

Chapitre 5- 10 : Protocoles et services réseau

BENJAMIN
DESROSIERS-BOSSÉ
2023

Chapitre 5- 10 - Sections et objectifs

 Protocoles réseau



Ethernet et protocole IP



Vérification de la connectivité



Protocole de résolution d'adresse



La couche transport

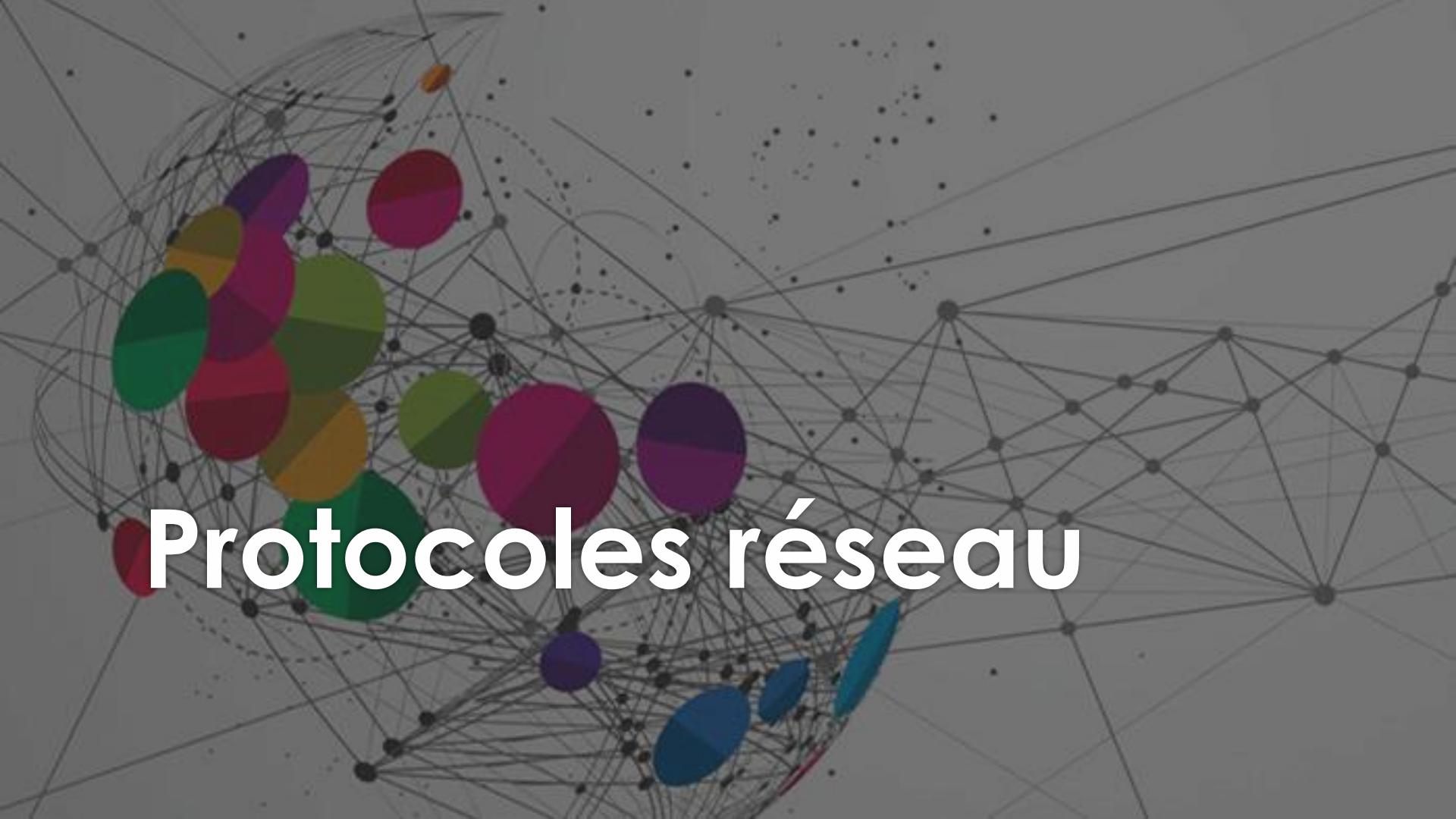


Services réseau



- J'ai besoin de votre participation spécifiquement aujourd'hui! Cela me permettra d'évaluer si vous maîtrisez les concepts du CCNA!

Protocoles réseau



Processus de communications réseau

Vues du réseau

- Vues du réseau
 - Petit réseau domestique
 - SOHO (petites entreprises ou bureaux à domicile)
 - Moyens et grands réseaux
 - Réseaux mondiaux



Processus de communication du réseau

Une session type : étudiant

- 
- A photograph showing five teenagers (three girls and two boys) sitting on a light-colored couch. They are all looking down at their smartphones, which are held horizontally. The background is a plain, light-colored wall.
- Une session type : étudiant
 - Déterminer l'origine du trafic entrant dans le réseau.
 - Par exemple, les données de Terry voyagent avec les données de milliers d'autres utilisateurs sur un réseau à fibre optique qui connecte le fournisseur d'accès à Internet (FAI) de Terry à plusieurs autres FAI, y compris celui qui est utilisé par la société du moteur de recherche. Finalement, la chaîne de recherche de Terry accède au site web de la société du moteur de recherche et est traitée par ses puissants serveurs. Les résultats sont ensuite codés et renvoyés sur le réseau du lycée de Terry et sur son téléphone.

Processus de communication du réseau

Une session type : gamer

- Une session type : gamer
 - Déterminer l'origine du trafic entrant dans le réseau.
 - À l'instar de nombreux réseaux domestiques, le réseau de Michelle se connecte à un FAI à l'aide d'un routeur et d'un modem. Ces appareils permettent au réseau domestique de Michelle de se connecter à un réseau de télévision par câble qui appartient au fournisseur d'accès à Internet de Michelle. Les fils du câble de l'ensemble du quartier de Michelle se connectent tous à un point central sur un poteau téléphonique, puis à un réseau à fibre optique. Ce réseau à fibre optique relie plusieurs quartiers qui sont desservis par le FAI de Michelle.



Processus de communication du réseau

Une session type : chirurgien

- Une session type : chirurgien
 - Déterminer l'origine du trafic entrant dans le réseau
 - Dr. Ismael Awad est un oncologue qui opère des patients atteints de cancer. Il est souvent amené à consulter des radiologues et d'autres spécialistes au sujet de ses patients. L'hôpital dans lequel travaille le docteur Awad est abonné à un service spécial appelé un « cloud ». Le cloud permet de stocker les données médicales, y compris les résultats d'IRM et de radio des patients, dans un espace central accessible via Internet.



Protocoles de communication

Que sont les protocoles ?

- Protocole – Règles de communication
 - Les protocoles réseau permettent aux ordinateurs de communiquer sur les réseaux.
 - Les protocoles réseau définissent les paramètres de codage, de formatage, d'encapsulation, de taille, de temporisation et de distribution des messages.

Avez-vous un exemple de ces composantes dans la vraie vie?



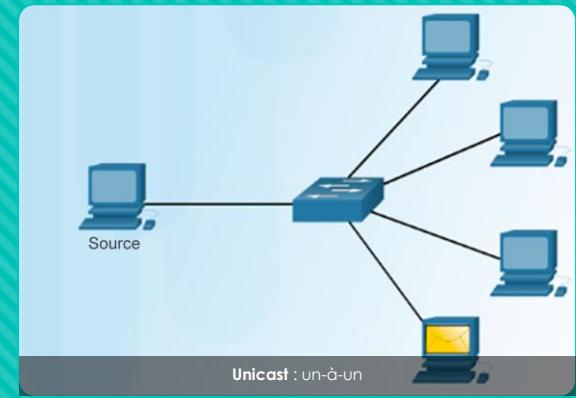
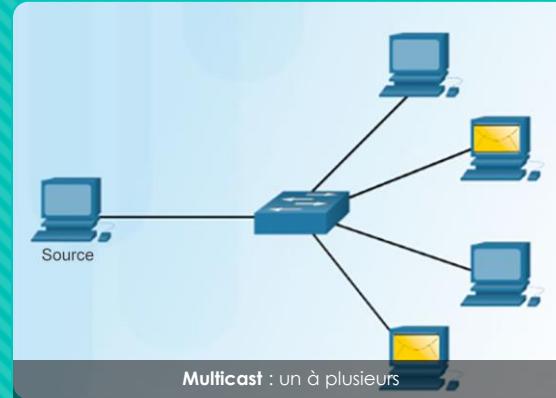
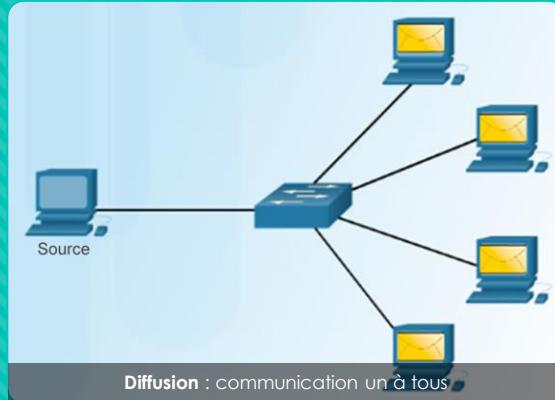
Protocoles de communication

Format, taille et temporisation

- **Format**
 - **Encapsulation** : processus consistant à placer un format de message à l'intérieur d'un autre.
 - **Décapsulation** : processus inverse à l'encapsulation.
- **Taille** : le message est divisé en plusieurs trames à l'envoi, puis recomposé conformément au message d'origine à la réception.
- **Temporisation** : inclut la méthode d'accès, le contrôle de flux et le délai de réponse.

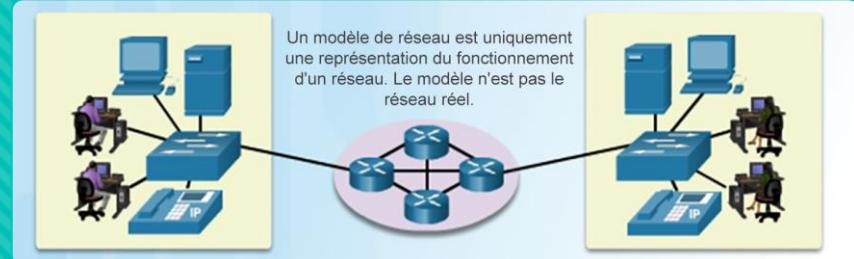
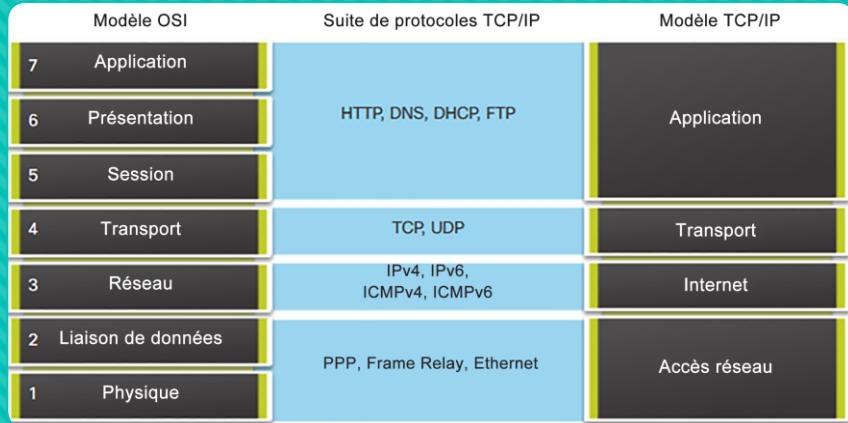


Quels problèmes ces fonctions préviennent?



Protocoles de communication Monodiffusion, multidiffusion et diffusion

À quelle couche retrouve-ton le plus de diffusion?



