Préparation à la certification CCNA 1

Cisco Certified Network Associate – Niveau 1

Document élaborer à partir du module de préparation CCNA 1

CCNA version 7.1 – Mise à jour Octobre 2022

Lycée de Lorgues Thomas Edison **Tayan JL**

Table des matières

Liste des modules de la formation CCNA 1 (v7)

Module	Objectif
1 - Les réseaux aujourd'hui	Expliquer les avancées des technologies réseau modernes.
2 - Configuration de base des commutateurs et des périphériques finaux	Mettre en œuvre les paramètres initiaux, y compris les mots de passe, l'adressage IP et les paramètres de la passerelle par défaut sur un commutateur de réseau et sur les périphériques finaux.
3 - Modèles et protocoles	Expliquer comment les protocoles réseau permettent aux périphériques d'accéder aux ressources de réseau locales et distantes.
4 - Couche physique	Expliquer comment les protocoles, services et supports réseau de couche physique prennent en charge les communications sur les réseaux de données.
5 - Systèmes numériques	Calculer les nombres entre les systèmes décimaux, binaires et hexadécimaux.
6 - Couche de liaison de données	Expliquer comment le contrôle d'accès au support dans la couche de liaison de données prend en charge la communication entre les réseaux.
7 - Commutation Ethernet	Expliquer comment l'Ethernet fonctionne sur un réseau commuté.
8 - Couche réseau	Expliquer comment les routeurs utilisent les protocoles et les services de la couche réseau pour permettre une connectivité de bout en bout.
9 - Résolution d'adresse	Expliquer comment les protocoles ARP et ND permettent de communiquer sur un réseau local.
10 - Configuration des paramètres de base d'un routeur	Mettre en œuvre les paramètres initiaux sur un routeur et des périphériques finaux.
11 - Adressage IPv4	Calculer un schéma de sous-réseau IPv4 pour segmenter efficacement votre réseau.
12 - Adressage IPv6	Mettre en œuvre un schéma d'adressage IPv6.
13 - ICMP	Utiliser différents outils pour tester la connectivité du réseau.
14 - Couche transport	Comparer les opérations des protocoles de la couche de transport dans la prise en charge de la communication de bout en bout.
15 - Couche d'application	Expliquer le rôle des protocoles de la couche application dans la prise en charge des applications destinées aux utilisateurs.
16 - Principes fondamentaux de la sécurité du réseau	Configurer les commutateurs et les routeurs avec des fonctionnalités de protection des périphériques pour renforcer la sécurité.
17 - Conception d'un réseau de petite taille	Mettre en œuvre la conception d'un petit réseau avec un routeur, un commutateur et des terminaux.

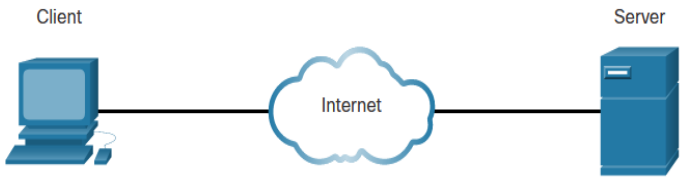
Module 1 :
Les réseaux aujourd'hui

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

1 - Les composants des réseaux (périphériques)

Client / Serveur

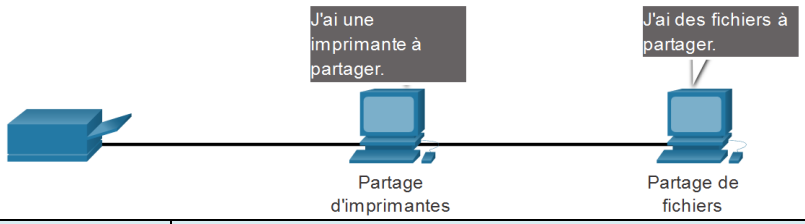
Serveur (messagerie, web, fichier, …) : Les serveurs sont des ordinateurs qui fournissent des informations aux appareils terminaux.



Client : Les clients sont des ordinateurs qui envoient des demandes aux serveurs pour récupérer des informations : page Web à partir d'un serveur Web, e-mail à partir d'un serveur de messagerie.

Peer-toPeer

Les ordinateurs peuvent jouer le rôle de serveur et de client simultanément.



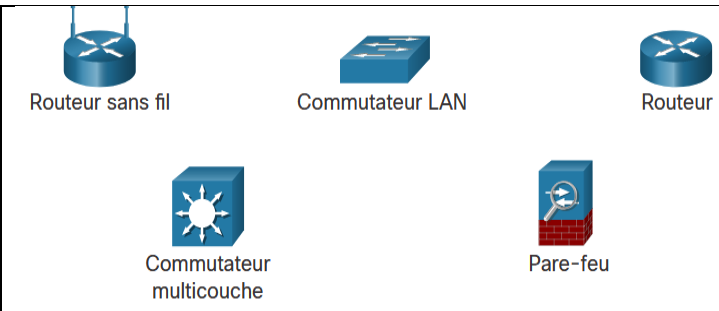
Avantages	Inconvénients
Facile à configurer Moins complexe Réduction des coûts Utilisé pour des tâches simples : transfert de fichiers et partage d'imprimantes	Pas d'administration centralisée Peu sécurisé Non évolutif Performances plus lentes

Périphériques finaux

Un périphérique final constitue soit la source soit la destination d'un message transmis à travers le réseau.

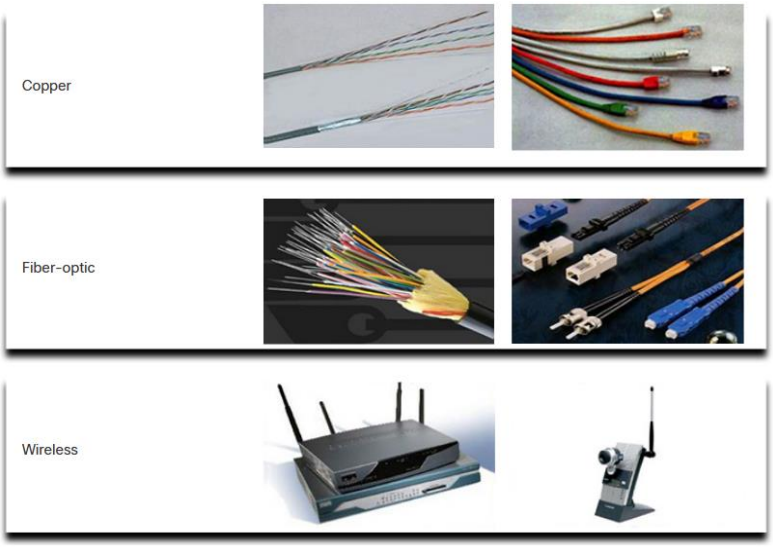
Périphériques réseaux intermédiaires

- Régénérer et retransmettre des signaux de communication.
- Gérer des informations indiquant les chemins qui existent à travers le réseau.
- Indiquer aux autres périphériques les erreurs de communication.
- Diriger des données vers d'autres chemins en cas d'échec.
-



- Classifier et diriger des messages en fonction des priorités.
- Autoriser ou refuser le flux de données, selon des paramètres de sécurité.

2 – Les supports



FILAIRE
Câble Ethernet
Câble série
(Impulsions électriques)

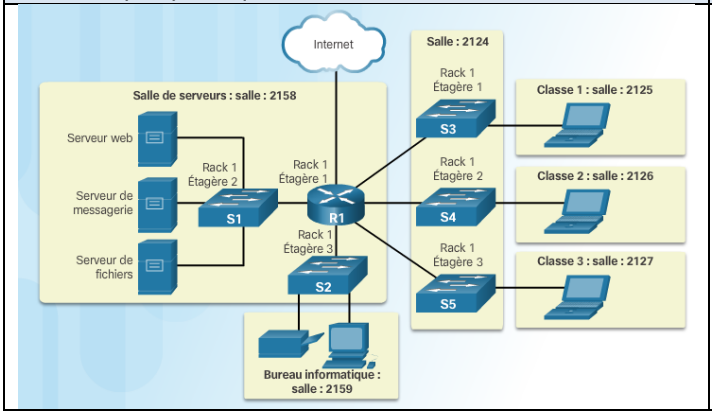
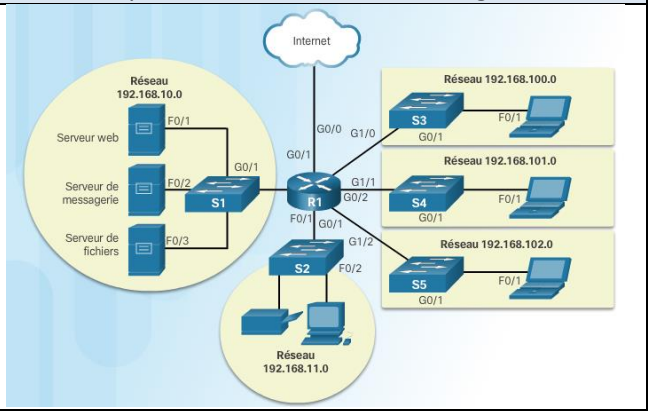
OPTIQUE
Fibre optique
(Impulsions lumineuses)

AERIEN
Wifi – Hertzien - Bluetooth
Wimax
(modulation de fréquences)

Choix du support :

- Quelle est la distance maximale sur laquelle les supports peuvent transporter correctement un signal ?
- Dans quel type d'environnement les supports seront-ils installés ?
- Quels sont la quantité de données et le débit de la transmission ?
- Quel est le coût des supports et de l'installation ?

3 – Topologies

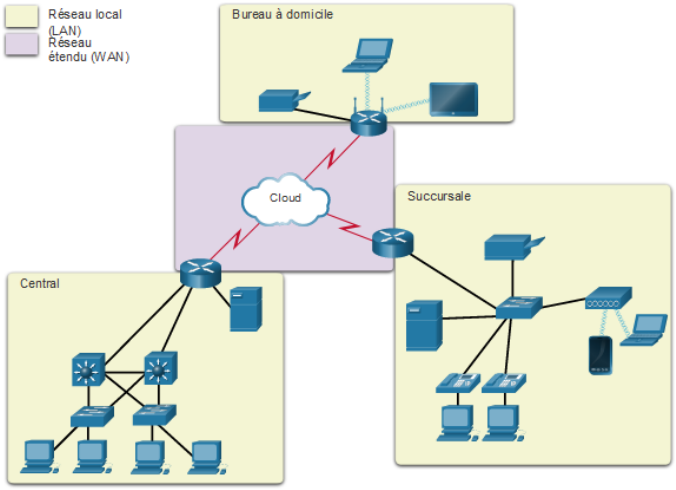
Topologie physique indiquent l'emplacement physique des périphériques intermédiaires et des câbles.	**Topologie logique** identifie les périphériques, les ports, et le schéma d'adressage.
	

Faire exercice 1.2.6 et 1.3.3

4 – Les types de réseaux

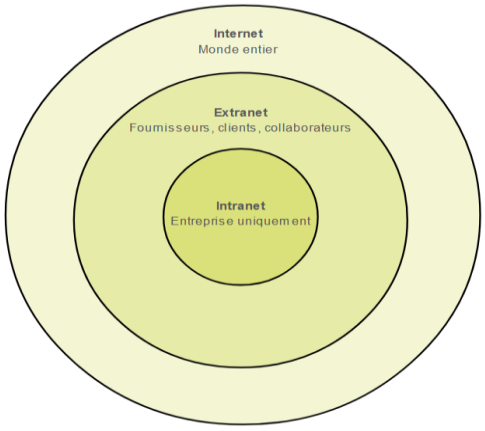
- **PAN** : Personnel Area Network (Réseau maison : ordinateur, imprimante, télé, tablette, …)
- **LAN** : Local Area Network (il s'agit généralement d'un réseau de petite ou moyenne entreprise ou d'un réseau domestique)
- **MAN** : Metropolitan Area Network – Réseau intermédiaire (couvre une zone plus vaste qu'un LAN, mais moins étendue qu'un WAN (par exemple, une ville)
- **WAN** : Wide Area Network ou réseau étendu (infrastructure réseau permettant d'accéder à d'autres réseaux au sein d'une zone géographique étendue, qui appartient généralement à un prestataire de services et dont la gestion est assurée par ce dernier) = **interconnexion de LAN**
  Les WAN sont habituellement gérés par plusieurs prestataires de services.

- **SAN** : Storage Area Network (infrastructure réseau conçue pour prendre en charge des serveurs de fichiers et pour fournir des fonctionnalités de stockage, de récupération et de réplication de données)
- **INTERNET -** Réseau mondial de réseaux interconnectés. Internet n'est pas détenu par une personne ou un groupe.



Intranet : Contrairement à Internet, un intranet est un ensemble privé de LAN et WAN internes à une entreprise qui est conçue pour être accessible uniquement pour les membres d'entreprises ou d'une filiale avec l'autorisation.

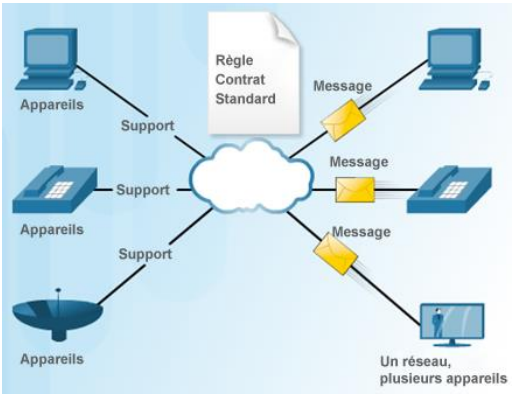
Extranet : Une entreprise peut utiliser un extranet pour fournir un accès sécurisé à leur réseau pour les personnes qui travaillent pour une autre entreprise qui ont besoin d'accéder à leurs données sur leur réseau.



