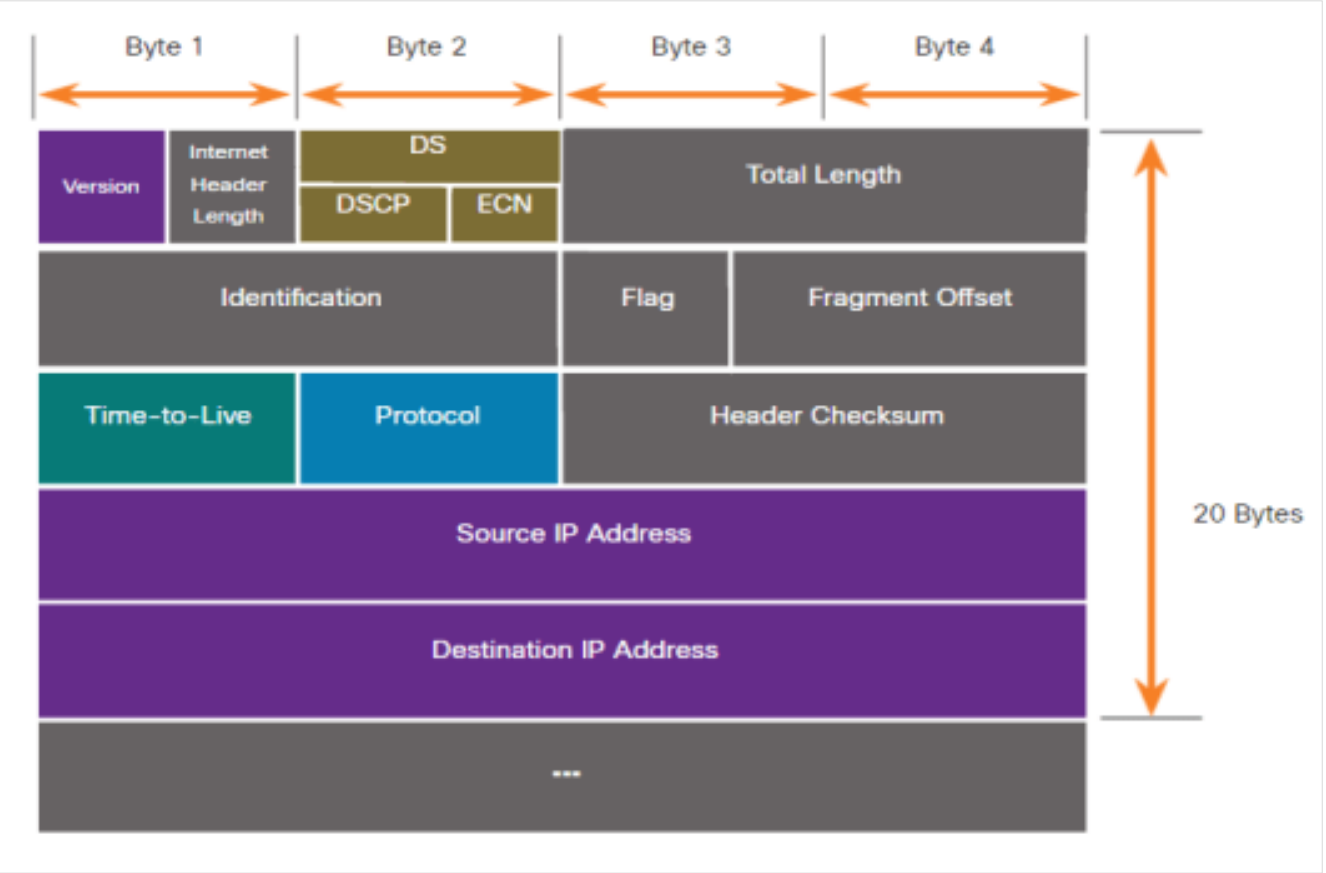


Résumé: IP a trois caractéristiques : **Sans connexion** , **Remise au mieux, Indépendant vis-à-vis des supports**

6.2.8 En-tête de paquet IPv4

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

- **Version**
- Services différenciés (ou DiffServ/DS)
- Somme de contrôle d'en-tête
- **Durée de vie** (Time to Live, TTL)
- Protocole
- **Adresse IPv4 source**
- **Adresse IPv4 de destination**



•**Résumé: L'en-tête de paquet IPv4** est utilisé pour **s'assurer que ce paquet est livré** à son prochain arrêt sur le chemin de son périphérique final de destination.

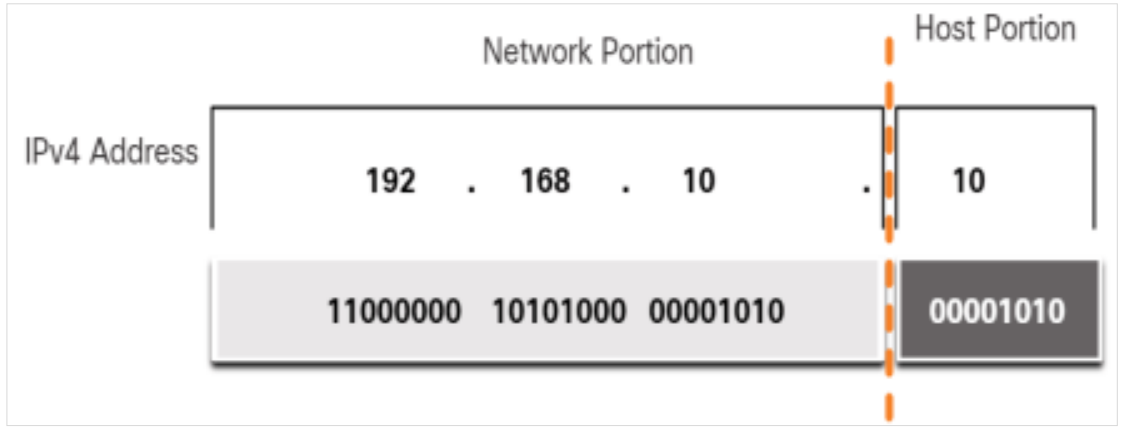
02

Ethernet et Protocole IP

6.3 Notions de base sur l'adressage IP

6.3.1 Parties réseau et hôte

- Les **bits** de la **partie réseau** de l'adresse doivent être **identiques** pour tous les périphériques installés sur le même réseau.
- Les **bits** de la **partie hôte** de l'adresse doivent être **uniques**, pour identifier un hôte spécifique dans un réseau.

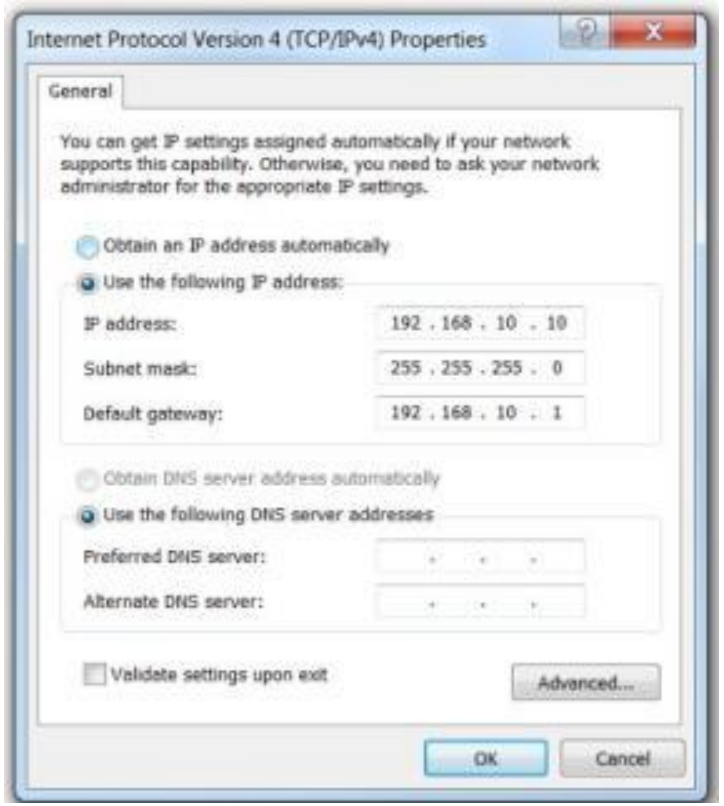


Résumé: Une **adresse IPv4** est une adresse hiérarchique de **32 bits** qui se compose d'une **partie réseau** et d'une **partie hôte**.

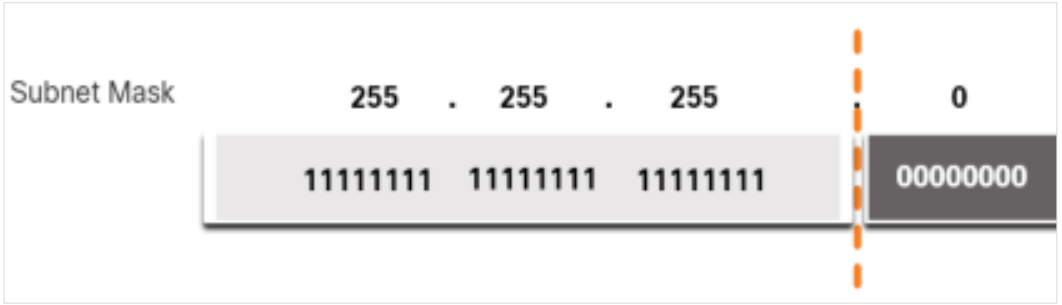
6.3.2 Masque de sous-réseau

Masque de sous-réseau

- Lorsqu'une **adresse IPv4** est attribuée à un appareil, le **masque de sous-réseau** est utilisé pour **déterminer l'adresse réseau de l'appareil**.
- La **masque de sous-réseau** est une séquence consécutive de **0 bits** suivie d'une séquence consécutive de **1 bits**.

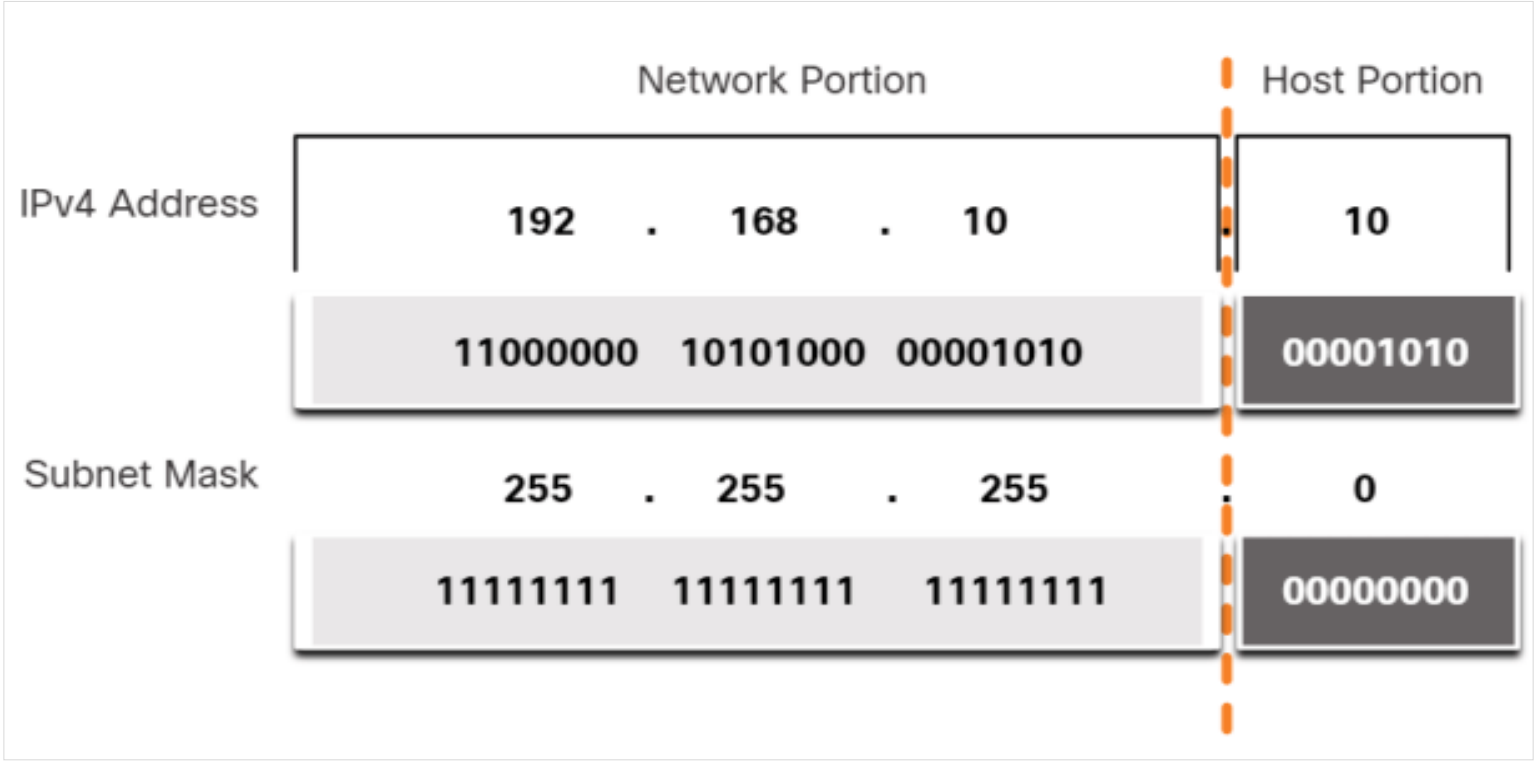


Remarque: *Une adresse IPv4 de **passerelle par défaut** est requise pour **atteindre les réseaux distants** et les adresses IPv4 du serveur DNS sont nécessaires pour traduire les noms de domaine en adresses IPv4.*



6.3.2 Masque de sous-réseau (suite)

- Le masque de sous-réseau **ne contient pas** réellement la partie réseau ou hôte d'une adresse IPv4.
- En réalité, le processus utilisé pour identifier la partie réseau et la partie hôte est appelé **l'opération AND.**



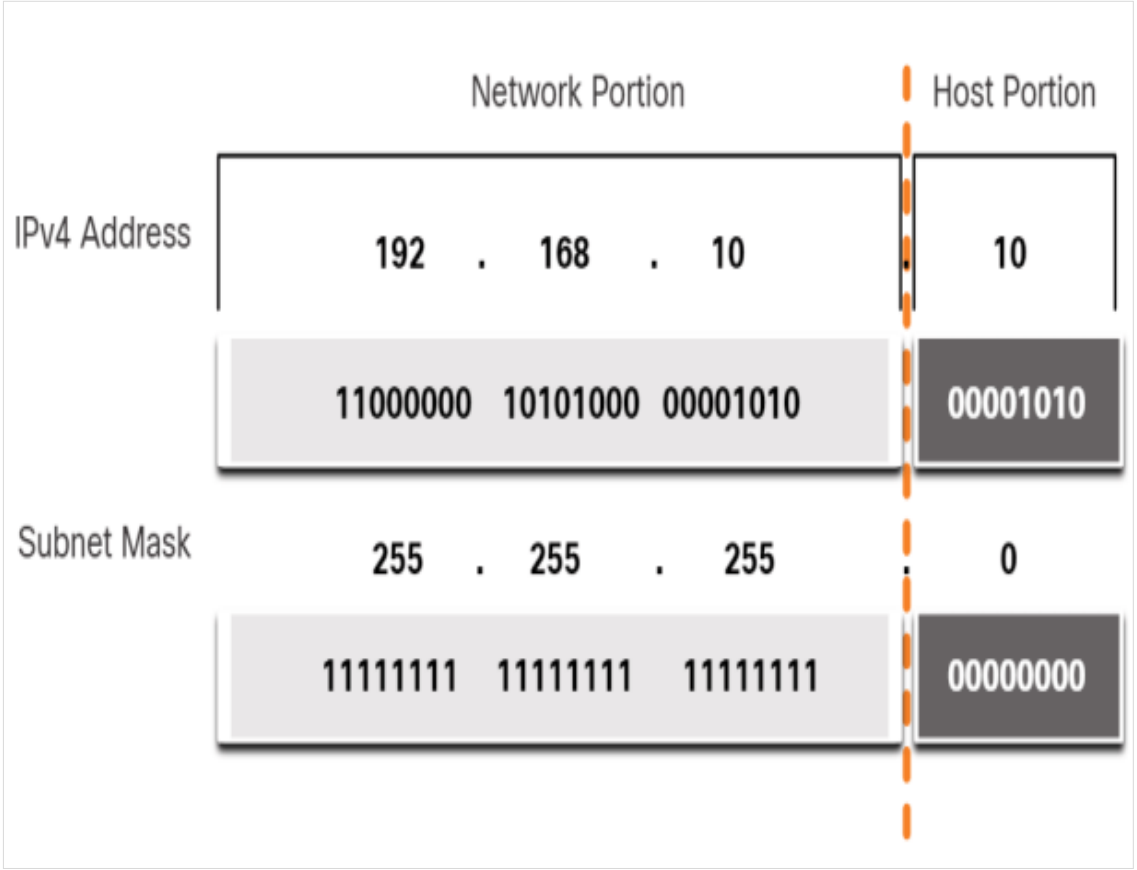
Associer une adresse IPv4 à son masque de sous-réseau

6.3.3 Longueur de préfixe

- Lorsque vous représentez une adresse IPv4 à l'aide d'une longueur de préfixe, l'adresse IPv4 est écrite suivie de la longueur du préfixe sans espace.

*Remarque: Une **adresse réseau** est également appelée **préfixe ou préfixe réseau.***

La longueur du préfixe est le nombre de bits mis à 1 dans le masque de sous-réseau.



Résumé: La **longueur du préfixe** est le **nombre de bits qui sont mis à 1** dans le masque de sous-réseau. Il est écrit en "**notation slash**", qui est notée par une barre oblique (**/**) suivie du n**ombre de bits mis à 1**

6.3.3 Longueur de préfixe (suite)

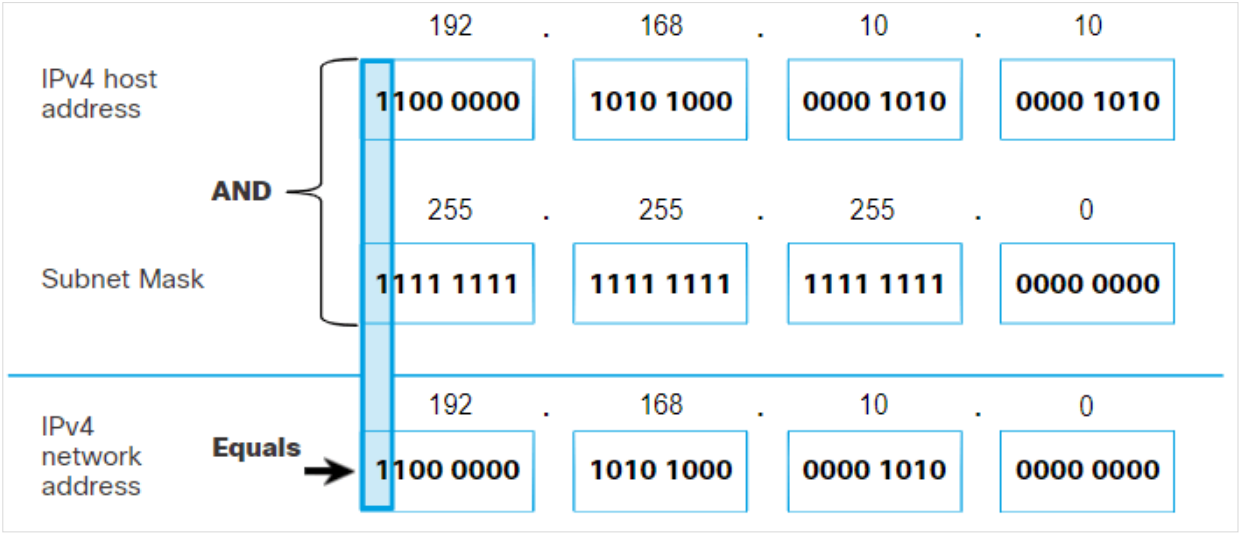
La **première colonne** contient la liste des **masques de sous-réseau** qui peuvent être utilisés avec une adresse d'hôte. La deuxième colonne indique l'adresse binaire 32 bits convertie. La dernière colonne affiche la longueur de préfixe obtenue.

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	11111111.111111.11111111.10000000	/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

6.3.4 - Déterminer le réseau: AND (ET)logique

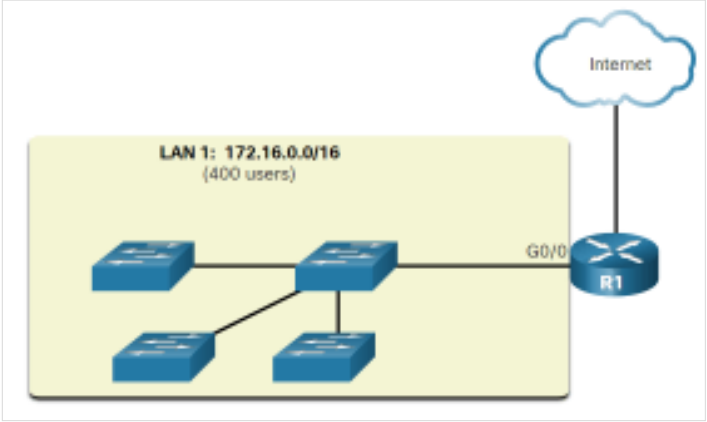
- Le **AND logique** est la comparaison de deux bits qui produisent les résultats indiqués ci-dessous.
  - 1 ET 1 = 1
  - 0 AND 1 = 0
  - 1 AND 0 = 0
  - 0 ET 0 = 0

Remarque: *Dans la logique numérique, **1** représente **Vrai** et **0** représente **Faux**. Lorsque vous utilisez une opération AND, les deux valeurs en entrée doivent avoir la valeur True (1) pour que le résultat soit True (1).*

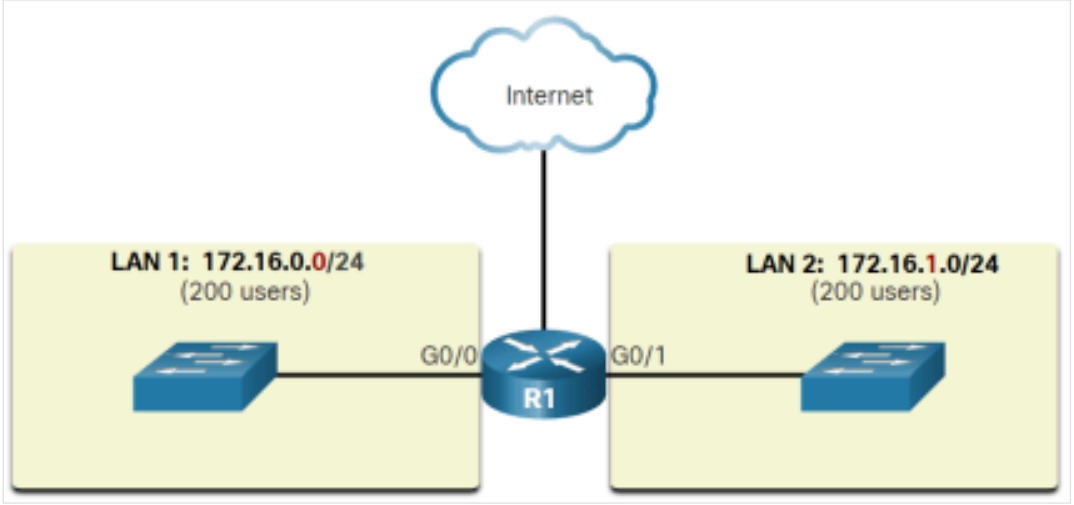


6.3.6 Création de sous-réseaux de domaines de diffusion

- Dans la figure, le réseau **LAN 1** connecte **400 utilisateurs** tous susceptibles de générer du **trafic de diffusion**, ce qui peut ralentir le fonctionnement du réseau et des appareils.
- La **segmentation en sous-réseaux** réduit le trafic global et améliore les performances réseau.



Un grand domaine de diffusion



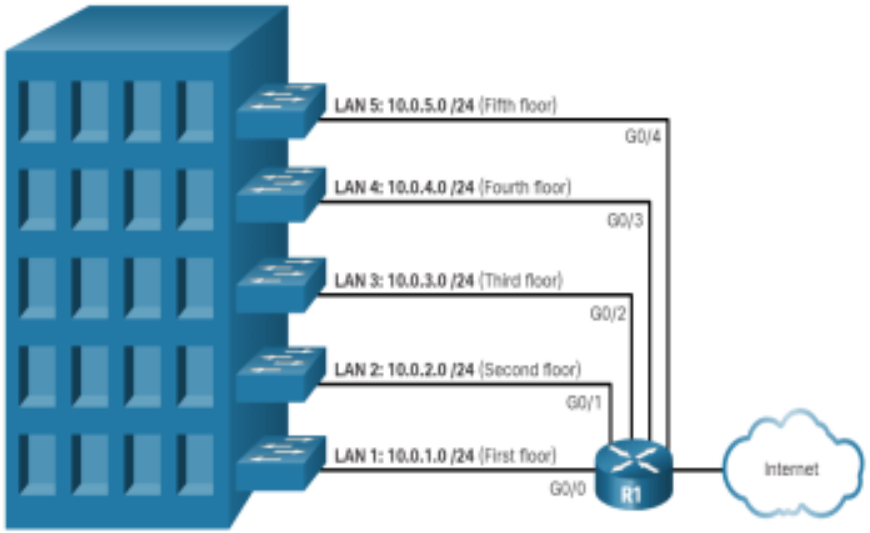
La communication entre les réseaux

Résumé: La **création de sous-réseaux** consiste à **réduire la taille du réseau** en créant de plus petits domaines de diffusion

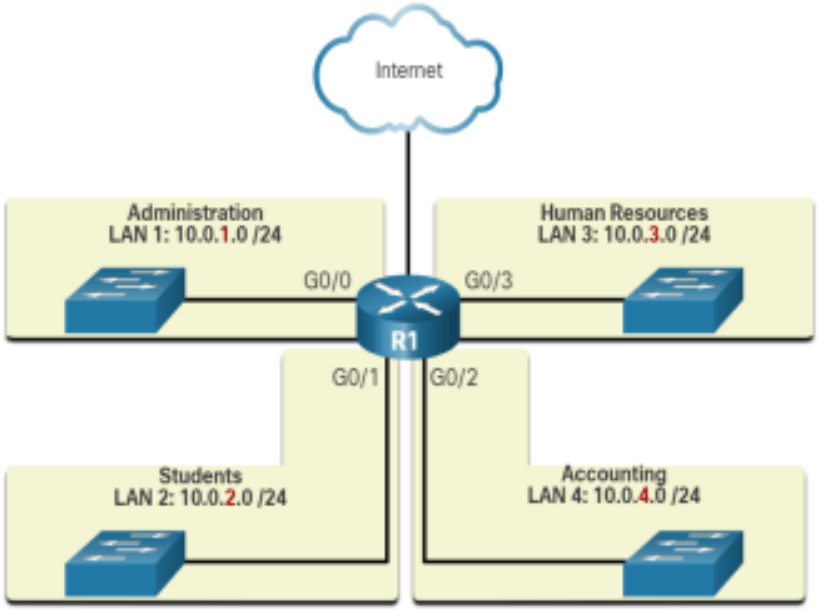
6.3.6 Création de sous-réseaux de domaines de diffusion (suite)

Les administrateurs du réseau peuvent **regrouper des périphériques** et des **services en sous-réseaux**, qui peuvent être définis selon divers facteurs.

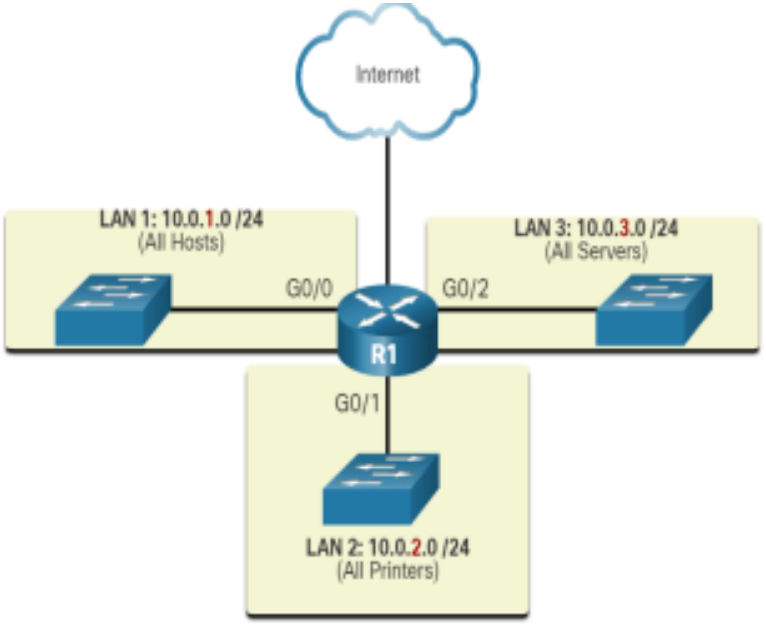
Emplacement



Par Département



Type de périphérique



02

Ethernet et Protocole IP

6.4 Les types d'adresses IPv4

Classes d'adresses IPv4 et masques de sous-réseau par défaut

Classes d'adresses

Les adresses IPv4 étaient basées sur les classes suivantes:

- **Classe A** (0.0.0.0/8 à 127.0.0.0/8) - Conçue pour prendre en charge des réseaux de très grande envergure avec plus de **16 millions d'adresses d'hôte**.
- **Classe B** (128.0.0.0 /16 à 191.255.0.0 /16) - Conçue pour répondre aux besoins des réseaux de moyenne à grande envergure avec jusqu'à **65000 adresses d'hôte environ**.
- **Classe C** (192.0.0.0 /24 à 223.255.255.0 /24) - Conçue pour prendre en charge des réseaux de petite taille avec un **maximum de 254 hôtes**.

Remarque: *Il existe également un bloc d'adresses de multidiffusion de* ***classe D*** *de* ***224****.0.0.0 à* ***239****.0.0.0 et un bloc d'adresses expérimentales de* ***classe E*** *de* ***240.****0.0.0 à* ***255****.0.0.0.*

Résumé: Les classes **A** (**0**.0.0.0/8 à **127**.0.0.0/8) **, B** (**128**.0.0.0 /16 à **191**.255.0.0 /16) et **C** (**192**.0.0.0 /24 à **223**.255.255.0 /24) sont les différentes plages d'adresses IP.

6.4.2 Adresses privées réservées

Adresses privées :

- 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 ne sont pas uniques** et peuvent être utilisées par n'importe quel réseau interne.