Protocoles de communication Modèles de référence

Protocoles de communication

Trois adresses

- Trois adresses importantes :
 - Adresse de protocole
 - Adresse d'hôte de réseau
 - Adresse physique

L'adressage est utilisé par le client pour envoyer des requêtes et d'autres données à un serveur. Le serveur utilise l'adresse du client pour renvoyer les données demandées au client qui a émis la requête.



Protocoles de communication

Encapsulation

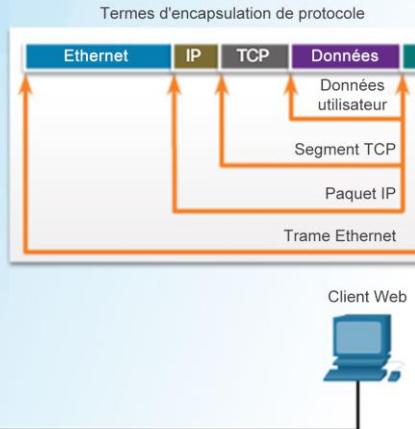
- Ce processus de division des données est appelé segmentation. La segmentation des messages présente deux avantages majeurs :
 - **Segmentation**
 - **Multiplexage**
- À mesure que les données d'application traversent la pile de protocoles, elles sont encapsulées à l'aide de diverses informations de protocole.
- La forme que prend les parties de données encapsulées à chaque couche est appelée « unité de données de protocole (PDU) ».

Protocoles de communication

Encapsulation (suite)

- Ce processus est inversé sur l'hôte récepteur. Il est alors appelé désencapsulation. Les données sont désencapsulées au fur et à mesure qu'elles se déplacent vers la partie supérieure de la pile et l'application de l'utilisateur final.

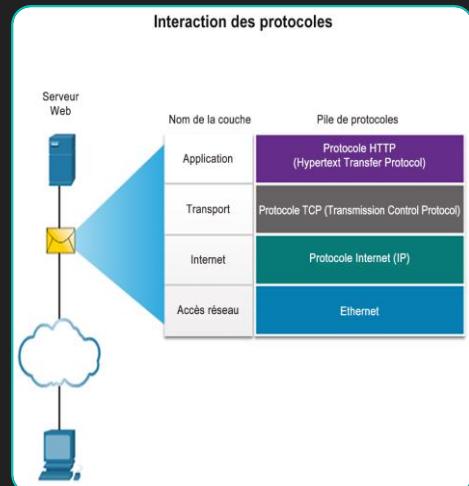
Fonctionnement des protocoles en matière de réception d'un message



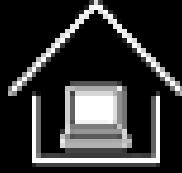
Protocoles de communication

Scénario : Envoyer et recevoir une page web

- **HTTP** : ce protocole d'application régit les interactions entre un serveur web et un client web.
- **TCP** : ce protocole de transport gère les conversations individuelles. Le protocole TCP divise les messages HTTP en petites parties appelées segments. Le protocole TCP est également responsable du contrôle de la taille et du débit d'échange des messages entre le serveur et le client.
- **IP** : ce protocole est chargé de récupérer les segments formatés par le protocole TCP, de les encapsuler sous forme de paquets, de leur attribuer les adresses appropriées (IP du destinataire et IP de l'expéditeur) et de les transmettre à l'hôte de destination.
- **Ethernet** : ce protocole d'accès réseau récupère les paquets transmis par le protocole IP et les formate pour assurer leur diffusion via les supports de réseau.



Protocoles Ethernet et IP

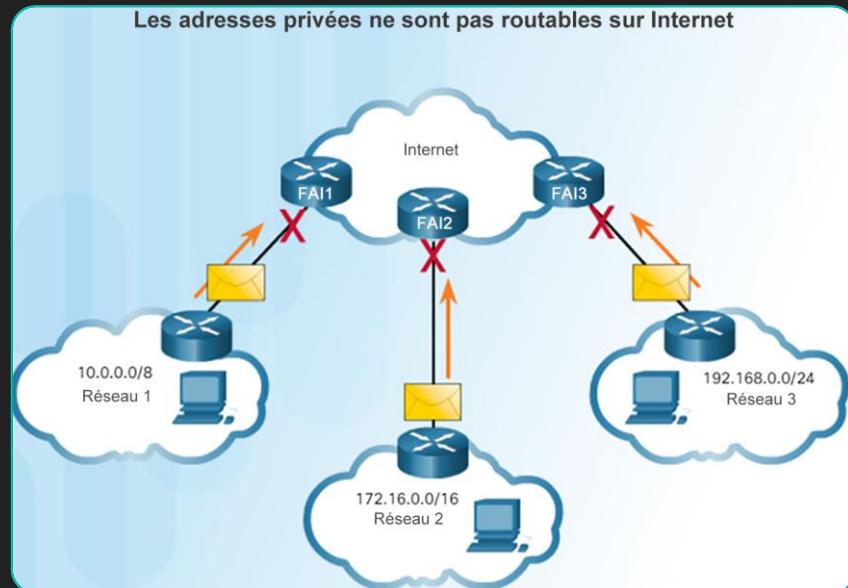


THERE'S NO PLACE LIKE
127.0.0.1

Types d'adresses IPv4

Adresses IP publiques et privées

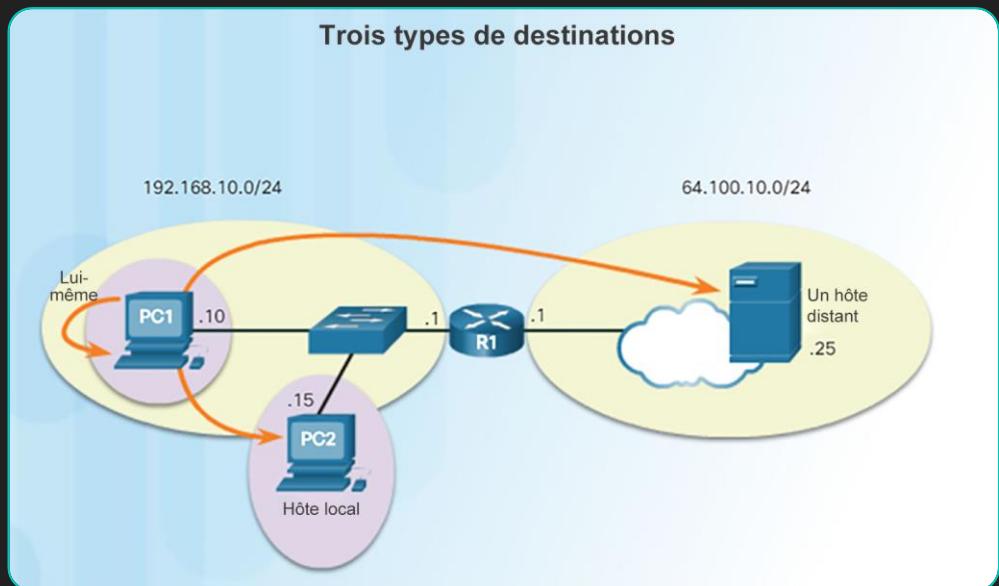
- Blocs d'adresses utilisés principalement par les entreprises pour attribuer des adresses IPv4 aux hôtes internes.
- Non spécifique à un réseau.
- Non autorisée sur Internet et filtrée par un routeur interne.
- Généralement, le routeur connecte le réseau interne à celui du FAI.



La passerelle par défaut

Décisions relatives aux transmissions entre les hôtes

- Un hôte peut envoyer un paquet à trois types de destinations :
 - **Lui-même** : un hôte peut s'envoyer une requête ping en envoyant un paquet à une adresse IPv4 spécifique, 127.0.0.1. L'envoi d'une requête ping à l'interface de bouclage permet de tester la pile de protocoles TCP/IP.
 - **Un hôte local** : il s'agit d'un hôte sur le même réseau local que l'hôte émetteur.
 - **Un hôte distant** : il s'agit d'un hôte sur un réseau distant. Les hôtes ne partagent pas la même adresse réseau.



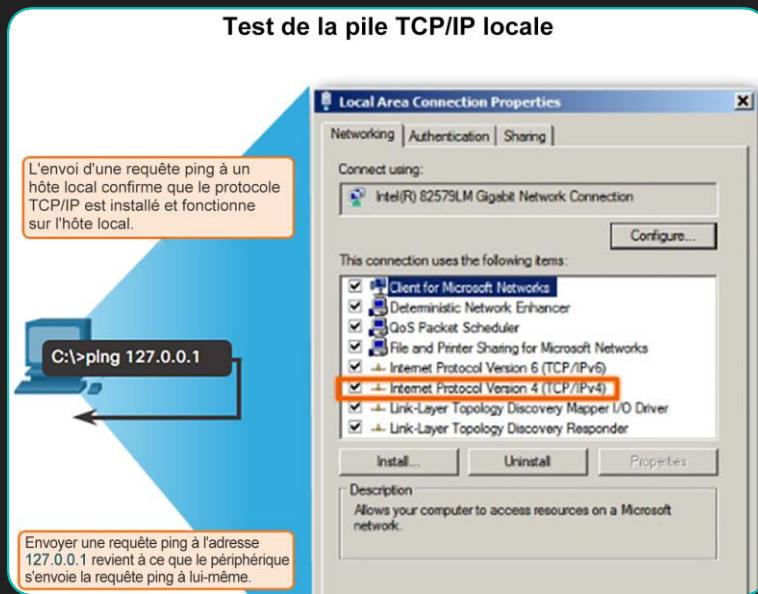
Vérification de la connectivité

Utilitaires ping et Traceroute

Ping – Test et pile locale

- La commande ping est un utilitaire de test qui utilise des messages de requête et de réponse d'écho ICMP pour tester la connectivité entre les hôtes.
- Pour tester la connectivité avec un autre hôte sur un réseau, une requête d'écho est envoyée à l'adresse d'hôte au moyen de la commande ping.
- Si l'hôte à l'adresse spécifiée reçoit une requête d'écho, il répond en envoyant une réponse d'écho.

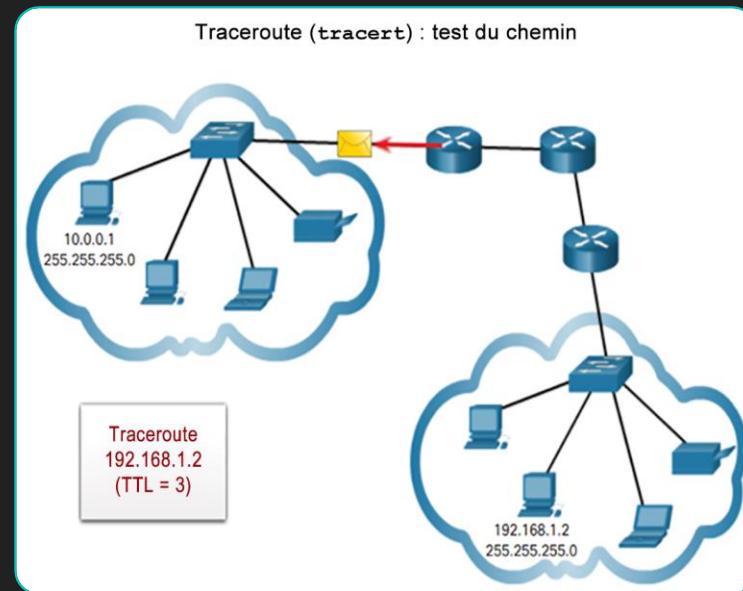
Ping pourrait-il servir à autre chose du point de vue sécurité?