Faire exercice 1.4.5

5 – Connexions Internet

Particulier / Petite entreprise	Entreprise
▪ Câble ▪ ADSL haut débit (ligne téléphonique / fibre optique) ▪ Cellulaire (réseaux 4G / 5G) ▪ Satellite ▪ Lignes commutée (vieux modem) Obsolète	▪ Satellite ▪ DSL d'entreprise (débit montant / descendant symétrique) ▪ Lignes louées à un FAI (très onéreux) ▪ Metro Ethernet (Wan Ethernet)

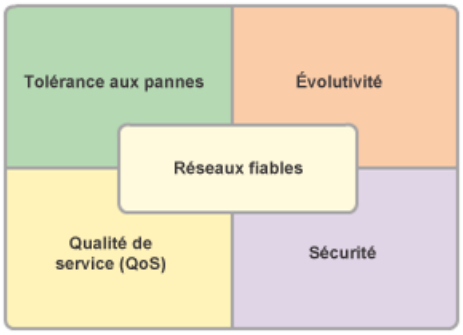


Réseaux convergents
Les réseaux convergents peuvent transmettre des données, de la voix et des flux vidéo entre différents types d'appareil, par le biais d'une même infrastructure réseau.

Cette infrastructure réseau utilise le même ensemble de règles, de contrats et de normes de mise en œuvre.

6 – Architecture des réseaux fiables

Architecture = infrastructure + les services + les protocoles



Lors de la mise en place d'un réseau, il faut respecter quatre caractéristiques :
- **La tolérance aux pannes** (prévoir des connexions redondantes).
- **L'évolutivité** (prendre en charge de nouveaux utilisateurs et applications sans affecter les performances du réseau).
- **La sécurité** (Sécurisation de l'information et des matériels).
- **La qualité de service** (QoS) (gestion des priorités entre le data, la voix, la vidéo, certains protocoles, …)

7 –Tendances des réseaux

- **BYOD (Bring Your Own Device)** : C'est la liberté donnée aux utilisateurs finaux d'utiliser leurs propres appareils pour accéder au réseau de l'entreprise ou d'un campus universitaire.
- **Collaboration en ligne** : Travailler avec une ou plusieurs autres personnes sur un projet commun.
- **Communication vidéo** : Améliore la collaboration et l'échange de savoir.
- **Cloud computing** : Permet de sauvegarder des données sur des serveurs sur internet : cloud public, privé (réservé à une entreprise, ou un gouvernement), hybride (une partie privée et autre publique), communautaire ou personnalisé (en fonction des besoins de l'entreprise)
- **Maisons intelligentes** (Objets connectés)
- **Réseau sur courant électrique** (CPL)
- **Large Bande Sans Fil** (Wireless Broadband Service). C'est une sorte de Wifi avec une portée plus importante. En France on utilise le terme de WiMax.

8 – Sécurité des réseaux

Il existe deux principaux types de sécurité :

- **Sécurité d'infrastructure réseau** (Sécurité physique des dispositifs de réseau - Prévention contre tout accès non – autorisé)
- **Sécurité des informations (**Protection de la documentation ou les données transmises sur le réseau)

Trois objectifs de sécurité du réseau :

- **Confidentialité** - uniquement les destinataires prévus puissent lire les données
- **Intégrité** - assurance que les données n'ont pas été altérées pendant leur transmission
- **Disponibilité** - garantie d'un accès rapide et fiable aux données pour les utilisateurs autorisés

Deux types de menaces :

- **Menaces internes** : appareils perdus ou volés, employés malveillants, utilisation abusive accidentelle par les employés.
- **Menaces externes** : virus, vers, logiciels espions, attaques zéro day (se produit le jour ou une vulnérabilité est détectée), attaques de déni de service, usurpation d'identité, interception et vol de données.

Sécurisation : antivirus, logiciel anti-espion, Pare feu dédié, liste de contrôle d'accès (ACL), VPN, système de prévention des intrusions.

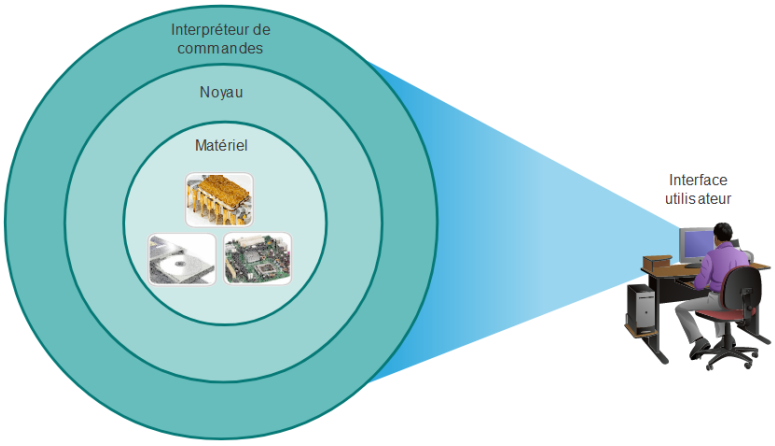
Faire exercice 1.6.6 - 1.7.10 et 1.8.3

Travail personnel : Questionnaire 1.10.2

I T : Technologie de l'Information

Module 2 :
Configuration de base des commutateurs et des terminaux

1 – Système d'exploitation



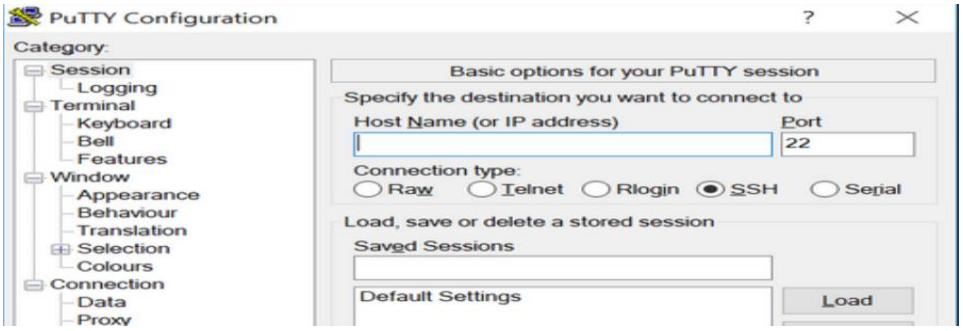
IOS
Système d'**E**xploitation **I**nterréseau

C'est le système d'exploitation installé sur les périphériques réseau (routeurs, commutateurs, pare-feu, …)

Noyau : élément qui assure la communication entre le matériel informatique et les logiciels, et gère l'utilisation des ressources matérielles pour satisfaire la configuration logicielle.
Interpréteur de commandes : Interface utilisateur qui permet aux utilisateurs de demander des tâches spécifiques à l'ordinateur. Ces requêtes peuvent être émises soit via l'interface graphique, soit via l'**I**nterface en **L**igne de **C**ommande **CLI**.

GUI : Une interface utilisateur graphique (GUI) telle que Windows, macOS, Linux KDE, Apple iOS ou Android, permet à l'utilisateur d'interagir avec le système à l'aide d'un environnement utilisant des graphiques, des icônes, des menus et des fenêtres.

Accès à l'interface de commande



Console (Serial) : Il s'agit d'un port de gestion permettant un accès hors réseau à un périphérique. L'accès hors bande désigne l'accès via un canal de gestion dédié qui est utilisé uniquement pour la maintenance des périphériques. L'avantage d'utiliser un port de console est que le périphérique est accessible même si aucun service réseau n'a été configuré. On utilise **un câble inversé (DB9 / RJ45)** ou un câble USB.

Terminal virtuel (SSH) : SSH est un moyen d'établir à distance une connexion CLI **sécurisée** via une interface virtuelle sur un réseau. À la différence des connexions de console, les connexions SSH requièrent des services réseau actifs sur le périphérique, notamment une interface active possédant une adresse IP.
Terminal virtuel (Telnet) : Telnet est un moyen non sécurisé d'établir une session CLI à distance via une interface virtuelle sur un réseau. A proscrire.

PuTTy est un logiciel d'émulation de terminal.
Il peut gérer différents types de communications : Console, Telnet, SSH, …
Equivalents à Putty : "Tera Term" ou "SecureCRT".

Exercice à faire 2.1.6

2 – Les principaux modes de commande

Mode d'exécution utilisateur : "**>**"
Il donne accès qu'a un nombre limité de commandes de surveillance de base.

Mode d'exécution privilégié : "**#**" ***enable***
Permet d'accéder à toutes les commandes et fonctionnalités.

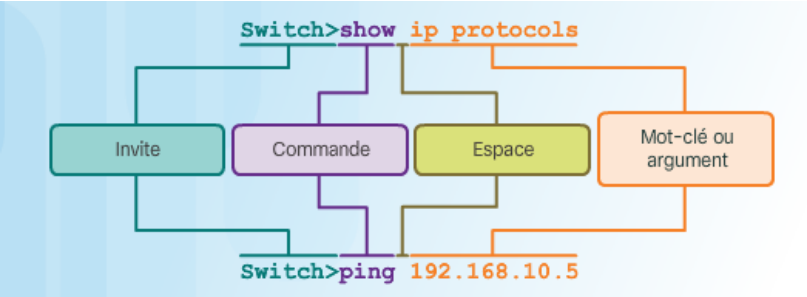
Mode de configuration globale : "**(config)#**" ***configure terminal***
Permet de configurer les interfaces, les lignes (console, VTY), VLAN, …

La commande "**exit**" vous permet de quitter le mode actuel et de remonter d'un niveau.
Les commandes "**end", "Ctrl+Z**" vous permettent de revenir directement au niveau privilège (**switch#**).

Exercice à faire 2.2.8

3 – Structure des commandes de base d'un commutateur

Invite + commande + espace + mot clé ou argument



4 – Configuration de base

Les mots de passe

- ✓ **Mot de passe de console** : sert à limiter l'accès des appareils via une connexion console (câble inversé) à partir d'un logiciel tel que PuTTy (mode sérial).
- ✓ **Mot de passe ligne VTY** : sert à limiter l'accès des appareils via le réseau à partir de logiciels tel que : Telnet, PuTTy (SSH), …
- ✓ **Mot de passe d'activation** (enable) : sert à restreindre l'accès au mode d'exécution privilégié. Le mot de passe est visible dans le fichier "running-config".
- ✓ **Mot de passe secret d'activation** (enable secret) : le mot de passe est chiffré, sert à restreindre l'accès au mode d'exécution privilégié.

Exemple de configuration de base

Switch>**enable**	Passage en mode d'exécution privilégié
Switch# **configure terminal** Switch(config)# **hostname Switch-BTS**	Passage en mode de configuration globale et attribution du nom d'hôte du commutateur (débute par une lettre, pas d'espaces, se termine par une lettre ou un chiffre, ne comporte que des lettres, des chiffres ou des tirets et comportent moins de 64 caractères).
Switch-BTS(config)# **enable secret toto**	Configuration de l'accès par mot de passe au commutateur

Switch-BTS(config)# **no ip domain-lookup**	Empêchez les recherches DNS indésirables
Switch-BTS(config)# **banner motd # L'acces au switch est interdite à toutes personnes non autorisées. #**	Configurez une bannière Message Of The Day de connexion. Le message est encadré entre deux # … #.
Switch-BTS(config)#**ip default-gateway 192.168.1.254** Switch-BTS#(config)# **interface vlan 1** Switch-BTS(config-if)# **ip address 192.168.1.1 255.255.255.0** Switch-BTS(config-if)# **no shutdown** Switch-BTS(config-if)# **exit**	Configuration de la passerelle pour joindre le routeur (indispensable si on veut configurer le commutateur à distance). Configuration de la SVI afin de permettre la gestion du commutateur à distance.
Switch-BTS(config)# **line con 0** Switch-BTS(config-line)# **password titi** Switch-BTS(config-line)# **login** Switch-BTS(config-line)# **exit**	Limitez l'accès au port de console.
Switch-BTS(config)# **line vty 0 15** Switch-BTS(config-line)# **password tata** Switch-BTS(config-line)# **login** Switch-BTS(config-line)# **end**	Configurez la ligne de terminal virtuel (VTY) pour que le commutateur autorise l'accès Telnet. Si vous ne configurez pas de mot de passe VTY, vous ne pourrez pas établir de connexion Telnet au commutateur.

Exercice à faire 2.4.8

5 – Enregistrement de la configuration actuelle

Switch-BTS**#copy running-config startup-config** ou **copy run start**.

Fichier de configuration initiale (**startup-config**) : il est stocké dans la NVRAM et reste intact si le routeur est mis hors tension.
Fichiers de configuration en cours (**running-config**) : au démarrage d'un commutateur, la configuration initiale (startup-config) est chargée dans la mémoire vive (RAM) et devient le fichier de configuration en cours. Ce fichier change immédiatement si un administrateur modifie un périphérique. Suite à cette modification, le fichier de configuration en cours devient différent du fichier de configuration initiale. Étant donné que la configuration en cours est stockée dans la mémoire vive, si l'alimentation est interrompue puis rétablie et que les changements n'ont pas été enregistré dans le fichier **startup-config**, toutes les modifications apportées seront perdues.

6 – Remarques

Adresses IP

- Chaque périphérique final d'un réseau doit être configuré avec une adresse IP.
- Autorisez les appareils à établir une communication de bout en bout sur Internet.
- La structure d'une adresse IPv4 est appelée « **notation décimale pointée** » et est composée de quatre nombres décimaux compris entre 0 et 255.

Configuration automatique des adresses IP des périphériques finaux

- Le protocole DHCP assure la configuration automatique des adresses IPv4 pour chaque appareil final utilisant DHCP. Aucune configuration supplémentaire n'est nécessaire.

Test de la connectivité de bout en bout

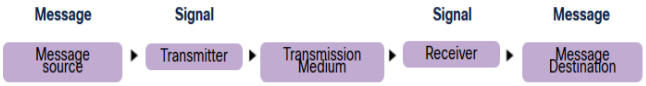
- La commande ping peut être utilisée pour tester la connectivité à un autre appareil sur le réseau ou à un site web sur Internet.