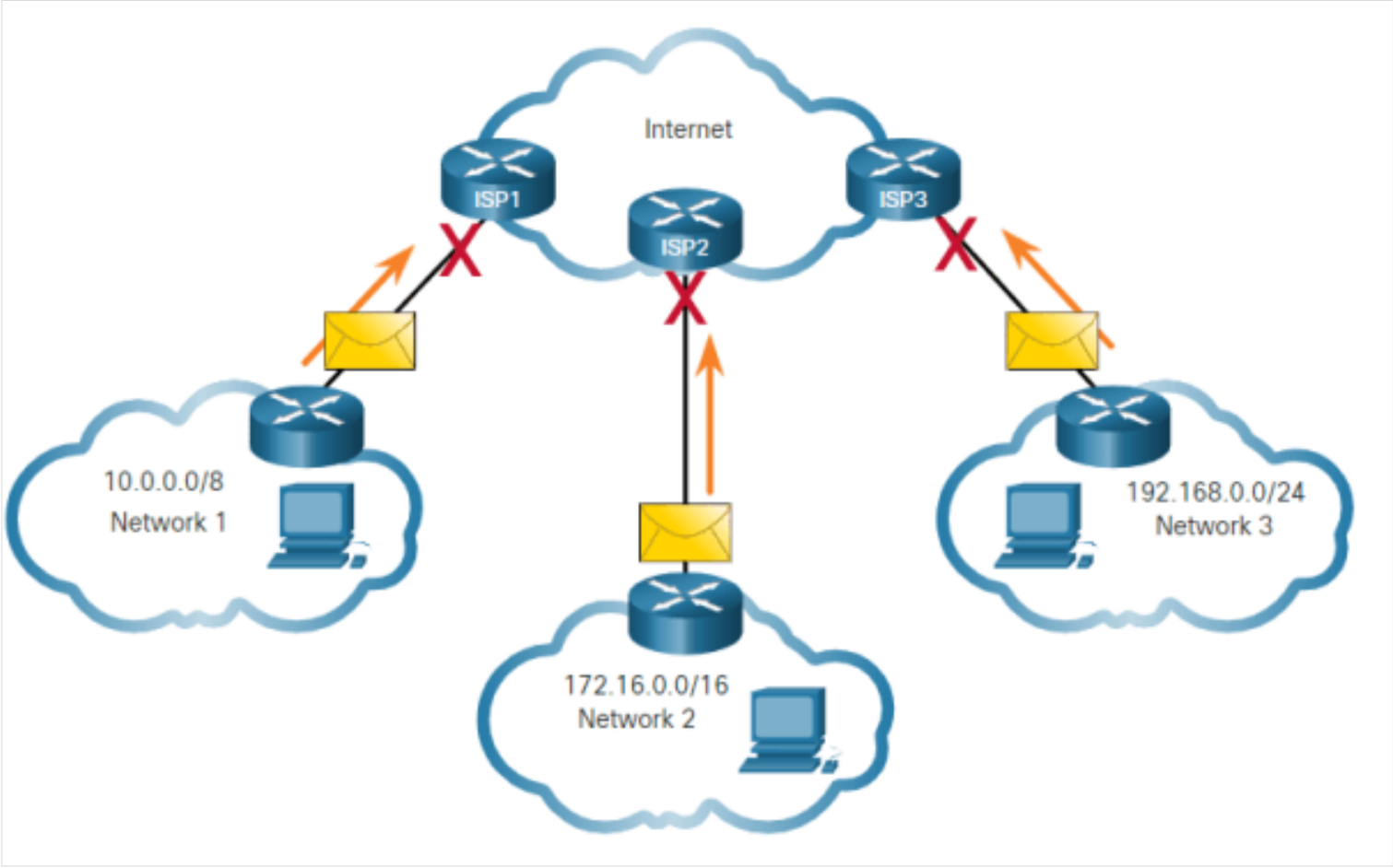
Les blocs d'adresses privées sont les suivants:

  - 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**

- Les adresses appartenant à ces blocs ne sont pas autorisées sur Internet et doivent être filtrées (rejetées) par les routeurs Internet.

6.4.2 Adresses privées réservées (suite)

- La plupart des entreprises utilisent des **adresses IPv4 privées** pour leurs hôtes internes.
- La traduction d'adresses réseau (**NAT**) est utilisée pour **convertir les adresses IPv4 privées en adresses IPv4 publiques**.



Les adresses privées ne sont pas routables sur Internet

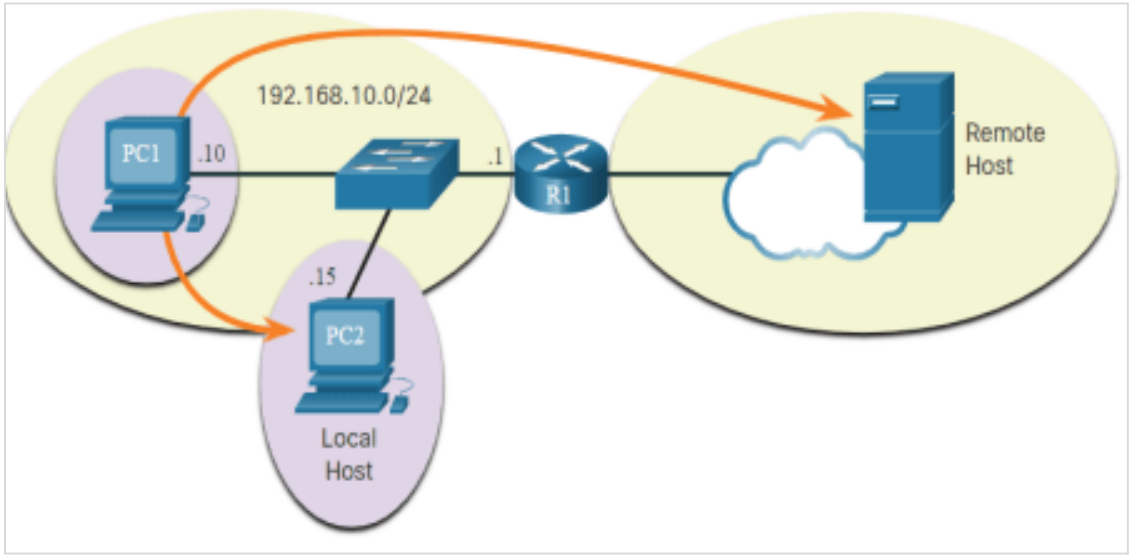
02

Ethernet et Protocole IP

6.5 La passerelle par défaut

6.5.1 Décisions relatives aux transmissions entre les hôtes

- La figure illustre la connexion PC1 à un hôte local sur le même réseau et à un hôte distant situé sur un autre réseau.
- Le dispositif terminal source détermine si un paquet est destiné à un hôte local ou à un hôte distant. La méthode de détermination varie selon la version IP:



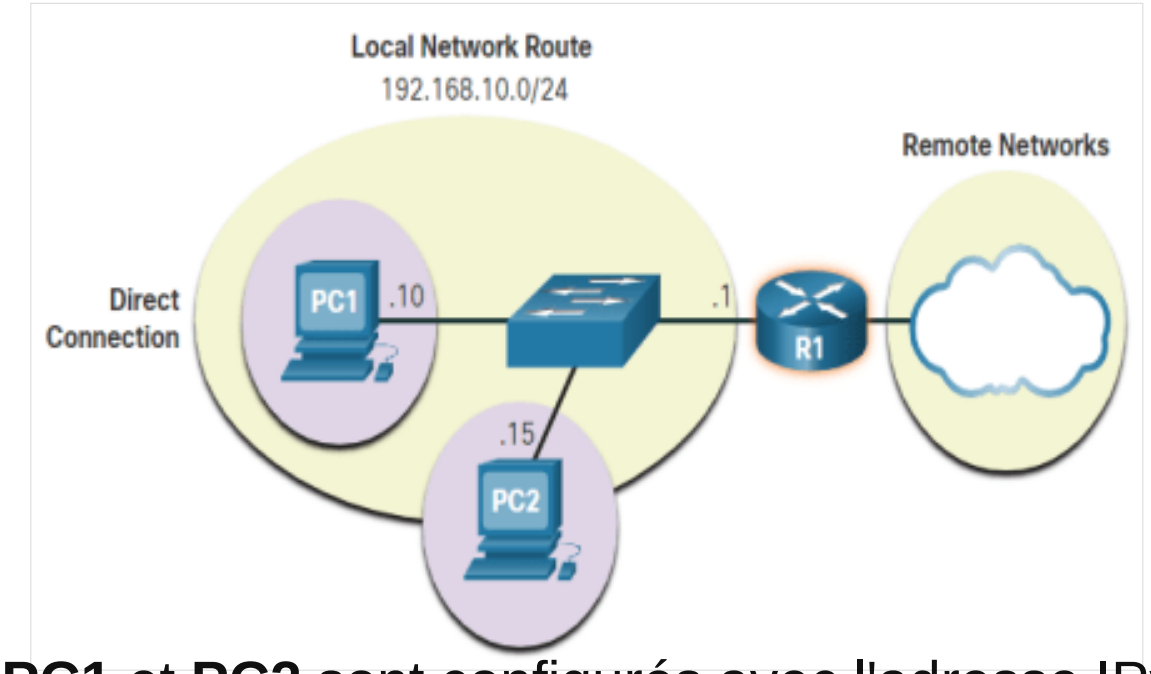
Résumé: Un autre rôle de la couche réseau est de **diriger les paquets entre les hôtes**. Un hôte peut envoyer un paquet à: **lui-même, à un autre hôte local**, et **à un hôte distant.**.

6.5.2 Passerelle par défaut

Sur un réseau, une passerelle par défaut est généralement un routeur avec les fonctionnalités suivantes:

- **Possède une adresse IP locale** située dans la même gamme d'adresses que les autres hôtes du réseau local.

- Le trafic ne peut pas être transféré en dehors du réseau local **s'il n'y a pas de passerelle par défaut**, si l'adresse de passerelle par défaut n'est pas configurée ou si la passerelle par défaut est en panne.



PC1 et **PC2** sont configurés avec l'adresse IPv4 **192.168.10.1** comme passerelle par défaut.

Résumé : La **passerelle par défaut** correspond au périphérique **réseau** **(routeur)** **capable d'acheminer le trafic vers d'autres réseaux**.

6.5.4 Tables de routage des hôtes

- La saisie de la commande **netstat -r** affiche trois sections relatives aux connexions réseau TCP/IP actuelles :
  - **Liste d'interfaces**
  - **Table de routage IPv4**
  - **Table de routage IPv6**

Remarque: *La sortie affiche uniquement la table de routage IPv4.*

```
C:\Users\PC1> netstat -r

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10      25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1     306
    192.168.10.0    255.255.255.0         On-link    192.168.10.10     281
   192.168.10.10  255.255.255.255         On-link    192.168.10.10     281
  192.168.10.255  255.255.255.255         On-link    192.168.10.10     281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1     306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10     281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1     306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10     281
```

Table de routage IPv4 pour PC1

- **Résumé**: Sur un hôte Windows, les commandes **route print** ou **netstat -r** permettent d'afficher la table de routage de l'hôte.

02

Ethernet et Protocole IP

6.6 IPv6

6.6.1 Nécessité du protocole IPv6

- L'IPv6 dispose d'un espace d'adressage plus large de **128 bits**, fournissant **340 undecillions** d'adresses possibles.
- La plupart des principaux FAI et fournisseurs de contenu tels que **YouTube, Facebook** et **NetFlix** ont également fait la transition.
- **Internet** est en passe de devenir un « **Internet des objets** ».

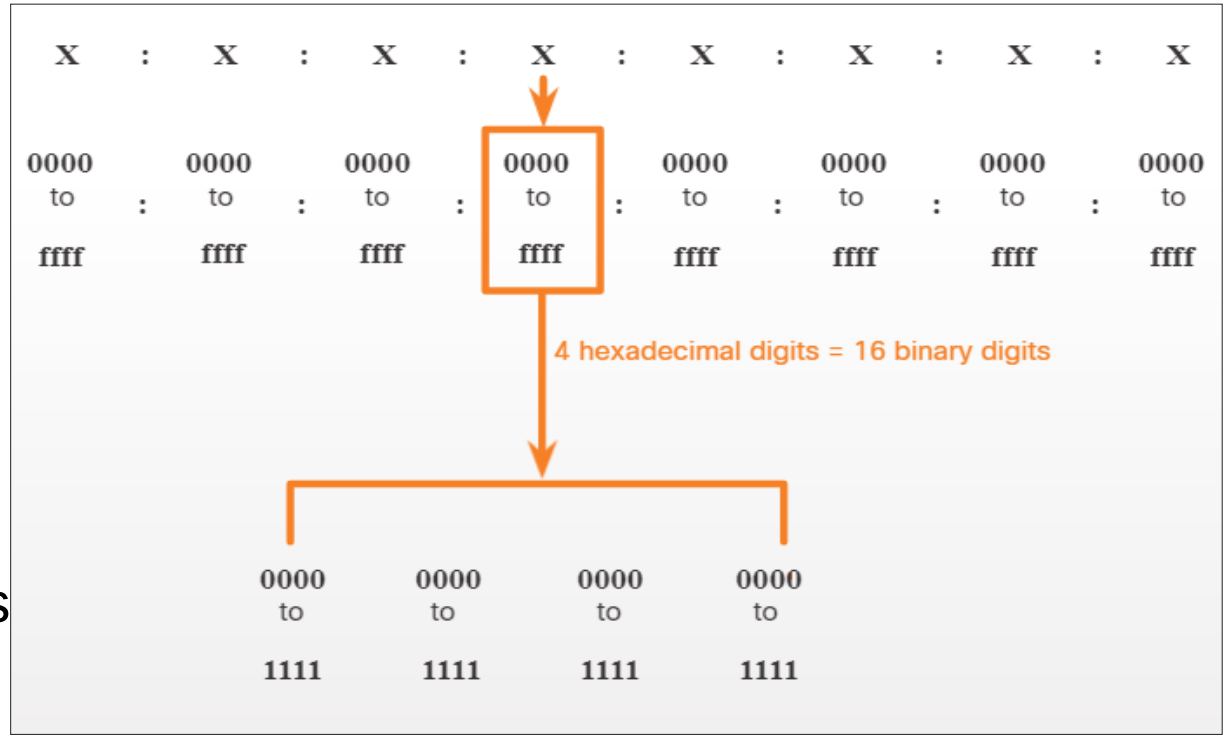
Dates d'épuisement des adresses IPv4 selon les RIR

Résumé : Le **manque d'espace d'adressage IPv4** a été le **facteur le plus décisif** pour la transition vers l'IPv6

6.6.2 Formats d'adresses IPv6

Format privilégié

- 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.
- Chaque «**x**» équivaut à un **hextet**, **16 bits**, ou à quatre caractères hexadécimaux.
- Les **adresses IPv6 ne sont pas sensibles** à la casse et peuvent être notées en minuscules ou en majuscules.




```
2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000: 0200
2001 : 0db8 : 0000 : 00a3 : abcd : 0000 : 0000: 1234
2001 : 0db8 : 000a : 0001 : c012 : 9aff : fe9a: 19ac
```

6.6.3 Règle n° 1 : omettre les zéros en début de segment

- **Règle 1:** Omettre tous les 0 (zéros) principaux dans n'importe quel hextet.
  - 01ab peut être représenté comme 1ab
- Cette règle s'applique uniquement aux **zéros de début de segment** et **NON aux zéros de fin**. L'omission de ces derniers rendrait l'adresse ambiguë. 01ab. Pour voir un exemple, reportez-vous au tableau ci-dessous.

Type	Format
Recommandé	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Sans zéros en début de segment	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200

6.6.4 Règle 2 - Double deux-points

Règle 2: Une suite de **double deux-points** (::) peut remplacer **toute chaîne unique et continue** d'un ou plusieurs segments de **16 bits** (hextets) comprenant uniquement des zéros.

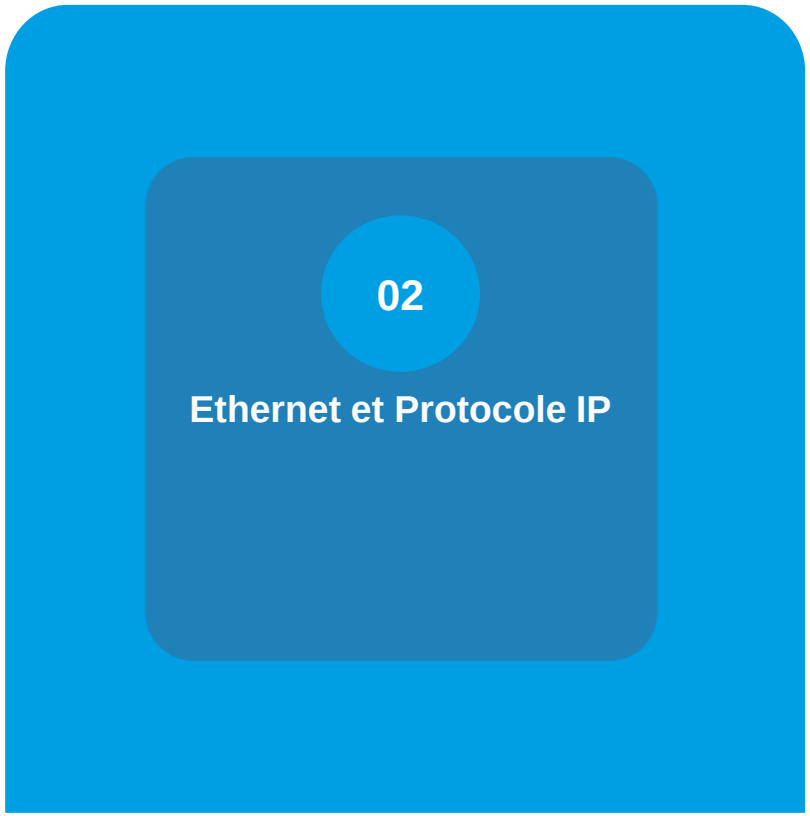
- **Exemple :** 2001:db8:cafe : 1:0:0:0:1 pourrait être représenté comme 2001:db8:cafe:1⁚⁚ 1.
- Le double deux-points (::) est utilisé à la place des trois hextets tout-0 (0:0:0).
- la suite de deux signes deux-points (::) ne peut être utilisée qu'une fois dans une adresse.
- **Voici un exemple d'utilisation incorrecte du double deux-points:** 2001:db8::abcd::1234.

Type	Format
Recommandé	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Compressés/Espaces	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200
Compressée	2001:db8:0:1111::200

6.6.5 Longueur de préfixe IPv6

- Le **préfixe** peut être **identifié par un masque de sous-réseau** en notation décimale à point ou une longueur de préfixe (notation de barre oblique).

- Comme pour IPv4, la **longueur du préfixe** est représentée en **notation slash** et est utilisée pour indiquer la partie réseau d'une adresse IPv6. Il peut aller de **0 à 128**.
- Il est fortement recommandé d'utiliser un **ID d'interface 64 bits** pour la plupart des réseaux.



6.7 Récapitulation d'Ethernet et des protocoles IP

6.7.1 Qu'ai-je appris dans ce module?

- Les réseaux LAN Ethernet et sans fil (**WLAN**) sont les deux technologies **LAN** les plus populaires. Il fonctionne sur les **couches physiques et de liaison de données** du modèle OSI et est défini dans les normes **IEEE 802.2 et 802.3**.
- **L'adresse MAC** peut être représentée à l'aide de **tirets, deux-points ou points** entre les groupes de chiffres.
- **IP version 4 (IPv4) et IP version 6 (IPv6)** sont les principaux protocoles de communication de couche réseau.
- Les **protocoles de couche réseau** effectuent quatre opérations de base telles que **l'adressage des périphériques finaux, l'encapsulation, le routage et la décapsulation**.
- Une **adresse IPv4** est une adresse hiérarchique de **32 bits** qui identifie un réseau et un hôte sur le réseau. Une adresse IPv6 est une adresse hiérarchique **128 bits.**
- La **longueur du préfixe** est le nombre de bits qui sont mis à **1** dans le masque de sous-réseau. Il est écrit en "notation slash", qui est notée par une barre oblique (/) suivie du nombre de bits mis à 1.

6.7.2 Qu'ai-je appris dans ce module?

- Le **processus** utilisé pour identifier la **partie réseau** et la **partie hôte** est appelé **l'opération AND**.
- Les **classes A, B et C** sont les différentes plages d'adresses IP.
- Le **routeur** qui est connecté au segment de réseau local constitue la **passerelle par défaut.**
- Sur un hôte Windows, les commandes **route print** ou **netstat -r** permettent d'afficher la table de routage de l'hôte.
- Deux **règles** permettent de **réduire le nombre de chiffres** qui sont requis pour représenter une adresse IPv6.
- La **longueur de préfixe** peut être comprise entre **0** et **128**.

Securité Réseau

Module 3

01 Protocoles réseau

02 Ethernet et Protocole IP

03 Vérification de la connectivité

04 Protocole ARP

05 La couche de transport

06 Services réseau

07

08 Lap pratiques

Objectifs du module

Titre du Module: Vérification de la connectivité

Objectif du module: Utiliser les outils de vérification de la connectivité ICMP

Titre du Rubrique	Objectif du Rubrique
ICMP	Expliquer comment le protocole ICMP sert à tester la connectivité du réseau.
Utilitaires ping et Traceroute	Utiliser les outils Windows, ping et Traceroute pour vérifier la connectivité du réseau.

03

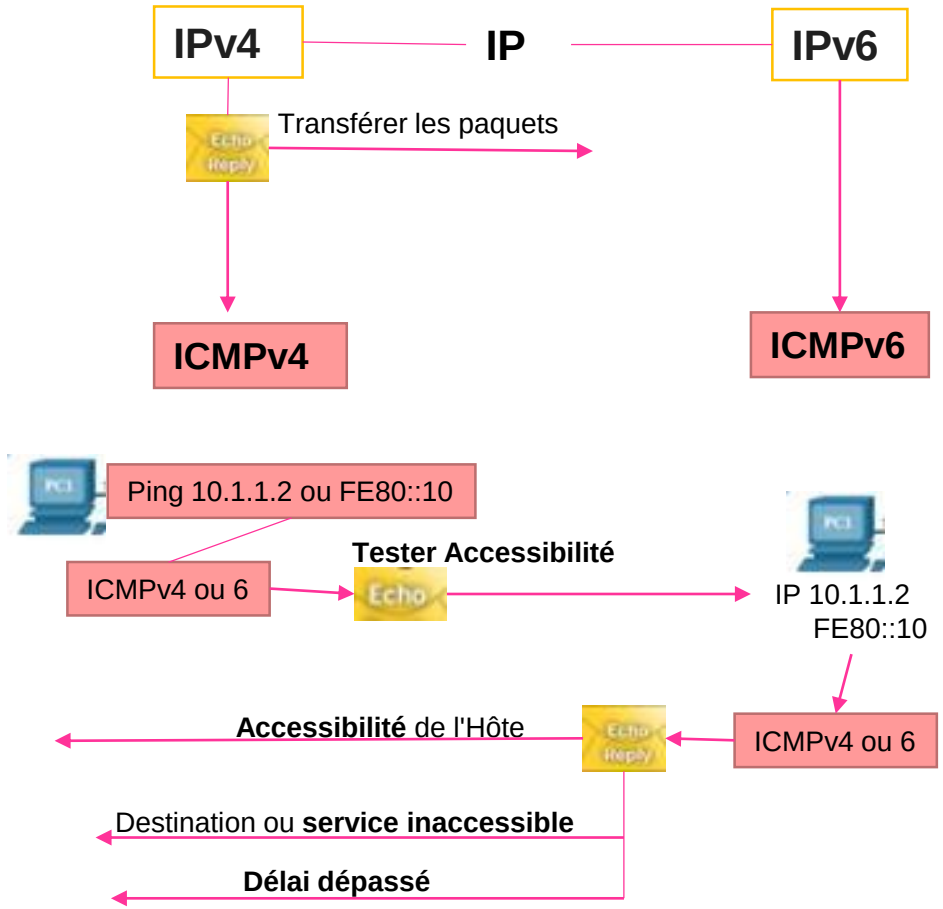
Vérification de la connectivité

7.1 ICMP

Vérification de la connectivité.

7.1.1 Messages ICMPv4

- Le **protocole ICMP** est disponible pour **IPv4** et **IPv6**. ICMPv4 est le protocole de message des réseaux IPv4. ICMPv6 fournit les mêmes services pour l'IPv6, mais offre des fonctionnalités supplémentaires.
- Les messages ICMP communs à ICMPv4 et ICMPv6 incluent la **confirmation de l'hôte**, **la destination** ou **le service inaccessible**, **la durée dépassée** et la **redirection** de la route.

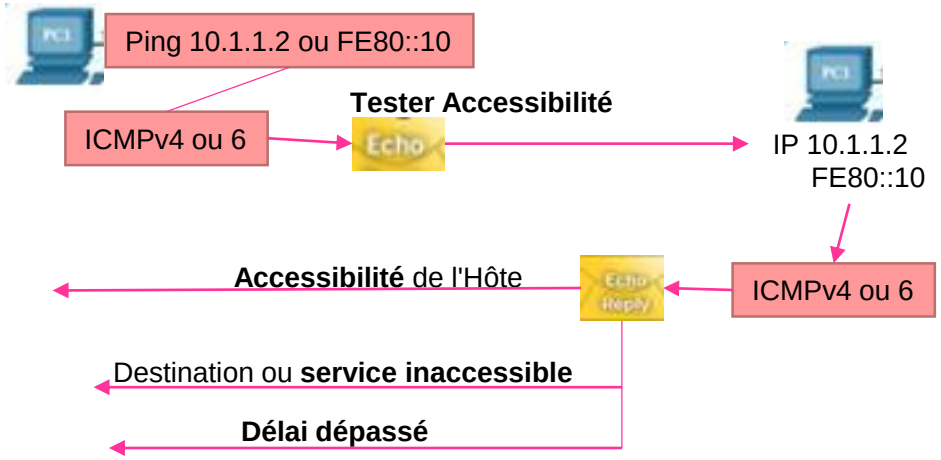


Résumé : Les messages **ICMP (IPv4 ou IPv6)** ont pour **objectif** de **fournir des commentaires** sur les problèmes liés au traitement de paquets IP dans certaines circonstances.

7.1.1 Messages ICMPv4 (Suite)

Host Confirmation (Confirmation de l’hôte)

- L’hôte local envoie un message ICMP **Echo Request** (Demande d’écho) à un autre hôte. Si l'hôte est disponible, l'hôte de destination répond en envoyant une **réponse d'écho**.



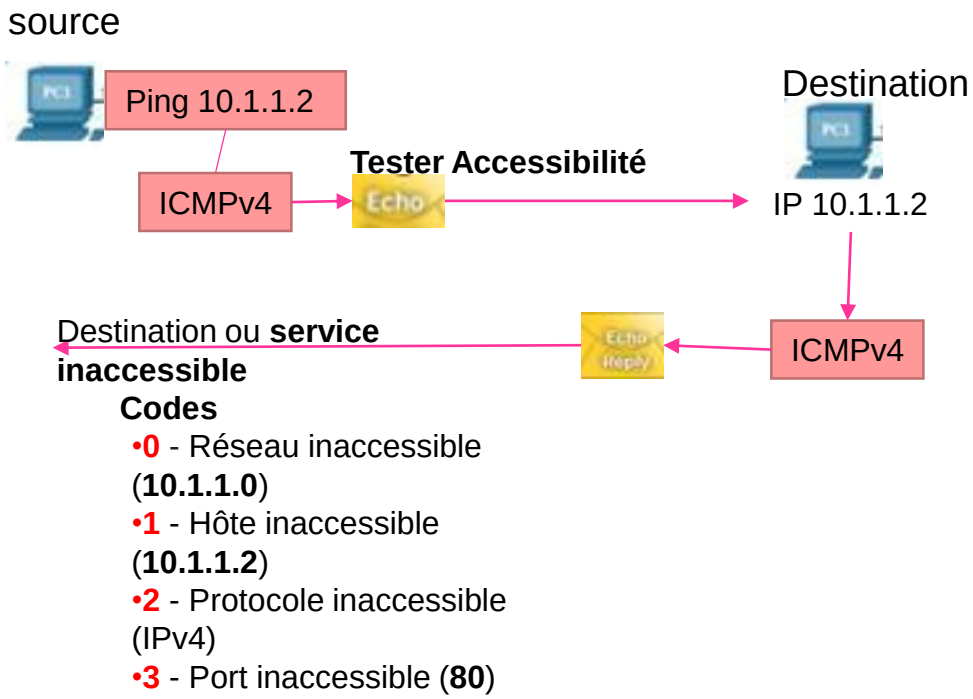
Résumé : Un message **ICMP Echo** (Écho ICMP) permet de **déterminer si un hôte est fonctionnel**.

7.1.1 Messages ICMPv4 (Suite)

Ce message comprend un **code indiquant pourquoi** le paquet n'a pas pu être livré.

Certains des codes de Destination Inaccessible pour l'ICMPv4 sont:

- **0** - Réseau inaccessible
- **1** - Hôte inaccessible
- **2** - Protocole inaccessible
- **3** - Port inaccessible

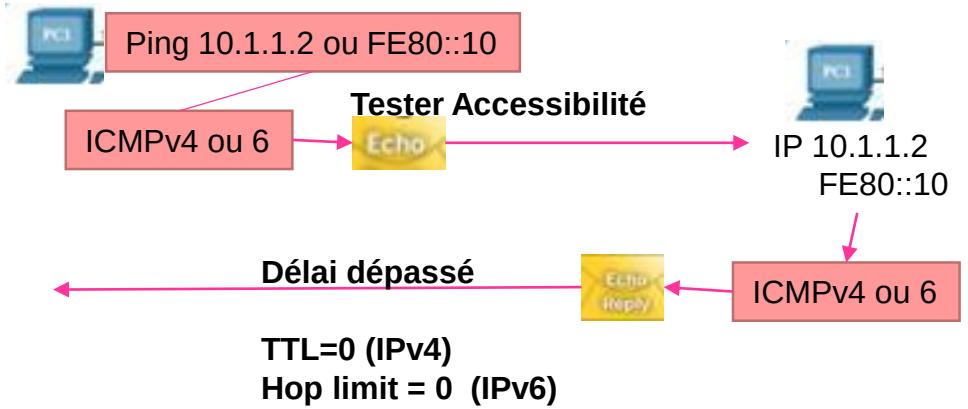


Résumé : Un **message ICMP Destination Inaccessible** peut être utilisé pour avertir la source qu'une destination ou un **service est inaccessible**.