Utilitaires Ping et Traceroute

Traceroute – Test du chemin

- Traceroute fournit les détails des périphériques entre les hôtes.
- Génère une liste de sauts déjà atteints le long du chemin :
 - **Durée de transmission(RTT)** – Heure de chaque tronçon le long du chemin.
 - **TTL IPv4 et limite du nombre de tronçons IPv6** - 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.
- Après que la destination finale a été atteinte, l'hôte répond par un message ICMP Port Unreachable (port inaccessible) ou ICMP Echo Reply (réponse d'écho), à la place du message ICMP Time Exceeded (délai dépassé).



Identification d'un système d'exploitation avec PING!

| | | | |
|----------------|----------------------|--------------|-----|
| MacOS/MacTCP | 2.0.x | TCP and UDP | 60 |
| MacOS/MacTCP | X (10.5.6) | ICMP/TCP/UDP | 64 |
| NetBSD | | ICMP | 255 |
| Netgear FVG318 | | ICMP and UDP | 64 |
| OpenBSD | 2.6 & 2.7 | ICMP | 255 |
| OpenVMS | 07.01.2002 | ICMP | 255 |
| OS/2 | TCP/IP 3.0 | | 64 |
| OSF/1 | V3.2A | TCP | 60 |
| OSF/1 | V3.2A | UDP | 30 |
| Solaris | 2.5.1, 2.6, 2.7, 2.8 | ICMP | 255 |
| Solaris | 2.8 | TCP | 64 |
| Stratus | TCP OS | ICMP | 255 |
| Stratus | TCP_OS (14.2-) | TCP and UDP | 30 |
| Stratus | TCP OS (14.3+) | TCP and UDP | 64 |
| Stratus | STCP | ICMP/TCP/UDP | 60 |
| SunOS | 4.1.3/4.1.4 | TCP and UDP | 60 |
| SunOS | 5.7 | ICMP and TCP | 255 |
| Ultrix | V4.1/V4.2A | TCP | 60 |
| Ultrix | V4.1/V4.2A | UDP | 30 |
| Ultrix | V4.2 – 4.5 | ICMP | 255 |
| VMS/Multinet | | TCP and UDP | 64 |
| VMS/TCPware | | TCP | 60 |
| VMS/TCPware | | UDP | 64 |
| VMS/Wollongong | 1.1.1.1 | TCP | 128 |
| VMS/Wollongong | 1.1.1.1 | UDP | 30 |
| VMS/UCX | | TCP and UDP | 128 |
| Windows | for Workgroups | TCP and UDP | 32 |
| Windows | 95 | TCP and UDP | 32 |
| Windows | 98 | ICMP | 32 |

| | | | |
|---------|-----------------------|--------------|-----|
| Windows | 98, 98 SE | ICMP | 128 |
| Windows | 98 | TCP | 128 |
| Windows | NT 3.51 | TCP and UDP | 32 |
| Windows | NT 4.0 | TCP and UDP | 128 |
| Windows | NT 4.0 SP5- | | 32 |
| Windows | NT 4.0 SP6+ | | 128 |
| Windows | NT 4 WRKS SP 3, SP 6a | ICMP | 128 |
| Windows | NT 4 Server SP4 | ICMP | 128 |
| Windows | ME | ICMP | 128 |
| Windows | 2000 pro | ICMP/TCP/UDP | 128 |
| Windows | 2000 family | ICMP | 128 |
| Windows | Server 2003 | | 128 |
| Windows | XP | ICMP/TCP/UDP | 128 |
| Windows | Vista | ICMP/TCP/UDP | 128 |
| Windows | 7 | ICMP/TCP/UDP | 128 |
| Windows | Server 2008 | ICMP/TCP/UDP | 128 |
| Windows | 10 | ICMP/TCP/UDP | 128 |

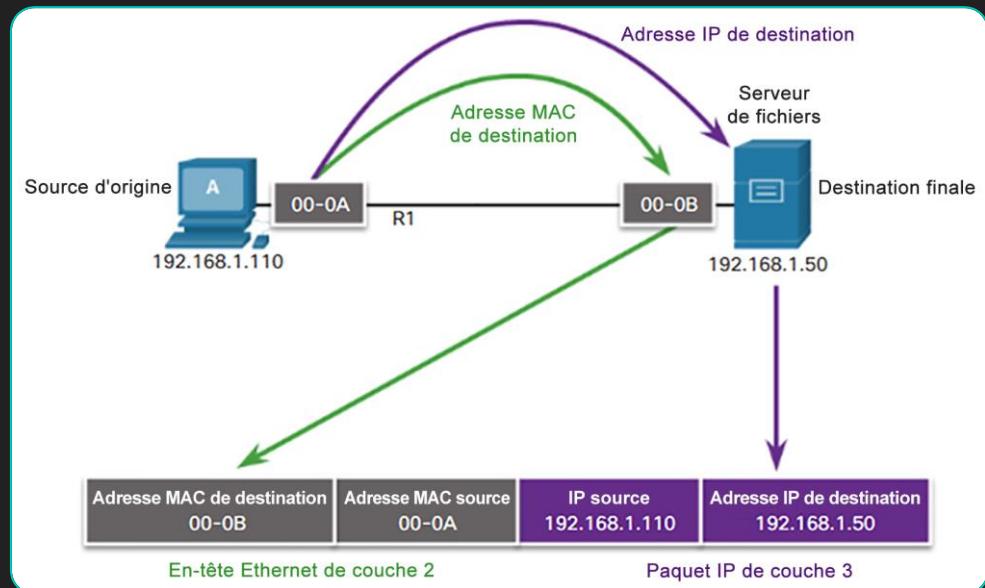
You can get the short version of default TTL values by this [table](#).



4.4 Protocole de résolution d'adresse

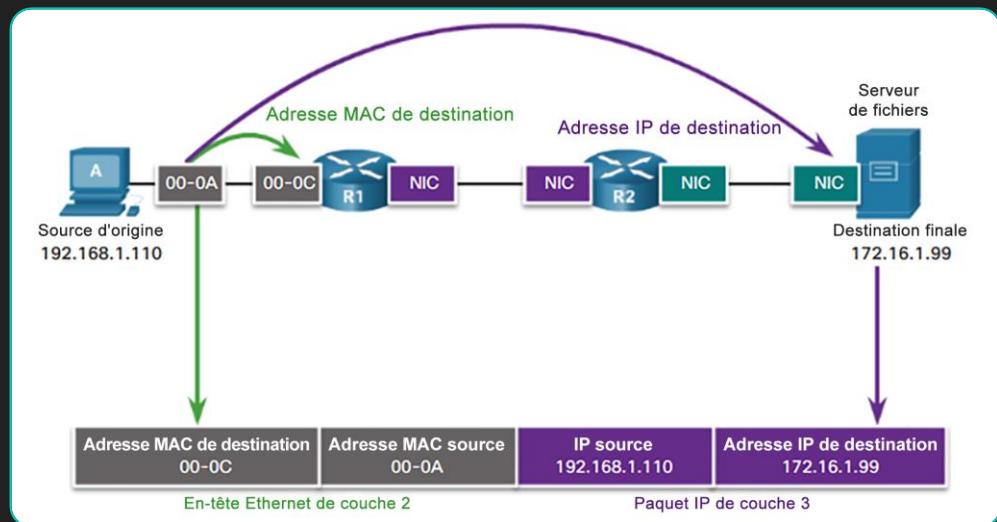
Adresses MAC et IP Destination sur le même réseau

- Deux adresses attribuées à un appareil Ethernet :
 - **Adresse MAC** (adresse physique de couche 2)
 - **Adresse IP** (adresse logique de couche 3)
- Un appareil doit posséder les deux adresses pour communiquer avec un autre appareil basé sur TCP/IP :
 - Utilise les adresses MAC source et de destination.
 - Il utilise les adresses IP source et de destination



Adresses MAC et IP Destination sur un réseau distant

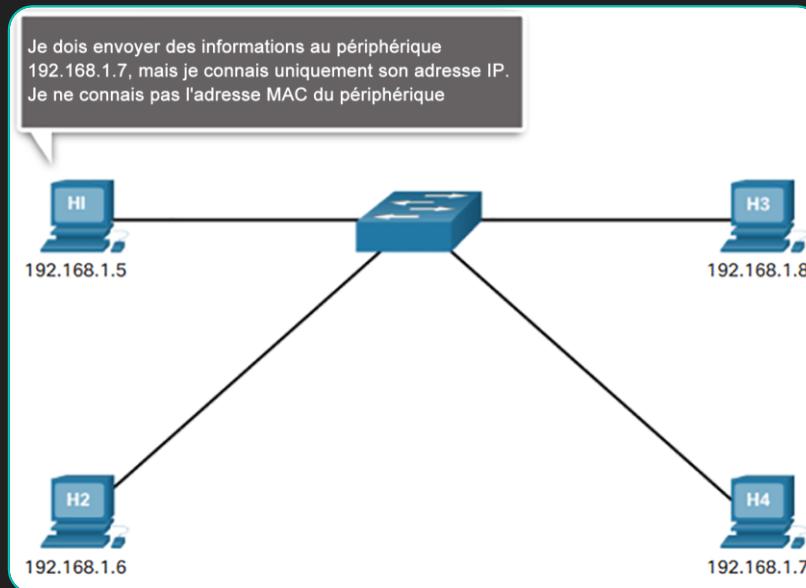
- Lors des communications avec un appareil sur un réseau distant, l'adresse MAC de destination correspond à l'adresse MAC de l'interface de l'appareil de couche 3 sur le même réseau que celui de l'appareil qui a envoyé le paquet.



Protocole ARP

Présentation du protocole ARP

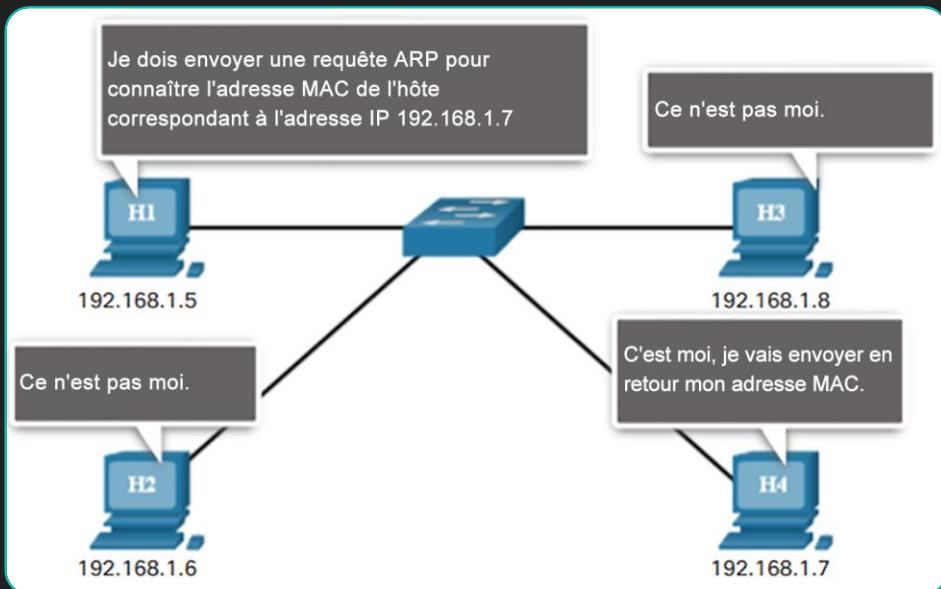
- Lorsqu'un périphérique envoie une trame Ethernet, celle-ci contient deux adresses :
 - Adresse MAC de destination** : l'adresse MAC de la carte réseau Ethernet qui correspond soit à l'adresse MAC du périphérique de destination finale soit à celle du routeur.
 - Adresse MAC source** : l'adresse MAC de la carte réseau Ethernet de l'expéditeur.
- Pour déterminer l'adresse MAC de destination, le périphérique utilise le protocole ARP. Le protocole ARP traduit les adresses IPv4 en adresses MAC et met à jour une table des mappages.