Travail personnel : Questionnaire 2.9.4

Module 3 :
Modèles et protocoles

1 – Règles de communication

Règles nécessaires pour communiquer

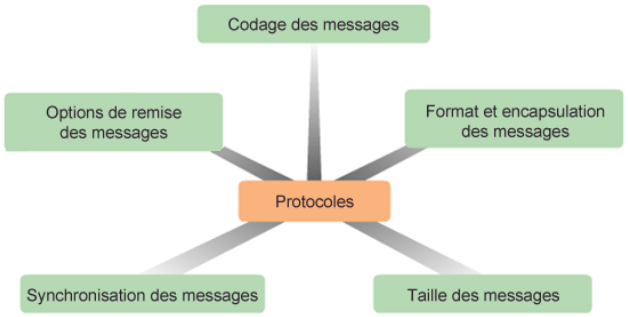


- Identification de l'expéditeur et du destinataire
- Même langage et syntaxe
- Débits identiques
- Règles communes pour la confirmation ou l'accusé de réception.
- Règles sur l'encapsulation des messages (diffère suivant le protocole → entêtes différents)
- Taille des messages
- Option de remise des messages (monodiffusion, multidiffusion, diffusion)
-

Pour communiquer il faut utiliser des protocoles.

Normes et protocoles réseaux

Les exigences d'un protocole :



- Codage des messages : adaptation du message au support de transmission.

- Taille des messages : Taille max d'une trame : 1524 octets.

- Synchronisation des messages : Méthode d'accès (quand on peut envoyer le message), contrôle du flux (même débit entre deux éléments du réseau), délai de réponse.

- Format et encapsulation des messages :

Un message qui est envoyé via un réseau informatique suit des règles de format spécifiques en vue de sa livraison et de son traitement. Les messages informatiques sont encapsulés, de la même manière qu'une lettre est placée dans une enveloppe. Chaque message informatique est encapsulé dans un format spécifique, appelé trame, avant d'être transmis via le réseau. La trame fait office d'enveloppe. Elle fournit l'adresse de la destination et celle de l'hôte source.

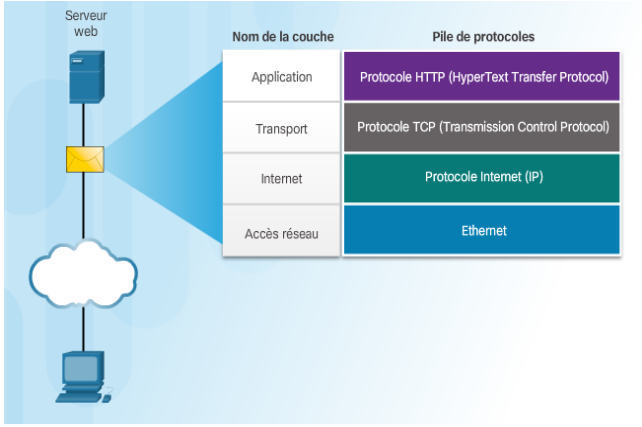
- Option de remise des messages : gestion des accusés de réception suivant le protocole utilisé.

(**Monodiffusion** : un à un, **diffusion** : un à tous, multidiffusion : un à plusieurs (classe D : Ip 224….)

Exercice à faire 3.1.12

2 – Interaction entre les protocoles

La communication entre un serveur web et un client web est un exemple d'interaction entre plusieurs protocoles.

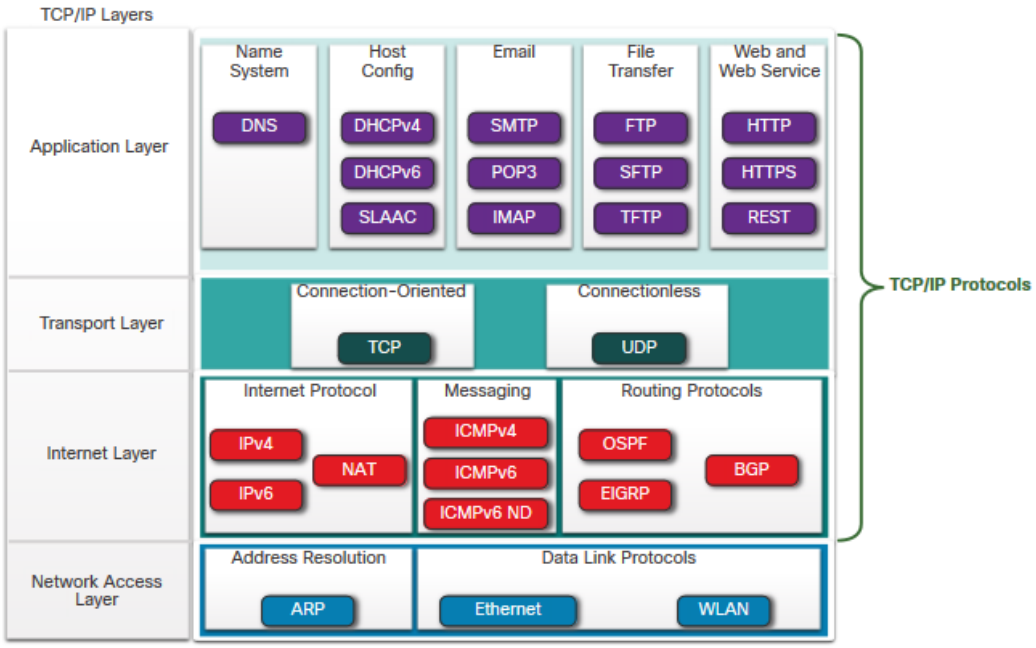


HTTP :
Régit la manière dont un serveur web et un client web interagissent. Définit le contenu et le format

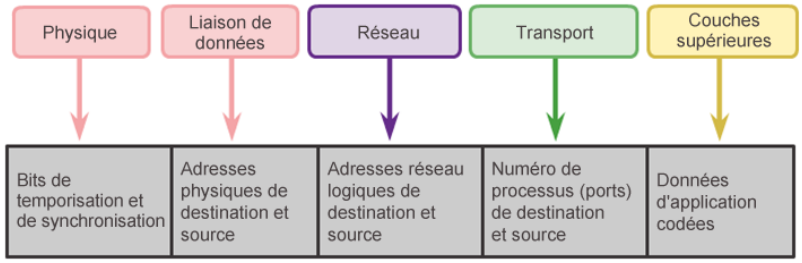
TCP :
Gère les conversations individuelles. Offre une garantie de livraison. Gère le contrôle du flux.

IP :
Fournit des messages globalement de l'expéditeur au destinataire

Ethernet : Fournit des messages d'une carte réseau à une autre carte réseau sur le même réseau local (LAN) Ethernet



PPP : Pount to Pount Protocole (encapsule les paquets pour les transmettre via une connexion série).



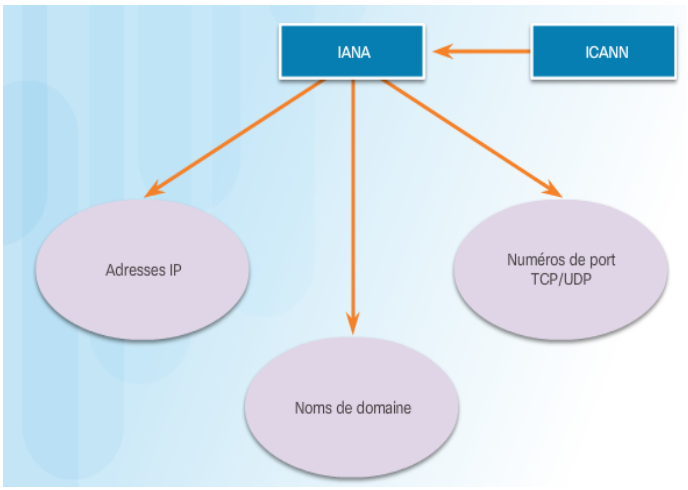
Exercice à faire 3.2.4

3 – Les normes ouvertes

Les organismes de normalisation conçoivent des normes ouvertes qui favorisent l'interopérabilité (un produit peut fonctionner indépendamment du système d'exploitation ou du logiciel ou du matériel), la concurrence et l'innovation.

Les modèle TCP/IP et le modèle OSI sont utilisés pour faciliter la normalisation dans le processus de communication

- Aide à la conception d'un protocole
- Encourage la concurrence
- Permet d'éviter que des changements technologiques ou fonctionnels dans une couche ne se répercutent sur d'autres couches, supérieures et inférieures.
- Fournit un langage commun pour décrire des fonctions et des fonctionnalités réseau.

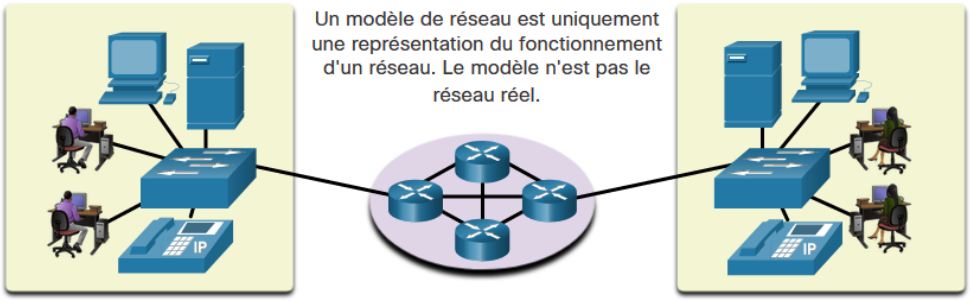


ICANN (Internet Corporation for Assigned Names and Numbers) : association basée aux États-Unis qui coordonne l'attribution des adresses IP, la gestion des noms de domaine et l'attribution des autres informations utilisées par les protocoles TCP/IP.

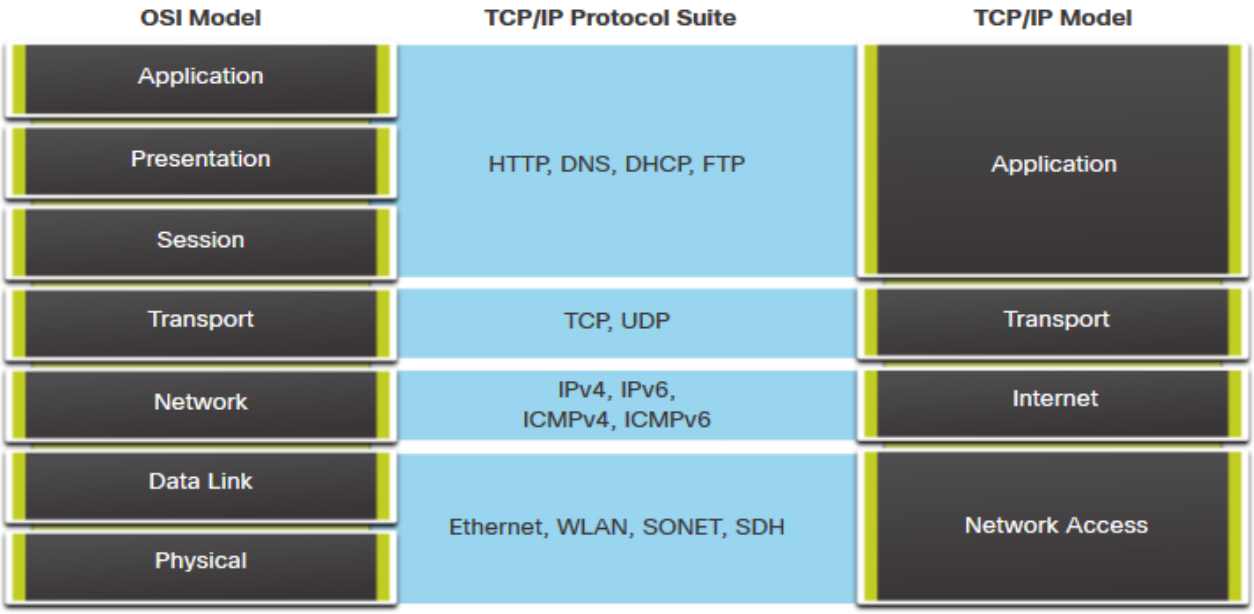
IANA (Internet Assigned Numbers Authority) : autorité chargée de superviser et de gérer l'attribution des adresses IP, la gestion des noms de domaine et les identificateurs de protocole pour le compte de l'ICANN.

4 – Modèles OSI et TCP/IP

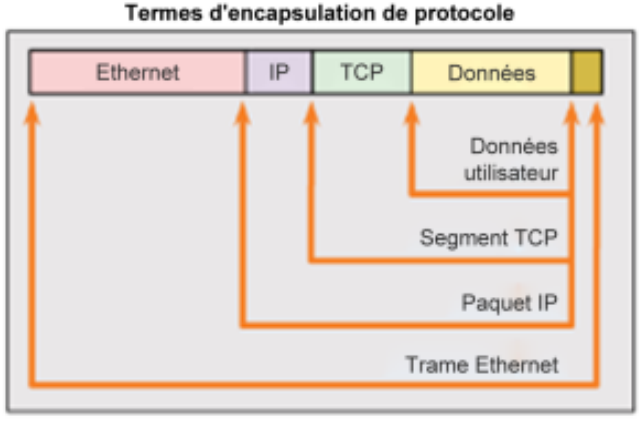
Des concepts complexes comme le fonctionnement d'un réseau peuvent être difficiles à expliquer et à comprendre. Pour cette raison, un modèle en couches est utilisé.



Deux modèles en couches décrivent les opérations réseau : modèle **OSI** et **TCP/IP**



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 plusieurs périphériques à travers 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.