7.1.1 Messages ICMPv4 (Suite)

Dépassement du délai

- Si un routeur reçoit un paquet et **décrémente le champ TTL de durée de vie du paquet IPv4 jusqu'à atteindre zéro**, il abandonne le paquet et envoie un message de dépassement de délai à l'hôte source.
- Si le routeur ne peut pas transmettre un paquet IPv6 parce que celui-ci a **expiré,** le protocole ICMPv6 envoie également un message de dépassement de délai.
- **IPv6** n'a pas de champ TTL. Il utilise le champ "**Hop Limit**" pour déterminer si le paquet a expiré.

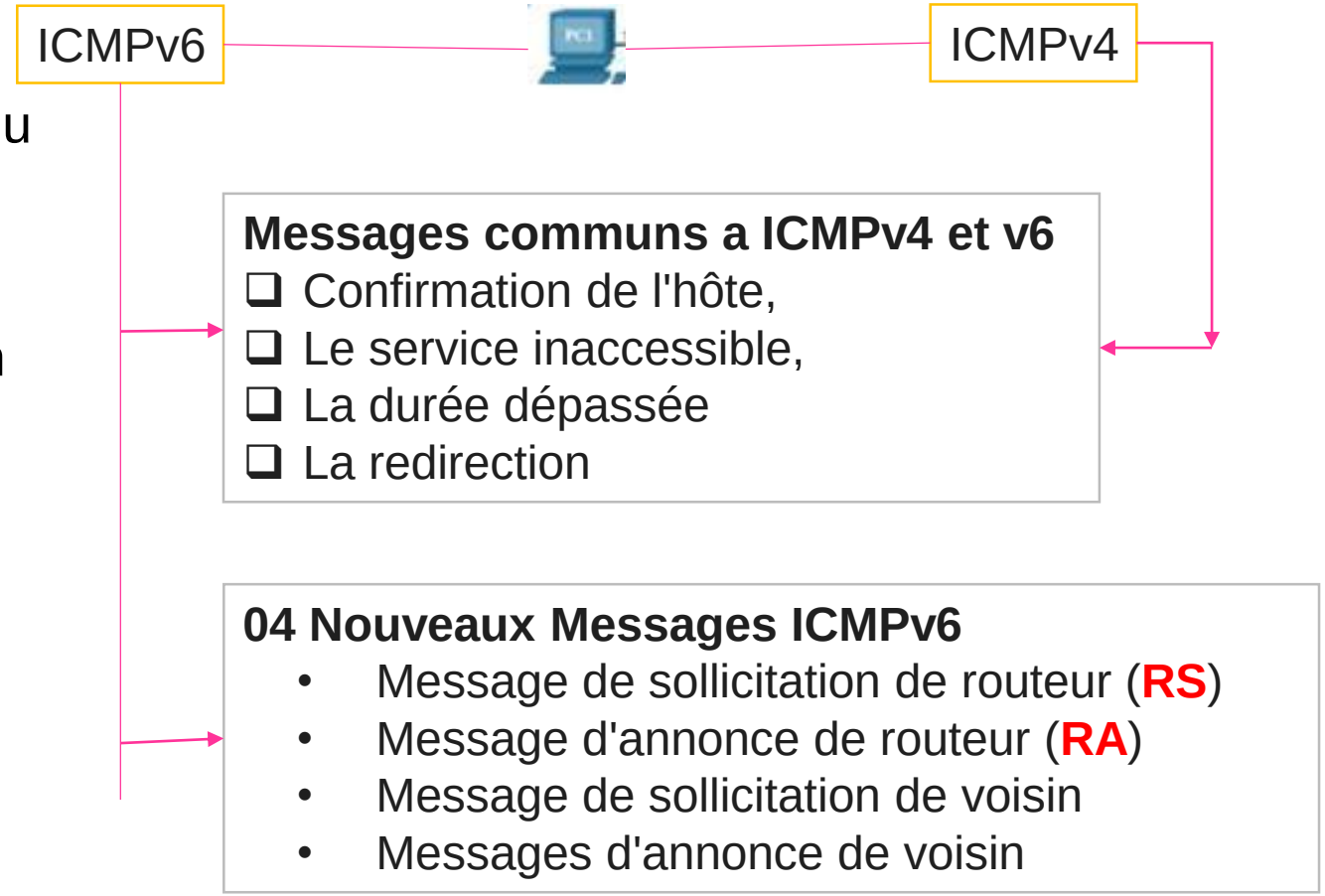



```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Résumé : 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**.

7.1.2 Messages RS et RA ICMPv6

- **Quatre nouveaux protocoles** dans le cadre du protocole Neighbor Discovery Protocol (**ND** ou **NDP**):
- Messages envoyés entre un routeur IPv6 et un périphérique IPv6 :
  - Message de **sollicitation de routeur (RS)**
  - Message **d'annonce de routeur** (**RA**)
- Messages envoyés entre des **périphériques IPv6** :
  - Message de **sollicitation de voisin**
  - Messages **d'annonce de voisin**



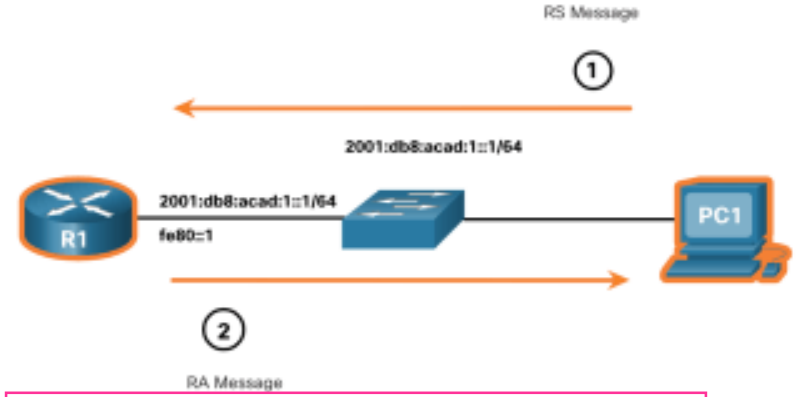
7.1.2 Messages RS et RA ICMPv6 (suite)

Sollicitation de routeur: Messagerie entre un routeur IPv6 et un périphérique IPv6

- Les messages **d'annonce de routeur** sont envoyés par **les routeurs** pour **fournir les informations d'adressage** aux hôtes via **la configuration SLAAC**.
- Un **routeur** envoie un message d'annonce de routeur régulièrement ou en **réponse à un message de sollicitation**. Un hôte utilisant la SLAAC utilise **l'adresse link-local** du routeur qui a envoyé le message d'annonce de routeur en tant que **passerelle par défaut.**

messages RS (ICMPv6)

«**Salut, je viens de démarrer. Existe-t-il un routeur IPv6 sur le réseau?** J'ai besoin de savoir comment obtenir les informations de mon adresse IPv6 dynamiquement.»



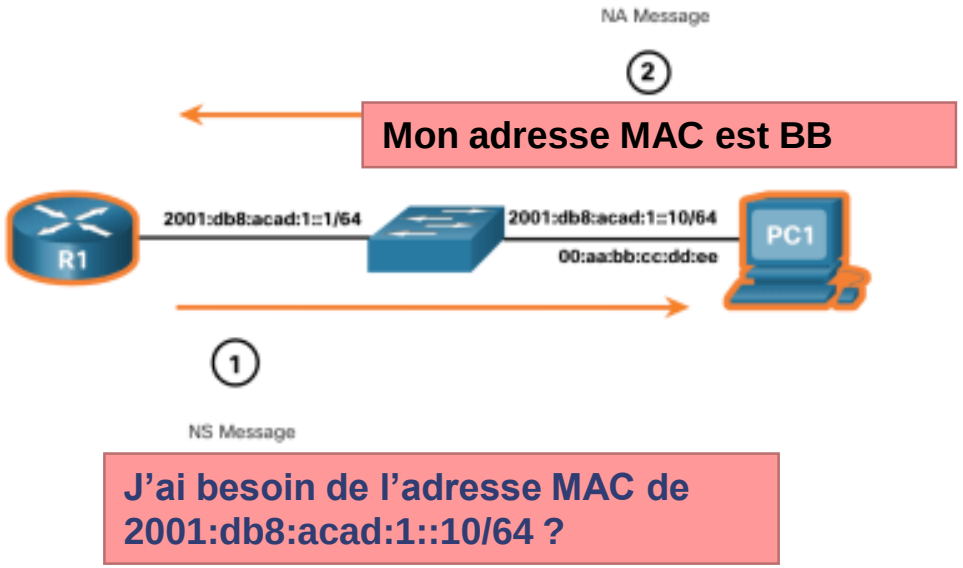
messages RA (ICMPv6)

. «**Salut à tous les appareils compatibles IPv6 »**
Je suis R1 et vous pouvez utiliser SLAAC pour créer une adresse de monodiffusion globale IPv6. Le préfixe est **2001:db8:acad:1::/64** utilisez mon adresse **locale fe80::1** comme **passerelle par défaut**

7.1.2 Messages RS et RA ICMPv6 (suite)

Résolution d'adresse: Messagerie entre périphériques IPv6

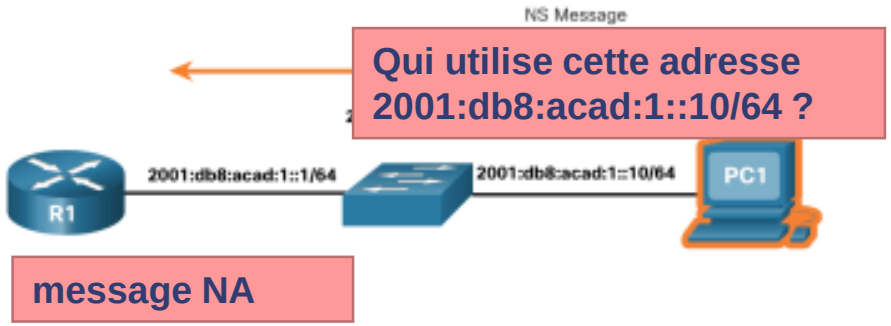
- Les **messages d'annonce de voisin** sont envoyés lorsqu'un appareil **connaît l'adresse IPv6** d'un terminal, **mais pas son adresse MAC.** Le principe est comparable à une requête ARP pour IPv4.



7.1.2 Messages RS et RA ICMPv6 (suite)

Détection des adresses dupliquées (DAD)

- Pour vérifier l'unicité d'une adresse, l'appareil enverra un **message NS** avec **sa propre adresse IPv6.**
- Si un autre appareil sur le réseau possède cette adresse, il **répondra par un message NA notifiant à l'appareil émetteur que l'adresse est utilisée**. Si aucun message d'annonce de voisin n'a été renvoyé au bout d'un certain temps, **l'adresse de monodiffusion est unique** et peut être utilisée.



7.2 Utilitaires ping et Traceroute

7.2.2 Ping - Tester la connectivité

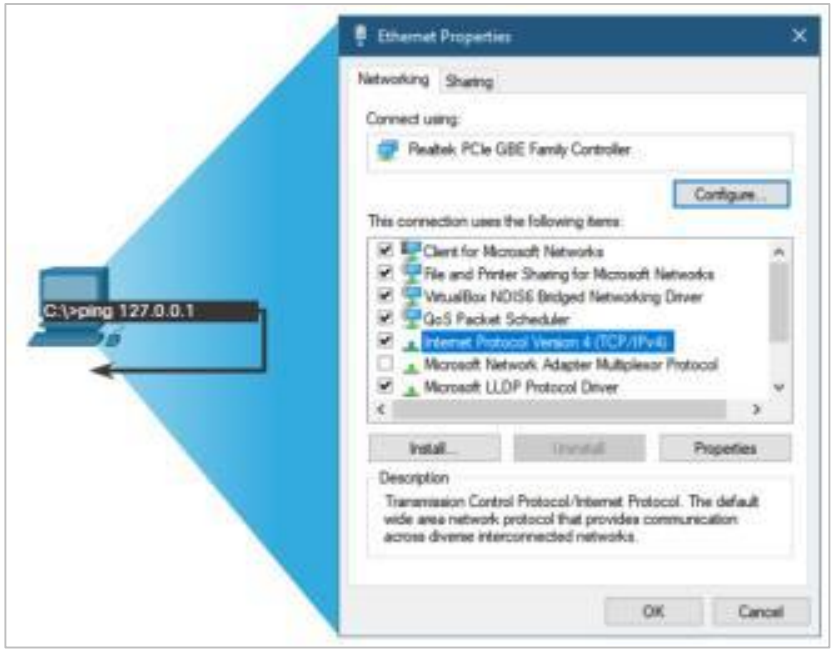
- Une fois **toutes les requêtes envoyées**, l'utilitaire **ping** affiche un résumé qui inclut le **taux de réussite** et la **durée de transmission moyenne** à destination.
- Les **types de tests de connectivité** effectués avec **ping** sont les suivants :
  - Envoi d'une requête ping sur **le bouclage local**
  - Testez la **passerelle par défaut** à l'aide d'une requête ping.
  - Envoi d'une requête ping à un **hôte distant**

```
C:\Users\JOSEPH>ping google.com

Envoi d'une requête 'ping' sur google.com [142.250.187.238] avec 32 octets de données :
Réponse de 142.250.187.238 : octets=32 temps=145 ms TTL=110
Réponse de 142.250.187.238 : octets=32 temps=162 ms TTL=110
Réponse de 142.250.187.238 : octets=32 temps=147 ms TTL=110
Réponse de 142.250.187.238 : octets=32 temps=153 ms TTL=110

Statistiques Ping pour 142.250.187.238:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 145ms, Maximum = 162ms, Moyenne = 151ms

C:\Users\JOSEPH>
```

Résumé: La commande **ping** est un **utilitaire de test** qui utilise des messages de **requête et de réponse d'écho ICMP** pour tester la connectivité entre les hôtes.

7.2.1 Testez le bouclage à l'aide d'une requête ping

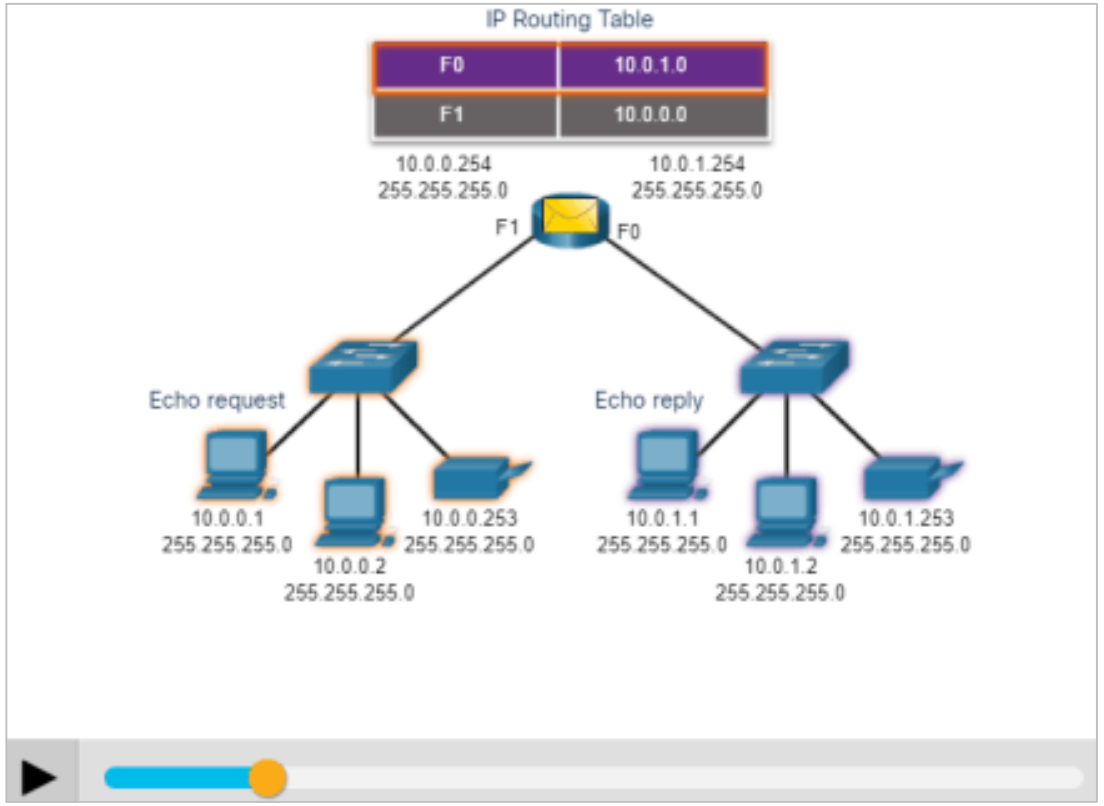
- Ping peut être utilisé pour tester la configuration interne d'IPv4 ou IPv6 sur l'hôte local.



- Pour réaliser ce test, nous exécutons la commande **ping** sur l'adresse de bouclage locale **127.0.0.1** pour l'IPv4 (et **::1** pour l'IPv6).
- Elle teste uniquement la configuration IP via la couche réseau du protocole IP.
- Si un message **d'erreur est généré**, cela indique que la suite **TCP/IP ne fonctionne pas sur l'hôte**.

7.2.5 Ping un hôte distant

- L'hôte local peut envoyer une requête ping à un **hôte IPv4** opérationnel sur un **réseau distant**.
- Le routeur utilise sa table de routage IP pour transférer les paquets.



7.2.6 Traceroute - Tester le chemin

Durée de transmission ou RTT (Round Trip Time)

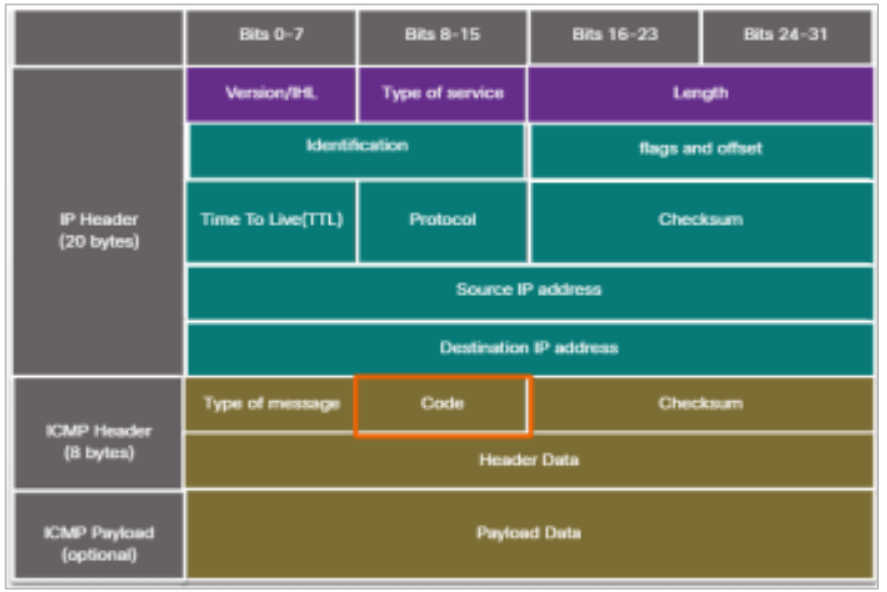
- Traceroute fournit un **temps d'aller-retour** pour **chaque saut** le long du chemin et indique si un saut ne répond pas.
- Le **temps aller-retour** est le temps que prend un paquet pour atteindre l'hôte distant et pour que la réponse de l'hôte revienne.
- Un astérisque (*) indique un paquet perdu ou sans réponse.

```
C:\Users\JOSEPH>tracert www.cisco.com

Détermination de l'itinéraire vers e2867.dsca.akamaiedge.net [23.216.97.48]
avec un maximum de 30 sauts :

  1    1 ms    1 ms    1 ms  192.168.1.1
  2  128 ms   51 ms  213 ms  10.0.0.254
  3   25 ms   34 ms   30 ms  10.18.34.1
  4   43 ms   28 ms   30 ms  10.18.34.28
  5   27 ms   27 ms   33 ms  10.18.34.33
  6   22 ms   17 ms   24 ms  10.22.34.156
  7  119 ms  121 ms  122 ms  ben109-129-ca126-1-2mse.iam.net.ma [81.192.254.41]
  8  155 ms  142 ms  132 ms  193.251.144.111
  9    *       *       *    Délai d'attente de la demande dépassé.
 10    *       *       *    Délai d'attente de la demande dépassé.
 11  142 ms  146 ms  130 ms  a23-216-97-48.deploy.static.akamaitechnologies.com [23.216.97.48]

Itinéraire déterminé.
```

Résumé: Traceroute (**tracert**) est un utilitaire qui **génère la liste des tronçons empruntés** sur le chemin. Cette liste peut fournir d'importantes informations pour la vérification et le dépannage.

7.2.7 Format de paquet ICMP

- **ICMP** est directement **encapsulé** sous la forme de **paquets IP**.
- ICMP utilise des **codes de message** pour différencier les différents types de messages ICMP.
- Voici quelques exemples de codes de message courants :
  - **0 -** Réponse d'écho (réponse à une commande ping)
  - **3 -** Destination inaccessible
  - **5 -** Redirection (utilisation d'une autre route pour atteindre la destination)
  - **8 -** Demande d'écho (dans le cadre d'une commande ping)
  - **11 -** Délai dépassé (la valeur TTL est égale à 0)



Utilitaires Ping et Traceroute

7.2.8 Packet Tracer - Vérifier l'adressage IPv4 et IPv6

Dans ce Packet Tracer, vous ferez ce qui suit:

- Vérifier la configuration des adresses IPv6 et IPv4.
- Test de la connectivité avec tracert et ping.

7.3 Récapitulation de vérification de la connectivité

Récapitulation de vérification de la connectivité

7.3.1 Qu'est-ce que j'ai appris dans ce module?

- La **suite TCP/IP** envoie des **messages ICMP** lorsque des **paquets IP rencontrent des problèmes** de transfert.
- **ICMPv4** est le protocole de messagerie pour **IPv4, tandis qu'ICMPv6** fournit ces mêmes services pour IPv6 et comprend des **fonctionnalités supplémentaires**.
- Les messages **ICMP communs à ICMPv4 et ICMPv6** incluent la confirmation de l'hôte, la destination ou le service inaccessible, la durée dépassée et la redirection de la route.
- **ICMPv6** inclut les **quatre messages ICMPv6** supplémentaires pour le Neighbor Discovery Protocol (**NDP**).
- Ces messages sont des messages de sollicitation de routeur (**RS**) et de publicité de routeur (**RA**) envoyés entre les routeurs IPv6 et les hôtes IPv6, ainsi que des messages de sollicitation de voisin (**NS**) et de publicité de voisin (**NA**) qui sont envoyés entre les périphériques IPv6.

7.3.2 Qu'est-ce que j'ai appris dans ce module? (suite)

- La commande ping est un **utilitaire de test** qui utilise des messages de requête et de réponse d'écho ICMP pour tester la connectivité entre les hôtes.
- Parmi les types de tests de connectivité effectués avec ping, mentionnons l'exécution de **ping de la boucle locale**, l'exécution de **ping de la passerelle par défaut** et l'exécution de **ping d'un hôte distant**.
- Traceroute (tracert) est un **utilitaire qui génère la liste des tronçons empruntés** sur un chemin.
- La commande **traceroute** utilise une fonction du **champ TTL** du protocole IPv4 et le champ de **limite de nombre de tronçons** du protocole IPv6 dans les en-têtes de couche 3, ainsi que le message ICMP de dépassement de délai.
- **ICMP** est directement encapsulé sous la **forme de paquets IP** comme charge utile de données. La charge utile des données ICMP contient des champs de données d'en-tête spéciaux.

Securité Réseau

Module 3

01 Protocoles réseau

02 Ethernet et Protocole IP

03 Vérification de la connectivité

04 Protocole ARP

05 La couche de transport

06 Services réseau

07

08 Lap pratiques

Objectifs du module

Titre du Module: Protocole ARP (Address Resolution Protocol)

Objectif du Module: Analyser les unités de données du protocole ARP sur un réseau.

Titre du Rubrique	Objectif du Rubrique
Adresses MAC et IP	Comparer les rôles de l'adresse MAC et de l'adresse IP.
ARP	Analyser ARP en examinant les trames Ethernet.
Problèmes liés au protocole ARP	Expliquer l'impact qu'ont les requêtes ARP sur le réseau et les performances des hôtes ainsi que les risques potentiels pour la sécurité.

04

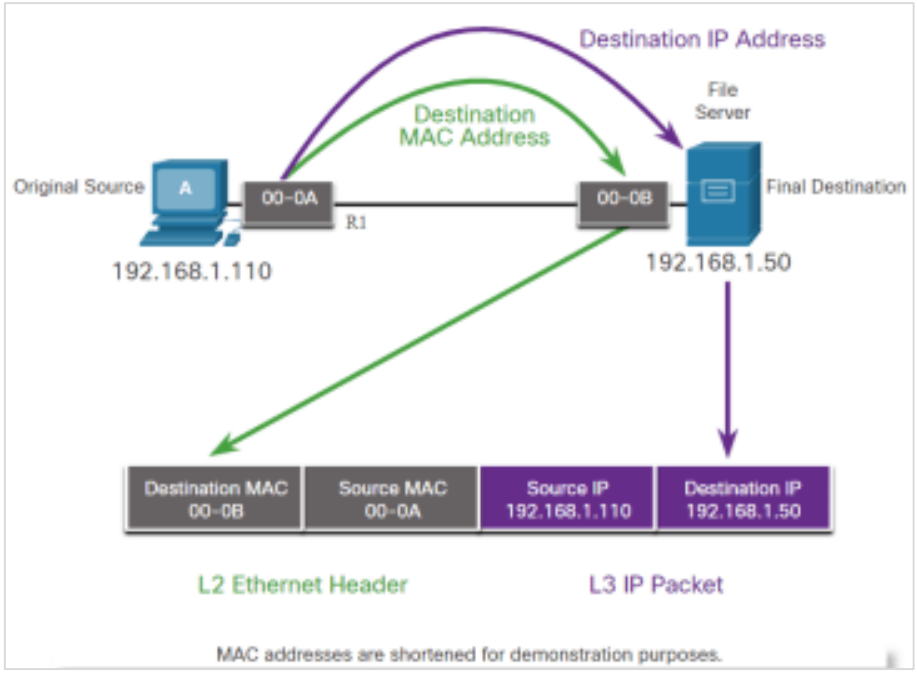
Protocole ARP

8.1 Les adresses MAC et IP

8.1.1 Destination sur le même réseau

- Chaque périphérique possède deux adresses principales sur un LAN Ethernet:

Adresses principales sur Ethernet LAN	Description
Adresse physique (L'adresse MAC Ethernet)	• Utilisée pour les communications entre cartes réseau Ethernet situées sur le même réseau. • Si l'adresse IP de destination appartient au même réseau, l'adresse MAC de destination est celle du périphérique de destination.
Adresse logique (l'adresse IP)	• Utilisée pour envoyer les paquets depuis la source initiale jusqu'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.



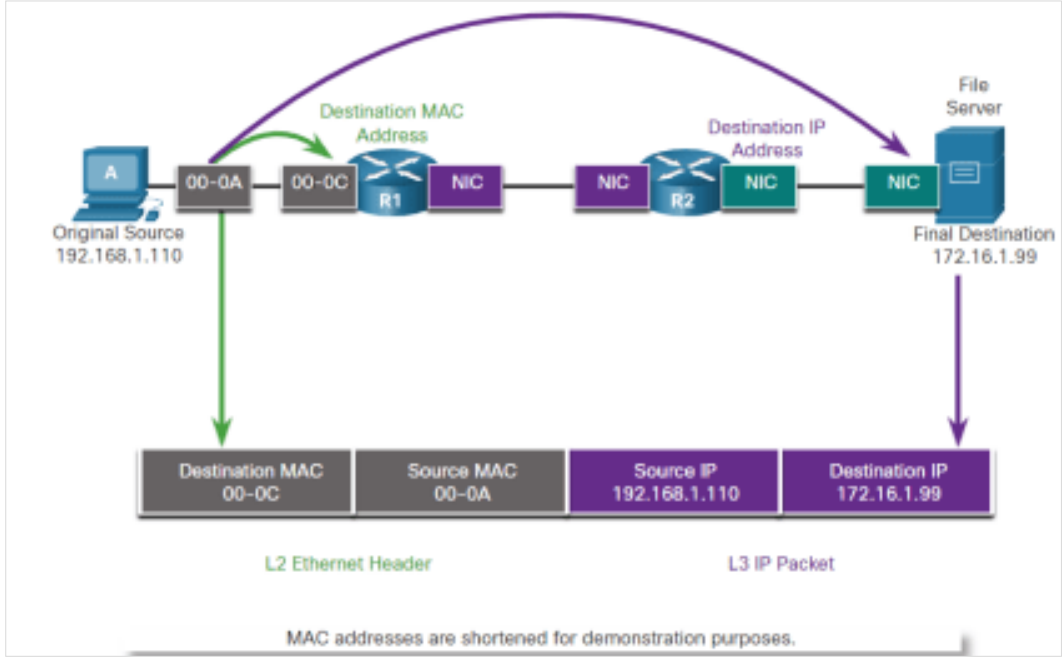
Communication via un réseau local

***Remarque**: la plupart des applications utilisent le système de noms de domaine (DNS) pour déterminer l'adresse IP à partir d'un nom de domaine tel que [www.cisco.com.](http://www.cisco.com)*

8.1.2 Destination sur le réseau distant

- 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.
- Le processus dans la figure est comme ci-dessous:

- Lorsque le **routeur** reçoit la trame Ethernet, il **désencapsule** les informations de couche 2.
- À l'aide de **l'adresse IP de destination**, il **détermine le périphérique du tronçon suivant**, puis **encapsule** le paquet IP dans une **nouvelle trame** liaison de données pour l'interface de sortie.
- **Si le périphérique du tronçon** suivant est la destination finale, l'adresse **MAC de destination** est celle de la carte réseau Ethernet du périphérique.



Communication avec un réseau distant

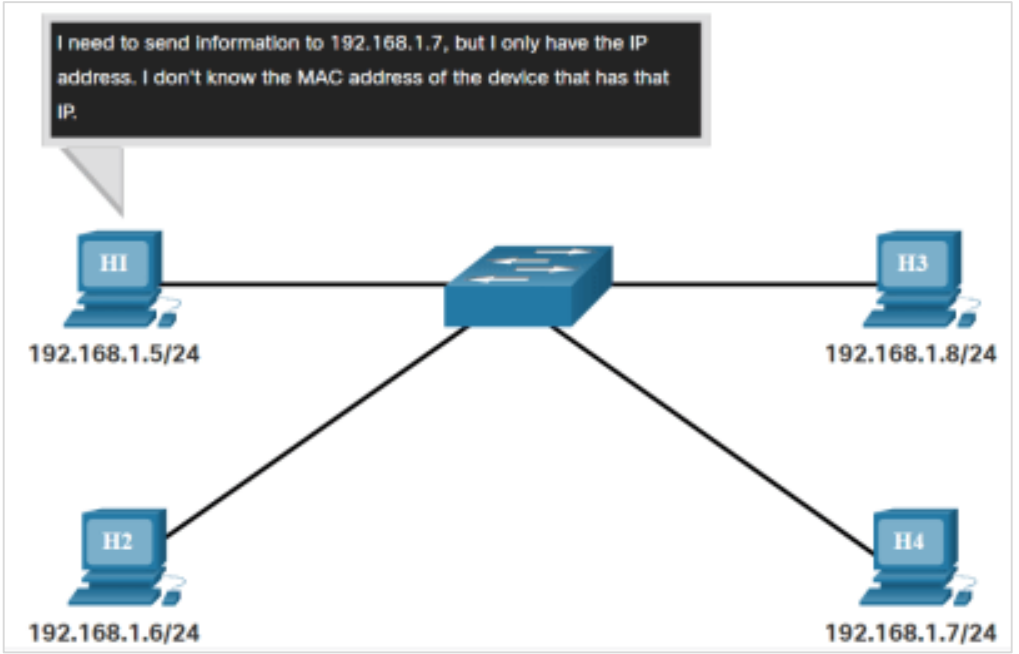
04

Protocole ARP

8.2 ARP

8.2.1 ARP Présentation

- Le **protocole ARP** assure **deux fonctions principales:**
  - la **résolution des adresses IPv4** en adresses MAC ;
  - **Tenir à jour un tableau des mappages** d'adresses IPv4 à MAC

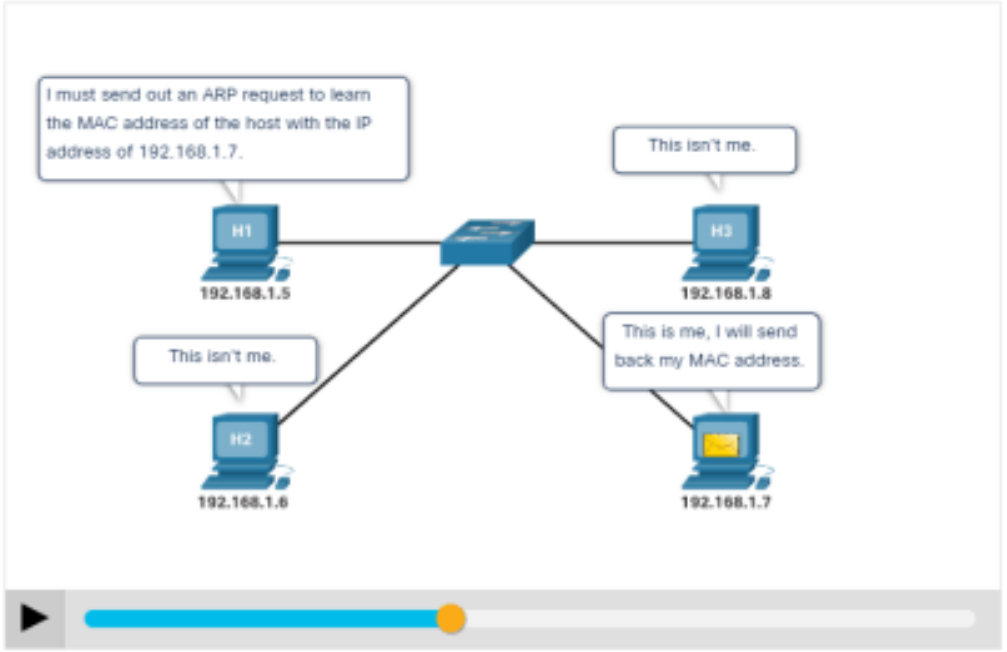


•**Résumé**: Un **périphérique** utilise le **protocole ARP** (Address Resolution Protocol) pour **déterminer l'adresse MAC de destination** d'un périphérique local lorsqu'il **connaît son adresse IPv4**.

8.2.2 Fonctions du protocole ARP

Cliquez sur Lecture pour voir une animation de fonction d'ARP.

- **Quand un paquet est envoyé à la couche liaison de données** pour être encapsulé dans une trame Ethernet, le périphérique consulte **une table** appelée **Table ARP** ou **Cache ARP** stockée dans **sa mémoire** pour connaître l'adresse MAC qui est mappée à l'adresse IPv4.
- Le périphérique d'envoi **recherchera dans sa table ARP une adresse IPv4 de destination** et une adresse MAC correspondante, si l'adresse IPv4 de destination du paquet **se trouve sur le même réseau** que l'adresse IPv4 source.
- Si le périphérique localise l'adresse IPv4, l'adresse MAC correspondante est utilisée comme adresse MAC de destination dans la trame.



8.2.8 Travaux pratiques - Utiliser Wireshark pour examiner les trames Ethernet

8.2.7 Tables ARP sur les périphériques réseau

Sur un routeur Cisco, la commande **show ip arp** permet d'afficher la table ARP.

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1            -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
Internet  209.165.200.225          -   a0e0.af0d.e141  ARPA   GigabitEthernet0/0/1
Internet  209.165.200.226          1   a03d.6fe1.9d91  ARPA   GigabitEthernet0/0/1
R1#
```