Protocole ARP

Fonctions du protocole ARP

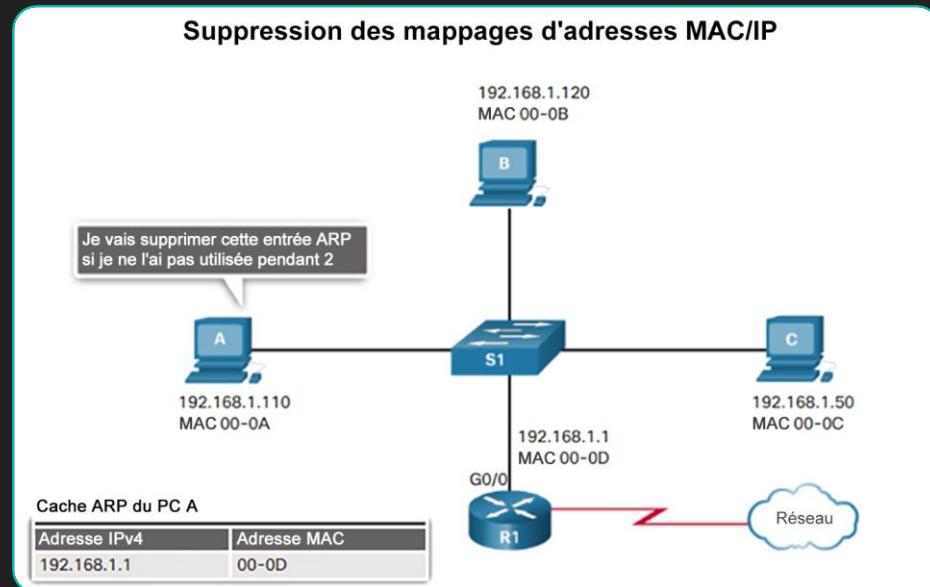
- Il permet de résoudre les adresses IPv4 en adresses MAC.
- Les mappages entre les adresses IPv4 et MAC sont conservés dans une table ARP.



Le protocole ARP

Suppression des entrées d'une table ARP

- Pour chaque périphérique, un compteur de cache ARP supprime les entrées ARP qui n'ont pas été utilisées pendant une période donnée.
- Des commandes permettent aussi de supprimer manuellement les entrées du tableau ARP totalement ou partiellement.
- Les routeurs et les hôtes du réseau stockent des tables ARP.



Le protocole ARP

Tables ARP sur les périphériques réseau

- Les routeurs et les hôtes du réseau stockent des tables ARP.
- Conservées dans une mémoire appelée cache ARP.
- Supprimées de la table lorsqu'elles deviennent obsolètes.

Table d'hôte APR

```
C:\> arp -a

Interface: 192.168.1.67 --- 0xa
 Internet Address      Physical Address      Type
 192.168.1.254          64-0f-29-0d-36-91    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
 224.0.0.252              01-00-5e-00-00-fc  static
 255.255.255.255         ff-ff-ff-ff-ff-ff    static

Interface: 10.82.253.91 --- 0x10
 Internet Address      Physical Address      Type
 10.82.253.92            64-0f-29-0d-36-91    dynamic
 224.0.0.22              01-00-5e-00-00-16    static
 224.0.0.251              01-00-5e-00-00-fb  static
 224.0.0.252              01-00-5e-00-00-fc  static
 255.255.255.255         ff-ff-ff-ff-ff-ff    static
```

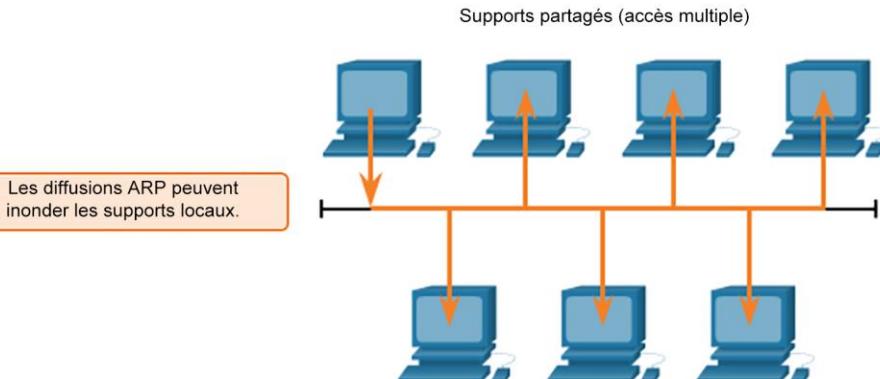
Problèmes liés au protocole ARP

Diffusions ARP

- Diffusions ARP : peuvent affecter les grands réseaux.

Pourquoi?

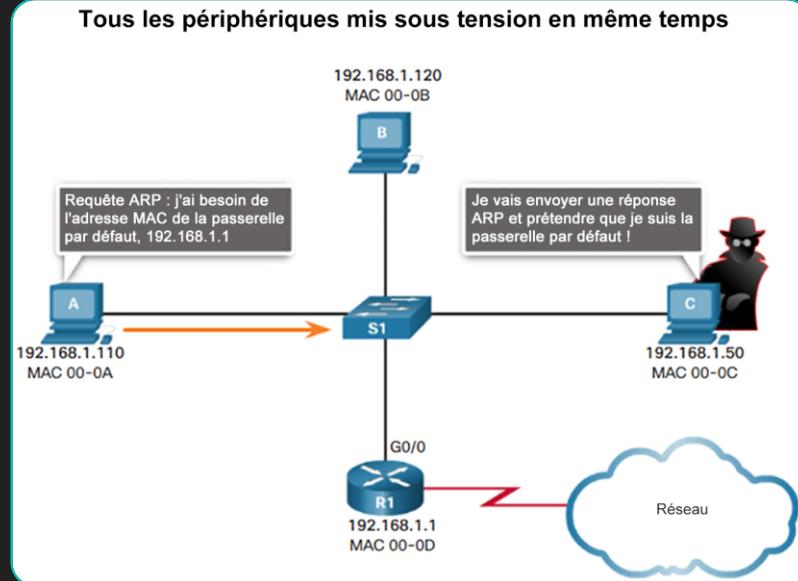
Diffusions ARP et sécurité



Problèmes liés au protocole ARP

Usurpation ARP

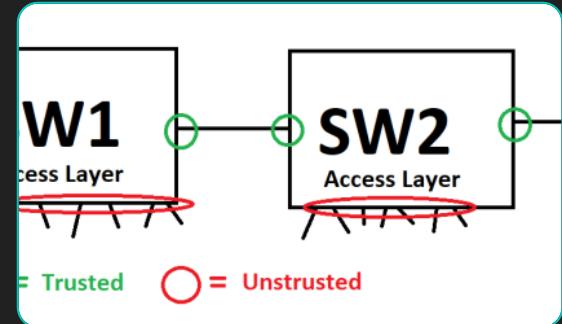
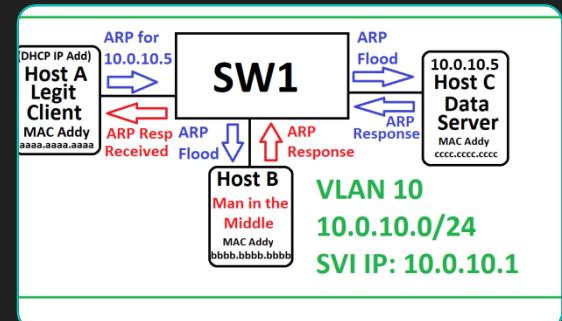
- Usurpation ARP (empoisonnement ARP) : risque de sécurité
 - Il s'agit d'une technique utilisée par un hacker pour répondre à une requête ARP concernant l'adresse IPv4 d'un autre périphérique tel que la passerelle par défaut.



Protection contre l'usurpation ARP

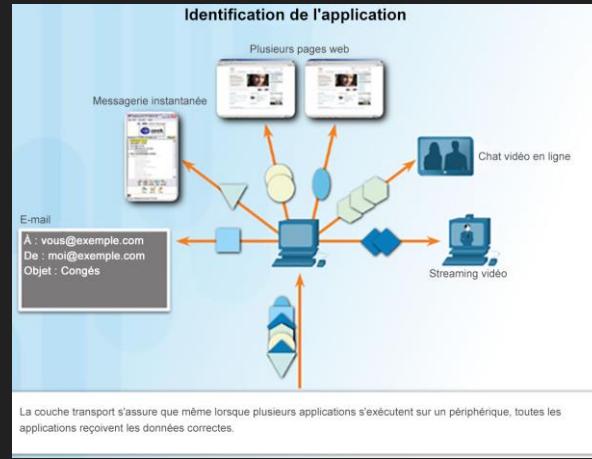
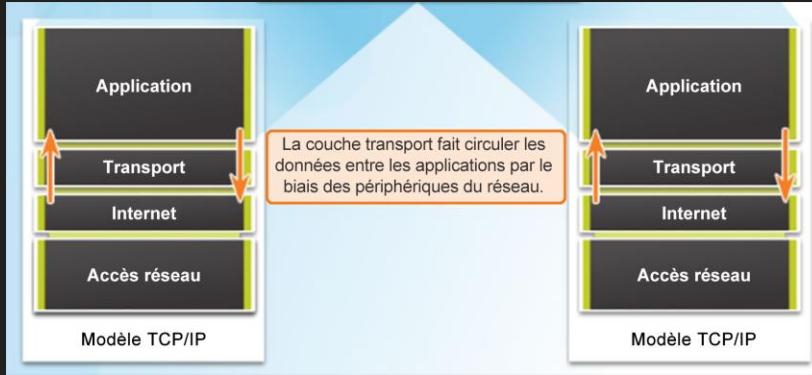
- Dynamic Arp Inspection est une fonctionnalité incluse dans tout les commutateurs depuis plus de 20 ans chez Cisco. La configuration n'écessite que 2 commandes:

```
S1(config)# ip arp inspection vlan XXX  
S1(config)# in fa6/3  
S1(config-if)# ip arp inspection trust
```



La couche transport





Caractéristiques de la couche transport

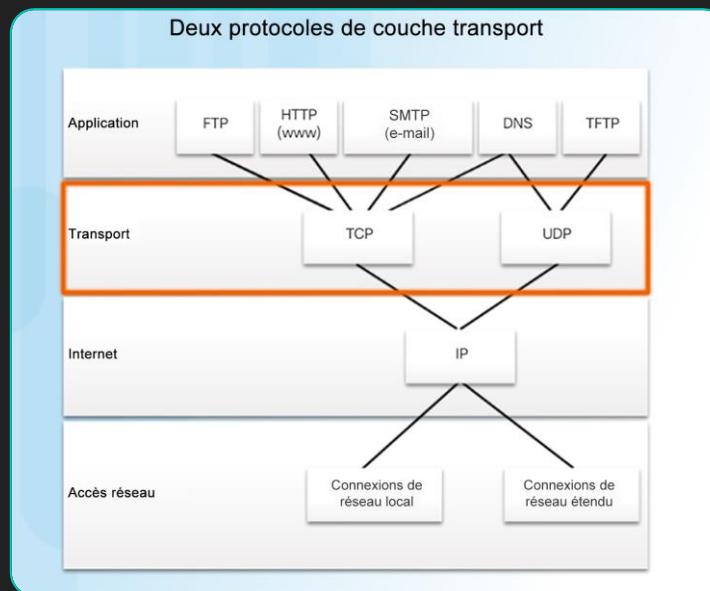
Rôle du protocole de couche transport dans les communications réseau

- Assure le suivi de chaque conversation.
- Déplace les données entre des applications sur des appareils réseau.
- Segmente les données et reconstitue les segments.
- Identifie les applications à l'aide d'un numéro de port.