PDU : **U**nité de **D**onnées de **P**rotocole

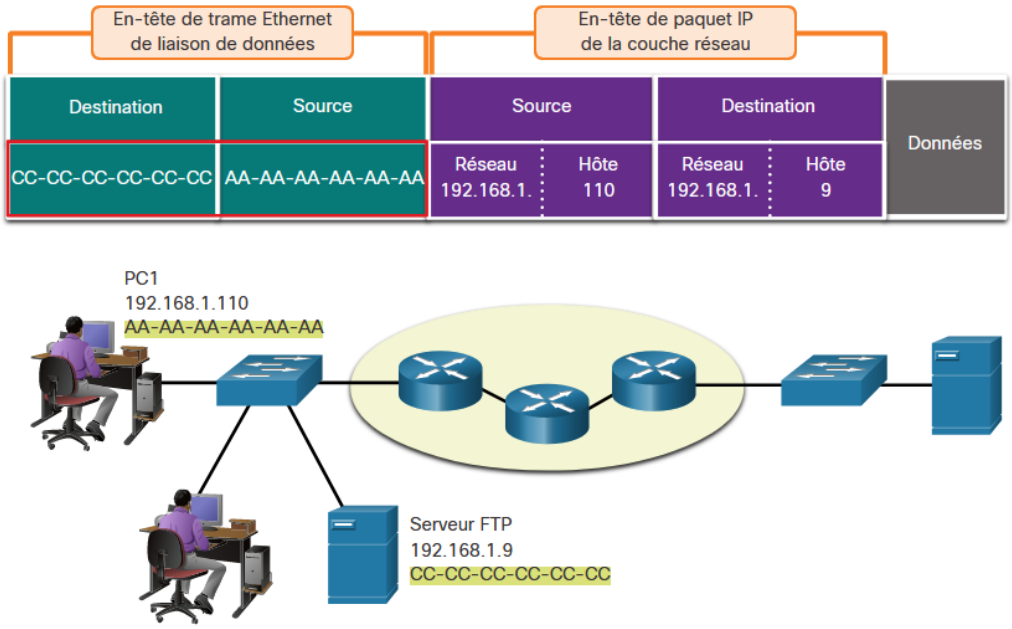
@ MAC : Adresse Physique = Adresse de liaison de données.

@ IP : Adresse logique = Adresse couche réseau

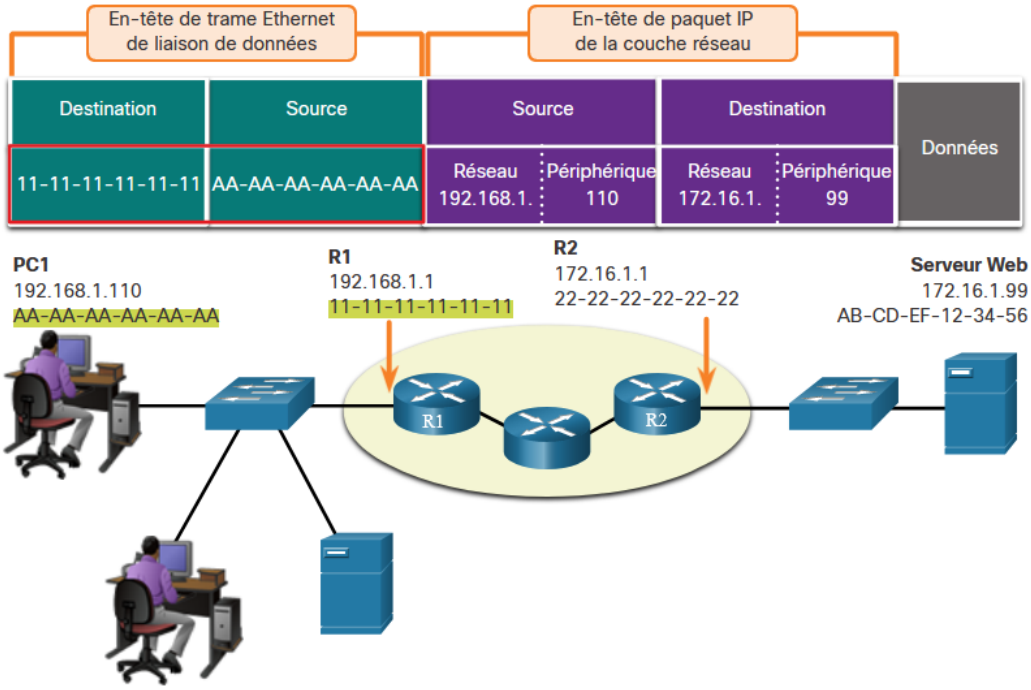
Exercice à faire – 3.3.6

5 – Communication avec un périphérique d'un même réseau ou d'un réseau distant

Périphériques sur le réseau distant



Périphériques sur un réseau distant



Communication entre le PC1 et le serveur FTP :

On est sur le même réseau => Source : @MAC et IP de PC1
Destination : @MAC et IP du serveur FTP

Communication entre le PC1 et le serveur web :

On est sur des réseaux différents => (Entre PC1 et R1) Source : @MAC et IP de PC1
Destination : @MAC R1 et @IP du serveur FTP
(Entre R1 et R3) Source : @MAC de R1 et IP de R1
Destination : @MAC R3 et @IP du serveur FTP
(Entre R3 et R2) Source : @MAC de R3 et IP de R1
Destination : @MAC de R2 et @IP du serveur FTP
(Entre R2 et Serveur WEB) Source : @MAC de R2 et IP de R1
Destination : @MAC et @IP du serveur FTP

Travail personnel : Questionnaire 3.8.2

Module 4 - Couche physique

1 – Connexion à la couche physique

Les éléments en lien avec la couche physique :

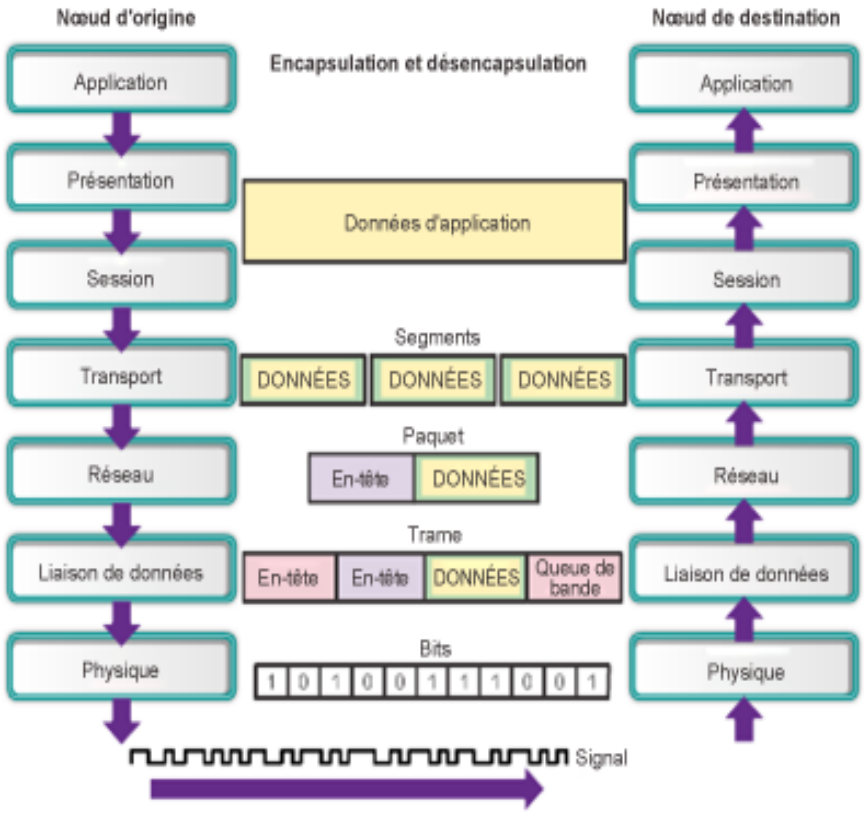
- Routeur filaire ou sans fil,
- Commutateur Ethernet,
- Carte réseau filaire
- Carte wifi

NIC = Carte d'Interface Réseau

Couche physique : code sous forme de signaux les chiffres binaires représentant les données.

Remarque : ISR (Routeur à Services Intégrés)
Dans un ISR, on peut trouver un composant de commutation (commutateur), un point d'accès sans fil, …

2 – La couche physique (modèle OSI)



Les données utilisateur sont segmentées par la couche transport, placées dans des paquets par la couche réseau, puis encapsulées sous forme de trames par la couche liaison de données.

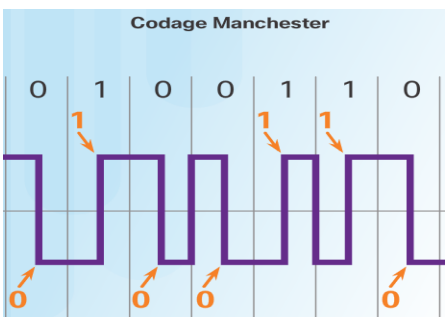
La couche physique code les trames et crée les signaux électriques, optiques ou ondulatoires (radio) qui représentent les bits dans chaque trame.

Ces signaux sont alors envoyés individuellement sur le support.

La couche physique du nœud de destination récupère ces signaux individuels sur les supports, les convertit en représentations binaires et transmet les bits à la couche liaison de données sous forme de trame complète.

Il existe trois formes élémentaires de support :

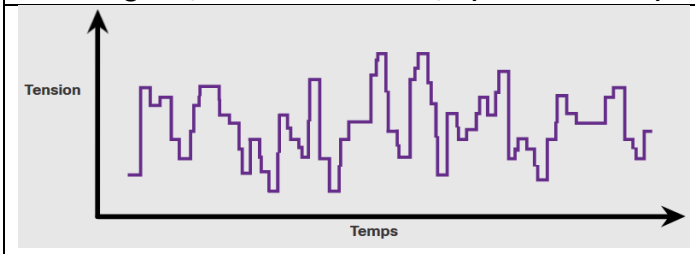
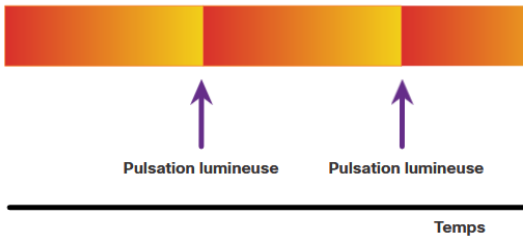
- Câble en cuivre (impulsions électrique),
- Câble à fibre optique (variations lumineuses),
- Sans fil.



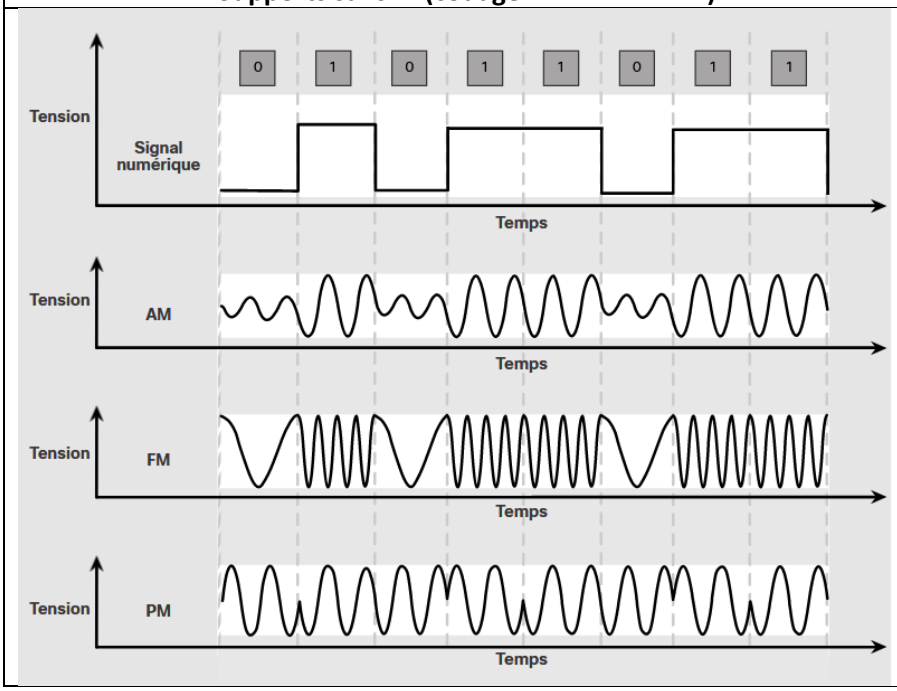
Les normes de la couche physique couvrent trois domaines :

- Composants physiques (cartes électroniques, supports, …),
- Codage Manchester (débit faible = 10 Mbit/s), codage …
- Signalisation (définir le type de signal représentant un 1 et 0)

Exercice à faire – 4.1.3

Codage 8B/10B débit de 1 Gbit/s (câble Ethernet)	Impulsions de lumière (fibre optique)
	

Supports sans fil (codage AM – FM – PM)



3 – Définitions

Bande passante : capacité d'un support à transporter des données. La bande passante numérique mesure la quantité d'informations pouvant circuler d'un emplacement à un autre pendant une période donnée. (En kbit/s)

Débit : Le débit est la mesure du transfert de bits sur le support pendant une période donnée. (kbit/s)

Analogie avec un tuyau d'arrosage :

Diamètre = bande passante et ouverture + ou – de la vanne = débit.

Le débit peut varier en fonction de :

- la quantité de trafic,
- le type de trafic,
- la latence : temps nécessaire pour voyager du point A au point B.

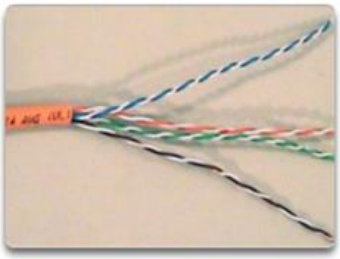
Débit applicatif = Débit – La surcharge de trafic

La surcharge de trafic : surcharge due à l'établissement de sessions, accusés de réception et encapsulation.

Exercice à faire – 4.2.7

4 – Caractéristiques du câblage en cuivre

Avantages	Inconvénients
Bon marché Facile à installer Faible résistance au courant	Limitation par la distance Problèmes d'interférences


Câble à paires torsadées non blindées (UTP)


Câble à paires torsadées blindées (STP)

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

Interférences de deux types :

- Electromagnétiques (EMI) ou radioélectriques (RFI) : moteur, éclairage fluorescent, … => blindage.
- Diaphonie : solution paire torsadée.