Sur les ordinateurs exécutant Windows 10, c'est la commande **arp –a** qui affiche la table ARP.

```
C:\Users\PC> arp -a
Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86     dynamic
  192.168.1.101         08-3e-0c-f5-f7-77     dynamic
  192.168.1.110         08-3e-0c-f5-f7-56     dynamic
  192.168.1.112         ac-b3-13-4a-bd-d0     dynamic
  192.168.1.117         08-3e-0c-f5-f7-5c     dynamic
  192.168.1.126         24-77-03-45-5d-c4     dynamic
  192.168.1.146         94-57-a5-0c-5b-02     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\Users\PC>
```

ARP

8.2.8 Travaux pratiques - Utiliser Wireshark pour examiner les trames Ethernet

Dans ce Travaux Pratiques, vous ferez ce qui suit:

- Utilisez Wireshark pour capturer et afficher des trames Ethernet afin d'étudier les adresses ARP et IP et MAC.
- Capturez et analysez des images ICMP.

04

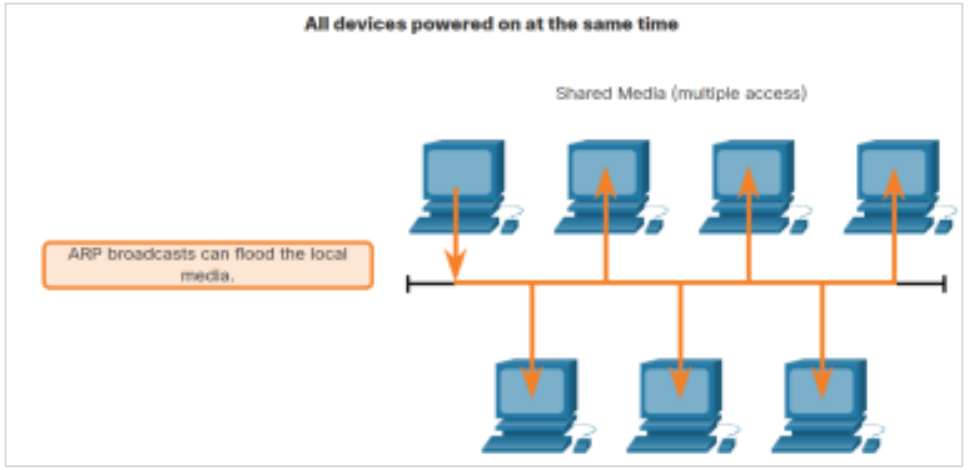
Protocole ARP

8.3 Les problèmes liés à ARP

8.3.1 Problèmes liés au protocole ARP - Diffusion de l'ARP et usurpation d'identité de l'ARP

Diffusions ARP

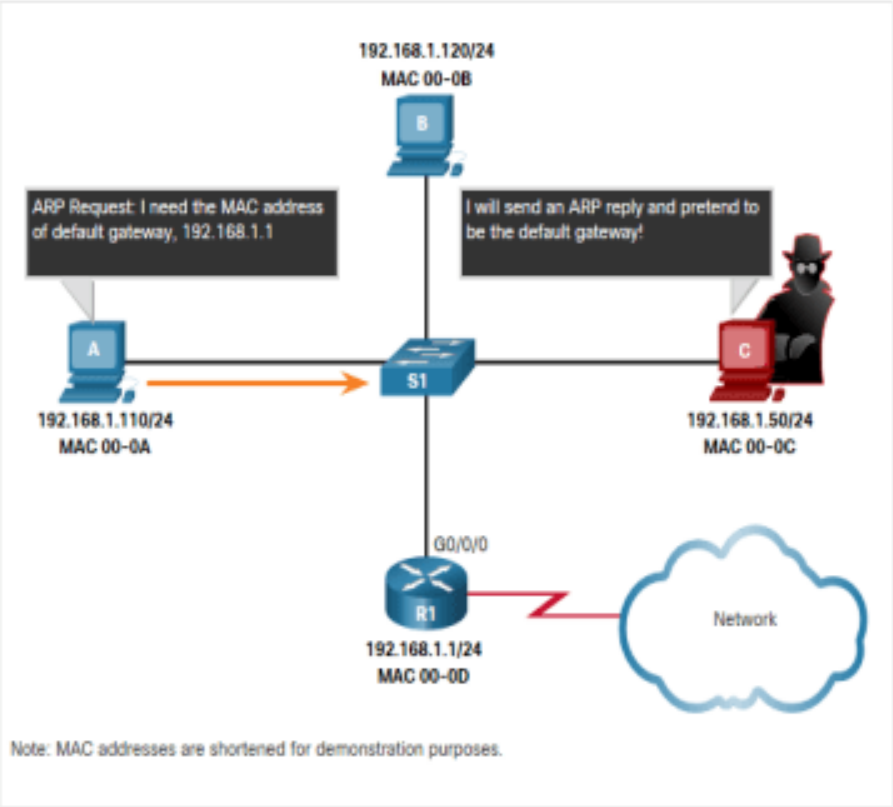
- Comme les **trames de diffusion**, les **requêtes ARP** sont **reçues et traitées** par chaque périphérique du réseau local.
- Sur un réseau d'entreprise type, **ces diffusions** auraient une **incidence minime** sur les **performances du réseau**.
- Si de nombreux appareils commencent à accéder aux services réseau en même temps, il peut y avoir une **réduction des performances** pendant une courte période.



8.3.1 Problèmes liés au protocole ARP - Diffusion de l'ARP et usurpation d'identité de l'ARP

Usurpation ARP

- L'utilisation du protocole ARP peut **créer un risque de sécurité potentiel.**
- Un **acteur de menace** peut utiliser **l'usurpation ARP** pour effectuer une **attaque d'empoisonnement ARP**.
  - Il s'agit d'une technique utilisée par un acteur de menace pour **répondre à une requête ARP** concernant l'adresse IPv4 d'un autre périphérique tel que la passerelle par défaut.
  - L'acteur de menace envoie une **réponse ARP avec sa propre adresse MAC.** Le destinataire de la **réponse ARP ajoute la mauvaise** adresse MAC à sa table ARP et envoie ces paquets à l'acteur de menace.



04

Protocole ARP

8.4 Récapitulation de protocole ARP (Address Resolution Protocol)

Récapitulation et questionnaire du module

8.4.1 Qu'est-ce que j'ai appris dans ce module ?

- Les **adresses IP** identifient l'adresse du **périphérique source** d'origine et celle du **périphérique de destination** finale.
- Les **adresses MAC** servent à **acheminer la trame liaison de données** contenant le paquet IP encapsulé d'une carte réseau à une autre sur le même réseau.
- **ARP** est utilisé pour **mapper l'adresse IPv4 logique avec l'adresse MAC de couche 2.**
- **ARP** fournit **deux fonctions de base**: résoudre les adresses IPv4 en adresses MAC et maintenir une table de mappages d'adresses IPv4 vers MAC.
- **Lorsque l'adresse IPv4 de destination est sur le même réseau que la source,** le processus ARP envoie l'adresse IPv4 à **tous les hôtes du réseau** afin que l'hôte avec l'adresse IPv4 correspondante puisse ré**pondre avec l'adresse MAC correspondante**
- 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.

8.4.1 Qu'est-ce que j'ai appris dans ce module ? (suite)

- **S'il n'y a pas d'entrée pour l'adresse IPv4 dans sa table ARP**, le périphérique d'envoi envoie une **requête ARP pour déterminer l'adresse MAC de destination**.
- **Seul le périphérique dont l'adresse IPv4 correspond à l'adresse IPv4 cible de la requête ARP envoie une réponse ARP.**
- Dans IPv6, Détection de voisin **ICMPv6 (ND)** est utilisé.
- Comme les **trames de diffusion**, les **requêtes ARP** sont reçues et traitées par chaque périphérique du réseau local.
- **L'usurpation ARP ou empoisonnement ARP** est une technique utilisée par un acteur de menace pour répondre à une requête ARP demandant l'adresse IPv4 d'un autre périphérique, tel que la **passerelle par défaut.**

Securité Réseau

Module 3

01 Protocoles réseau

02 Ethernet et Protocole IP

03 Vérification de la connectivité

04 Protocole ARP

05 La couche de transport

06 Services réseau

07

08 Lap pratiques

Objectifs du module

Titre du Module: La couche de transport

Objectif du Module: Expliquer comment les protocoles de la couche transport prennent en charge la fonctionnalité du réseau.

Titre du Rubrique	Objectif du Rubrique
Caractéristiques de la couche transport	Expliquer comment les protocoles de la couche de transport prennent en charge les communications réseau.
Établissement de sessions dans la couche de transport	Expliquer comment la couche de transport établit des sessions de communication.
Fiabilité de la couche transport	Expliquer comment la couche de transport établit des communications fiables.

05

La couche transport

9.1 Les caractéristiques de la couche de transport

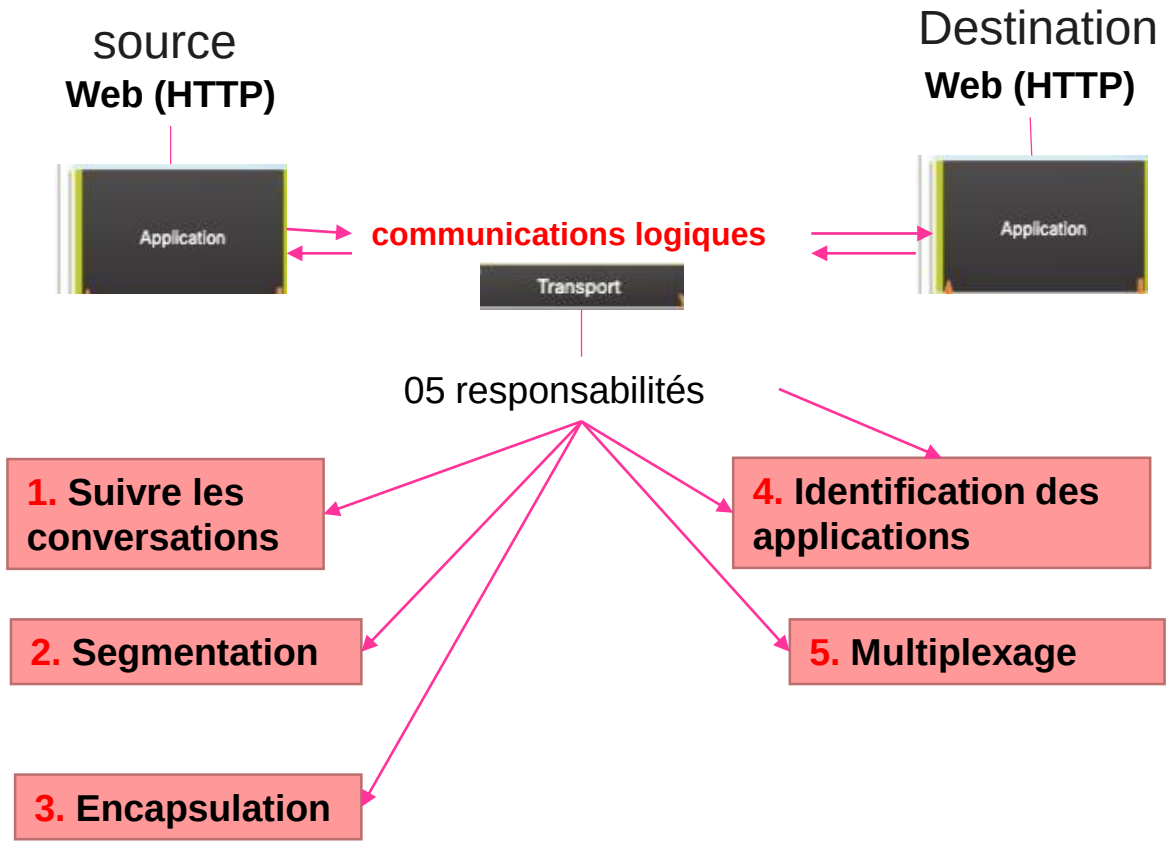
9.1.1. Rôle de la couche transport

- La **couche de transport** est responsable des **communications logiques** entre les applications exécutées sur différents hôtes.
- Comme le montre l'illustration, la couche transport constitue la **liaison entre la couche application** et les **couches inférieures** chargées de la transmission sur le réseau.
- La couche transport inclue deux protocoles : **TCP** (Transmission Control Protocol) et **UDP** (User Datagram Protocol).

9.1.2 Responsabilités de la couche de transport

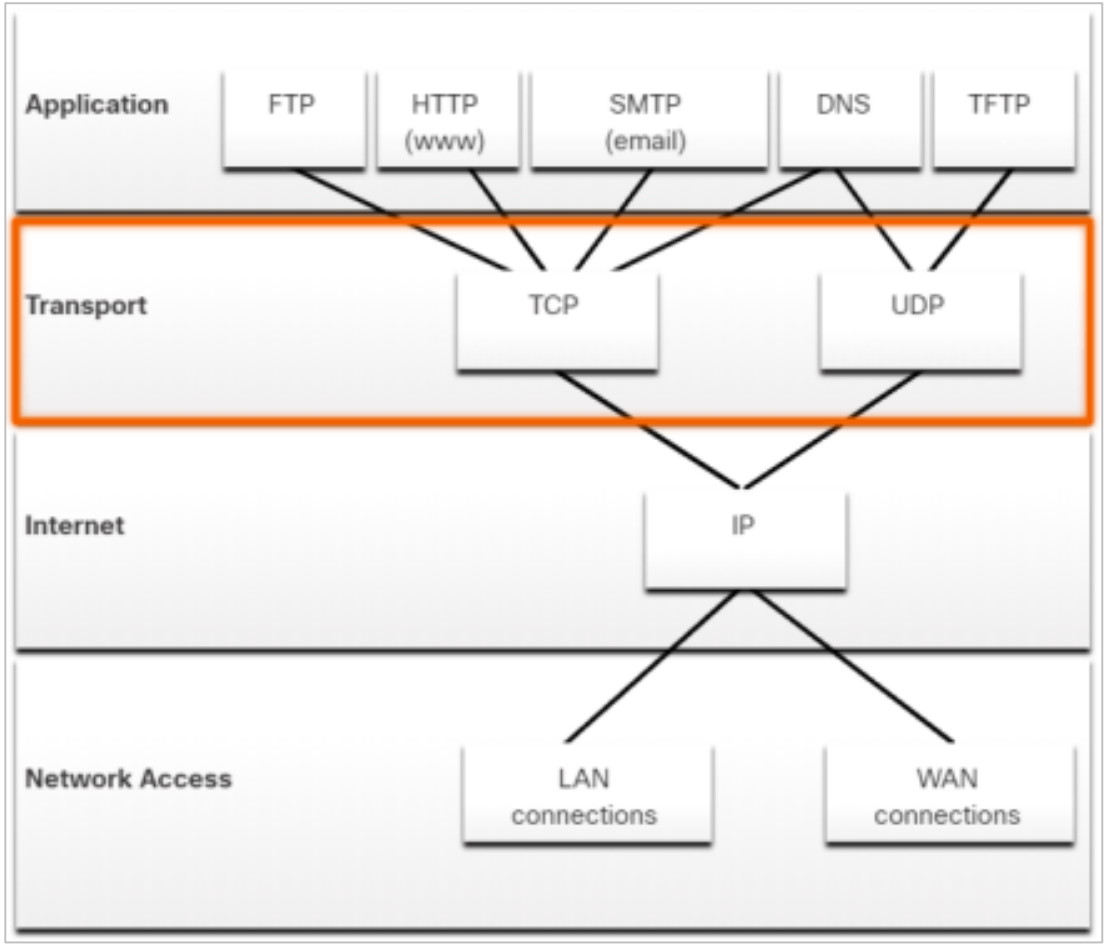
La **couche de transport** a les responsabilités suivantes:

- **Suivre les conversations** individuelles
- **Segmentation des données** et **reconstitution** des segments
- **Ajouter les informations d'en-tête**
- **Identifier, séparer et gérer** plusieurs conversations
- Utiliser la **segmentation** et le **multiplexage** pour permettre à différentes conversations de communication d'être entrelacées sur le même réseau



9.1.3 Protocoles de la couche de transport

- Les protocoles de La couche de transport (**TCP et UDP**) **spécifient comment transférer des messages** entre les hôtes.
- **TCP et UDP** sont responsables de la gestion des **exigences de fiabilité** d'une conversation.

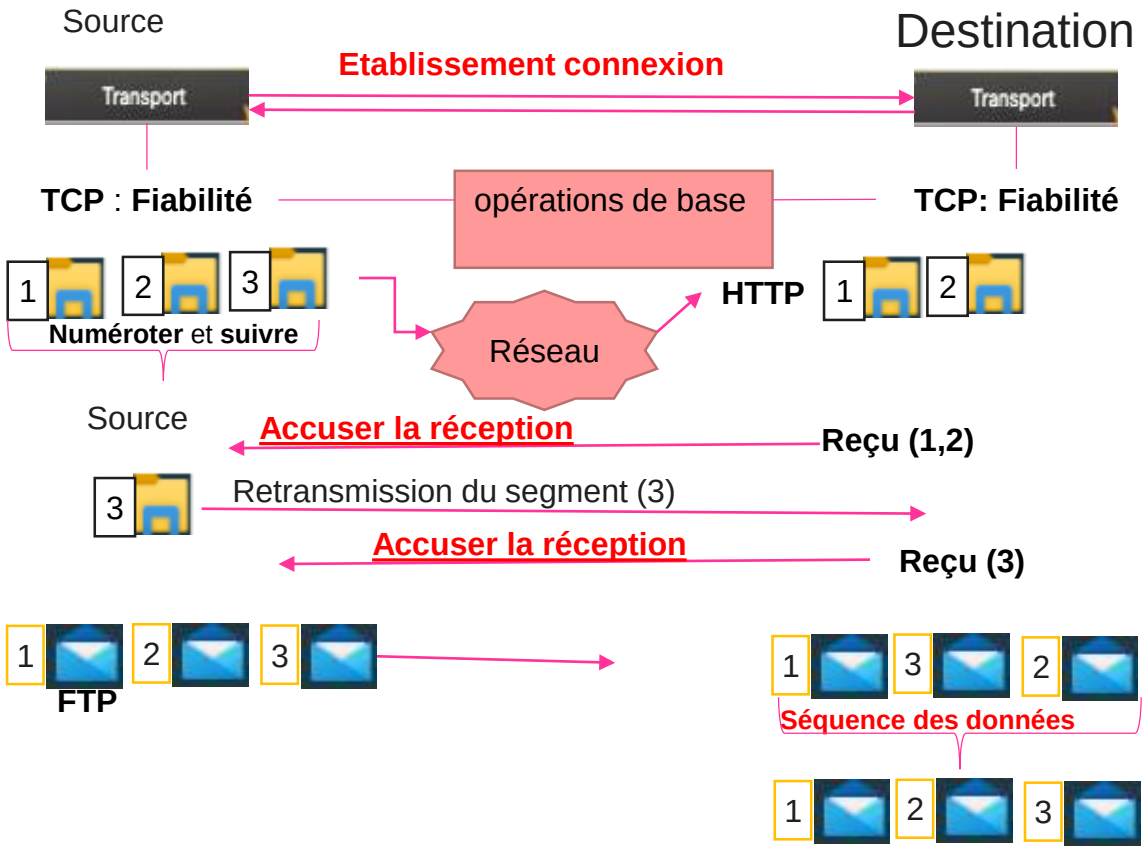


9.1.4 Protocole TCP (Transmission Control Protocol)

▪**TCP** assure la **fiabilité** et le **contrôle du flux**.

▪Les opérations de base de TCP:

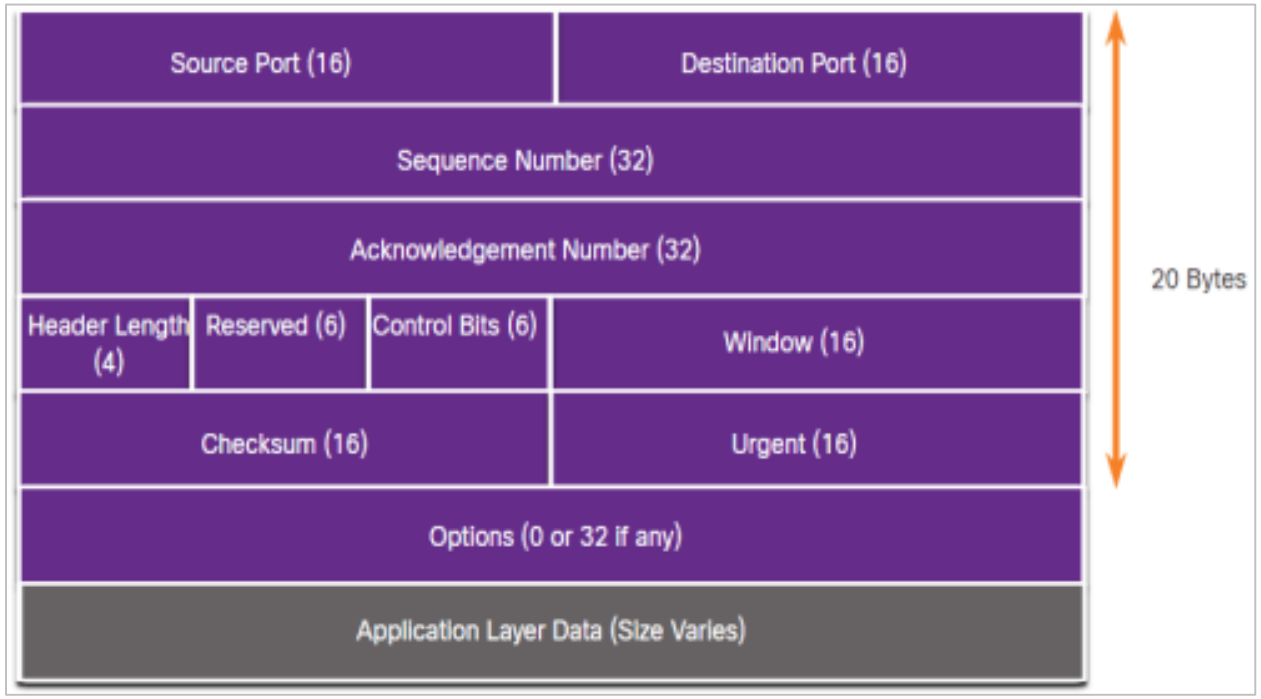
- **Numéroter** et **suivre les segments** de **données transmis** à un hôte spécifique à partir d'une application spécifique
- **Accuser la réception** des données reçues
- **Retransmettre** toute donnée non reconnue après un certain temps
- **Séquence des données** qui pourraient arriver dans un ordre incorrect
- **Envoyer des données** à un taux **efficace et acceptable** par le destinataire



***Remarque**: Le TCP divise les données en segments.*

9.1.5 En-tête TCP

- **TCP est un protocole avec état**, ce qui signifie qu'il **garde une trace de l'état de la session** de communication.
- Un **segment TCP** ajoute **20 octets** (c'est-à-dire 160 bits) de surcharge lors de l'encapsulation des **données de la couche d'application**.
- La figure montre les champs d'un en-tête TCP.



9.1.6 Champs d'en-tête TCP

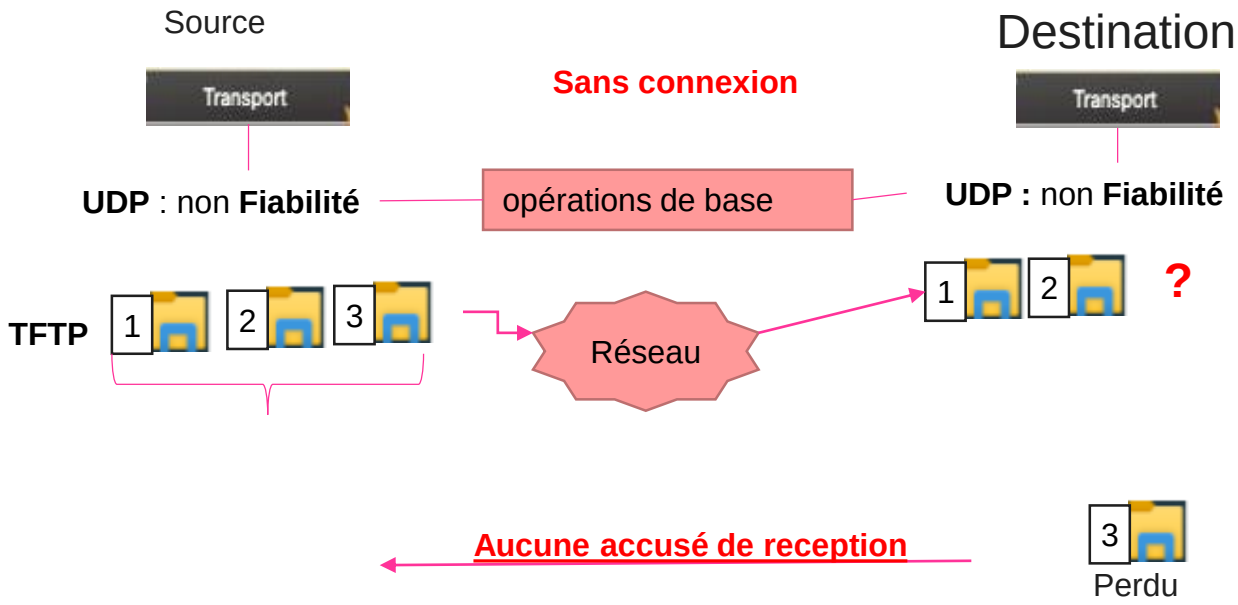
Le tableau identifie et décrit les dix champs d'un en-tête TCP.