Caractéristiques de la couche transport

Mécanismes de la couche transport

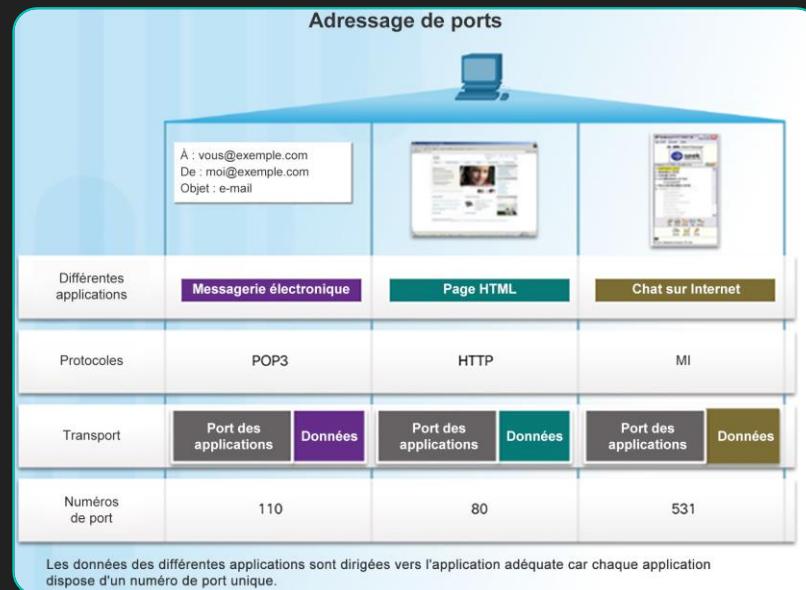
- La segmentation des données en parties plus petites permet à plusieurs communications différentes, provenant de nombreux utilisateurs, d'être imbriquées (multiplexées) sur le même réseau.
- La couche transport est également responsable de la gestion des exigences de fiabilité d'une conversation.
- La suite de protocoles TCP/IP propose deux protocoles de couche transport :
 - **TCP (Transmission Control Protocol)**
 - **Protocole UDP (User Datagram Protocol)**



Caractéristiques de la couche transport

Ports TCP locaux et distants

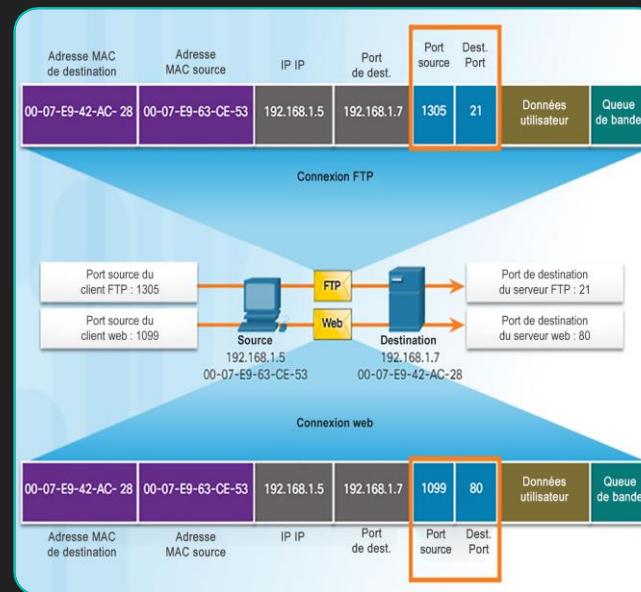
- Les protocoles TCP et UDP gèrent ces conversations simultanées multiples au moyen de champs d'en-tête identifiant ces applications de façon unique. Ces identificateurs uniques sont les numéros de port :
 - Le **numéro du port source** est associé à l'application d'origine sur l'hôte local.
 - Le **numéro de port de destination** est associé à l'application de destination sur l'hôte distant.



Caractéristiques de la couche transport

Paires d'interfaces de connexion

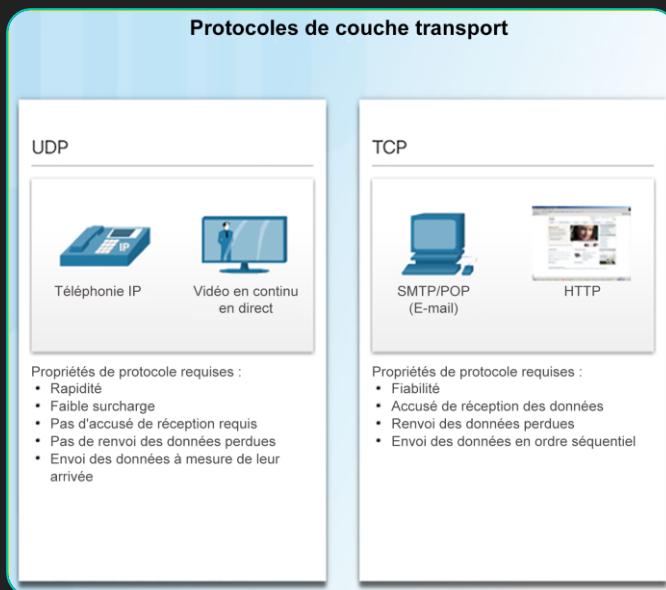
- La combinaison de l'adresse IP source et du numéro de port source, ou de l'adresse IP de destination et du numéro de port de destination, est appelée **interface de connexion**.
- L'interface de connexion sert à identifier le serveur et le service demandés par le client.
- Les interfaces de connexion 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.



Caractéristiques de la couche transport

TCP et UDP

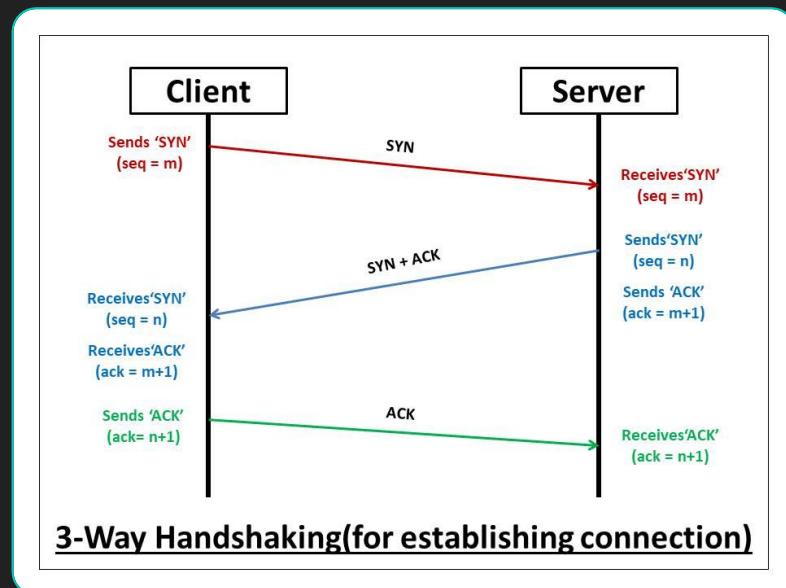
- TCP
 - Utilisé pour la plupart des principaux protocoles TCP/IP.
 - Fiable, accuse réception des données, renvoie les données perdues, fournit les données dans un ordre séquentiel.
 - Exemples : e-mail, HTTP
- UDP
 - Rapide, faible surcharge, ne nécessite pas d'accusés de réception, ne renvoie pas les données perdues, fournit les données à mesure qu'elles arrivent.
 - Exemples : VoIP, streaming vidéo en direct



Fonctionnement de la couche transport

Une session TCP – Partie 1 : établissement et interruption de la connexion

- Une connexion TCP est établie en trois étapes :
 1. Le client demande l'établissement d'une session de communication client-serveur avec le serveur.
 2. Le serveur accorde réception de la session de communication client-serveur et demande l'établissement d'une session de communication serveur-client.
 3. Le client accorde réception de la session de communication serveur-client.



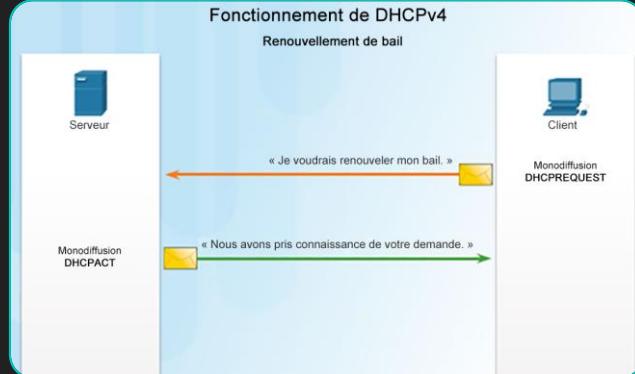
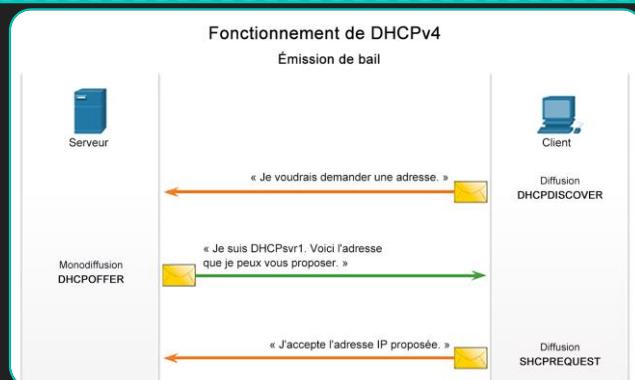
A black and white photograph showing a person's lower body from the side. They are wearing light-colored, possibly white, trousers and dark, lace-up boots. To their left is a white wooden chair with a curved backrest. The background is a plain, light-colored wall.

Services réseau

DHCP

Présentation du protocole DHCP

- Protocole DHCP (Dynamic Host Configuration Protocol)
 - Fournit des informations sur l'adressage IP, comme l'adresse IP, le masque de sous-réseau, la passerelle par défaut, l'adresse IP du serveur DNS et le nom de domaine.
 - Messages
 - Détection
 - Offre
 - Requête
 - ACK (accusé de réception)



DHCP

Format du message DHCPv4

Un message DHCP comporte les champs suivants :

- **Code OP (opération)** : indique le type général du message.
- **Type de matériel** : indique le type de matériel utilisé sur le réseau.
- **Longueur de l'adresse matérielle** : spécifie la longueur de l'adresse.
- **Sauts** : contrôle le transfert des messages.
- **Identificateur de transaction** : champ utilisé par le client pour comparer la requête avec les réponses reçues des serveurs DHCPv4.
- **Secondes** : indique le nombre de secondes qui se sont écoulées depuis le début de la tentative d'acquisition ou de renouvellement d'un bail par un client.
- **Indicateurs** : champ utilisé par un client qui ne connaît pas son adresse IPv4 au moment d'envoyer une requête.

| 8 | 16 | 24 | 32 |
|---|-----------------------------|---|---------------------|
| Code OP (1) | Type de matériel (1) | Longueur de l'adresse matérielle (1) | Tronçons (1) |
| Identificateur de transaction | | | |
| Secondes - 2 octets | | Indicateurs - 2 octets | |
| Adresse IP du client (CIADDR) - 4 octets | | Votre adresse IP (YIADDR) - 4 octets | |
| Adresse IP du serveur (SIADDR) - 4 octets | | Adresse IP de la passerelle (GIADDR) - 4 octets | |
| Adresse matérielle du client (CHADDR) - 16 octets | | Nom du serveur (SNAME) - 64 octets | |
| Nom du fichier de démarrage - 128 octets | | Options DHCP – variable | |

DHCP

Format du message DHCPv4 (suite)

Un message DHCP comporte les champs suivants :

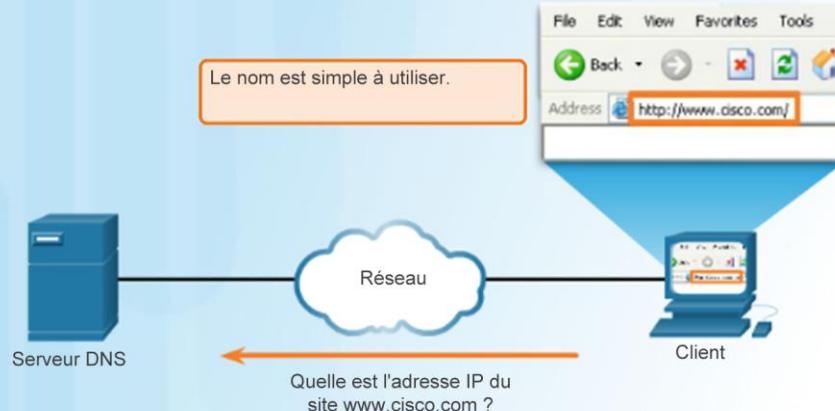
- **Adresse IP du client** : champ utilisé par un client qui renouvelle son crédit-bail avec une adresse valide et utilisable, et non lors de l'acquisition d'une adresse.
- **Votre adresse IP** : champ utilisé par le serveur pour attribuer une adresse IPv4 au client.
- **Adresse IP du serveur** : champ utilisé par le serveur pour indiquer l'adresse du serveur que le client doit utiliser pour l'étape suivante du processus d'amorçage.
- **Adresse IP de la passerelle** : achemine les messages DHCPv4 lorsque des agents de relais DHCPv4 sont impliqués.
- **Adresse matérielle du client** : représente la couche physique du client.
- **Nom du serveur** : utilisé par le serveur qui envoie un message DHCPOFFER ou DHCPACK.
- **Nom du fichier de démarrage** : peut être utilisé par un client pour demander un type de fichier de démarrage spécifique dans un message DHCPDISCOVER.
- **Options DHCP** : contient les options DHCP, notamment plusieurs paramètres requis pour fournir les fonctions DHCP de base.