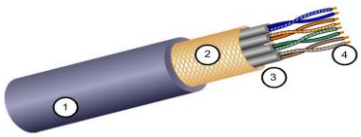

Câble coaxial

UTP : Câble à paires torsadées non blindées (U : Unshield)

Les paires n'ont pas toutes le même nombre de torsades => renforce l'effet d'annulation de diaphonie.

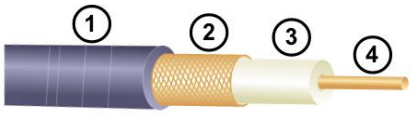
STP : Câble à paires torsadées blindées (S : Shield)

Une meilleure protection contre le bruit que l'UTP
Plus cher que UTP



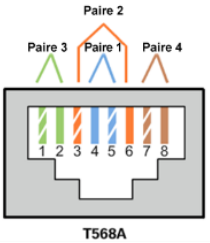
Cable coaxial

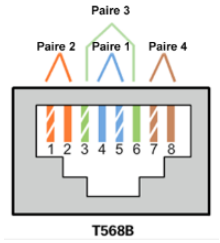
Installations sans fil- fixer les antennes aux appareils sans fil.
Installations d'internet par câble- câblage des locaux des clients.

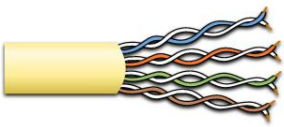


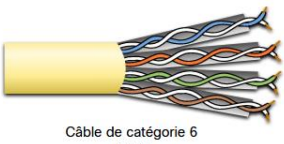
Câble droit ou croisé (la catégorie de câble est liée au débit)

DROIT	CROISE
Entre des périphériques différents (hôte et commutateur ; commutateur et routeur)	Périphériques similaires (entre deux commutateurs ; deux hôtes)



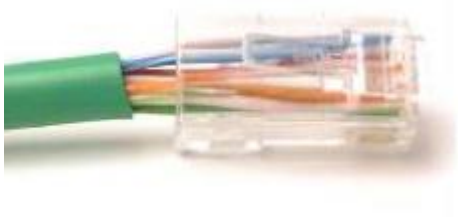



Câble de catégories 5 et 5e (UTP)


Câble de catégorie 6 (STP)

Catégorie 5e : 1 Gbit/s **Catégorie 6 : 10 Gbit/s** **Catégorie 8 : 40 Gbit/s**

Câble inversé : câble servant à connecter le port console (routeur, commutateur) au port série d'un ordinateur.

Câble mal raccordé	Câble correctement raccordé
	

Exercice à faire – 4.3.6

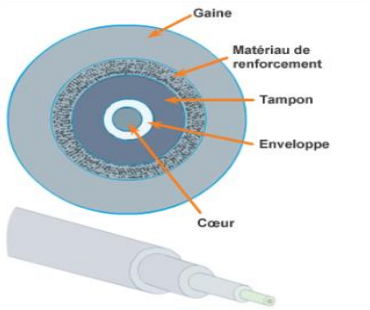
5 – Fibre optique

Transmet les données sur de plus longues distances

Transmet avec une atténuation moindre.

Elle est insensible aux perturbations électromagnétiques et radioélectriques.

Il existe la fibre monomode (9 µm - laser) et multimode (30 µm - LED)



Problèmes de mise en œuvre	Câblage à paires torsadées non blindées (UTP)	Câblage à fibre optique
Bande passante	10 Mbit/s - 10 Gbit/s	10 Mbit/s - 100 Gbit/s
Distance	Relativement courte (1 à 100 mètres)	Relativement longue (1 à 100 000 mètres)
Résistance aux perturbations électromagnétiques et radioélectriques	Faible	Haute (résistance totale)
Résistance aux risques électriques	Faible	Haute (résistance totale)
Coûts des supports et des connecteurs	Moins élevé	Plus élevé
Compétences requises pour l'installation	Moins élevé	Plus élevé
Précautions à prendre concernant la sécurité	Moins élevé	Plus élevé

Fibre multimode (MMF)	Fibre monomode (SMF)
- distances moyennes (quelques Km) - Emetteur : LED - Utilisé dans les campus, réseaux d'entreprise, …	- Prix élevé - Distances élevés (100 km) - Emetteur : LASER - Utilisé pour connecter les applications de téléphonie et de télévision par câble longue distance.

Exercice à faire – 4.5.7

6 – Support sans fil

Contraintes	Avantages
- La zone de couverture - les interférences (téléphones, fours à micro-ondes, éclairage fluorescent, …) - La sécurité (faible) - Support partagé (mode **semi-duplex** uniquement)	- Economie sur le câblage - Mobilité des hôtes

Normes sans fil			
Wi Fi	Bluetooth	Wi MAX	ZigBee

WLAN = WiFi LAN

Exercice à faire – 4.6.4

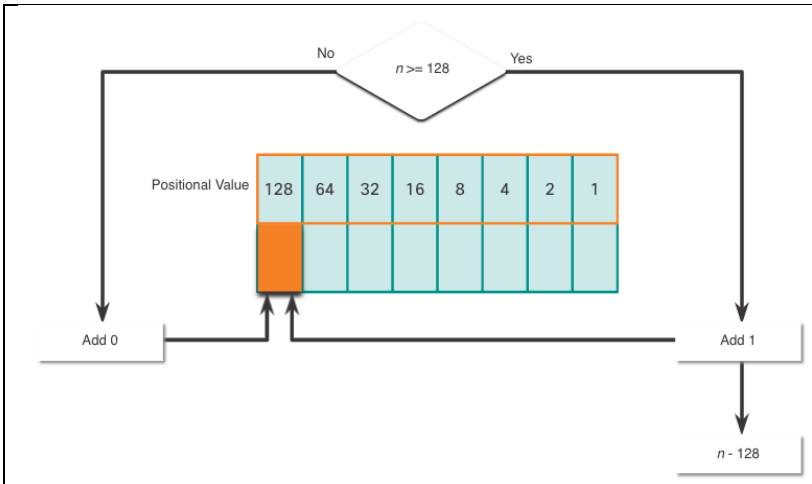
Travail personnel : Questionnaire 4.7.3

Module 5 : Systèmes numériques

1 – Conversion binaire → décimal

Valeur pondérée	128	64	32	16	8	4	2	1
Nombre binaire (11000000)	1	1	0	0	0	0	0	0
Calcul	1x128	1x64	0x32	0x16	0x8	0x4	0x2	0x1
Ajoutez-les...	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Le résultat	**192**							

2 – Conversion décimal → binaire



Commencez dans la position 128 (le bit le plus significatif). Le nombre décimal de l'octet (n) est-il égal ou supérieur à 128 ?

Si non, enregistrez un binaire 0 dans la valeur de position 128 et passez à la valeur de position 64.

Si la réponse est oui, indiquez la valeur binaire 1 dans la valeur pondérée 128 et soustrayez 128 au nombre décimal.

Répétez ces étapes en se déplaçant vers la gauche.

3 – Conversion décimal → hexadécimal

- Convertir le nombre décimal en chaînes binaires 8 bits.
- Divisez les chaînes binaires en groupes de quatre à partir de la position la plus à droite.
- Convertissez chacun des quatre nombres binaires en leur équivalent hexadécimal.

4 – Conversion hexadécimal → décimal

- Convertir le nombre hexadécimal en chaînes binaires 4 bits.
- Créez un regroupement binaire 8 bits à partir de la position la plus à droite.
- Convertissez chaque regroupement binaire 8 bits en chiffres décimaux équivalents.

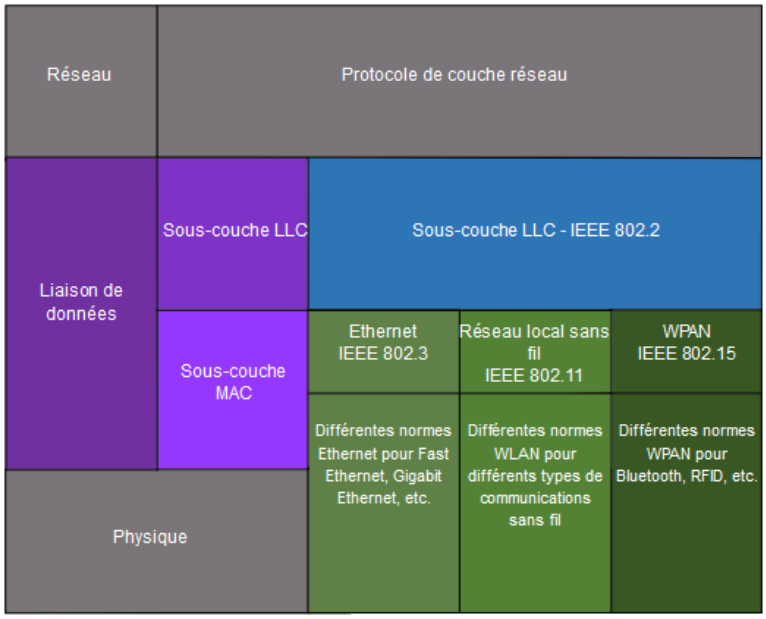
Travail personnel : Questionnaire 5.3.2

Module 6 : Couche liaison de données

1 – La fonction de la couche "liaison de données"

La couche liaison de données effectue les opérations suivantes :

- Autorise les couches supérieures à accéder au support.
- Accepte les données, les paquets de couche 3 et les encapsule dans des trames de couche 2.
- Contrôle la manière dont les données sont placées et reçues sur le support.
- Échange les trames entre les points de terminaison via le support d'un réseau.
- Reçoit des données encapsulées et les achemine vers le protocole de couche supérieure approprié.
- Effectue la détection des erreurs et rejette toute image corrompue.



La Couche liaison de données se compose de deux sous-couches :

Sous-couche LLC (Logical Link Control) : elle fait le lien entre le logiciel et le matériel (c'est le pilote de la carte réseau). Elle ajoute des informations de contrôle pour faciliter la transmission du paquet jusqu'au nœud suivant.

Contrôle d'accès au support (MAC).
- encapsulation des données (ajout des adresses MAC + le CRC).
- contrôle de l'accès au support.
- gestion des conflits (CSMA-CD).
- détection des erreurs.

A chaque saut au long du chemin, un routeur exécute quatre fonctions de base de couche 2 :

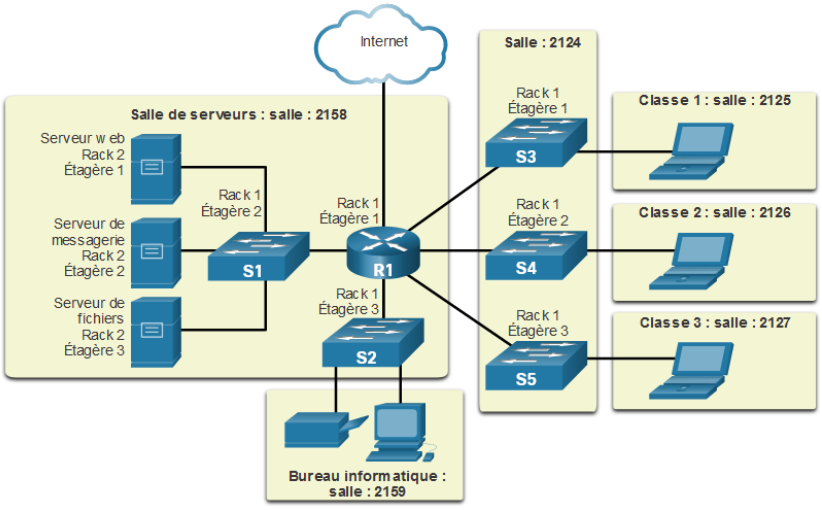
- Il accepte une trame d'un support réseau ;
- Désencapsule la trame pour exposer le paquet encapsulé.
- Réencapsule le paquet dans une nouvelle trame ;
- Transmet la nouvelle trame sur le support du segment réseau suivant.

Organismes définissants les normes pour la couche 2 : ISO, ANSI, IEEE et UIT.

Exercice à faire – 6.1.5

2 – Topologies du réseau

La topologie d'un réseau consiste à décrire l'organisation ou la relation des périphériques réseau et les interconnexions existant entre eux.

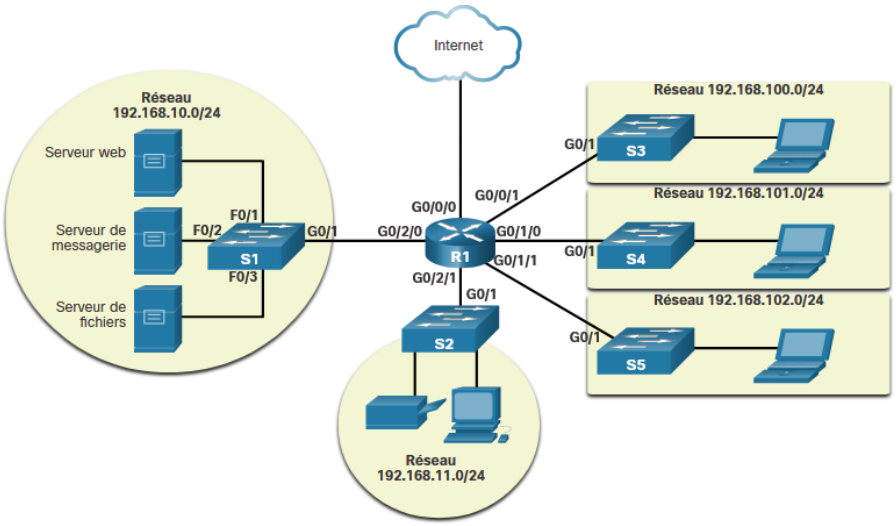


Topologie physique

Affiche les connexions physiques et la manière dont les périphériques sont interconnectés.

Nom des périphériques, emplacement (bâtiment, salle, étagère, …).