Champ d'en-tête TCP	Description
Port Source	Champ 16 bits utilisé pour identifier l'application source par le numéro de port.
Port de destination	Champ de 16 bits utilisé pour identifier l'application de destination par le numéro de port.
Numéro de séquence	Champ 32 bits utilisé à des fins de réassemblage de données.
Numéro d'accusé de réception	Champ 32 bits est utilisé pour indiquer que les données ont été reçues et l'octet suivant est prévu de la source.
Longueur d'en-tête	Champ 4 bits connu sous le nom de « offset de données » qui indique la longueur de l'en-tête du segment TCP.
Réservé	Un champ de 6 bits qui est réservé pour une utilisation future.
Bits de contrôle	Un champ de 6 bit utilisé comprennent des codes de bits qui indiquent l'objectif et la fonction du segment TCP.
Taille de fenêtre	Champ 16 bits utilisé pour indiquer le nombre d'octets qui peut être acceptés.
Somme de contrôle	Un champ de 16 bits utilisé pour la vérification des erreurs de l'en-tête du segment et des données.
Urgent	Champ 16 bits utilisé pour indiquer si les données contenues sont urgentes.

9.1.7 UDP (Transport of Data User Datagram Protocol)

▪**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.

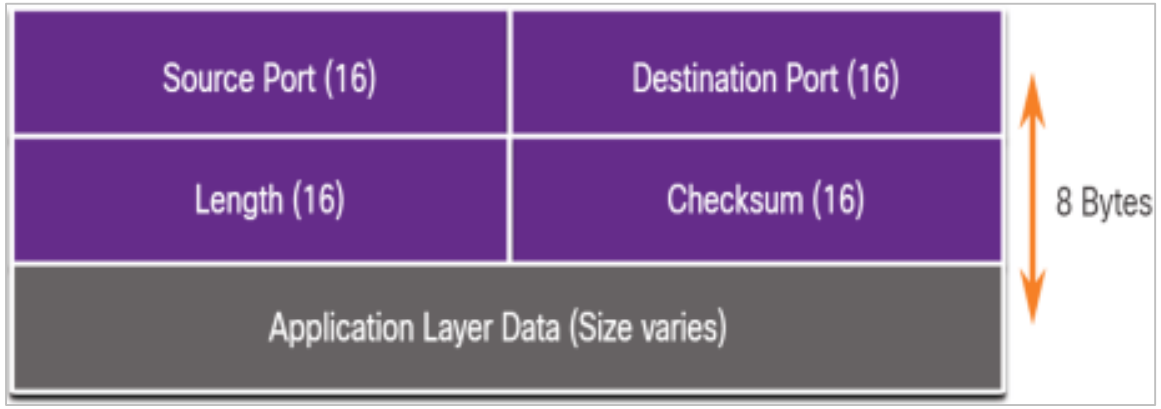
- UDP est un protocole **sans connexion**.
- UDP est également connu comme un protocole de **livraison du meilleur effort**, car il **n'y a pas d'accusé de réception** des données à la destination.



***Remarque**: UDP divise les données en datagrammes qui sont également appelés segments*

9.1.8 En-tête UDP

- **UDP** est un protocole **sans état,** ce qui signifie que **ni le client, ni le serveur, ne suit l'état de la session** de communication.
- Si la fiabilité est nécessaire dans le cadre de l'utilisation d'UDP comme protocole de transport, **elle doit être prise en charge par l'application**.
- L'en-tête UDP n'a que **quatre champs** et nécessite **8 octets** (c'est-à-dire 64 bits). La figure montre les champs d'un en-tête UDP.



9.1.9 En-tête UDP

Le tableau identifie et décrit les quatre champs d'un en-tête UDP.

Champ d'en-tête UDP	Description
Port Source	Champ 16 bits utilisé pour identifier l'application source par le numéro de port.
Port de destination	Champ de 16 bits utilisé pour identifier l'application de destination par le numéro de port.
Longueur	Champ 16 bits indiquant la longueur de l'en-tête de datagramme UDP.
Somme de contrôle	Champ 16 bits utilisé pour la vérification des erreurs de l'en-tête et des données du datagramme.

Deux types

Ports réservés
[0 à 1023]

Ports inscrits
[1024 à 49151]

Ports privés et/ou **Dynamiques**
[49152 à 65535]

Attribués par l'IANA à une **entité demandeuse (Cisco)**

Par exemple: **IANA** a attribué le port **49** a Cisco pour le protocole **TACAS+ et 1812 pour Radius**

Attribués par le système d'exploitation **lorsqu'une connexion à un service est lancée**

Réservés aux services au niveau des applications serveurs (web, FTP, SMTP…)

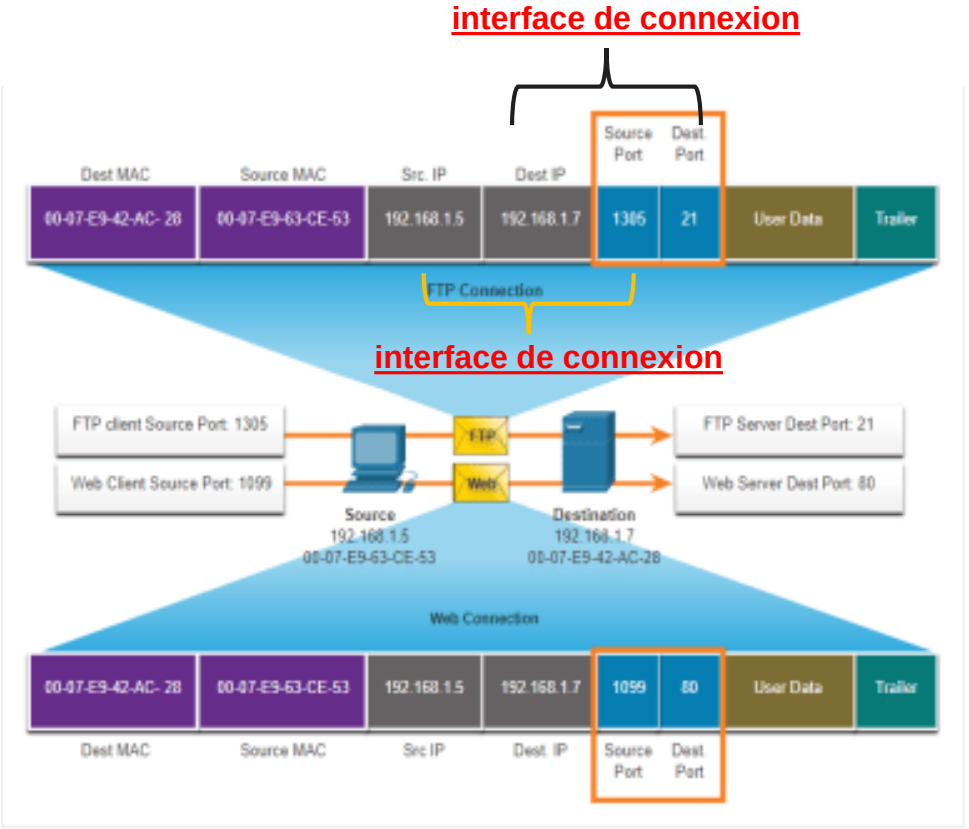
Groupes de numéros de port (Suite)

Numéros de ports reconnus

Numéro de port	Protocole	Application
20	TCP	FTP (File Transfer Protocol) - Données
21	TCP	File Transfer Protocol (FTP) - Contrôle
22	TCP	SSH (Secure Shell)
23	TCP	Telnet
25	TCP	Protocole SMTP
53	UDP, TCP	Service de noms de domaine (Domain Name Service, DNS)
67	UDP	Serveur DHCP (Dynamic Host Configuration Protocol)
68	UDP	Client DHCP (Dynamic Host Configuration Protocol)
69	UDP	Protocole TFTP (Trivial File Transfer Protocol)
80	TCP	Protocole HTTP (Hypertext Transfer Protocol)
110	TCP	Protocole POP3 (Post Office Protocol version 3)
143	TCP	IMAP (Internet Message Access Protocol)
161	UDP	Protocole SNMP (Simple Network Management Protocol)
443	TCP	protocole HTTPS (Hypertext Transfer Protocol Secure)

9.1.10 Paire d'interfaces de connexion

- 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**.
- 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.**



05

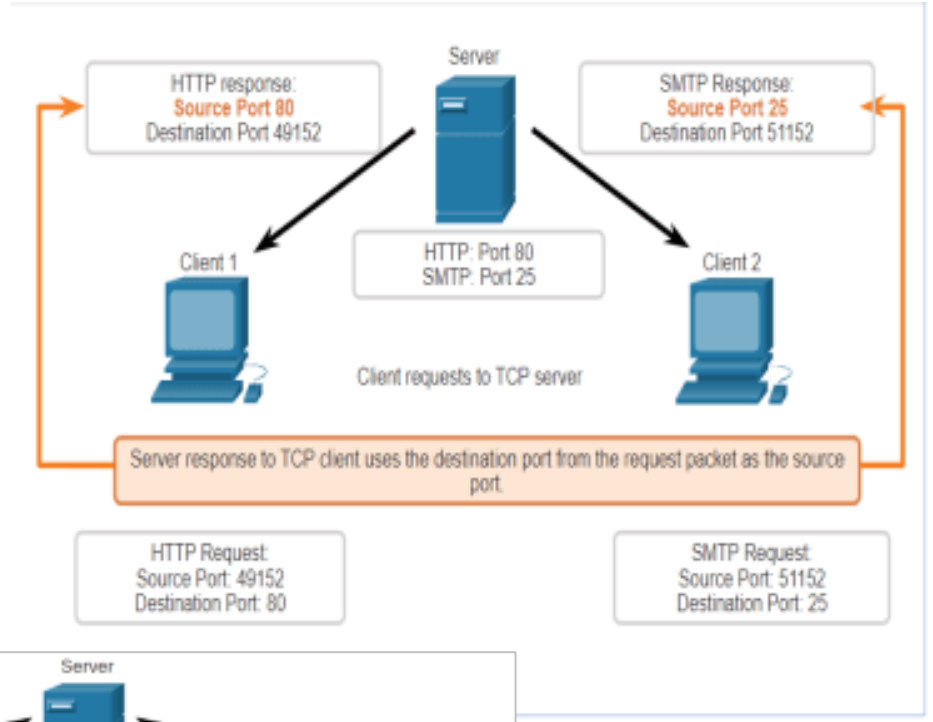
La couche transport

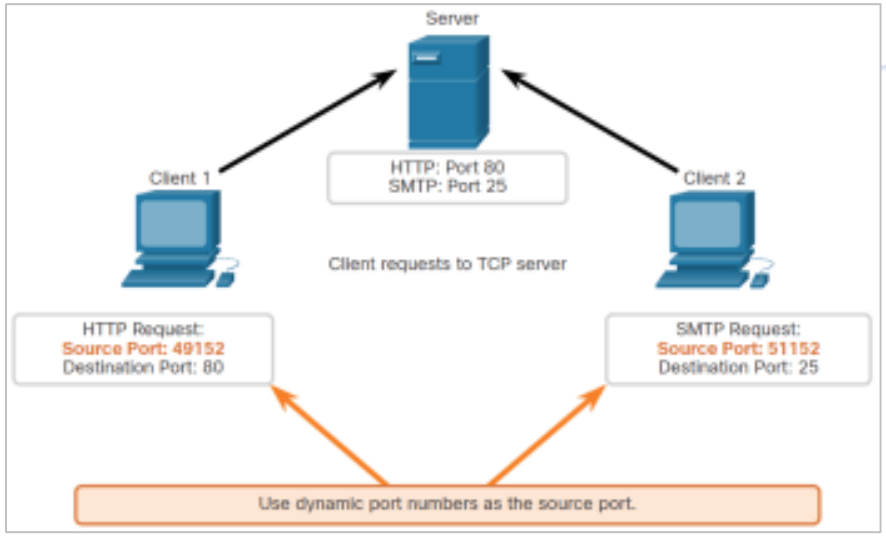
9.2 Établissement de sessions dans la couche de transport

9.2.1 Processus de serveur TCP

Chaque processus de demande s'exécutant sur un **serveur** est configuré pour utiliser un **numéro de port**.

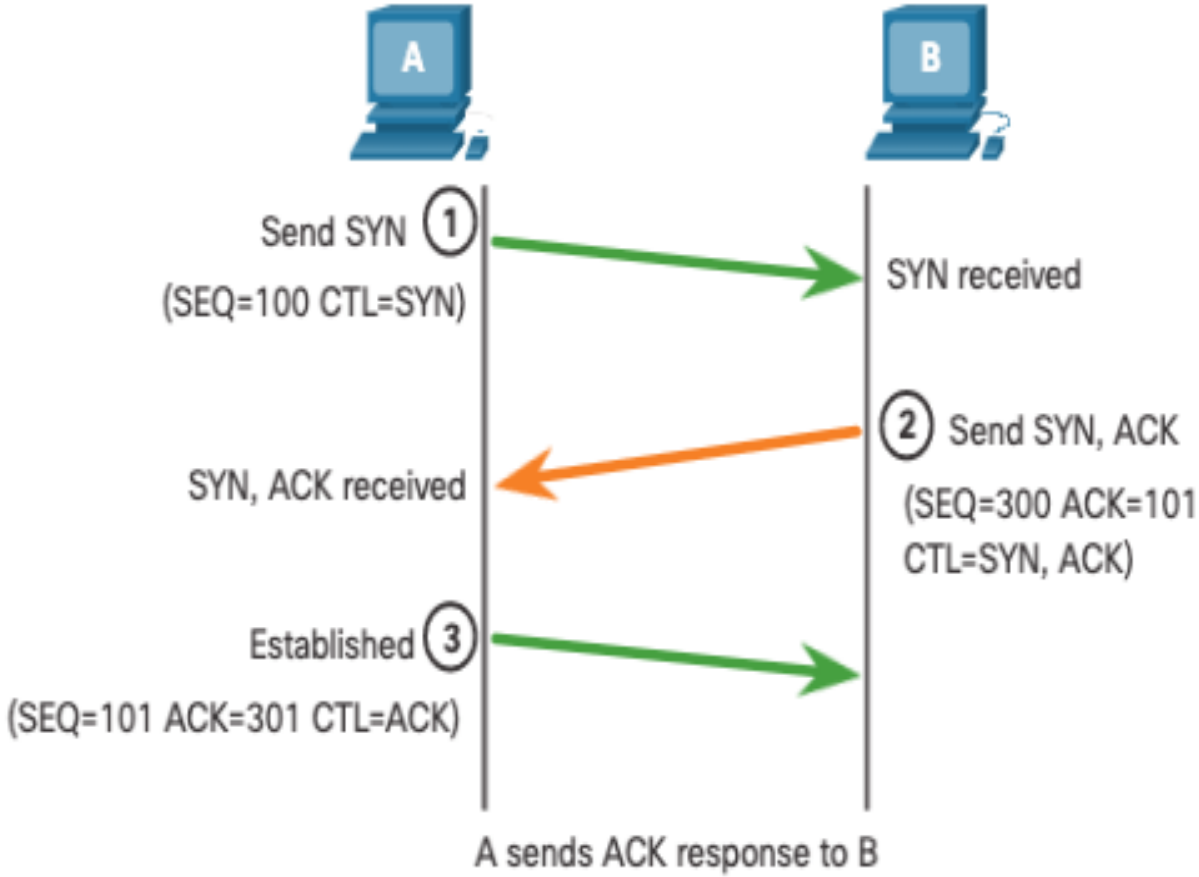
- **Deux services ne peuvent pas** être affectés au **même numéro de port** d'un serveur au sein des mêmes services de la couche transport.
- **Une application** de serveur active affectée à un **port spécifique** est considérée comme étant **ouverte**, ce qui signifie que la ***couche transport*** **accepte et traite** les segments adressés à ce port.





9.2.2 Établissement de connexion TCP

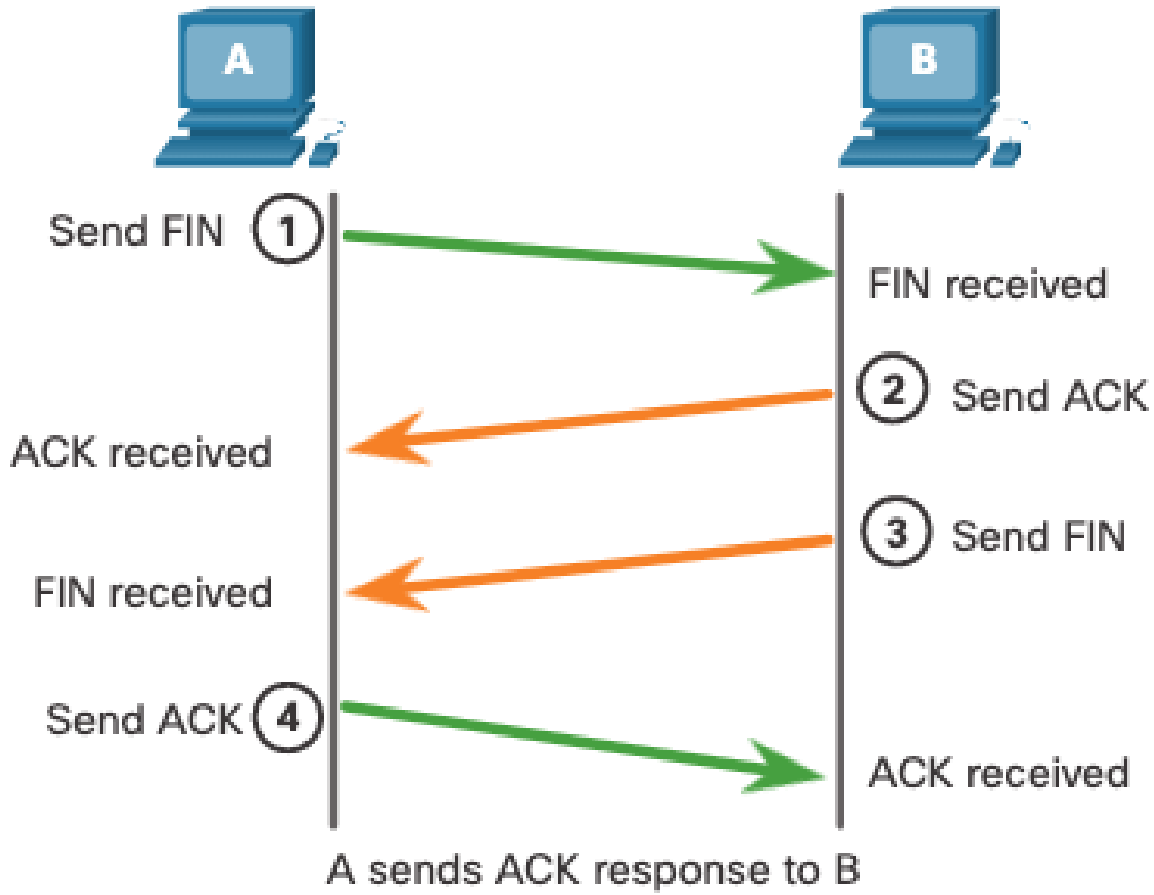
- **Étape 1**: Le **client** demande **l'établissement d'une session** (SYN) de communication client-serveur avec le **serveur.**
- **Étape 2**: Le serveur **accuse la réception (ACK)** de la session de communication client-serveur et **demande l'établissement (SYN)** d'une session de communication serveur-client.
- **Étape 3**: Le client **accuse réception (SYN)** de la session de communication serveur-client.



9.2.6 Travaux pratiques - Utilisation de Wireshark pour observer la connexion TCP en trois étapes

9.2.3 Terminer une session

- **Étape 1**: Quand le client **n'a plus de données** à envoyer dans le flux, il envoie un segment dont l'indicateur **FIN** est défini.
- **Étape 2**: Le serveur envoie un segment **ACK** pour indiquer la bonne réception du segment FIN afin de **terminer la session** du client au serveur.
- **Étape 3:** Le serveur envoie un segment **FIN** au client pour terminer la session du serveur au client.
- **Étape 4**: Le client répond à l'aide d'un **segment ACK** pour accuser la réception du segment FIN envoyé par le serveur.



9.2.6 Travaux pratiques - Utilisation de Wireshark pour observer la connexion TCP en trois étapes

Établissement de session de couche de transport

9.2.6 Travaux pratiques - Utilisation de Wireshark pour observer la connexion TCP en trois étapes

Au cours de ces travaux pratiques, vous aborderez les points suivants :

- **Partie 1:** Préparer les hôtes pour la capture du trafic
- **Partie 2:** Analyser les paquets à l'aide de Wireshark
- **Partie 3:** Afficher les paquets à l'aide de tcpdump

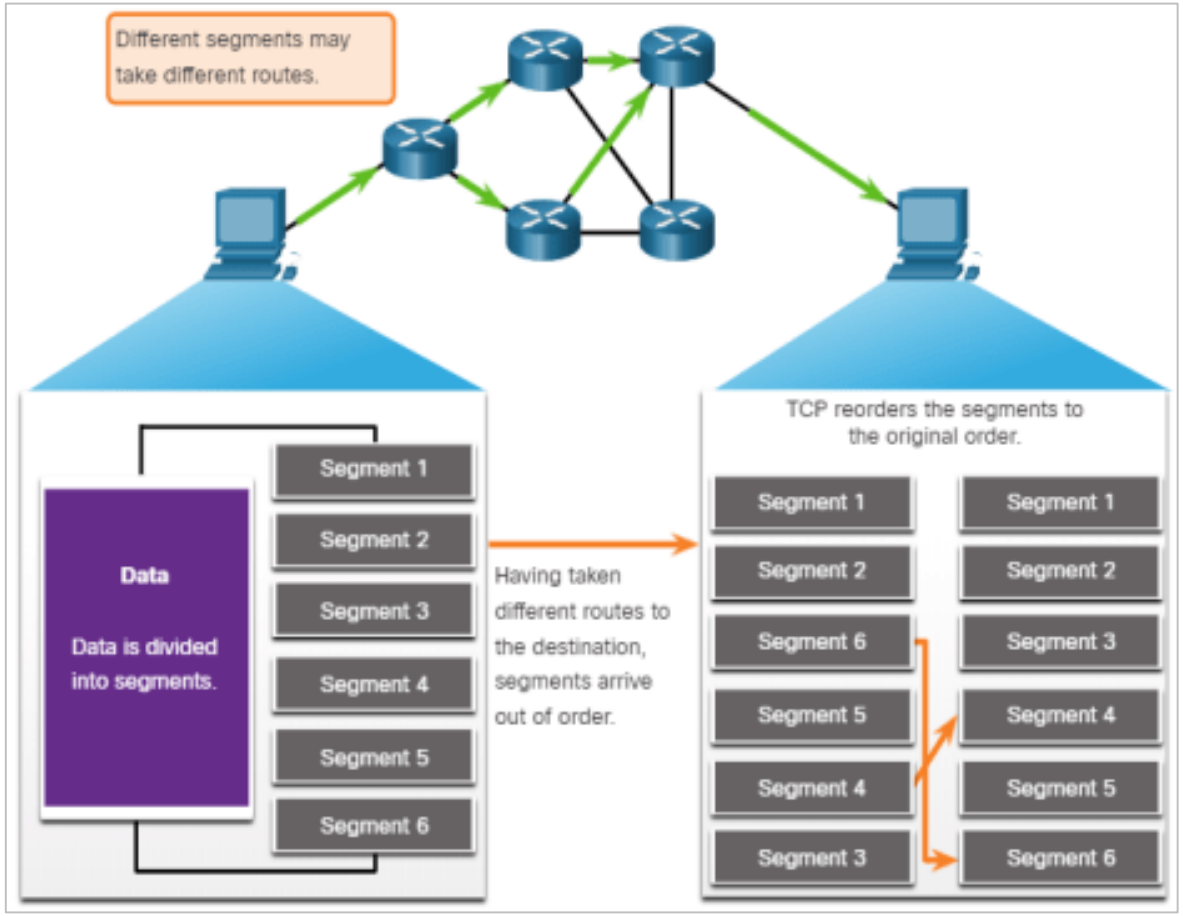
05

La couche transport

9.3 Fiabilité de la couche de transport

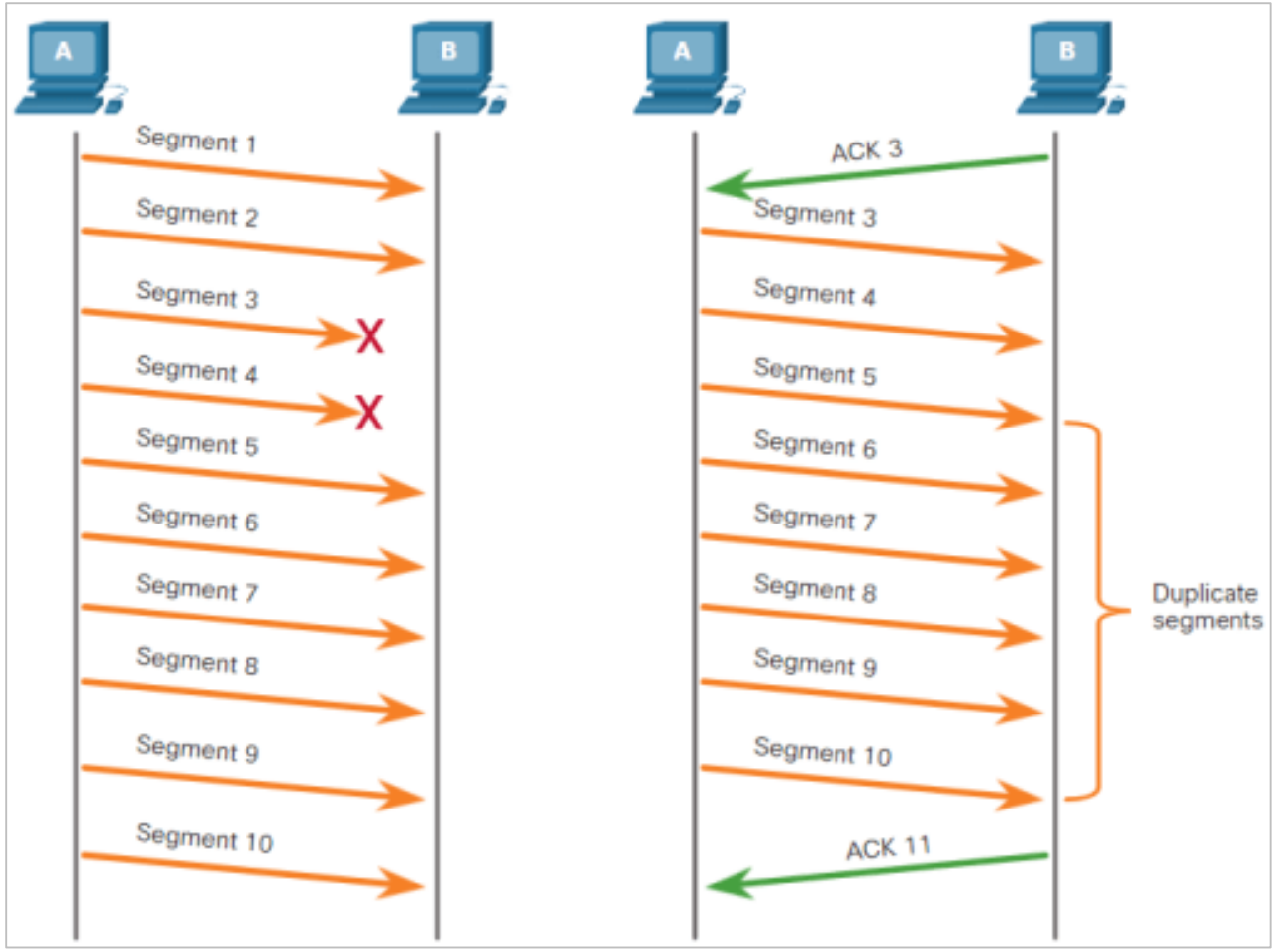
9.3.1 Fiabilité du TCP - Livraison garantie et commandée

- Il peut arriver que des segments TCP **n'arrivent pas à la destination** ou qu'ils soient hors d'usage.
- Toutes les données doivent être reçues et les données de ces segments doivent être **réassemblées dans l'ordre d'origine**.
- Pour cela, des **numéros d'ordre** sont affectés à l'en-tête de chaque paquet.



9.3.3 Fiabilité du TCP - Perte de données et retransmission

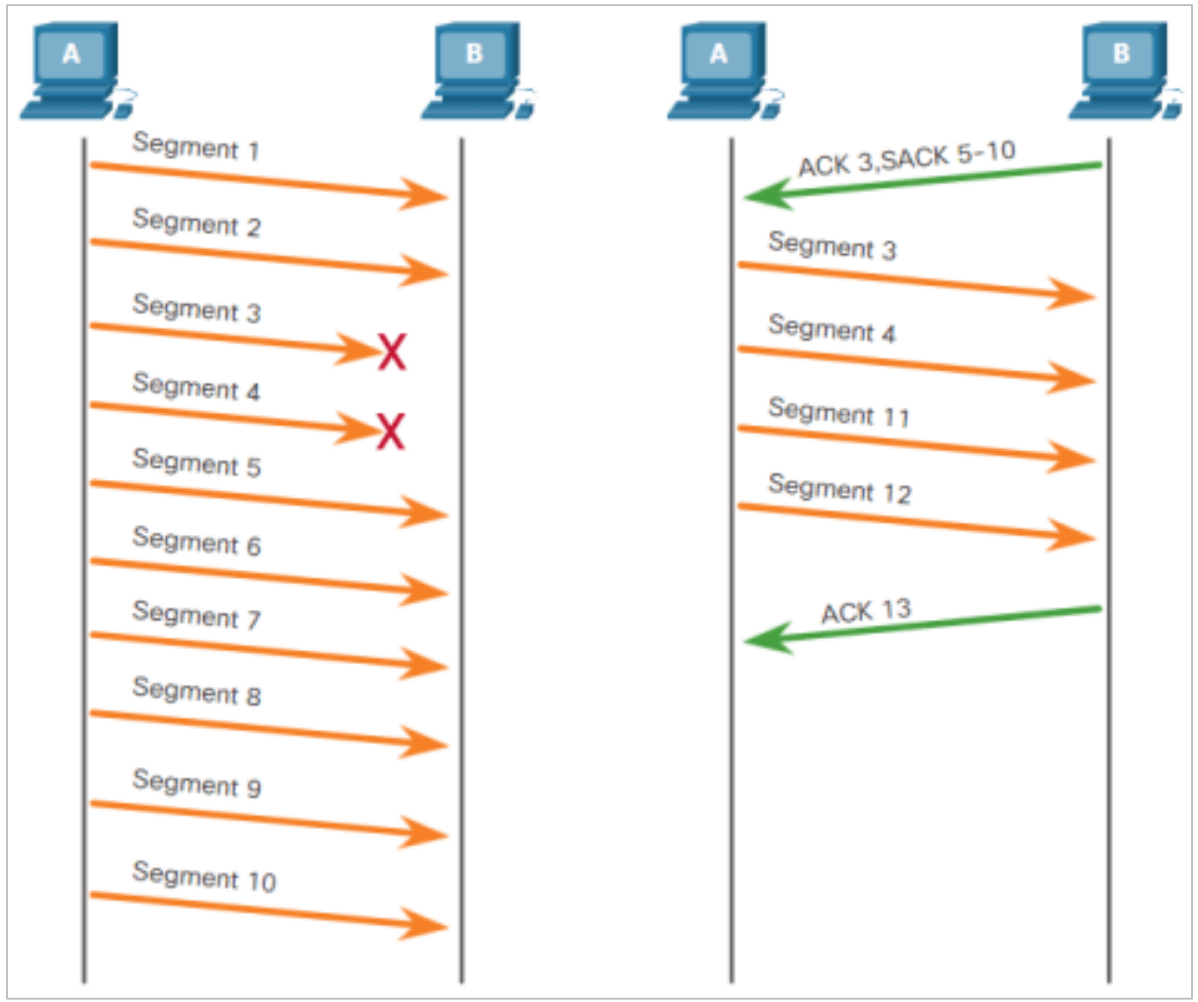
- Quelle que soit la conception d'un réseau, la perte de données se produit occasionnellement.
- Le **protocole TCP** fournit des **méthodes de gestion des pertes** de segments.
- Parmi elles se trouve un mécanisme de **retransmission des segments** pour les données **sans accusé de réception**.