DNS

Présentation du protocole DNS

- Système de noms dynamique (DNS)
 - Gère et fournit des noms de domaine et les adresses IP associées.
 - Hiérarchie de serveurs.
 - **90 % des malwares qui attaquent des réseaux utilisent DNS pour mener à bien leurs campagnes.**

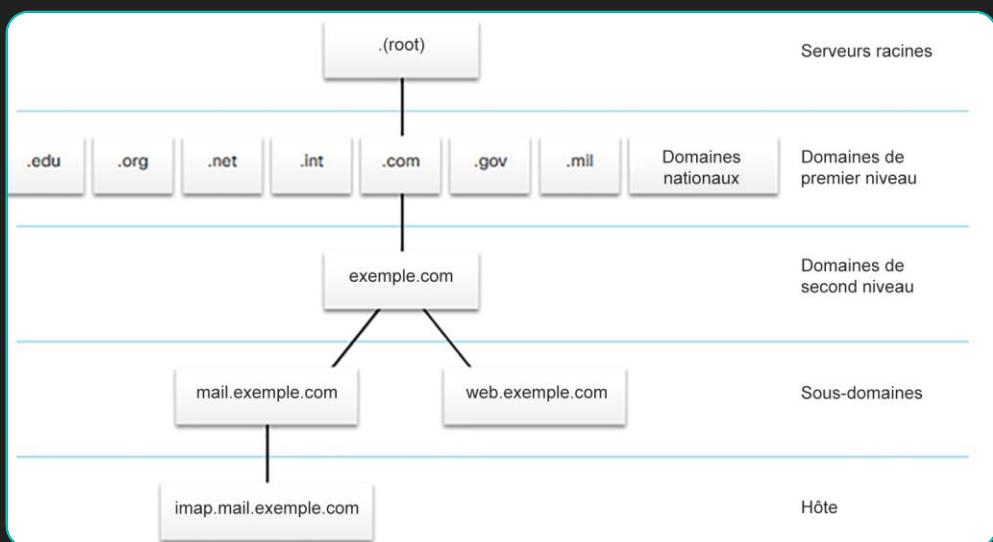
Le service DNS traduit les noms en adresses IP



DNS

Hiérarchie de domaines DNS

- Système de noms dynamique (DNS)
 - Le DNS se compose d'une hiérarchie de domaines génériques de premier niveau qui incluent les domaines .com, .net, .org, .gov, .edu et de nombreux domaines nationaux, tels que .br (Brésil), .es (Espagne), .uk (Royaume-Uni), etc.
 - Les domaines de second niveau sont représentés par un nom de domaine suivi d'un domaine de premier niveau.
 - Les sous-domaines composent le niveau suivant de la hiérarchie DNS et représentent en quelque sorte une division des domaines de second niveau.
 - Enfin, un quatrième niveau peut représenter un hôte dans un sous-domaine.

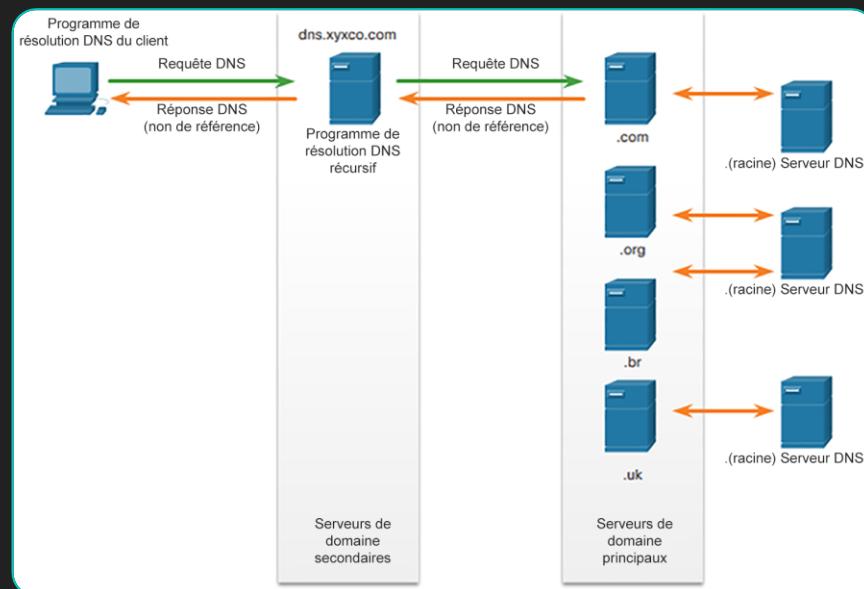


DNS

Processus de recherche DNS

Voici quelques termes clés à connaître concernant le système DNS :

- **Programme de résolution** : un client DNS qui envoie des messages DNS afin d'obtenir des informations sur l'espace de noms de domaine demandé.
- **Récursion** : action effectuée lorsqu'un serveur DNS doit envoyer une requête au nom d'un programme de résolution DNS.
- **Serveur de référence** : un serveur DNS qui répond aux messages de requête avec des informations stockées dans des enregistrements de ressources concernant un espace de noms de domaine enregistré sur le serveur.
- **Programme de résolution récursive** : un serveur DNS qui envoie une requête récursive concernant les informations demandées dans la requête DNS.

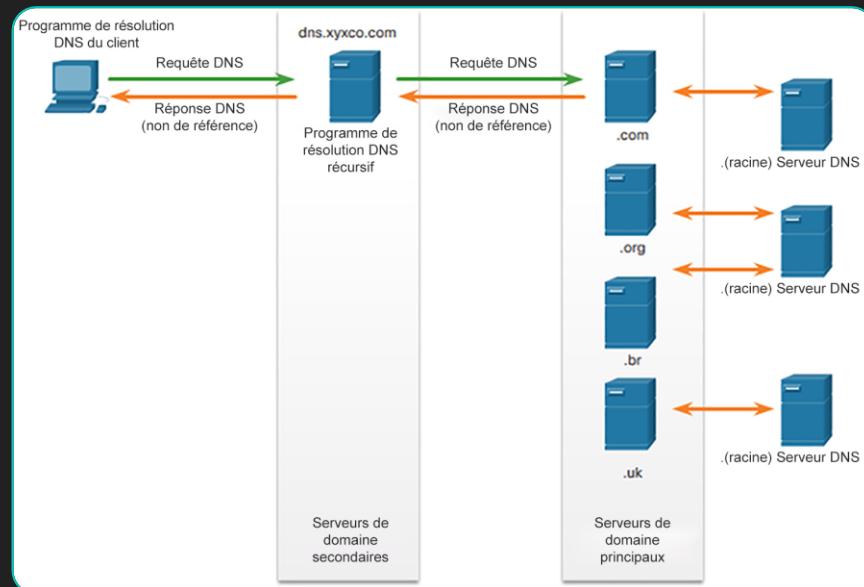


DNS

Processus de recherche DNS (suite)

Voici quelques termes clés à connaître concernant le système DNS :

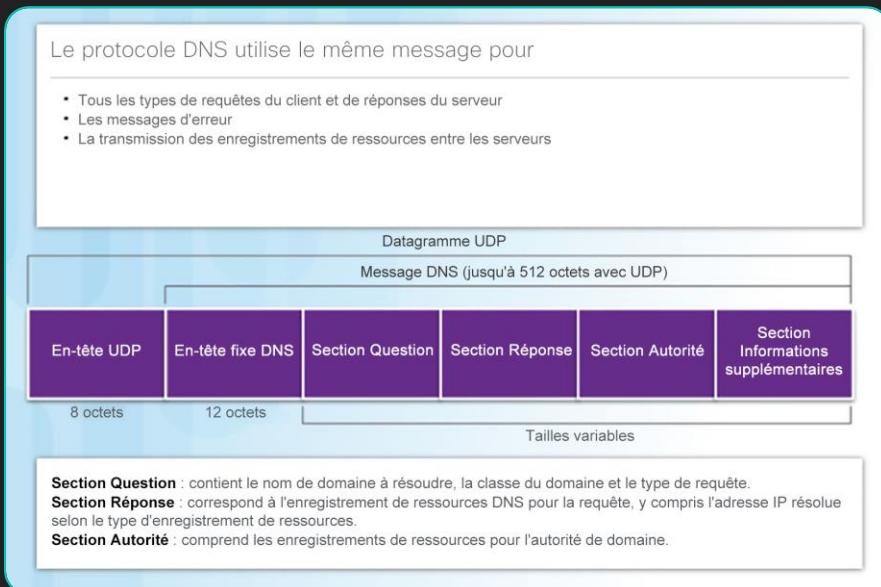
- **Nom de domaine complet** : le nom complet d'un périphérique tel que spécifié dans la base de données DNS distribuée.
- **Enregistrement de ressources** : format utilisé dans les messages DNS se composant des champs suivants : NAME, TYPE, CLASS, TTL, RDLENGTH et RDATA.
- **Zone** : une base de données qui contient des informations sur l'espace de noms de domaine enregistré sur un serveur de référence.



DNS

Format du message DNS

- DNS utilise le port UDP 53 pour les requêtes et les réponses DNS.
- Les requêtes DNS sont envoyées par un client et les réponses sont émises par des serveurs DNS.
- Si la taille d'une réponse DNS est supérieure à 512 octets notamment lorsque le DNS dynamique (DDNS) est utilisé, le port TCP 53 est utilisé pour traiter le message.
- Types d'enregistrements DNS :
 - **A** – Adresse IPv4 de terminal
 - **NS** - Serveur de noms autorisé
 - **AAAA** - adresse IPv6 d'un périphérique
 - **MX** - Enregistrement d'échange de courrier électronique

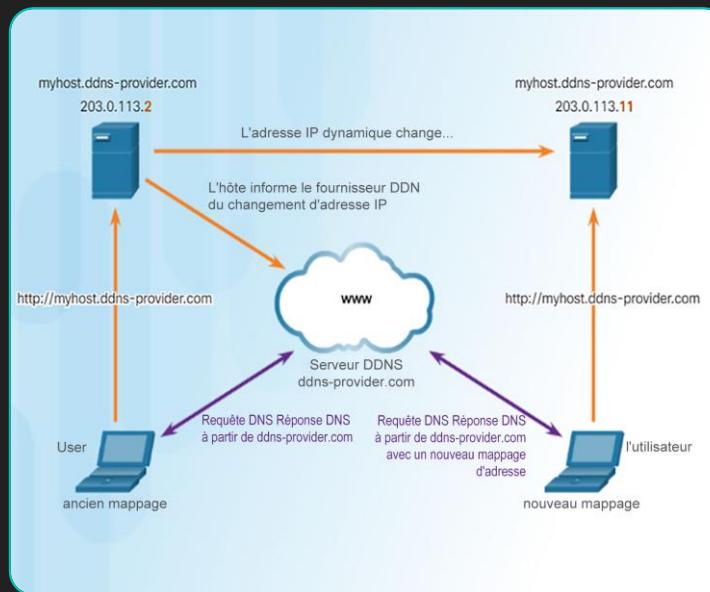


DNS

DNS dynamique

■ DNS dynamique (DDNS)

- Permet à un utilisateur ou à une entreprise d'enregistrer l'adresse IP correspondant à un nom de domaine comme avec DNS.
- Lorsque l'adresse IP du mappage est modifiée, le nouveau mappage peut être diffusé presque instantanément via le DNS.