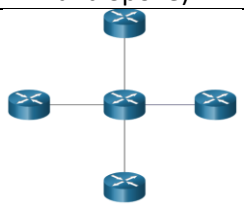
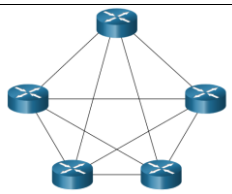
Tous les périphériques sont représentés.

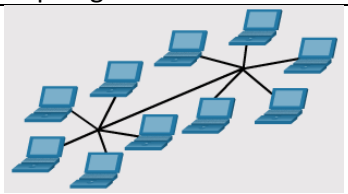
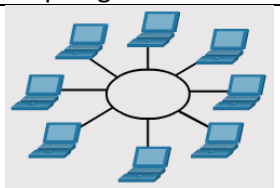
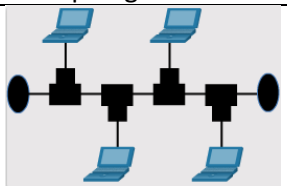


Topologie logique : identifie les connexions virtuelles entre les périphériques à l'aide d'interfaces de périphériques et des schémas d'adressage IP.

Adresses IP, nom des ports (F0/1, G0/1, …),

Nom des réseau (192.168.0.0).

Topologies physiques de réseau étendu courantes (WAN)			
Point à point	Topologie en étoile (Hub and Spoke)	Maillée	Hybride : maillage partiel
			

Topologies physiques de réseau local (LAN)			
Topologie en étoile	Topologie en étoile étendue	Topologie en anneau	Topologie en bus
			

On peut avoir les modes : bidirectionnel simultané (duplex intégral) ou non simultané (semi duplex).

Gestion des conflits
Certains réseaux à accès multiple ont besoin de règles pour décider de la manière dont les périphériques partagent les supports physiques. Deux méthodes élémentaires de contrôle d'accès sont utilisées pour les supports partagés : CSMA/CD et CSMA/CA

Accès avec gestion des conflits : tous les nœuds fonctionnant en mode semi-duplex → CSMA/CD et CSMA/CA dans le cas du Wifi.

- **CSMA/CD** : **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection
  Accès Multiple avec Ecoute de Porteuse et Détection de Collision
  ⇨ Utilisé sur les réseaux locaux Ethernet en mode semi-duplex

- **CSMA/CA** : **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **A**voidance
  Accès Multiple avec Ecoute de Porteuse et Prévention des Collisions
  Le principe et d'éviter les collisions en patientant avant d'effectuer une transmission.
  ⇨ Utilisé sur un réseau local sans fil (WLAN).

Remarque : Il n'y a pas de collision en mode Full Duplex (une paire torsadée pour l'envoie et une autre pour la réception). Obligatoire à partir d' 1 Gbit/s.

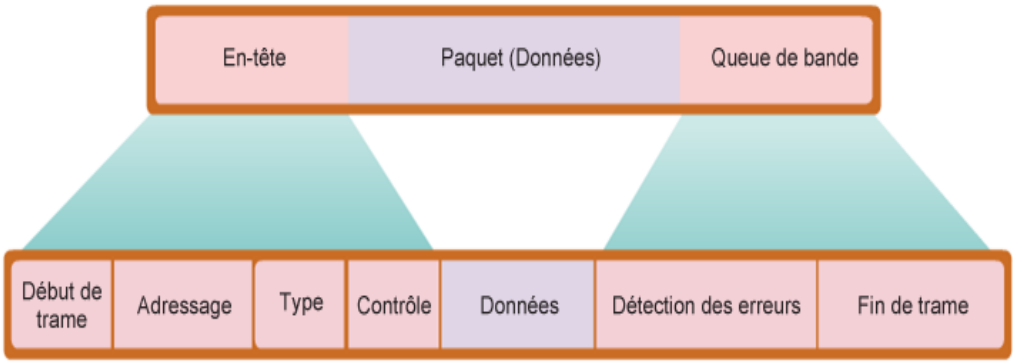
Accès contrôlé : les nœuds utilisent le support à tour de rôle (principe du jeton).

Exercice à faire – 6.2.9

3 – La trame

La trame de liaison de données comprend trois éléments de base :

- En-tête - Données - Queue de bande



Contrôle : identifie les services de contrôle de flux spéciaux comme la qualité de service (QoS).

Ethernet II

8 octets	6 octets	6 octets	2 octets	46 à 1 500 octets	4 Byoctetstes
Préambule	Adresse de destination	Adresse source	Type	Données	Séquence de contrôle de trame

- La taille minimale des trames Ethernet est de 64 octets et la taille maximale de 1 518 octets.
- Les trames inférieures à la taille minimum ou supérieures à la taille maximum sont abandonnées.
- Les trames abandonnées sont souvent le résultat de collisions ou d'autres signaux rejetés et donc traités comme étant non valides.

Préambule : (8 octets) permet la synchronisation entre les périphériques d'envoi et de réception.
Succession de 1010101010101010...11

Adresse MAC destination : il peut s'agir d'une adresse de monodiffusion, de multidiffusion ou de diffusion.

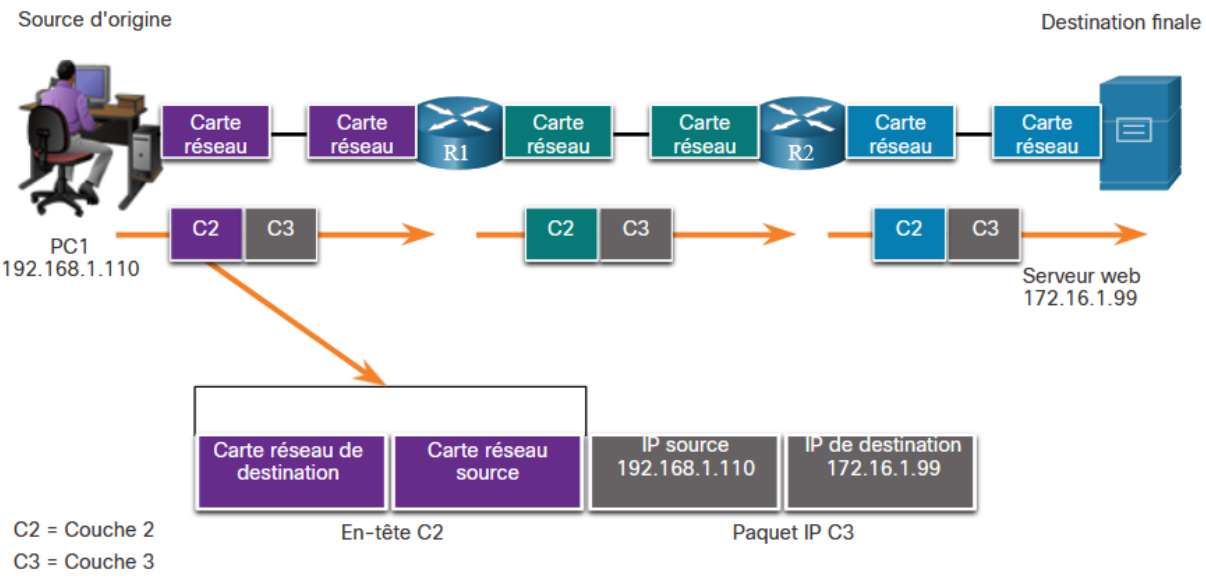
Adresse MAC source : il doit s'agir d'une adresse de monodiffusion.

Type (ou Ether Type) : Identification de la couche supérieure (valeur hexadécimale).
0x800 → IPv4 0x86DD → IPv6 0x806 → ARP
Ether type > 0x800 => Trame Ethernet 2
Ether type < 0x800 => Trame 802.3 (le champ type indique la longueur de la trame.

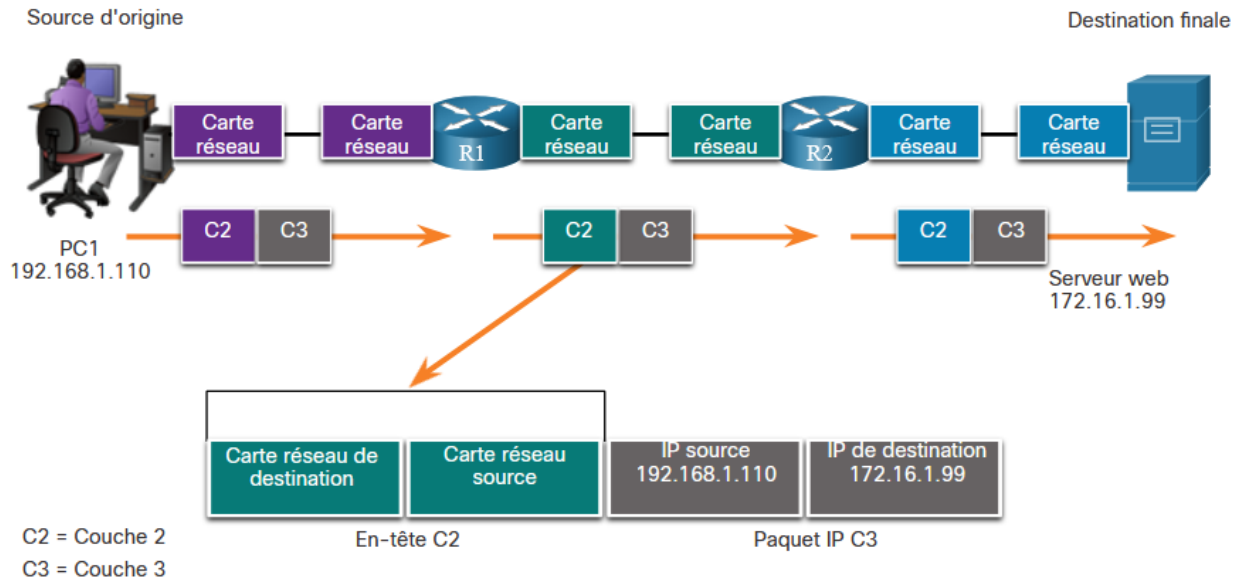
Données : comprise entre 46 et 1500 octets.

Séquence de contrôle de trame : Utilisation du CRC pour détecter une erreur.

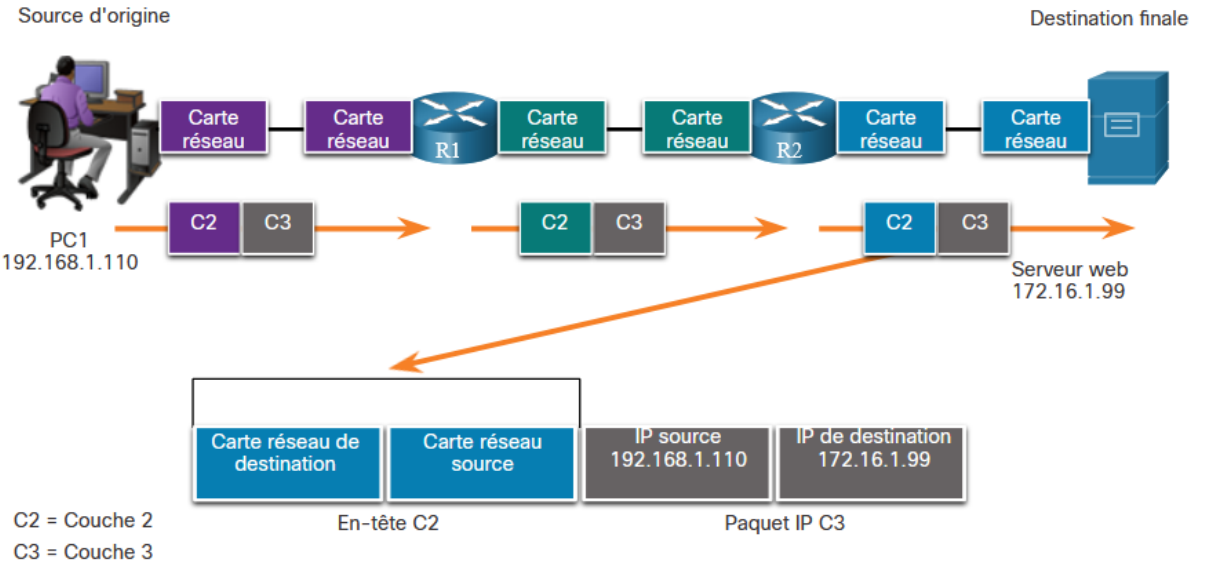
Transmission HOTE → ROUTEUR (Passerelle)



Transmission ROUTEUR → ROUTEUR



Transmission ROUTEUR → HOTE

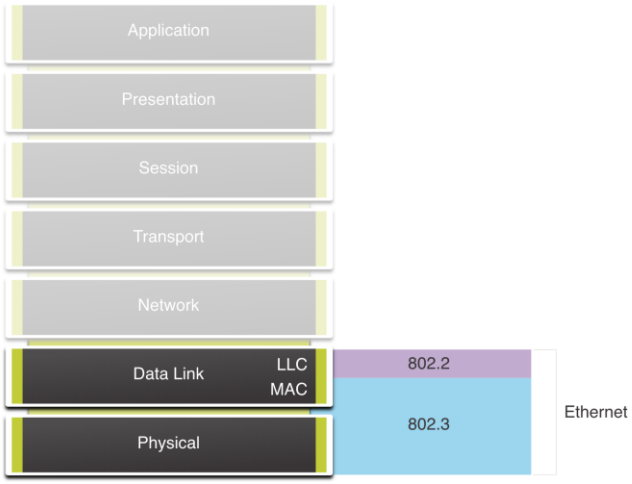


Exercice à faire – 6.3.5

Travail personnel : Questionnaire 6.4.2

Module 7 : Commutation Ethernet

1 – La trame Ethernet



Ethernet est une famille de technologies de réseau définies par les normes IEEE 802.2 et 802.3.

Sous-couche LLC: (IEEE 802.2) Place des informations dans la trame pour identifier le protocole de couche réseau utilisé pour la trame.