9.3.3 Fiabilité du TCP - Perte de données et retransmission (suite)

- Aujourd'hui, les systèmes d'exploitation hôtes utilisent généralement une **fonctionnalité TCP facultative** appelée reconnaissance sélective (**SACK**), négociée au cours du processus a trois étapes.

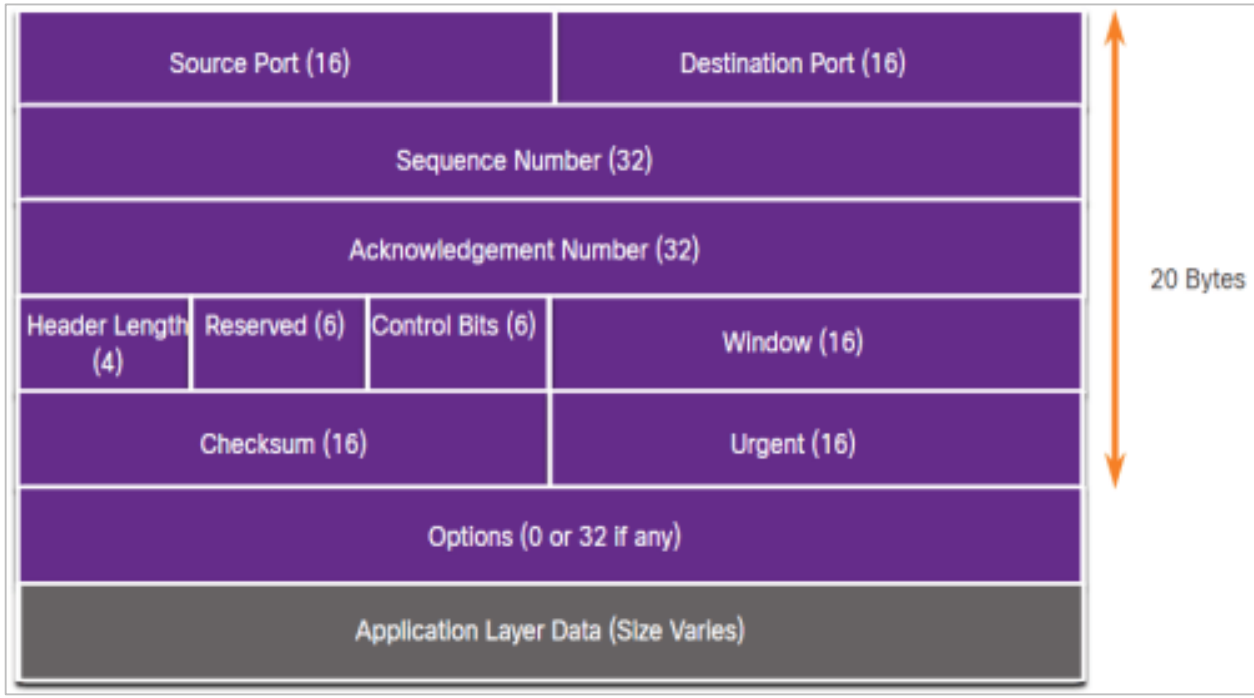
- **Si les deux hôtes prennent en charge SACK**, le récepteur peut explicitement reconnaître **quels segments (octets) ont été reçus**, y compris les **segments discontinus**.



9.3.5 Contrôle de flux TCP - Taille de fenêtre et accusés de réception

L'en-tête TCP inclut un champ de 16 bits appelé **taille de fenêtre**.

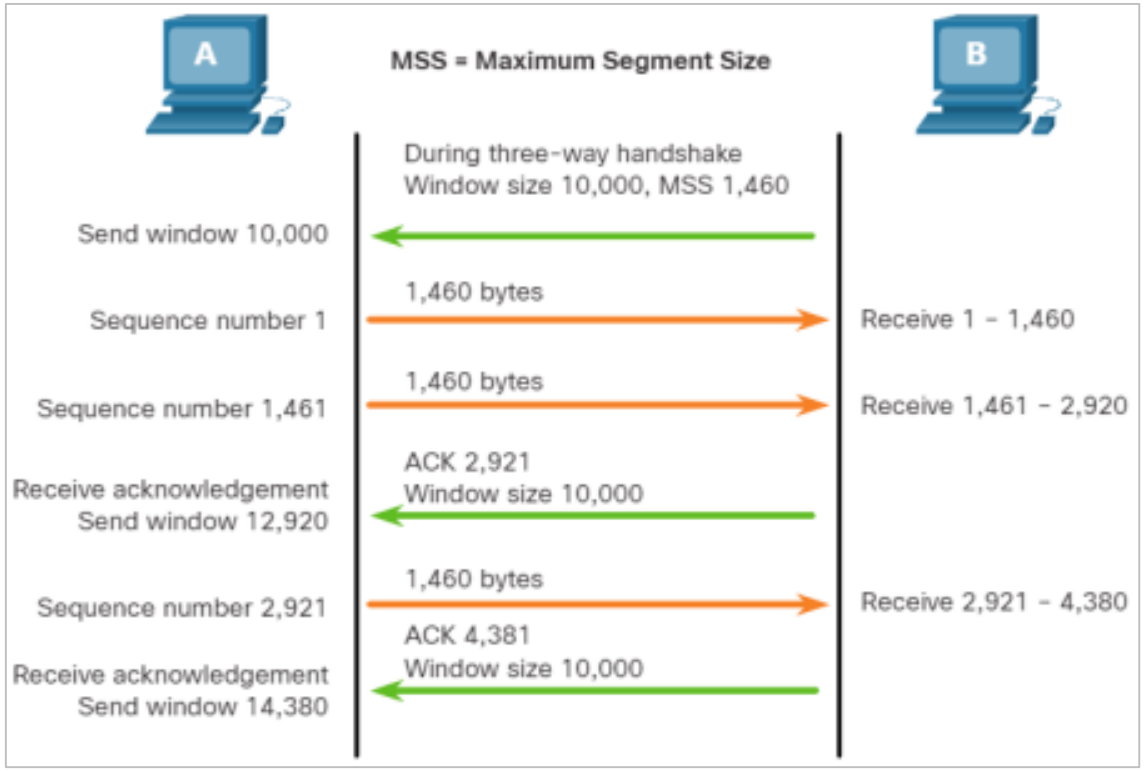
- La **taille de fenêtre** détermine le **nombre d'octets** qui peuvent être **envoyés avant de recevoir un accusé de réception.**
- Le **numéro d'accusé de réception** est le **numéro du prochain octet attendu**.



Résumé: 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**.

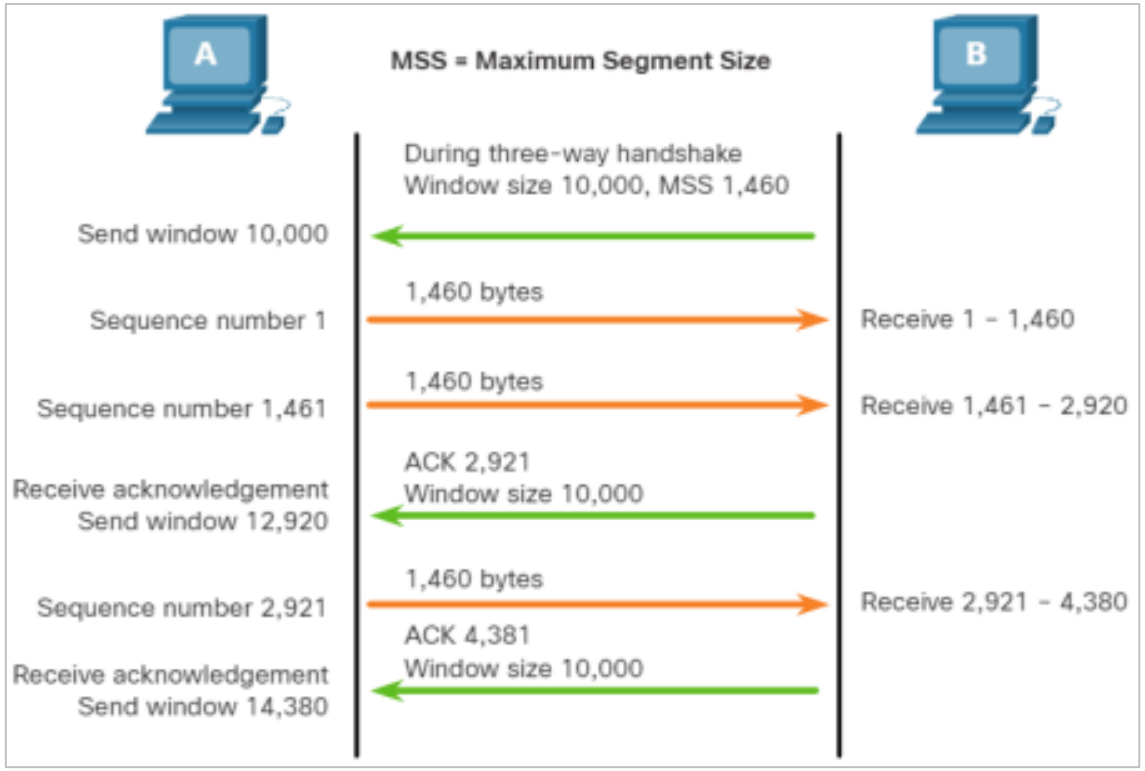
9.3.5 Contrôle de flux TCP - Taille de fenêtre et accusés de réception

- La figure illustre un exemple de **taille de fenêtre** et **d'accusés de réception**.
- 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 la fenêtre de la destination.
- Une fois que le périphérique source a reçu un accusé de réception**, il peut continuer à envoyer plus de données pour la session**.



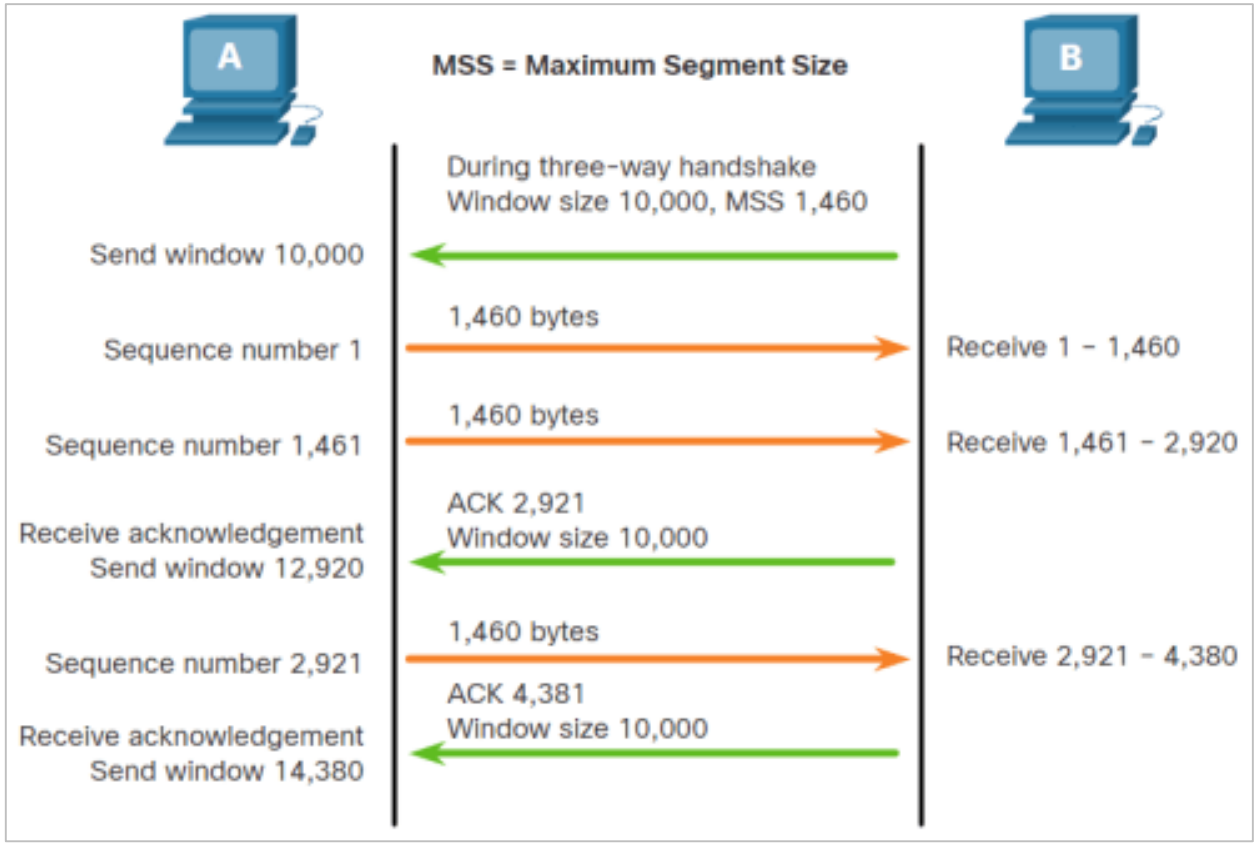
9.3.5 Contrôle de flux TCP - Taille de fenêtre et accusés de réception

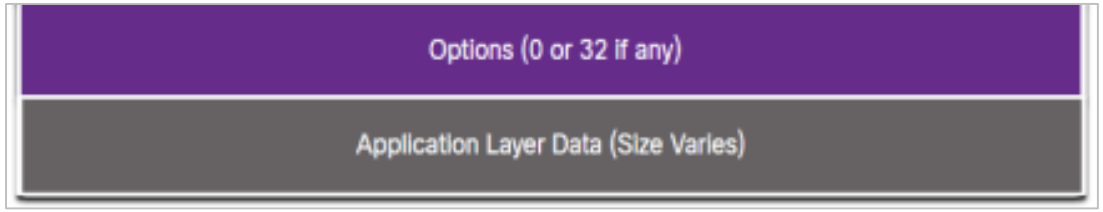
- La destination **n'attend pas que tous les octets** de sa **taille de fenêtre** aient été reçus avant de répondre par un accusé de réception.
- Une fois que **tous les octets ont été reçus et traités**, la destination **envoie des accusés de réception** afin d'informer la source **qu'elle peut continuer** à envoyer des octets supplémentaires.
- **Une destination** qui envoie des accusés de réception au fur et à mesure qu'elle traite les octets reçus, et **l'ajustement continu de la fenêtre d'envoi source**, sont connus sous le **nom de fenêtres coulissantes**.
- **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.



9.3.6 Contrôle de flux TCP - Taille maximale du segment (MSS)

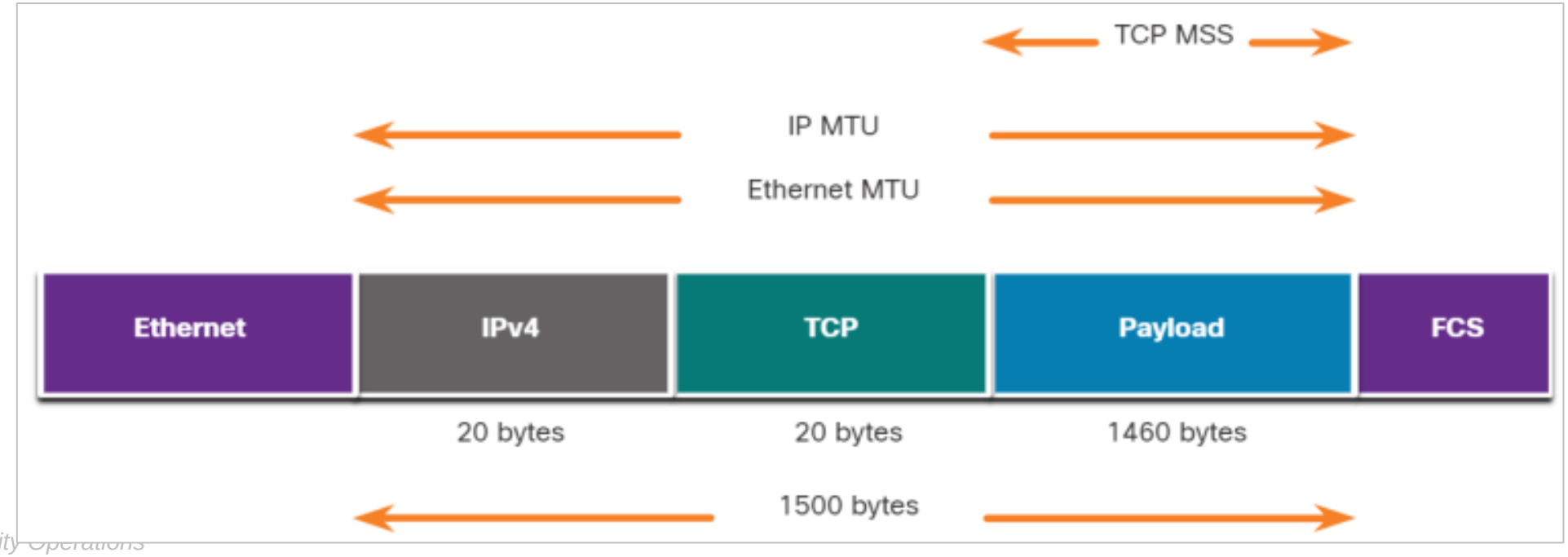
- Dans la figure, la source transmet **1 460** octets de données dans chaque segment TCP. Il s'agit de la **taille maximale de segment** (MSS) que le **périphérique de destination** peut recevoir.
- Le **MSS** fait partie du **champ d'options** de l'en-tête TCP qui spécifie la plus **grande quantité de données**, en octets, qu'un périphérique peut recevoir dans un seul segment TCP.
- La **taille MSS** n'inclut pas **l'en-tête TCP**.
- **MSS** est inclus lors de la **connexion à trois étapes.**





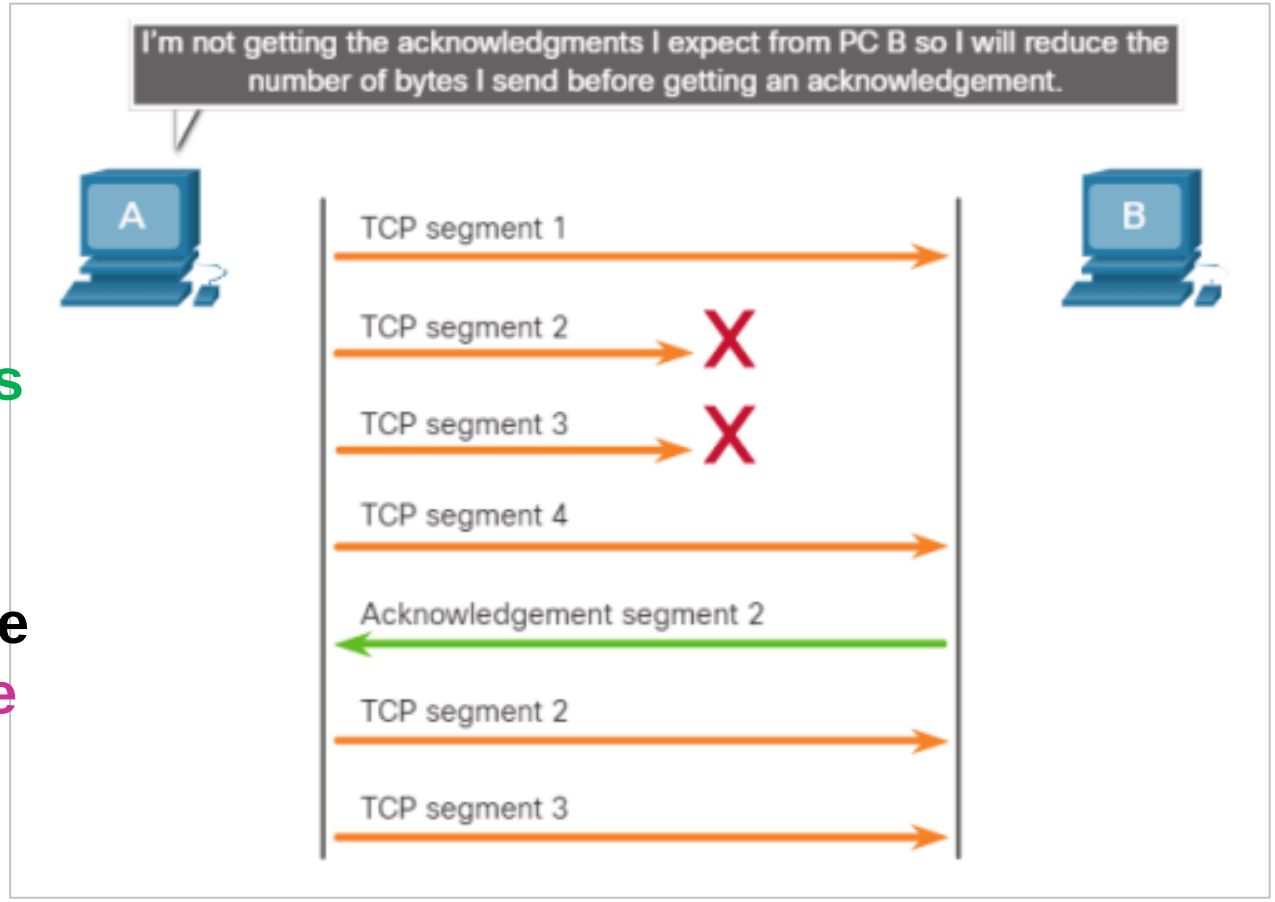
9.3.6 Contrôle de flux TCP - Taille maximale du segment (MSS)

- Un hôte détermine la valeur de son champ MSS en **soustrayant les en-têtes IP** et **TCP de la MTU Ethernet**.
- La **MTU par défaut** d'une interface Ethernet est de **1 500 octets**. En retranchant l'en-tête IPv4 de **20 octets** et l'en-tête TCP de **20 octets**, la taille par défaut du **MSS** sera de **1460 octets,** comme le montre la figure.



9.3.7 Contrôle de flux TCP - Prévention des encombrements

- Afin **d'éviter** et **de contrôler l'encombrement** du réseau, le protocole TCP utilise divers **mécanismes, minuteurs** et **algorithmes de gestion** des encombrements.
- Comme illustré dans la figure, PC A **détecte une congestion** et **réduit donc le nombre d'octets** qu'il envoie avant de recevoir un accusé de réception de PC B.



Fiabilité de couche transport

9.3.8 Travaux pratiques - Découvrir Nmap

- L'analyse des ports fait généralement partie d'une attaque de reconnaissance.
- Diverses méthodes d'analyse des ports peuvent être utilisées.
- Nous allons étudier comment se servir de l'utilitaire de Nmap. Nmap est un utilitaire réseau puissant qui est utilisé pour la découverte du réseau et pour l'audit de sécurité.

05

La couche transport

9.4 Récapitulation de la couche de transport

9.4.1 Qu'ai-je appris dans ce module ?

- La **couche transport** est la **liaison** entre la couche application et les couches inférieures du modèle OSI qui sont **responsables de la transmission du réseau**.
- La **couche transport** comprend à la fois les **protocoles TCP et UDP**. Les protocoles de couche de transport spécifient comment transférer des messages entre les hôtes et sont responsables de la **gestion des exigences de fiabilité d'une conversation**.
- La **couche de transport** est responsable du **suivi des conversations** (sessions), de la **segmentation des données** et de la **réassemblage des segments**, **de l'ajout d'informations d'en-tête, de l'identification des applications et du multiplexage** des conversations.
- Le **protocole TCP** est **dynamique** et **fiable.** Il accuse la réception des données, **renvoie les données perdues**, fournit les données dans un **ordre séquentiel**. Le protocole TCP est utilisé pour le courrier électronique et le Web.
- Le **protocole UDP** est **sans état et rapide**. Il a une faible surcharge, **ne nécessite pas d'accusé de réception, ne renvoie pas les données perdues** et livre les données dans **l'ordre où elles arrivent**. Le protocole UDP est utilisé pour **VoIP et DNS**.

Qu'est ce que j'ai appris dans ce Module? (suite)

- Les **protocoles de couches de transport TCP et UDP** utilisent des **numéros de port** pour **gérer plusieurs conversations simultanées**. C'est pourquoi les champs d'en-tête TCP et UDP identifient un **numéro de port** d'application **source et de destination**.
- La **connexion en trois étapes** vérifie que le périphérique de destination est bien présent sur le réseau. Elle s'assure que le périphérique de destination a **un service actif** et qu'il **accepte les requêtes sur le numéro de port de destination** que le client qui démarre la session a l'intention d'utiliser.
- Pour que le message original soit compris par le destinataire, toutes les données doivent être reçues et les données de ces segments doivent être **réassemblées dans l'ordre original.**
- Aujourd'hui, les systèmes d'exploitation hôtes utilisent généralement une fonctionnalité TCP facultative appelée **reconnaissance sélective (SACK),** négociée au cours de la connexion en trois étapes.
- 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.

Securité Réseau

Module 3

01 Protocoles réseau

02 Ethernet et Protocole IP

03 Vérification de la connectivité

04 Protocole ARP

05 La couche de transport

06 Services réseau

07

08 Lap pratiques

Objectifs du module

Titre du module: Services réseau

Objectif du Module: Expliquer comment les services réseau rendent possibles les fonctionnalités réseau.

Titre du Rubrique	Objectif du Rubrique
DHCP	Expliquer comment les services DHCP assurent la fonctionnalité du réseau.
DNS	Expliquer comment les services DNS assurent la fonctionnalité du réseau.
NAT	Expliquer comment les services NAT assurent la fonctionnalité du réseau.
Services de transfert et de partage des fichiers	Expliquer comment les services de transfert des fichiers assurent la fonctionnalité du réseau.
Adresse e-mail	Expliquer comment les services de messagerie assurent la fonctionnalité du réseau.
HTTP	Expliquer comment les services HTTP assurent la fonctionnalité du réseau.

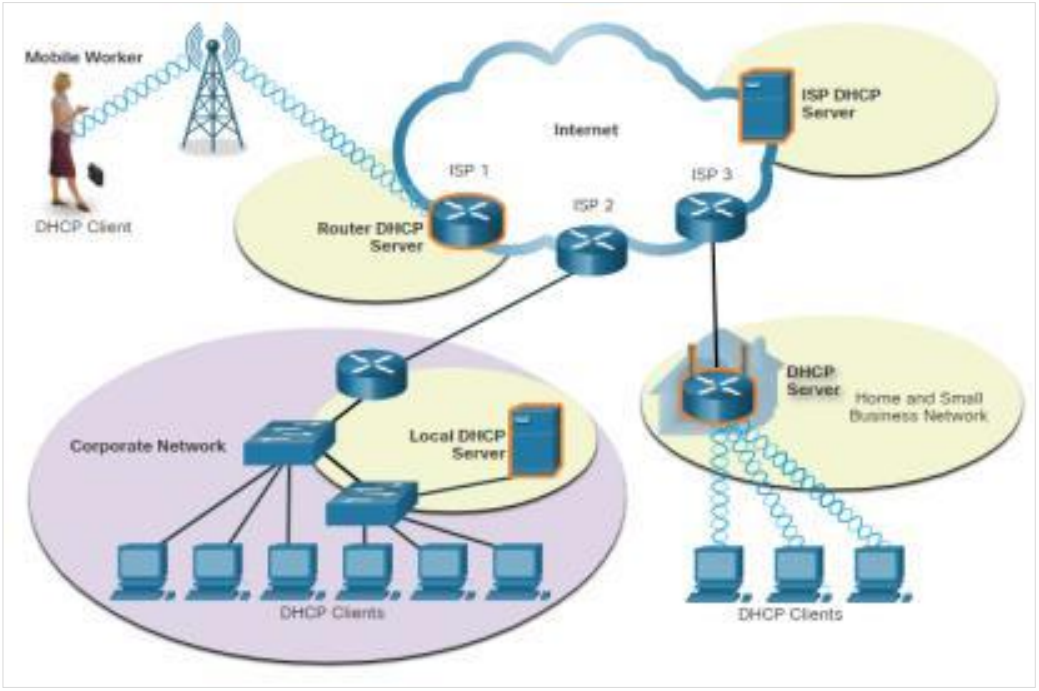
06

Les services réseaux

10.1 DHCP

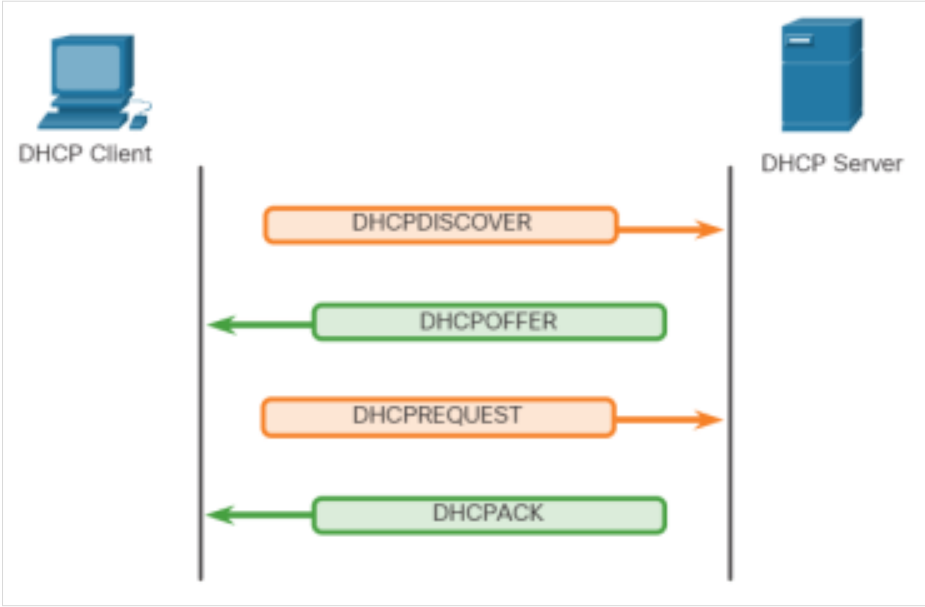
10.1.1 protocole DHCP (Dynamic Host Configuration Protocol)

- Deux types d'adressage:
  - **Dynamique** – Le protocole DHCP pour IPv4 automatise l'affectation des adresses IPv4, des masques de sous-réseau, des passerelles et d'autres paramètres réseau IPv4.
  - **Statique** - L'administrateur réseau saisit manuellement l'adresse IP sur les hôtes.