Demo Dynamic DNS

- Accès internet résidentiel avec IP dynamique à distance

DNS

Le protocole WHOIS

Le protocole WHOIS :

- WHOIS est un protocole basé sur TCP qui est utilisé pour identifier les propriétaires de domaines Internet dans le système DNS.

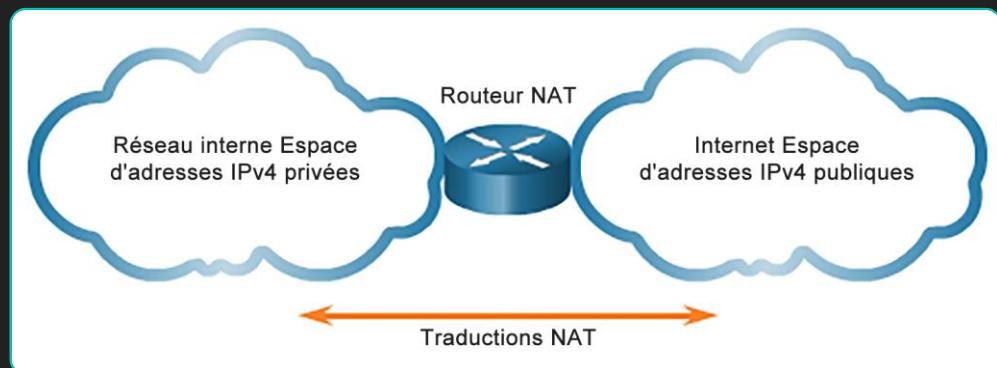
[Demo lacitec.on.ca](#)

The screenshot shows a web browser displaying the ICANN WHOIS search results for the domain `cisco.com`. The page has a dark blue header with the ICANN WHOIS logo and navigation links for About WHOIS, Policies, Get Involved, WHOIS Complaints, and Knowledge Center. Below the header is a search bar containing `www.cisco.com` and a "Lookup" button. The main content area displays the search results for `cisco.com`, showing the original query and the contact information for the registrant, admin, and technical contacts. The registrant contact is listed as Info Sec, Cisco Technology Inc., with a mailing address at 170 West Tasman Drive, San Jose CA 95134 US, and phone numbers +1 4085273842 and +1 4085264575. The admin contact is also listed as Info Sec, Cisco Technology Inc., with the same mailing address and phone numbers. The technical contact is listed as Network Services, Cisco Technology Inc., with a mailing address at 170 W Tasman Drive, San Jose CA 95134 US, and phone numbers +1 4085279223 and +1 4085267373. The status of the domain is shown as "Status" at the bottom right of the results panel.

NAT

Présentation du protocole NAT

- Traduction d'adresses de réseau (NAT)
 - Il n'existe pas suffisamment d'adresses IPv4 publiques pour pouvoir attribuer une adresse unique à chaque périphérique connecté à Internet.
 - Les adresses IPv4 privées sont utilisées au sein d'une entreprise ou d'un site pour permettre aux périphériques de communiquer localement.
 - Les adresses IPv4 privées ne sont pas routables sur Internet.
 - Utilisées sur les appareils périphériques.

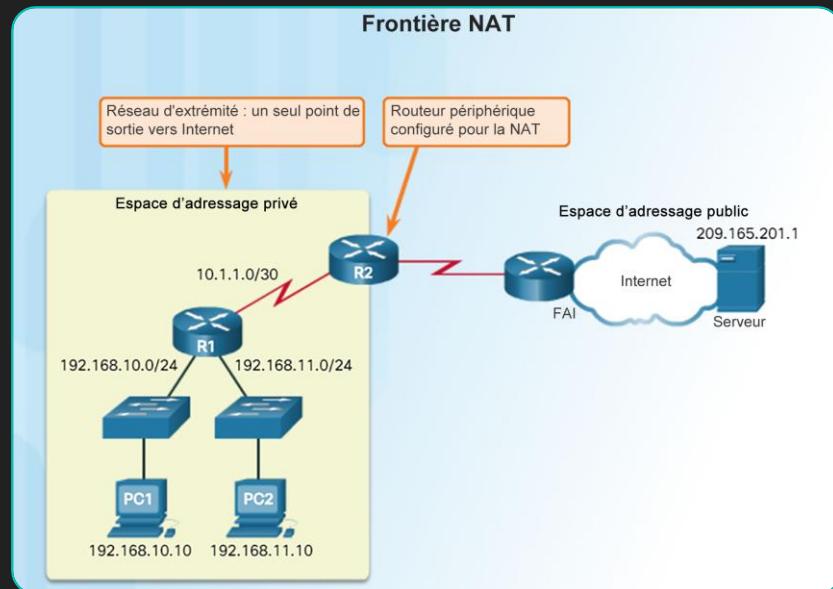


Y-a-t-il un avantage d'utiliser NAT du point de vue sécurité?

NAT

Routeurs compatibles NAT

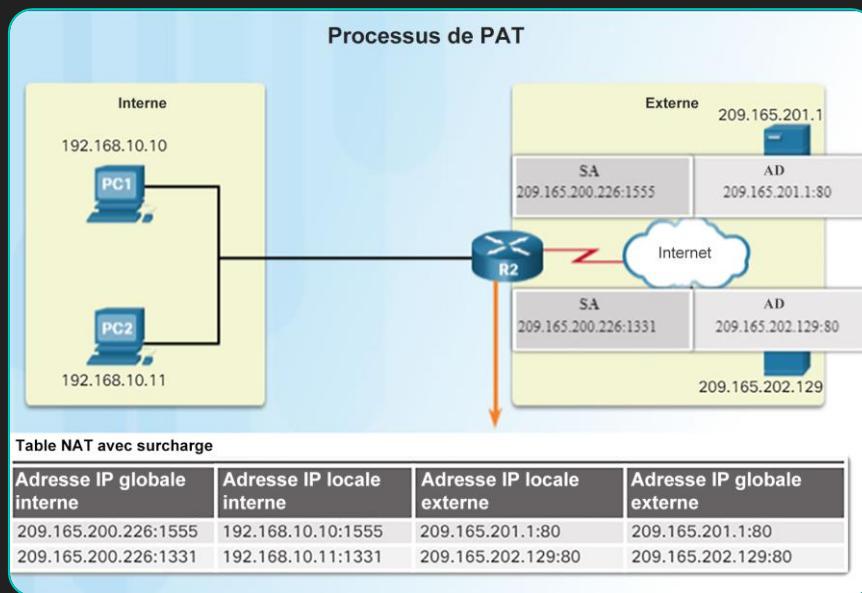
- Traduction d'adresses de réseau (NAT)
- Lorsqu'un périphérique interne envoie du trafic hors du réseau, le routeur configuré pour la NAT traduit l'adresse IPv4 interne du périphérique en une adresse publique du pool NAT.
- Pour les périphériques externes, tout le trafic entrant sur le réseau et sortant de celui-ci semble posséder une adresse IPv4 publique du pool d'adresses fourni.
- Un routeur NAT fonctionne généralement à la périphérie d'un réseau d'extrémité.



NAT

Traduction d'adresses de port

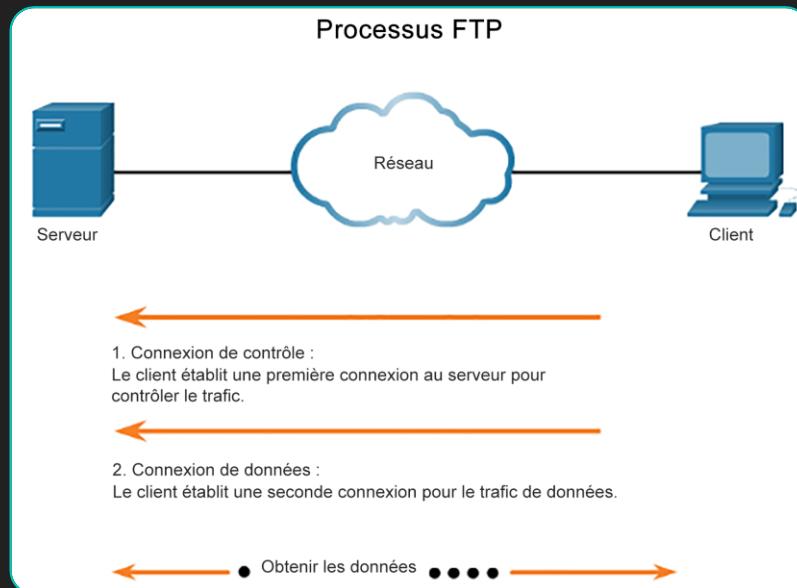
- Port Address Translation (PAT)
 - Un à plusieurs : traduction de plusieurs adresses internes en une ou plusieurs adresses IP publiques.



Services de transfert et de partage des fichiers

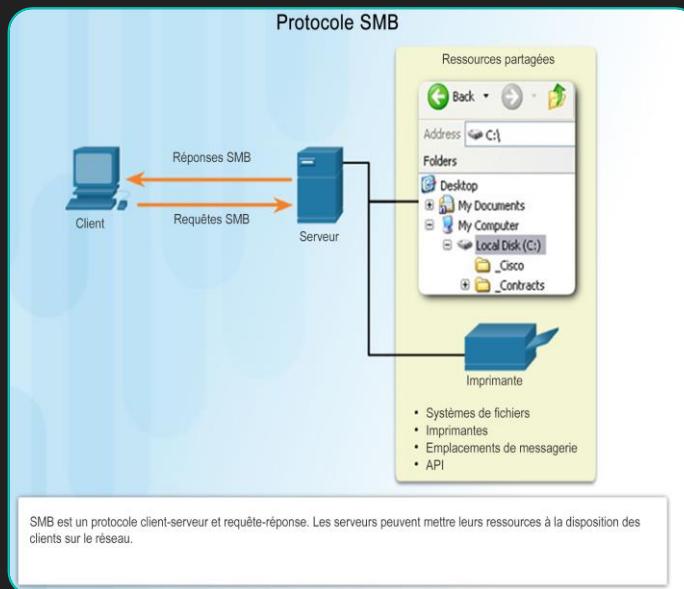
FTP et TFTP

- FTP (File Transfer Protocol)
 - Basé sur TCP.
 - Utilisé pour envoyer et extraire des données d'un serveur.
- Protocole TFTP (Trivial File Transfer Protocol)
 - Basé sur UDP.
 - Rapide, mais peu fiable.
- Server Message Block (SMB)
 - Protocole de partage de fichiers basé sur un client/serveur.



Services de transfert et de partage des fichiers SMB

- Server Message Block (SMB)
 - Protocole de partage de fichiers basé sur un client/serveur.
 - Ce format utilise un en-tête de taille fixe suivi d'un paramètre et d'un composant de données de taille variable.
 - Les messages SMB peuvent initier, authentifier et interrompre des sessions, contrôler l'accès aux fichiers et aux imprimantes, et permettre à une application d'envoyer ou de recevoir des messages vers ou depuis un autre appareil.