Sous-couche MAC : (IEEE 802.3, 802.11 ou 802.15) Responsable de l'encapsulation des données et du contrôle d'accès aux supports, et fournit l'adressage de couche de liaison de données

Ethernet II

8 octets	6 octets	6 octets	2 octets	46 à 1 500 octets	4 Byoctetstes
Préambule	Adresse de destination	Adresse source	Type	Données	Séquence de contrôle de trame

- La taille minimale des trames Ethernet est de 64 octets et la taille maximale de 1 518 octets.
- Les trames inférieures à la taille minimum ou supérieures à la taille maximum sont abandonnées.
- Les trames abandonnées sont souvent le résultat de collisions ou d'autres signaux rejetés et donc traités comme étant non valides.

Préambule : (8 octets) permet la synchronisation entre les périphériques d'envoi et de réception.
Succession de 1010101010101010...11

Adresse MAC destination : il peut s'agir d'une adresse de monodiffusion, de multidiffusion ou de diffusion.

Adresse MAC source : il doit s'agir d'une adresse de monodiffusion.

Type (ou Ether Type) : Identification de la couche supérieure (valeur hexadécimale).
0x800 → IPv4 0x86DD → IPv6 0x806 → ARP
Ether type > 0x800 => Trame Ethernet 2
Ether type < 0x800 => Trame 802.3 (le champ type indique la longueur de la trame.

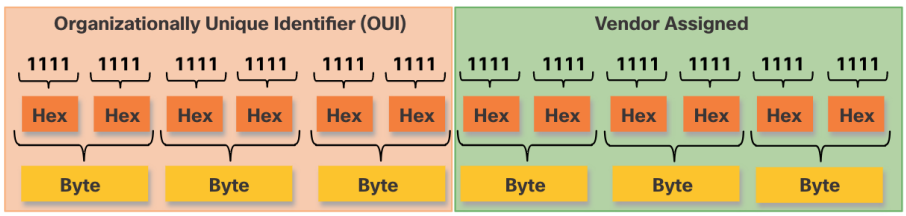
Données : comprise entre 46 et 1500 octets.

Séquence de contrôle de trame : Utilisation du CRC pour détecter une erreur

Exercice à faire – 7.1.5

2 – Adresses MAC Ethernet (ou adresse Physique)

Adresse MAC = 48 bits = 6 octets = 12 chiffres hexadécimaux = 6 combinaisons de 2 chiffres hexadécimaux.



OUI : **O**rganizationally **U**nique **I**dentifier (Identifiant du revendeur de cartes réseaux attribué par IEEE).

Un peu de vocabulaire :

- Monodiffusion : unicast (un vers un)
- Multidiffusion : multicast (un vers plusieurs) **– L'adresse MAC** commence toujours par 01-00-5E- … et l'adresse IP est comprise entre 224.0.0.0 → 239.255.255.255
- Diffusion : Broadcast (un vers tous) **- Adresse MAC de diffusion** : FF-FF-FF-FF-FF-FF

Protocole ARP (Address Resolution Protocol)

- Résolution des adresses IPv4 en adresse MAC.

- Tenue d'une table des mappages.

Dans la table, une ligne relie l'adresse MAC à l'adresse IPv4

```
Router# show ip arp

                     Age
Protocol  Address          (min)  Hardware Addr   Type   Interface
Internet  172.16.233.229     -    0000.0c59.f892  ARPA   Ethernet0/0
Internet  172.16.233.218     -    0000.0c07.ac00  ARPA   Ethernet0/0
Internet  172.16.168.11      -    0000.0c63.1300  ARPA   Ethernet0/0
Internet  172.16.168.254     9    0000.0c36.6965  ARPA   Ethernet0/0
```

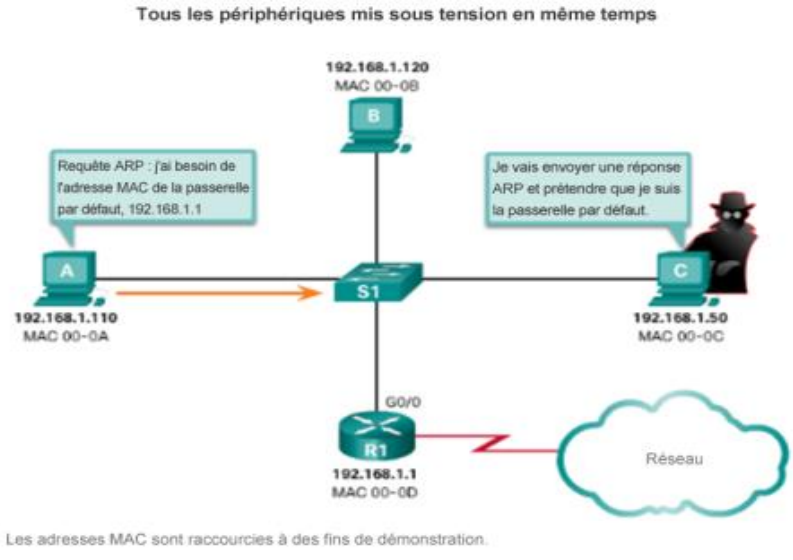
Pour la résolution des adresses

Le destinataire est sur le même réseau

- ⇨ Recherche dans la table ARP
- ⇨ Si pas d'adresse dans la table alors le commutateur envoie une requête ARP.

Le destinataire est sur un réseau distant

- ⇨ Envoi vers la passerelle (@IP)



Les problèmes liés au protocole ARP

Diffusion ARP
Les requêtes ARP peuvent inonder les segments (réseaux ou sous réseaux) locaux.

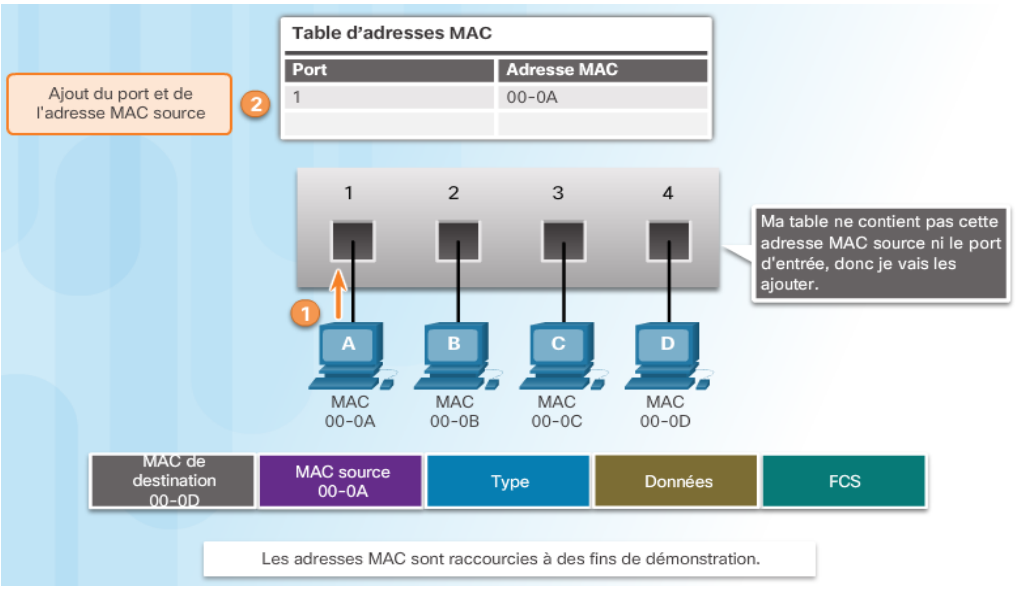
Usurpation ARP
Les cybercriminels peuvent répondre aux requêtes et prétendre être des prestataires de services. Exemple : la passerelle par défaut

4 – La table d'adresses MAC

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

Le commutateur examine l'adresse MAC source de la trame et le numéro du port par lequel la trame est entrée dans le commutateur. Si l'adresse MAC source n'existe pas, elle est ajoutée à la table, tout comme le numéro du

port d'entrée. Si l'adresse MAC source existe, le commutateur réinitialise le compteur d'obsolescence de cette entrée. Par défaut, les commutateurs Ethernet conservent les entrées dans la table pendant 5 minutes.



Remarque : la table d'adresses MAC est parfois appelée table de mémoire associative (CAM).

Exercice à faire – 7.3.6

5 – Les méthodes de transmission et vitesse de commutation

Commutateur du type "Store and Foward"

Le commutateur reçoit l'intégralité de la trame en mémoire et calcule le CRC.
Si le CRC est OK => transmission vers l'adresse de destination via le bon port.

Commutateur du type "Cut-Through"

Le commutateur achemine la trame avant qu'elle ne soit entièrement reçue.

- **Fast Forward** (la plus rapide) : transmet le paquet immédiatement après la lecture de l'adresse de destination.
- **Fragment-Free** : on transmet après avoir reçu les 64 premiers octets (la plupart des erreurs et des collisions se produisent dans les 64 premiers octets).

Mise en mémoire tampon sur les commutateurs

- Mémoire axée sur les ports (1 port = 1 mémoire).
- Mémoire centralisée et partagée par tous les ports.

Les paramètres du port de commutateur

Duplex intégral : les deux extrémités de la connexion peuvent envoyer et recevoir simultanément.
Semi-duplex : seule une extrémité de la connexion peut envoyer à la fois.
Sur les liaisons Ethernet, les problèmes de performances découlent souvent du fait qu'un des ports de la liaison fonctionne en mode semi-duplex et l'autre en mode duplex intégral.

Mode AUTO-MDIX

- Détecte le type de connexion requis et configure l'interface en conséquence.
- Réduit le nombre d'erreurs de configuration.

Trame RUNT : trame incomplète suite à une collision.

Exercice à faire – 7.4.6

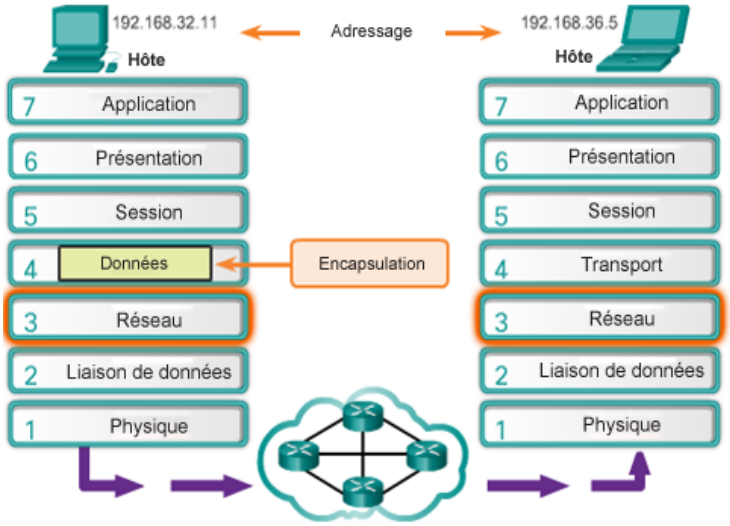
Travail personnel : Questionnaire 7.5.2

Module 8 : Couche réseau

1 – Protocole de couche réseau (IPv4 et IPv6)

Utilité de la couche réseau dans le cadre de la communication de données

- Transport de bout en bout
- Adressage des périphériques finaux
- Encapsulation
- Routage
- Désencapsulation



Les protocoles de couche réseau transfèrent les PDU de la couche transport entre les hôtes.

Caractéristiques du protocole IP

- Sans connexion : Il n'y a pas de connexion avec la destination établie avant l'envoi des paquets de données.

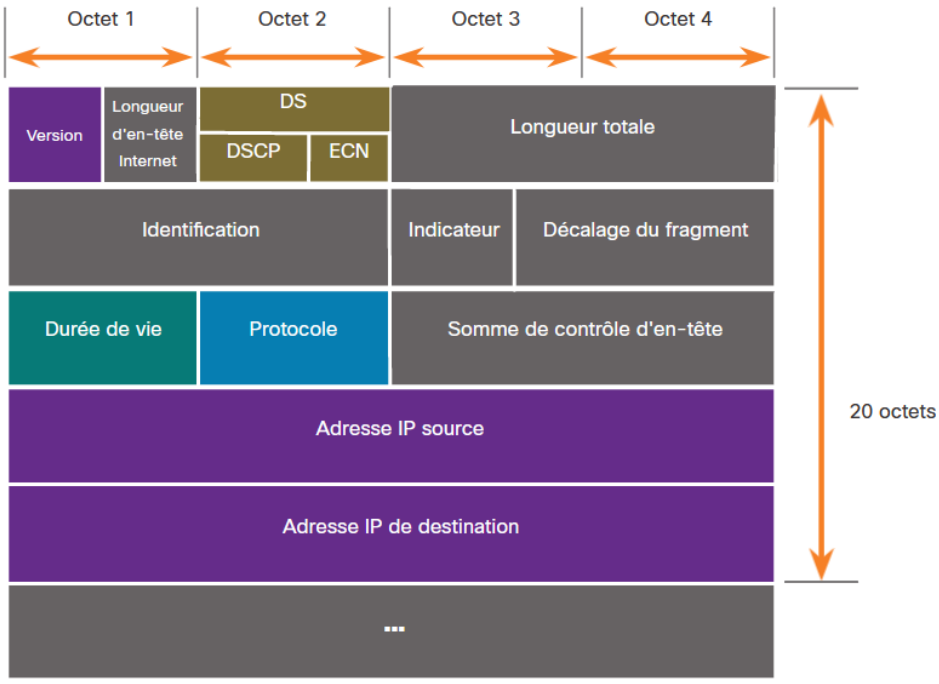
- Acheminement au mieux : la livraison n'est pas garantie (peu fiable).

- Indépendant vis-à-vis des supports.

Remarque : La fiabilité est assurée par la couche transport (protocole TCP).

Exercice à faire – 8.1.7

2 – Paquet IPv4



Version = 0100 => 4

Services différenciés (DS) est un champ de 8 bits utilisé pour définir la priorité de chaque paquet.

Somme de contrôle de l'en-tête : elle est utilisée pour détecter la corruption de l'en-tête.