10.1.2 Fonctionnement du protocole DHCP

- L'opération **DHCP** inclut: DHCPDISCOVER, DHCPPOFFER, DHCPPREQUEST, DHCPACK et DHCPNAK.



Processus DHCP:

- Le **client** diffuse un message **DHCPDISCOVER** pour identifier les ***serveurs DHCP disponibles*** sur le réseau.
- Un **serveur DHCP** répond par un message **DHCPOFFER** , qui offre un bail au client.
- Le **client** envoie un message **DHCPREQUEST** qui identifie **explicitement le serveur** et l'offre de bail qu'il accepte.
- Si l'adresse IPv4, est toujours disponible, le serveur renvoie le message **DHCPACK** .
- Sinon, le serveur sélectionné répond par un message **DHCPNAK** .

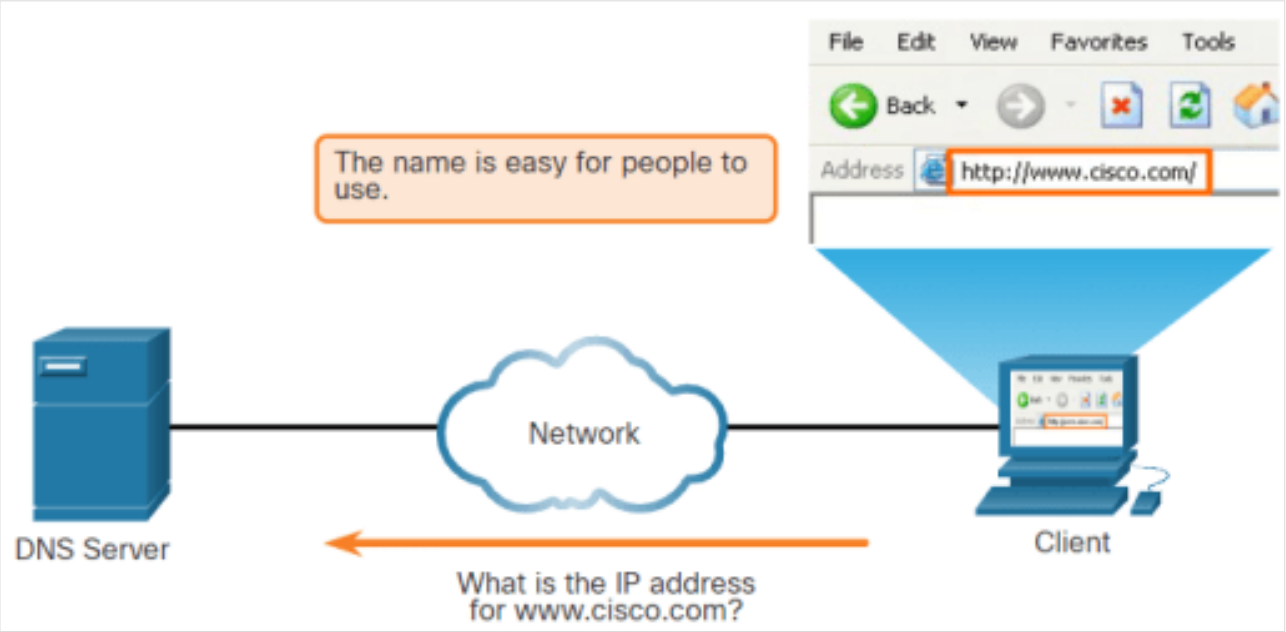
06

Les services réseaux

10.2 DNS

10.2.1 Présentation du protocole DNS

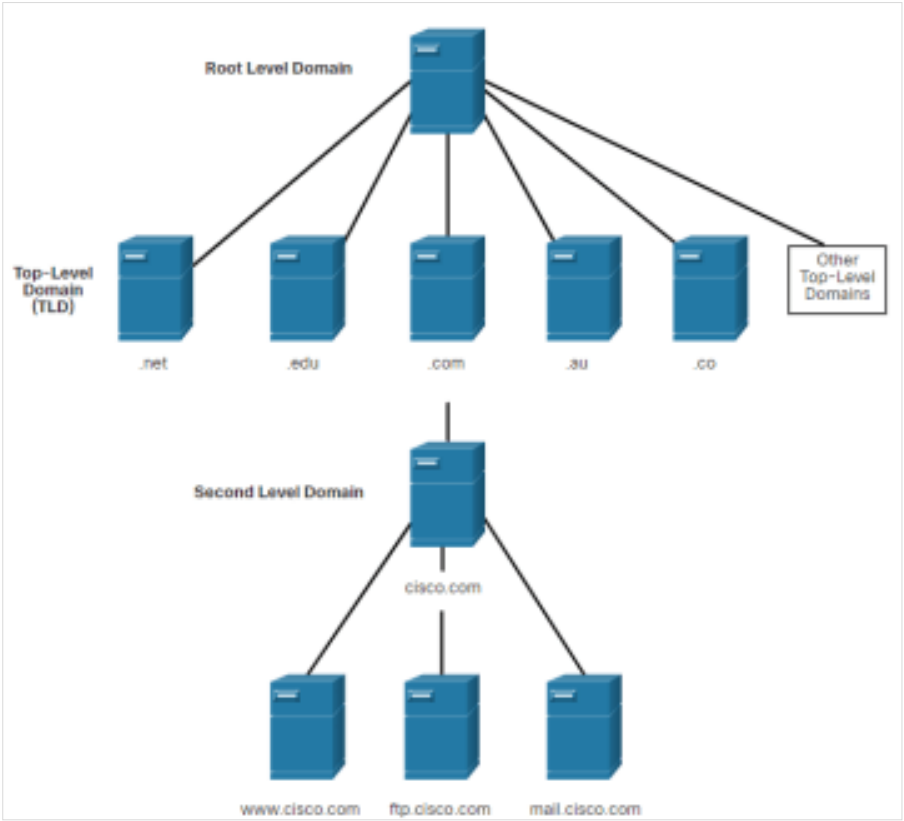
- Le système de **noms de domaine** (DNS) **gère** et **fournit** des noms de domaine et les **adresses IP associées**.
- L'ordinateur client dans la figure enverra une demande au serveur DNS pour obtenir l'adresse IP de www.cisco.com.
- Le **trafic DNS malveillant** peut être détecté **par l'analyse du protocole et l'inspection d**es informations de surveillance DNS.



Le service DNS traduit les **noms** en adresses **IP**

10.2.2 Hiérarchie de domaines DNS

- DNS se compose d'une hiérarchie de domaines génériques.
- Domaine premier niveau : .**net, .com, .edu, .au. bj**
- Les domaines de second niveau sont représentés par un **nom de domaine** suivi **d'un domaine de premier niveau**. Exemple: **cisco**.**com**
- Les **sous-domaines** composent le niveau suivant de la hiérarchie DNS et représentent en quelque sorte une **division des domaines de second niveau**. Exemple: **www.cisco.com**
- Un **quatrième niveau** peut représenter un **hôte dans un sous-domaine**.

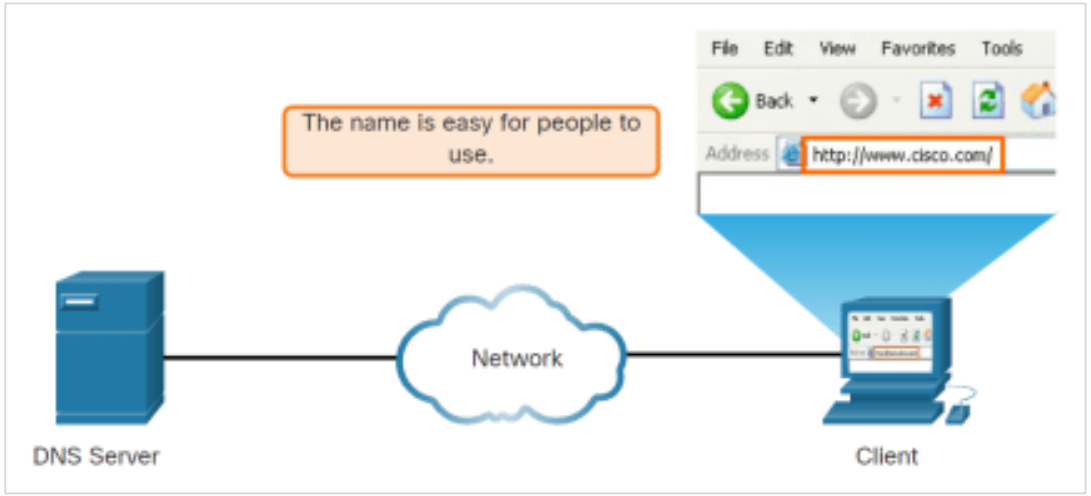


Hiérarchie DNS

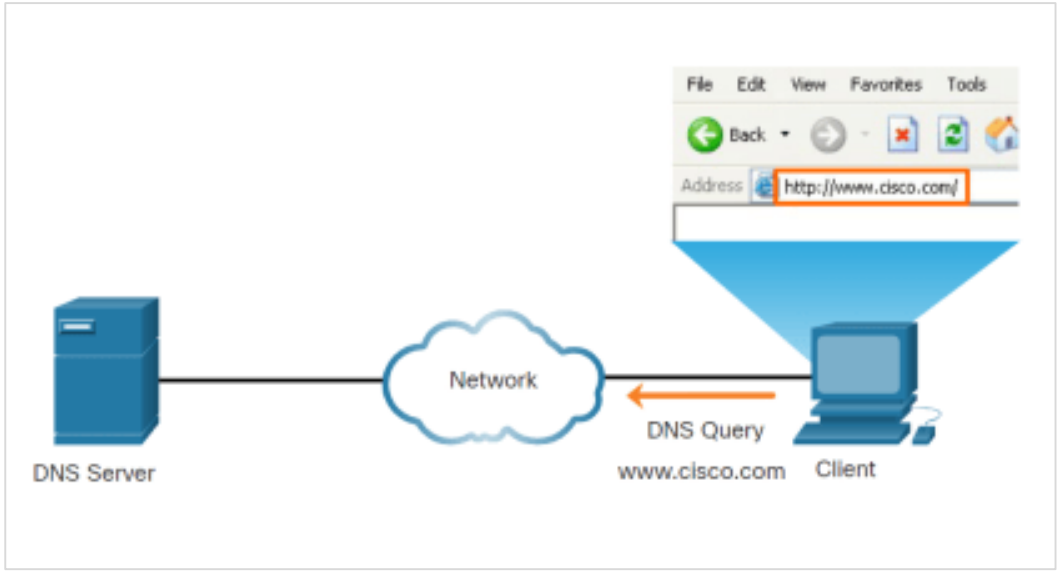
10.2.3 Le processus de recherche DNS

Étapes impliquées dans la résolution DNS:

Étape 1 - L'utilisateur saisit un URL (**FQDN)** dans un champ Adresse de l'application du navigateur.



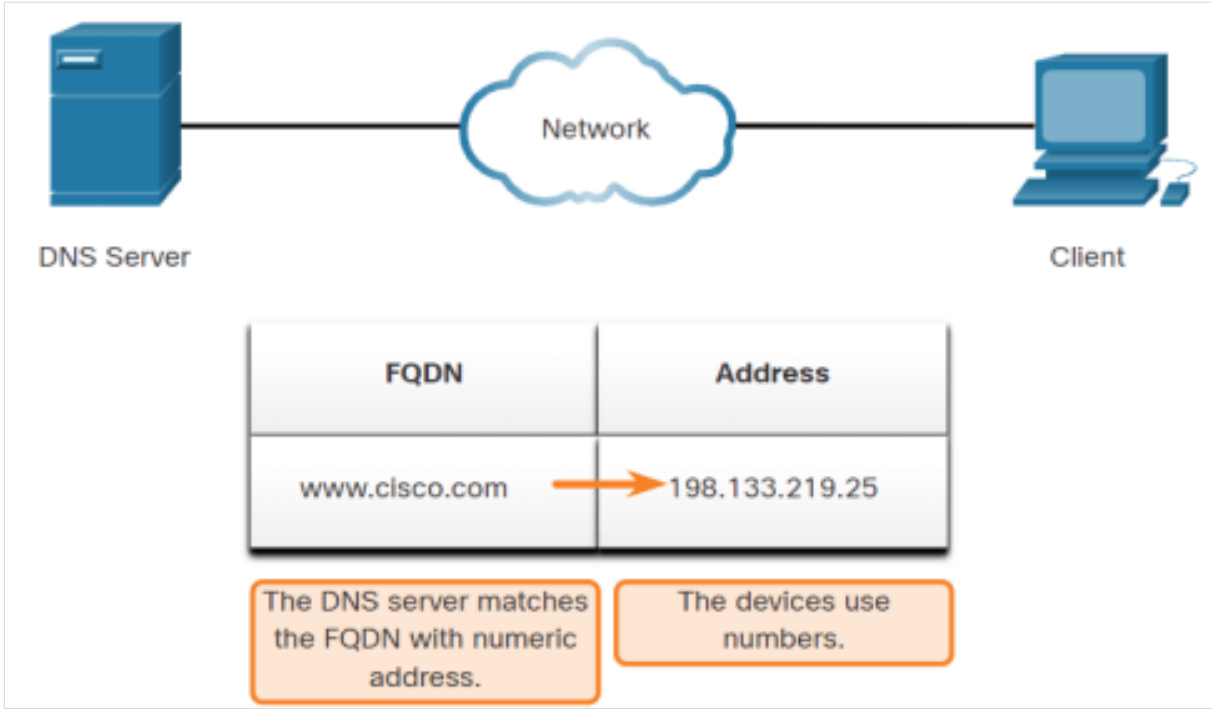
Étape 2 - Une **requête DNS** est envoyée au serveur DNS désigné pour **l'ordinateur client.**



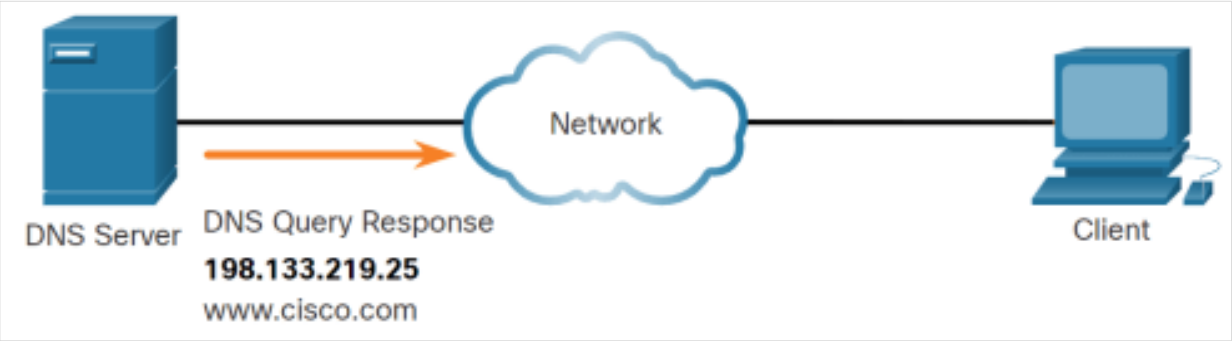
10.2.3 Le processus de recherche DNS

Étapes impliquées dans la résolution DNS:

Étape 3 - Le **serveur DNS** correspond au **URL** avec **son adresse IP**.



Étape 4 - La **réponse à la requête DNS** est renvoyée au client avec l'adresse IP du FQDN.

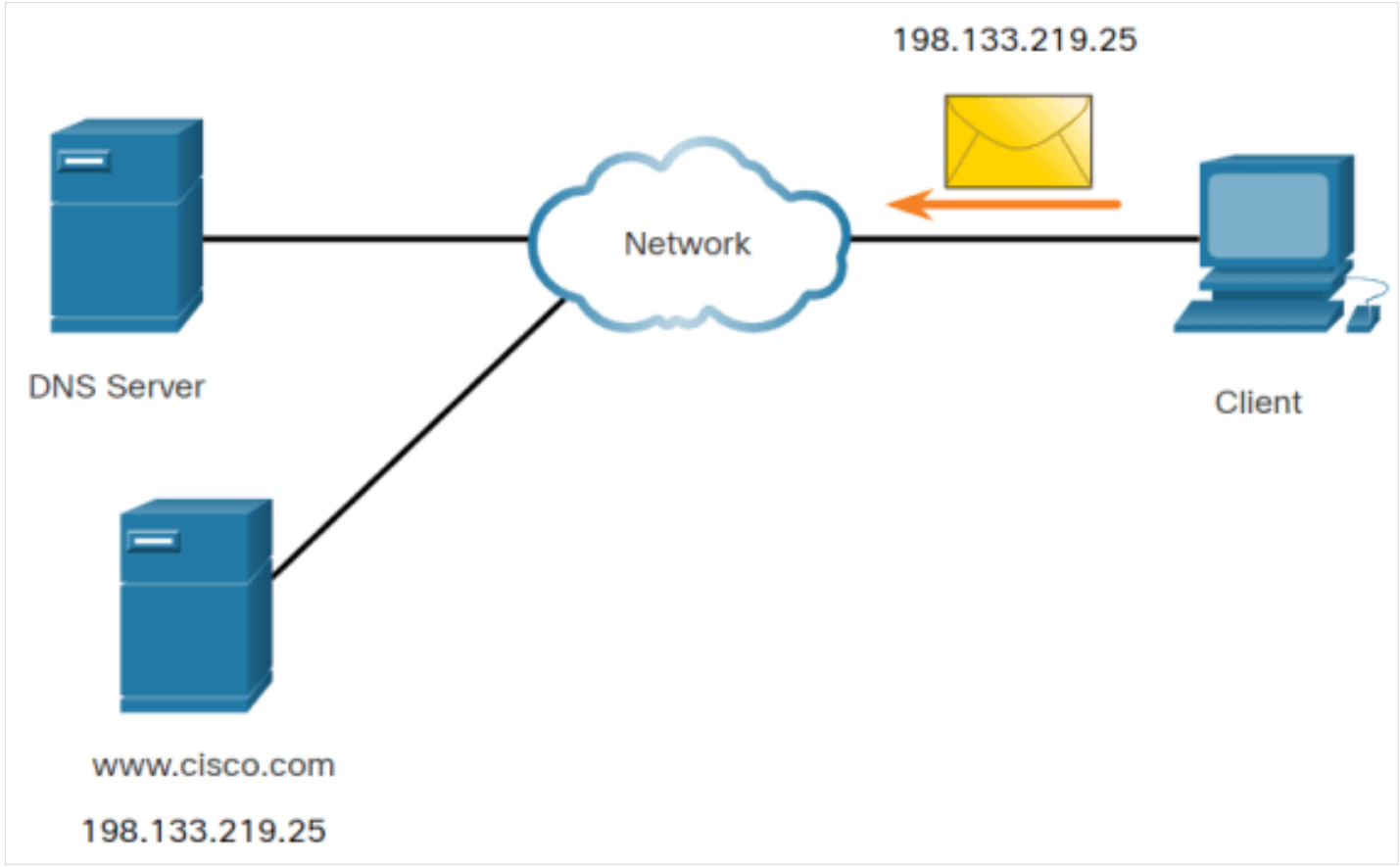


DNS

10.2.3 Le processus de recherche DNS

Étapes impliquées dans la résolution DNS:

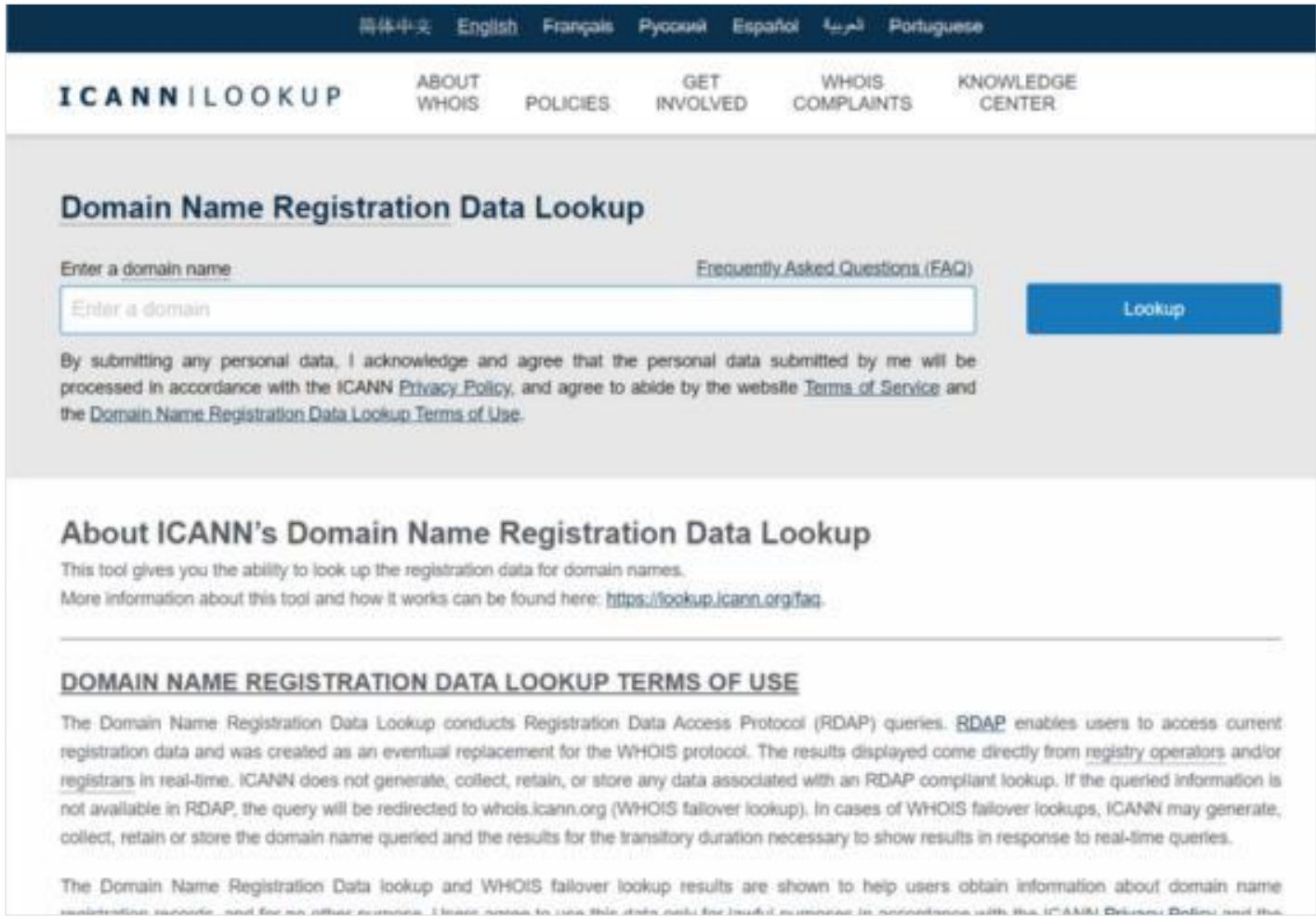
Étape 5 - Le serveur DNS correspond au **FQDN** avec son adresse IP.



10.2.7 Travaux pratiques - Utilisation de Wireshark pour examiner une capture DNS UDP

10.2.6 Le protocole WHOIS

- **WHOIS** est un **protocole basé sur TCP** qui est utilisé pour **identifier les propriétaires de domaines Internet** dans le système DNS.
- **WHOIS** reste un bon point de départ pour **identifier les sites Internet potentiellement dangereux** qui pourraient avoir été consultés via le réseau.
- Recherche ICANN un **outil WHOIS** basé sur Internet, est utilisé pour obtenir l'enregistrement une URL.



DNS

10.2.7 Travaux pratiques - Utilisation de Wireshark pour examiner une capture DNS UDP

- Au cours de ces travaux pratiques, vous aborderez les points suivants:
  - Communiquerez avec un serveur DNS en envoyant une requête DNS à l'aide du protocole de transport UDP.
  - Vous utiliserez Wireshark pour examiner les échanges de requêtes et de réponses DNS avec le même serveur.

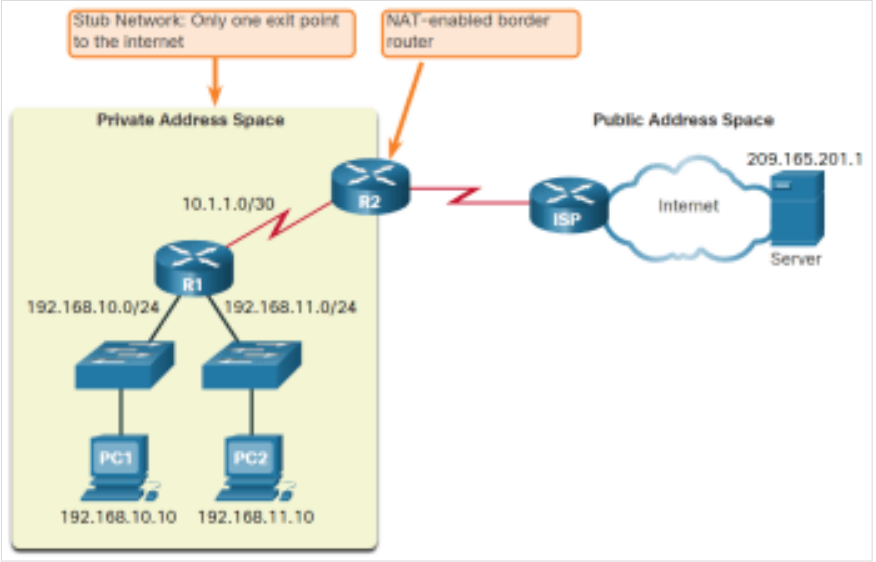
06

Les services réseaux

10.3 NAT

10.3.1 Qu'est-ce que la fonction NAT ?

- L'utilisation de NAT consiste à **limiter la consommation des adresses IPv4 publiques**.
- La traduction d'adresse réseau **(NAT**) assure la **traduction des adresses privées** en **adresses publiques**.
- Un **routeur NAT** fonctionne généralement à la périphérie d'un réseau d'extrémité

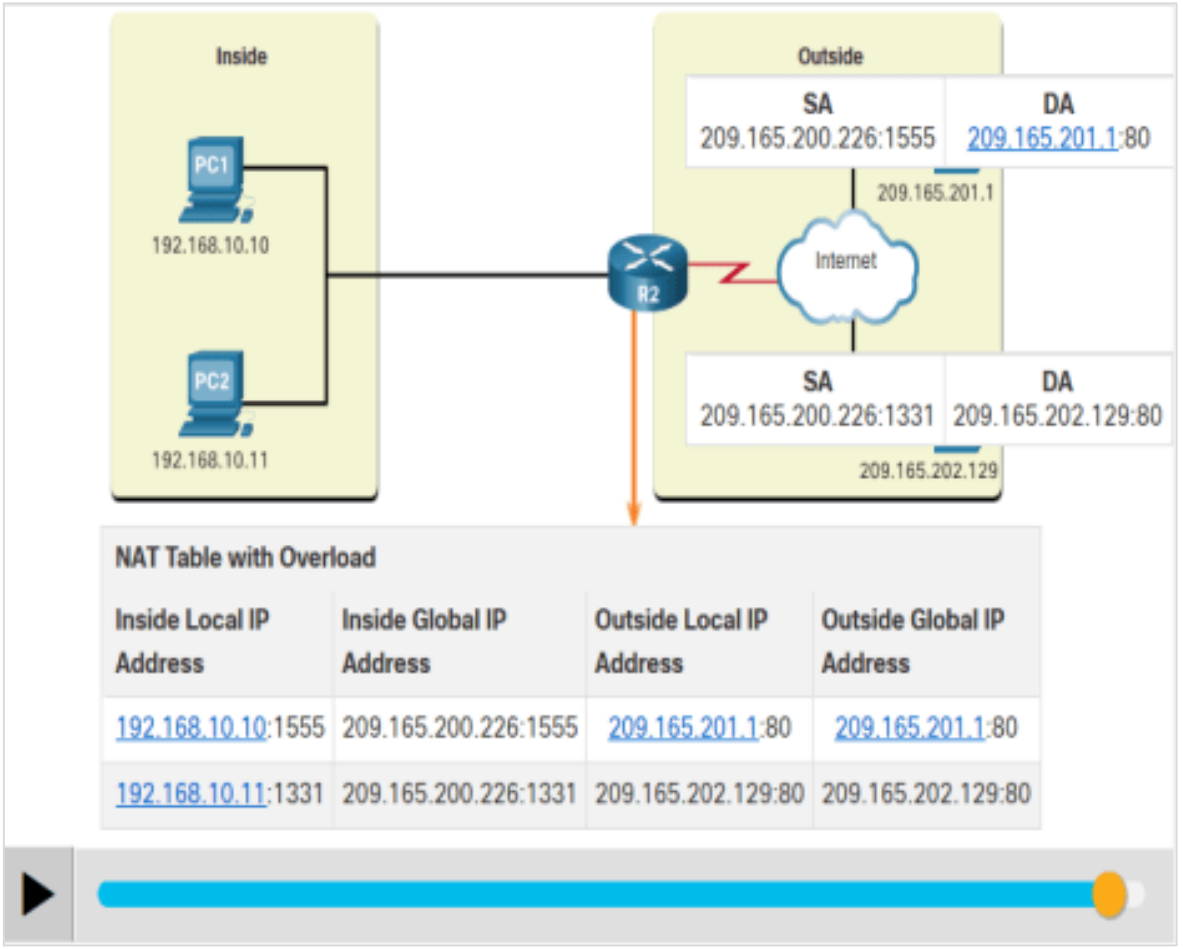


***Remarque**: La connexion au FAI peut utiliser une adresse privée ou une adresse publique qui est partagée parmi les clients. Pour les besoins de ce module, une adresse publique est représentée.*

10.3.4 Port Address Translation (PAT)

- La **traduction d'adresses de port** (PAT), également appelée **surcharge NAT**, mappe **plusieurs adresses IPv4 privées** à **une seule adresse IPv4 publique unique** ou à **quelques adresses.**
- La **fonction PAT** ajoute des **numéros de port source uniques** à l'adresse globale interne, de façon à permettre de **distinguer les traductions**.