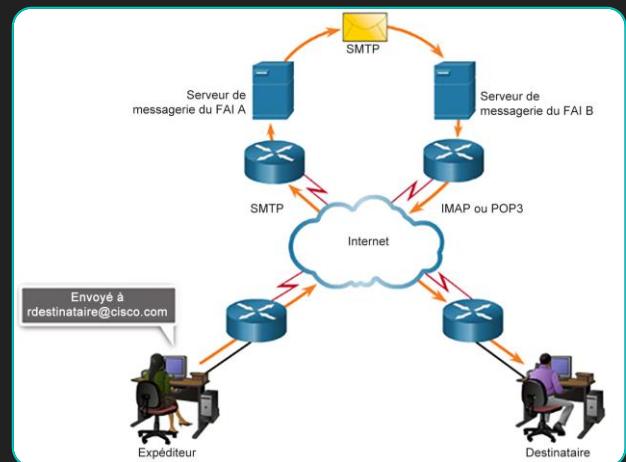


E-mail

Présentation de la messagerie électronique

- Le message prend en charge trois protocoles pour son exécution :
 - Protocole SMTP
 - protocole POP3 (Post Office Protocol version 3)
 - IMAP

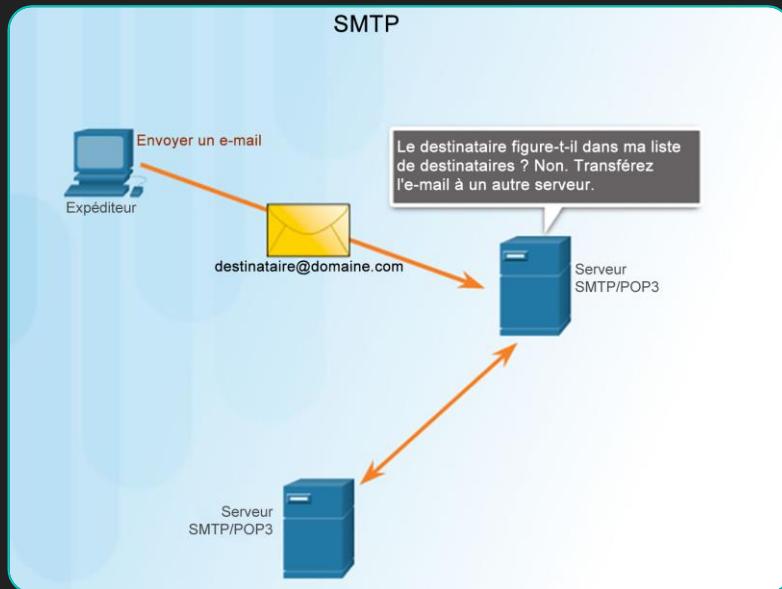
Le processus de couche application qui envoie les e-mails utilise le protocole SMTP. Un client récupère ses e-mails à l'aide de l'un des protocoles de couche application, POP3 ou IMAP.



Quel protocole est le plus utilisé de nos jours POP ou IMAP?

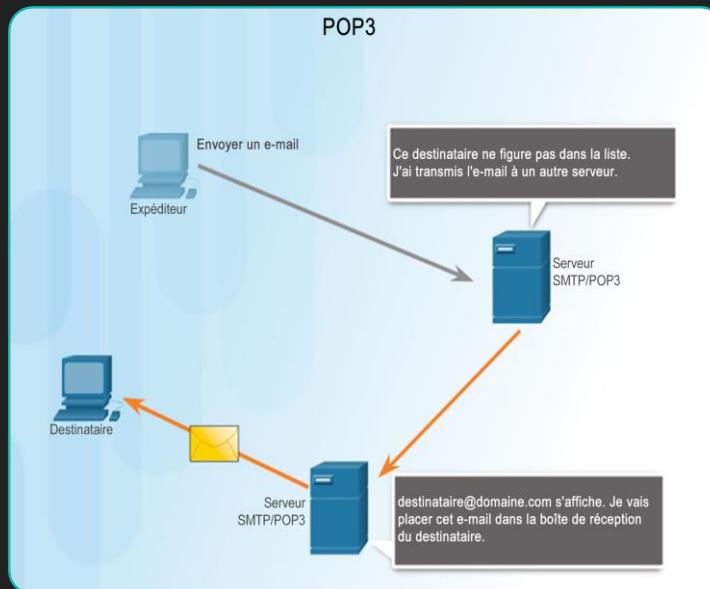
E-mail SMTP

- SMTP
 - Protocole SMTP : port 25
- Une fois la connexion établie, le client essaie d'envoyer l'e-mail au serveur via la connexion.
- Lorsque le serveur reçoit le message, il place celui-ci dans un compte local, si le destinataire est local, ou transfère le message vers un autre serveur de messagerie.



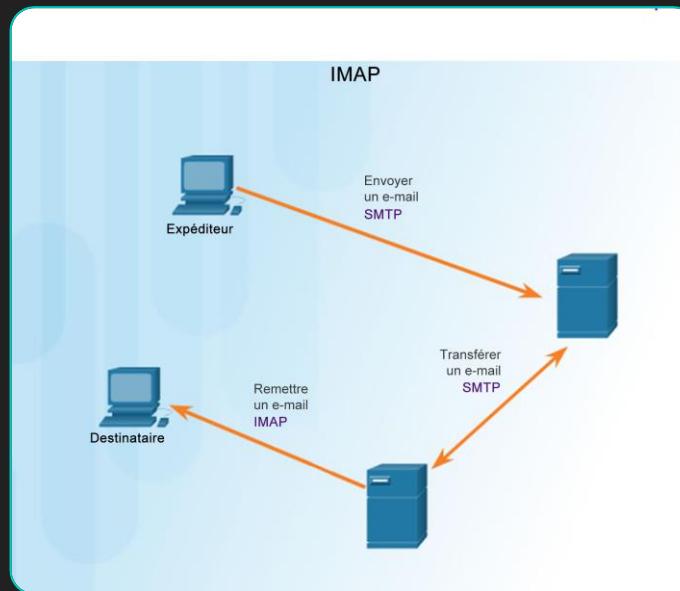
E-mail POP3

- Avec POP3, le courriel est téléchargé du serveur au client puis supprimé du serveur.
- Avec POP3, les e-mails sont téléchargés vers le client et supprimés du serveur, de sorte que les messages ne sont jamais stockés au même endroit.



E-mail IMAP

- Lorsque l'utilisateur se connecte à un serveur IMAP, des copies des messages sont téléchargées vers l'application client.
- Lorsqu'un utilisateur décide de supprimer un message, le serveur synchronise cette action et supprime le message du serveur.

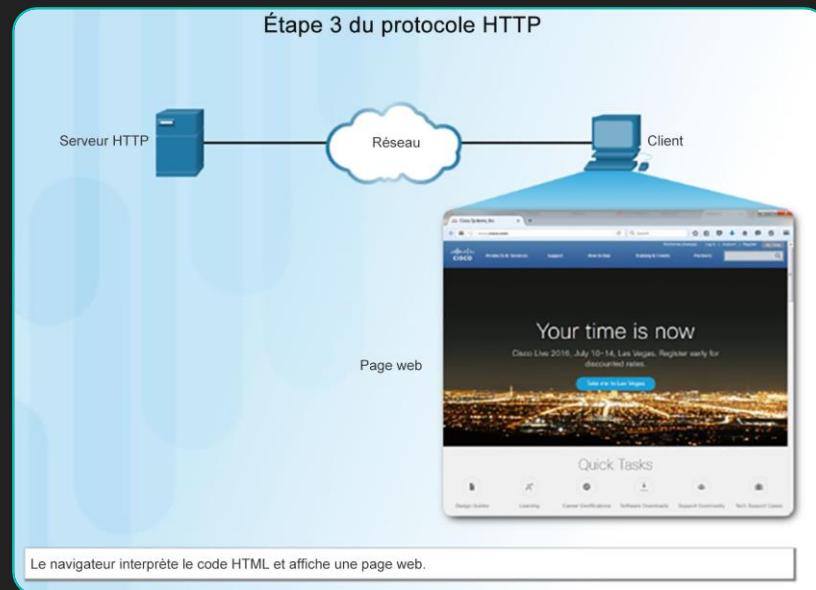


HTTP

Présentation du protocole HTTP

- Protocole HTTP (Hypertext Transfer Protocol) :
 - Port 80
 - Régit la manière dont un serveur web et un client web interagissent.
 - Basé sur TCP
 - Inclut des réponses de serveur spécifiques.
- Étapes :
 1. Le client lance une requête HTTP à un serveur.
 2. HTTP renvoie le code d'une page web.
 3. Le navigateur interprète le code HTML et affiche une page web.

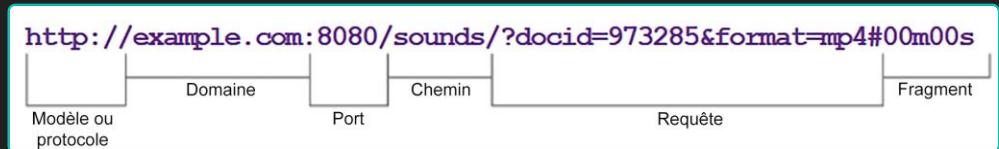
Le protocole HTTP est le protocole le plus utilisé?



HTTP

L'URL HTTP

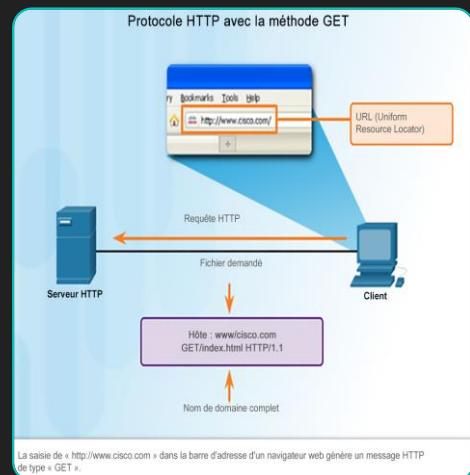
- Les URL HTTP peuvent également indiquer le port du serveur chargé de traiter les opérations HTTP.
- En outre, elles peuvent spécifier une chaîne de requête et un fragment.
- La chaîne de requête contient généralement des informations qui ne sont pas gérées par le processus de serveur HTTP lui-même, mais par un autre processus qui s'exécute sur le serveur.



Services réseau

Le protocole HTTP

- 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** : requête client visant à obtenir des données. Un client (navigateur web) envoie le message GET au serveur web pour demander des pages HTML.
 - **POST** : envoie des données devant être traitées par une ressource.
 - **PUT** : télécharge des ressources ou du contenu vers le serveur web.
 - **DELETE** : supprime la ressource spécifiée.
 - **OPTIONS** : renvoie les méthodes HTTP prises en charge par le serveur.
 - **CONNECT** : demande à un serveur proxy HTTP de transmettre la session HTTP TCP à l'hôte de destination souhaité.



HTTP

Code d'état HTTP

- Les réponses du serveur HTTP sont identifiées à l'aide de divers codes d'état qui informent l'application hôte du résultat des requêtes que le client a envoyées au serveur. Les codes sont répartis en cinq groupes.
 - **1xx** - Information
 - **2xx** – Succès
 - **3xx** – Redirection
 - **4xx** – Erreur du client
 - **5xx** – Erreur du serveur

| 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. |
| 4xx - Erreur du client | | |
| 403 | Interdit | La demande est comprise par le serveur, mais ne sera pas traitée, peut-être parce que le demandeur n'est pas autorisé à afficher la ressource. |
| 404 | Introuvable | Le serveur ne trouve pas la ressource demandée. |