Cliquez sur Lecture dans la figure pour voir une animation du processus PAT.



06

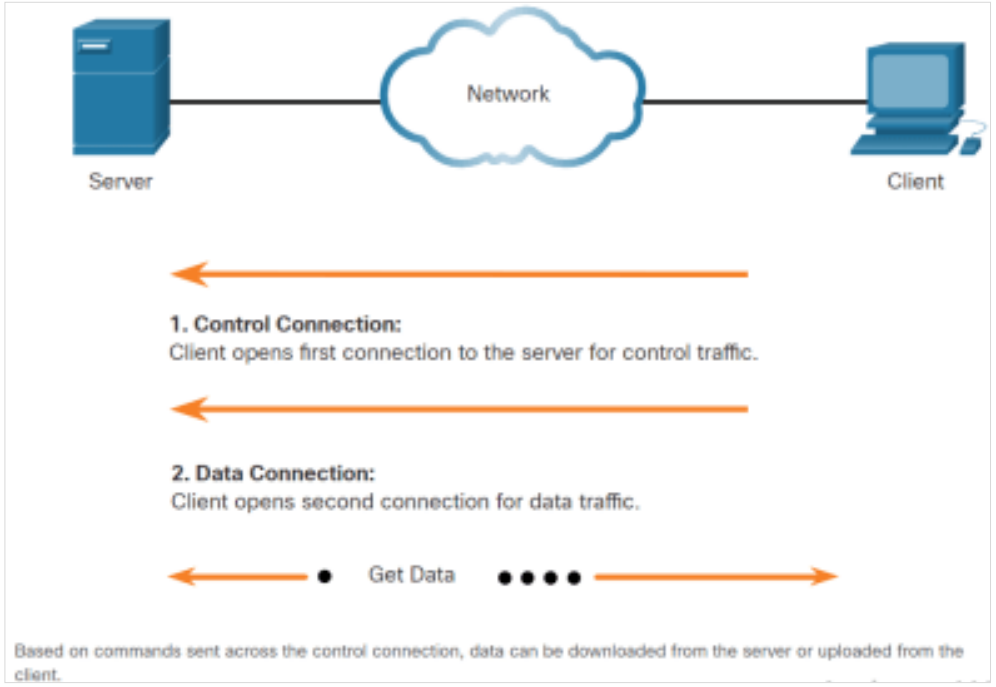
Les services réseaux

10.4 Les services de transfert et de partage des fichiers

10.4.1 FTP et TFTP

Différence entre FTP et TFTP

- Le **protocole FTP** permet de **transférer des données** entre un **client** et un **serveur**.
- FTP sert à **envoyer** et à **extraire** des données d'un serveur FTP.
- **FTP** nécessite deux connexions entre le client et le serveur.
  - **Connexion de contrôle (21)**: le client établit une première connexion au serveur pour **contrôler le trafic**.
  - **Connexion de données (20)**: le client établit une seconde connexion pour le trafic de **données.**
- **TFTP** est un protocole de **transfert de fichiers simplifié** qui utilise le numéro de port **UDP réservé 69.**



Services de transfert et de partage des fichiers

Travaux pratiques - Utilisation de Wireshark pour l'examen de captures TCP et UDP

- Au cours de ces travaux pratiques, vous aborderez les points suivants:
    - Identifier les champs d'en-tête TCP ainsi que les opérations TCP à l'aide de la capture de session FTP de Wireshark
    - Identifier les champs d'en-tête UDP ainsi que les opérations UDP à l'aide de la capture de session TFTP de Wireshark

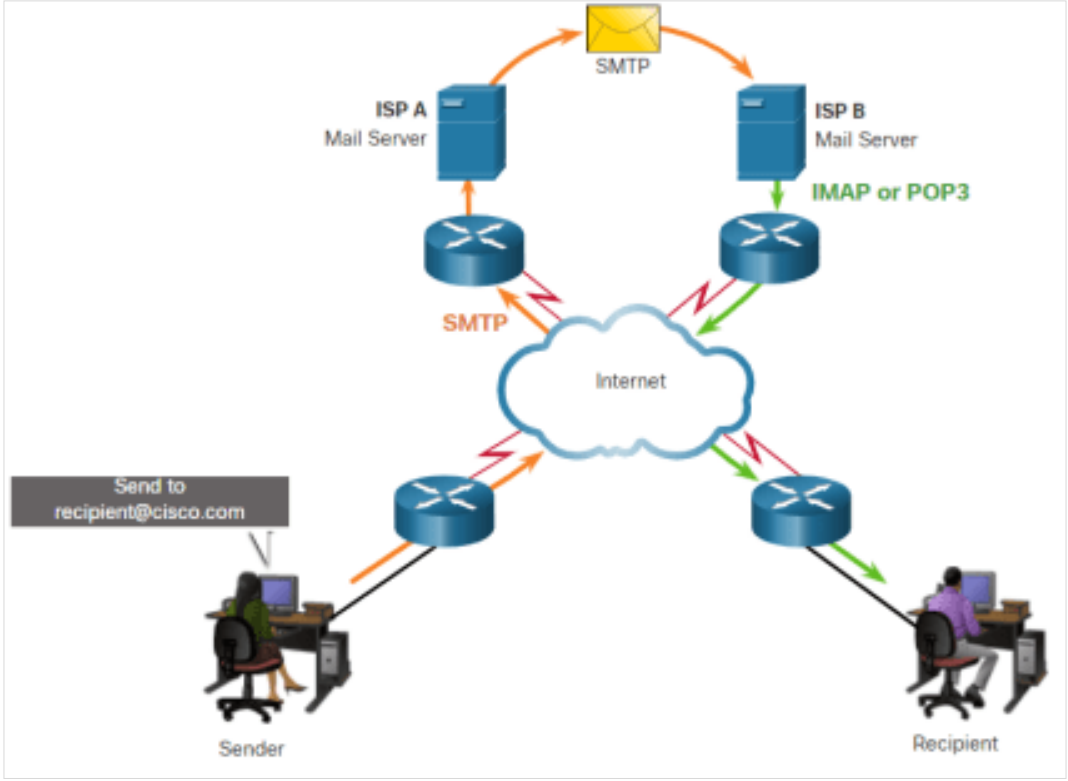
06

Les services réseaux

10.5 Les e-mails

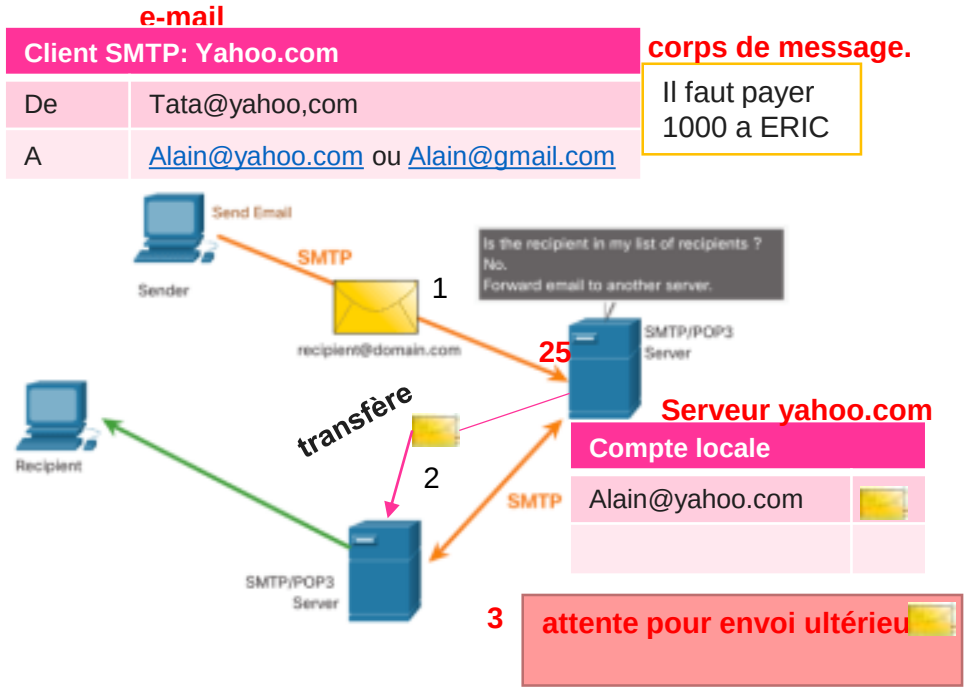
10.5.1 Protocoles de messagerie

- 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 e-mails font appel à trois protocoles distincts : **SMTP** (Simple Mail Transfer Protocol), **POP** (Post Office Protocol) et **IMAP** (Internet Message Access Protocol).



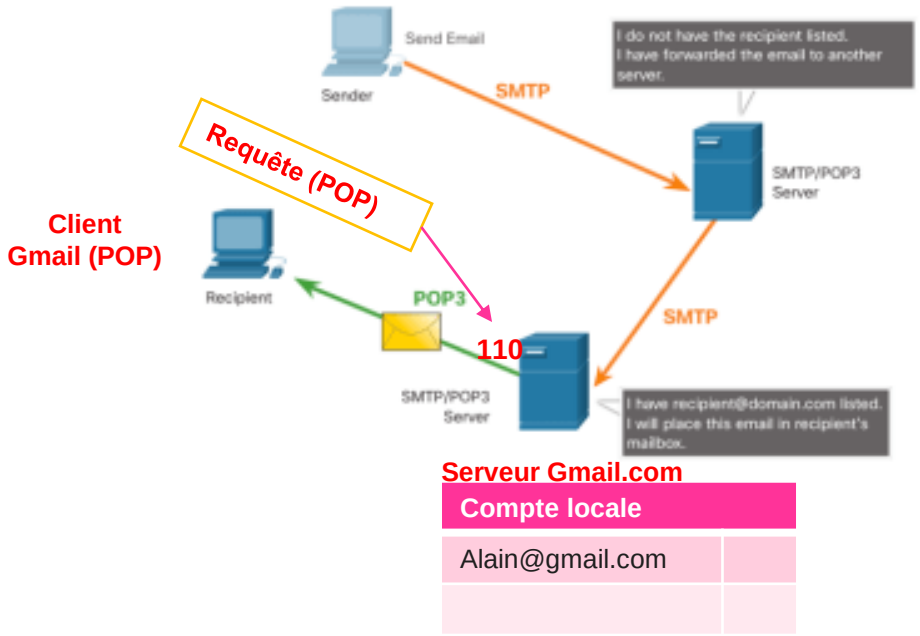
E-mail
10.5.2 SMTP

- Lorsqu'un **client** envoie un **e-mail**, le processus **SMTP client** se connecte à un processus **SMTP serveur** sur le port **réservé 25.**
- 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.
- 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.



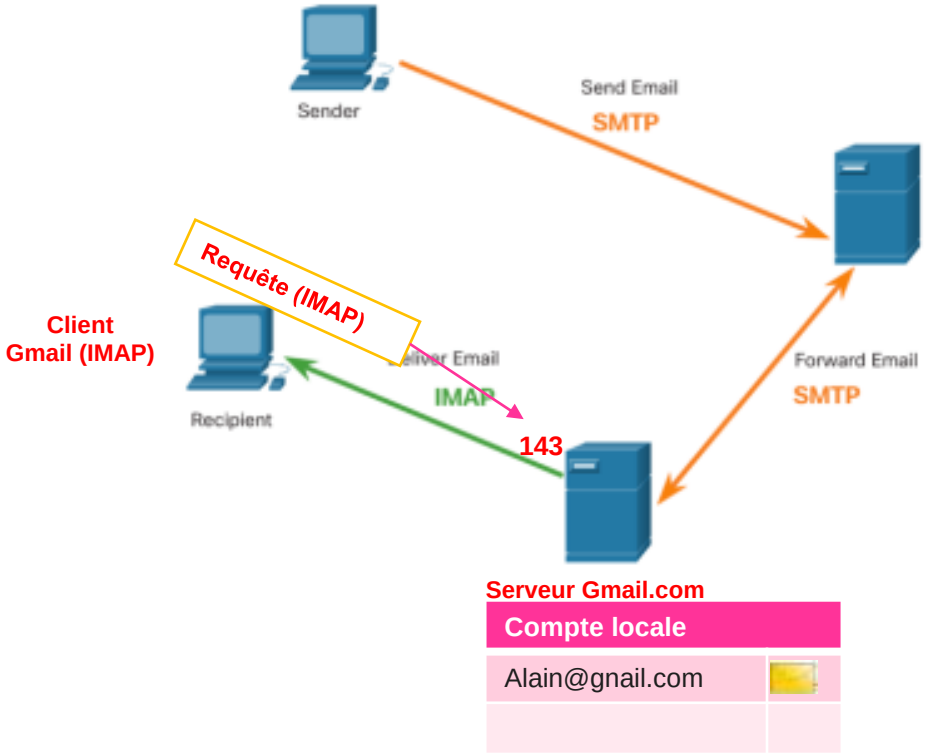
10.5.3 POP3

- Le protocole POP3 permet à une application de **récupérer des e-mails** à partir d'un serveur de messagerie.
- En utilisant POP3, l'e-mail est **téléchargé** sur le client et **est supprimé** du serveur
- Le serveur démarre le service POP3 en écoutant passivement les éventuelles requêtes de connexion client sur le **port TCP 110**.



Adresse e-mail
10.5.4 IMAP

- Le protocole de messagerie IMAP (Internet Message Access Protocol) décrit une autre méthode de **récupération des messages** électroniques.
- Lorsque l'utilisateur se connecte à un serveur IMAP, des copies des **messages sont téléchargées** vers l'application client. Les messages originaux sont **conservés sur le serveur** jusqu'à ce qu'ils soient supprimés manuellement.



06

Les services réseaux

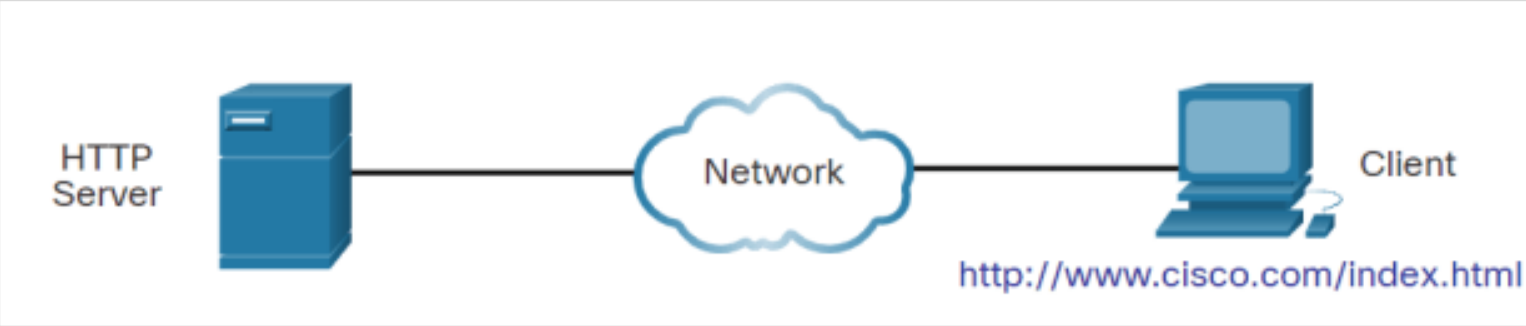
10.6 HTTP

10.6.1 HTTP et HTML

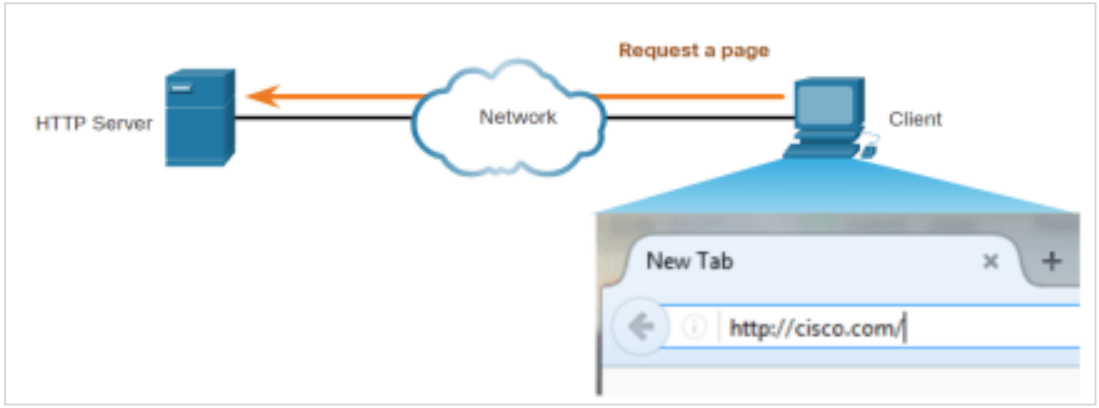
- Jetez un oeil sur la façon dont une page Web est ouverte dans un navigateur.
  Exemple: http://www.cisco.com/index.html

Etape 1: Le navigateur commence par interpréter les trois parties de l'adresse URL :

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

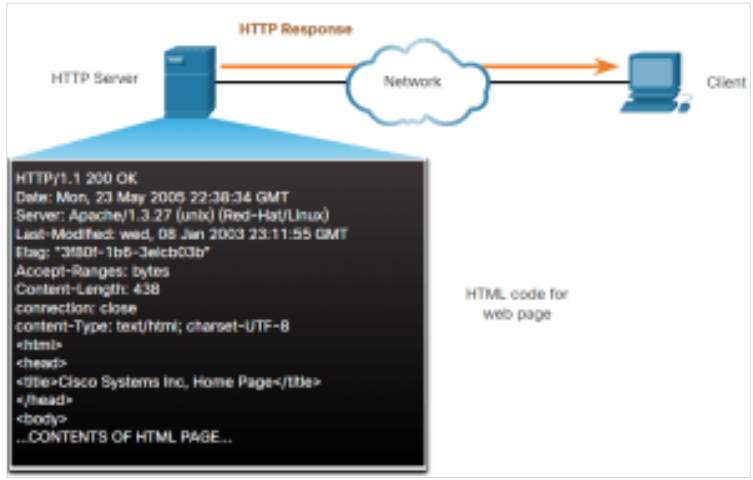


10.6.2 HTTP et HTML (suite)



- **Étape 2:** Le **client** initie une **requête HTTP** à un serveur en envoyant une **requête GET** au serveur et demande le fichier **index.html.**

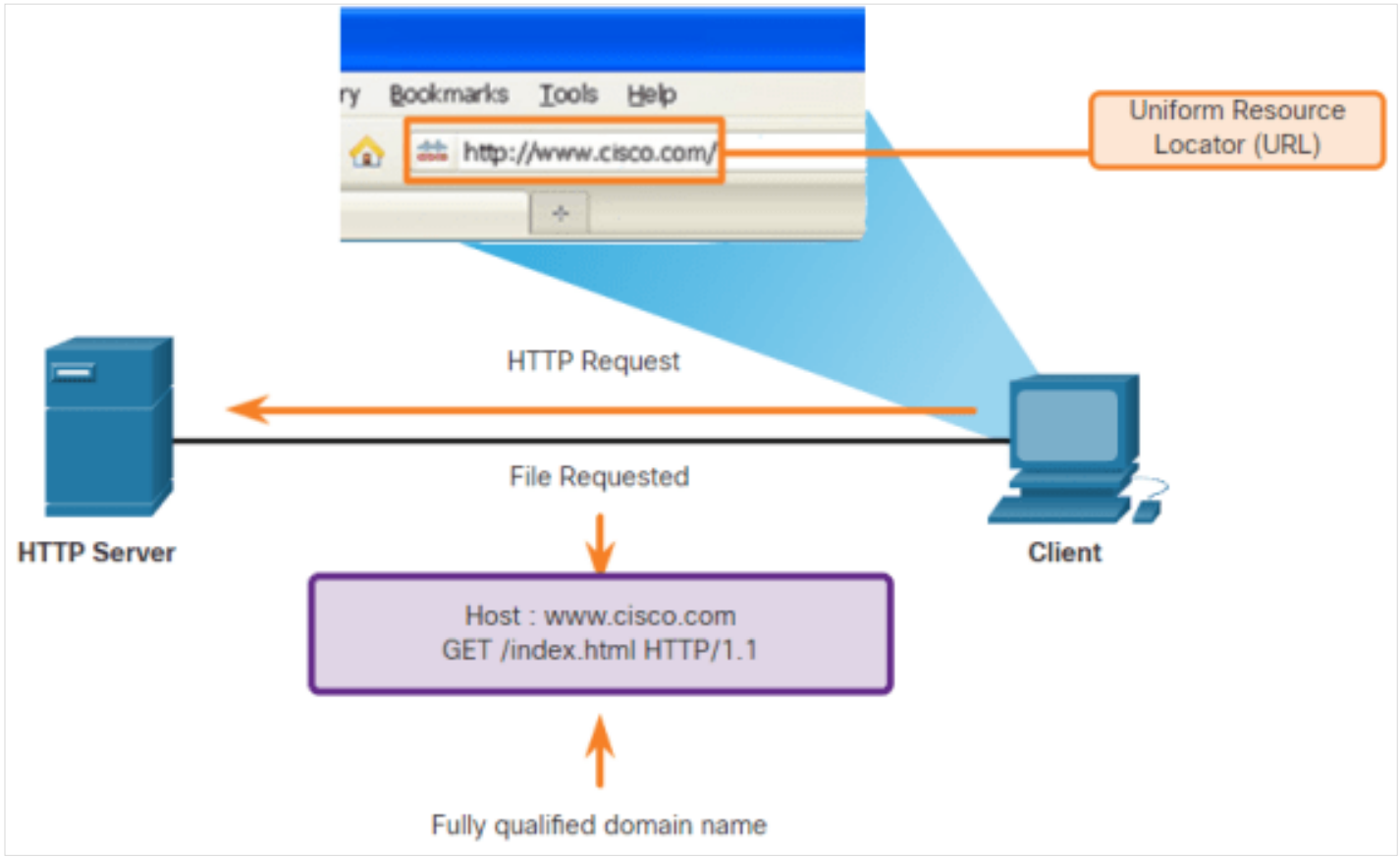
- **Étape 3:** En **réponse** à la demande, le serveur envoie le **code HTML** de cette page Web au navigateur.



- **Étape 4:** Le navigateur **déchiffre le code HTML** et met en forme la page pour la fenêtre du navigateur.

10.6.3 Opération HTTP

- **HTTP** est un protocole de **requête/réponse** qui utilise le port TCP **80**. Il est flexible mais **n'est pas un protocole sécurisé**.
- Lorsqu'un client envoie une requête à un serveur web, il utilise l'une **des six méthodes** spécifiées par le protocole HTTP:
  - GET
  - POST
  - PUT
  - DELETE
  - OPTIONS
  - CONNECT



10.6.7 Travaux Pratiques – Utiliser Wireshark pour examiner le trafic HTTP et HTTPS

10.6.4 Codes d'état HTTP

- Les **codes de l'état HTTP** sont composés de **caractères numériques**.
- Le **premier nombre** indique le **type du message**.
- Les **cinq groupes de codes d'état** sont **1xx** - Informational, **2xx** - Success, **3xx** - Redirection, **4xx** - Client Error et **5xx** - Server Error
- Le tableau ci-dessous explique certains codes d'état courants:

Code	État	Signification
1xx - Informations		
100	Continuer	Le client doit continuer avec la requête. Le serveur a vérifié que cette requête peut être satisfaite.
2xx - Succès		
200	OK	La requête a abouti.
202	Accepté	La requête a été acceptée, mais son traitement n'est pas terminé.

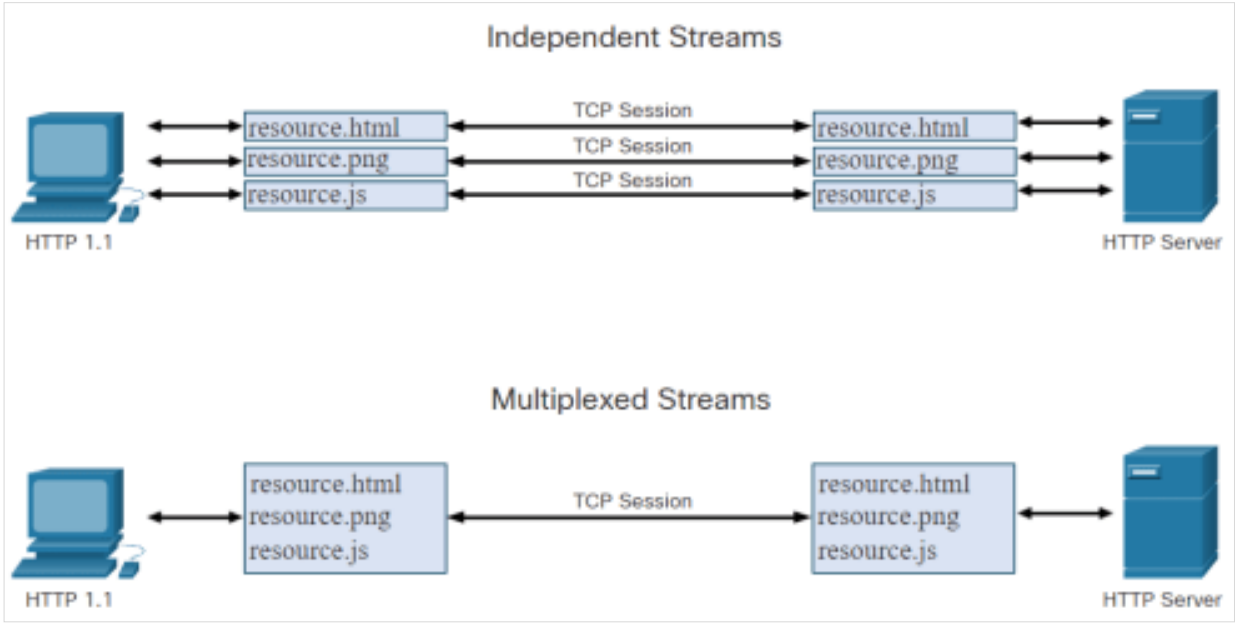
10.6.4 Codes d'état HTTP (Suite)

Code	État	Signification
4xx – Erreur du client		
403	Interdit	La demande est comprise par le serveur, mais la ressource ne sera pas remplie. Cela est peut-être dû au fait que le demandeur n'est pas autorisé à afficher la ressource.
404	Introuvable	Le serveur ne trouve pas la ressource demandée. Cela peut être dû à une URL obsolète ou incorrecte.

10.6.7 Travaux Pratiques – Utiliser Wireshark pour examiner le trafic HTTP et HTTPS

10.6.5 HTTP/2

- Le **but de HTTP/2** est **d'améliorer les performances HTTP** en traitant les problèmes de latence qui existaient dans la **version HTTP 1.1** du protocole.
- **HTTP/2** utilise le même format d'en-tête que **HTTP 1.1** et utilise **les mêmes codes d'état.**
- Il existe de nombreuses fonctionnalités importantes à **HTTP/2 qu'un analyste de la cybersécurité** doit connaître:
  - Multiplexage
  - Serveur PUSH
  - Un protocole binaire
  - Compression de l'en-tête



10.6.7 Travaux Pratiques – Utiliser Wireshark pour examiner le trafic HTTP et HTTPS

10.6.6 HTTP sécurisé (HTTPS)

- Pour une communication sécurisée via l'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 requête client-réponse serveur qu'HTTP, mais le flux de données est chiffré à l'aide du **protocole SSL** (Secure Socket Layer) ou **TLS** (Transport Layer Security) avant d'être acheminé via le réseau.
- **HTTPS/2** est spécifié pour utiliser **HTTPS sur TLS** avec **l'extension ALPN** (Application-Layer Protocol Negotiation) pour TLS 1.2 ou version ultérieure

10.6.7 Travaux Pratiques – Utiliser Wireshark pour examiner le trafic HTTP et HTTPS

HTTP

10.6.7 Travaux Pratiques – Utiliser Wireshark pour examiner le trafic HTTP et HTTPS

- Au cours de ces travaux pratiques, vous aborderez les points suivants:
    - Capture et affichage du trafic HTTP
    - Capture et affichage du trafic HTTPS

06

Les services réseaux

10.7 Récapitulation des services réseau

Récapitulation des services réseau

10.7.1 Qu'est-ce que j'ai appris dans ce module?

- Le protocole DHCP pour IPv4 automatise l'affectation des adresses IPv4. Le contraire de l'adressage dynamique est l'adressage statique.
- L'opération DHCP inclut: DHCPDISCOVER, DHCPPOFFER, DHCPPREQUEST, DHCPACK et DHCPNAK.
- Le service DNS traduit les noms en adresses IP Il y a cinq étapes impliquées dans la résolution DNS.
- La traduction d'adresse réseau (NAT) assure la traduction des adresses privées en adresses publiques. Un routeur NAT fonctionne généralement à la périphérie d'un réseau d'extrémité.
- La traduction d'adresses de port (PAT), également appelée surcharge NAT, mappe plusieurs adresses IPv4 privées à une seule adresse IPv4 publique unique ou à quelques adresses.
- Il a été développé en vue de permettre le transfert de fichiers entre un client et un serveur.TFTP est un protocole de transfert de fichiers simplifié qui utilise le numéro de port UDP réservé 69.

10.7.2 Qu'est-ce que j'ai appris dans ce module?

- Les clients de messagerie communiquent avec les serveurs de messagerie pour envoyer et recevoir des messages.
- Le courrier électronique prend en charge trois protocoles distincts pour fonctionner : SMTP, POP et IMAP.
- Les navigateurs Web et les serveurs Web interagissent en suivant les quatre étapes.
- HTTP est un protocole de requête-réponse qui utilise le port TCP 80.
- Lorsqu'un client, généralement un navigateur web, envoie une requête à un serveur web, il utilise l'une des six méthodes spécifiées par le protocole HTTP: GET, POST, PUT, DELETE, OPTIONS et CONNECT.
- Codes d'état HTTP: 1xx, 2xx, 3xx, 4xx et 5xx.
- 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.

Merci