TTL (Time to live) : Limite la durée de vie du paquet.

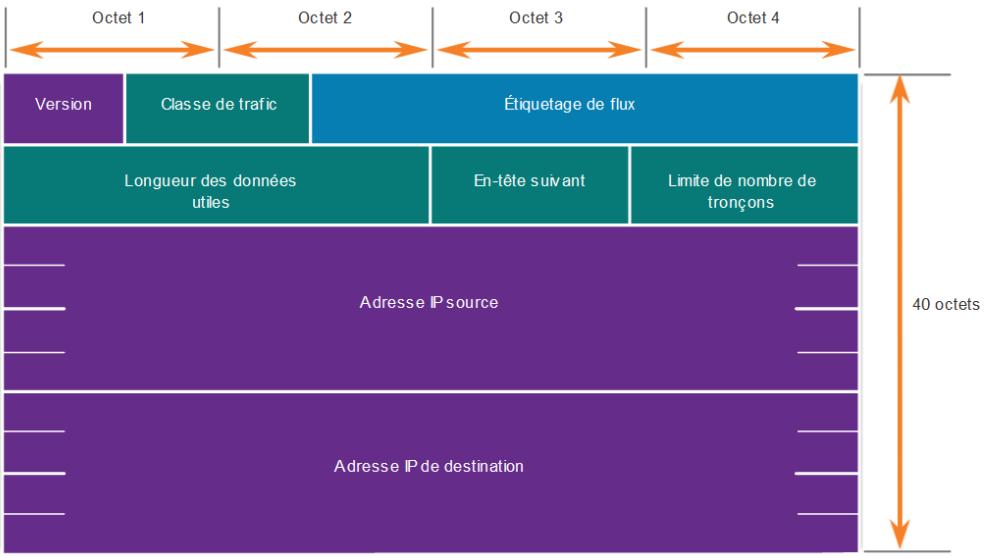
Protocole : protocole à utiliser pour la couche supérieure (TCP, UDP ou ICMP).

Les limites du protocole IPv4

- Manque d'adresses IP
- Croissance de la table de routage Internet
- Absence de connectivité de bout en bout (à cause des serveurs NAT)

Exercice à faire – 8.2.4

3 – Protocole IPv6



Version = 0110 => 6

Classe de trafic : priorité du paquet.

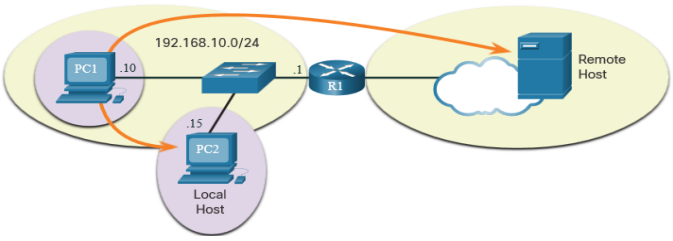
Etiquetage de flux : Tous les paquets ayant la même étiquette reçoivent le même traitement.

Longueur des données utiles : longueur totale des données (sans l'en-tête).

En-tête suivant : protocole à utiliser pour la couche supérieure.
Limite du nombre de tronçons = TTL

Exercice à faire – 8.3.5

4 – Méthodes de routage des hôtes



Deux cas :

Les appareils sur les réseaux directement connectés sont accessibles directement.

Les appareils sur des réseaux distants sont accessibles via une passerelle.

Passerelle par défaut (Routeur ou commutateur de niveau 3)

- Route le trafic vers d'autres réseaux.
- Possède une adresse IP locale située dans la même plage d'adresses que les autres hôtes du réseau.
- Peut recevoir des données et en transmettre.

Table de routage de routeur

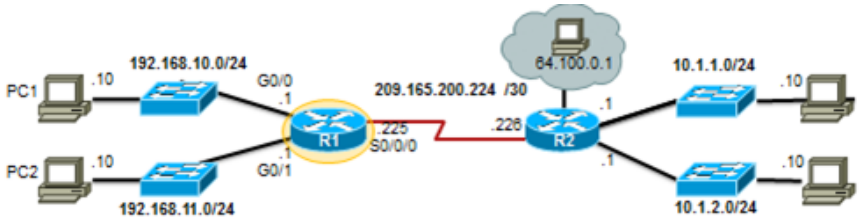
- La table de routage du routeur stocke les routages réseau que le routeur connaît.
- Utilisez la commande show ip route pour afficher la table de routage d'un routeur Cisco.
- La table de routage du routeur contient également des informations sur la méthode de détection du routage, sa fiabilité et son évaluation.
- Elle précise aussi quelle interface vous devez utiliser pour atteindre cette destination spécifique.

C : identifie **un réseau connecté directement**, créé automatiquement lorsqu'une interface est configurée avec une adresse IP et activée.

L : indique qu'il s'agit d'une **interface locale**. Fournit l'adresse IPv4 de l'interface sur le routeur.

D : Route dynamyque (échange d'infos avec d'autres routeurs).

```
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
        Serial0/0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
        Serial0/0/0
        192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
```




```
D    10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
```

A	Indique la façon dont le réseau a été « appris » par le routeur.
B	Identifie le réseau de destination.
C	Identifie la distance administrative (fiabilité) de la route source.
D	Identifie la métrique pour atteindre le réseau distant.
E	Identifie l'adresse IP du tronçon suivant pour atteindre le réseau distant.
F	Identifie le temps écoulé depuis que le réseau a été découvert.
G	Identifie l'interface de sortie du routeur utilisée pour atteindre le réseau de destination.

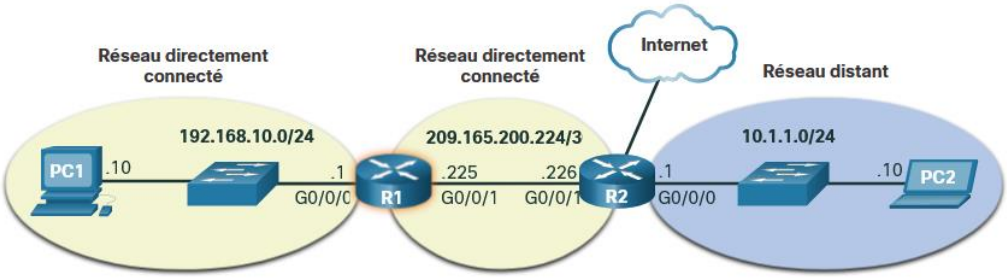
Exemple d'une route par défaut : S 0.0.0.0/0 [1/0] via S0/0/0

Route Statique (S) : idéal pour de petits réseaux. Elle est configurée manuellement par l'administrateur.

Route Dynamique (D) : permet de découvrir les réseaux à partir des infos des autres routeurs. Actualisation des routes en direct sans intervention de l'administrateur.

Exercice à faire – 8.4.5

5 – Table de routage IPv4




```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0 S* 0.0.0.0/0 [1/0] via 209.165.200.226,
GigabitEthernet0/0/1
      10.0.0.0/24 is subnetted, 1 subnets
O 10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigabiteThernet0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L 192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L 209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

- **L** - Adresse IP de l'interface locale directement connectée
- **C** – Réseau directement connecté
- **S** — La route statique a été configurée manuellement par un administrateur
- **O** – Route dynamique apprise à partir du protocole **OSPF**
- **D** - Route dynamique apprise à partir du protocole **EIGRP**

Exercice à faire – 8.5.7

Travail personnel : Questionnaire 8.6.2

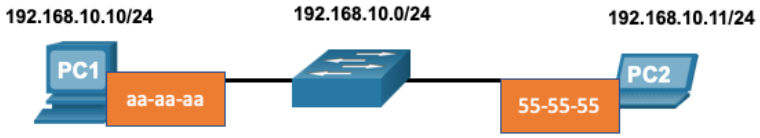
Module 9 : Résolution d'adresse

1 – Adresses MAC et IP

Destination sur un même réseau

Deux adresses primaires sont attribuées à un appareil sur un réseau local Ethernet :

- **Adresse physique de couche 2 (l'adresse MAC)** - Utilisée pour les communications de NIC à NIC sur le même réseau Ethernet.
- **Adresse logique de couche 3 (l'adresse IP)** - Utilisée pour envoyer le paquet de l'appareil source à l'appareil de destination.

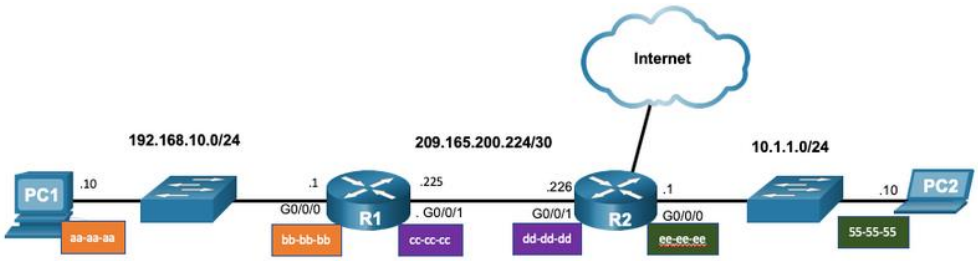


Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

Les adresses de couche 2 sont utilisées pour livrer des trames d'un NIC à un autre NIC 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.

Destination sur un réseau distant

Lorsque l'adresse IP de destination se trouve sur un réseau distant, l'adresse MAC de destination est celle de la passerelle par défaut.



Destination MAC	Source MAC	Source IPv4	Destination IPv4
bb-bb-bb	aa-aa-aa	192.168.10.10	10.1.1.10

Exercice à faire – 9.1.4

2 – ARP (Address Resolution Protocol)

Protocole ARP :
- Résolution des adresses IPv4 en adresse MAC.

- Tenue d'une table des mappages.

Dans la table, une ligne relie l'adresse MAC à l'adresse IPv4 d'un même hôte.

```
Router# show ip arp

                     Age
Protocol  Address          (min)  Hardware Addr   Type   Interface
Internet  172.16.233.229     -    0000.0c59.f892  ARPA   Ethernet0/0
Internet  172.16.233.218     -    0000.0c07.ac00  ARPA   Ethernet0/0
Internet  172.16.168.11      -    0000.0c63.1300  ARPA   Ethernet0/0
Internet  172.16.168.254     9    0000.0c36.6965  ARPA   Ethernet0/0
```

Pour la résolution des adresses

Le destinataire est sur le même réseau
- ⇨ Recherche dans la table ARP
- ⇨ Si pas d'adresse dans la table alors le commutateur envoie une requête ARP.

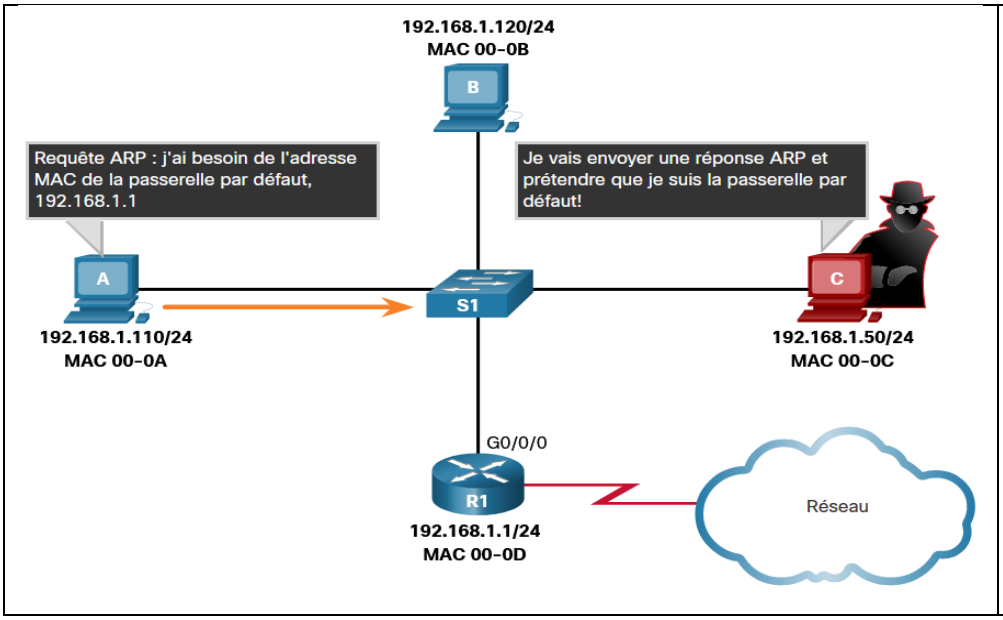
Le destinataire est sur un réseau distant
- ⇨ Envoi vers la passerelle (@IP)

Problèmes liés au protocole ARP

Génère du trafic sur le réseau à cause de la **diffusion ARP sur un** segment local (réseaux ou sous réseaux).

Diffusion ARP

Les requêtes ARP peuvent inonder les segments (réseaux ou sous réseaux) locaux.



Usurpation ARP

Dans certains cas, 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 pirate pour répondre à une requête ARP concernant l'adresse IPv4 d'un autre périphérique tel que la passerelle par défaut, comme l'illustre la figure.

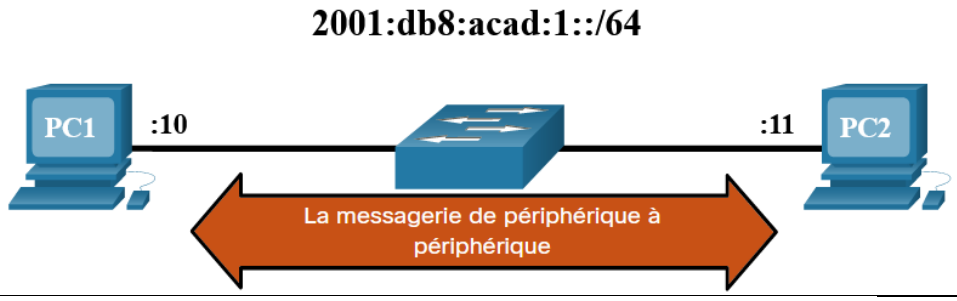
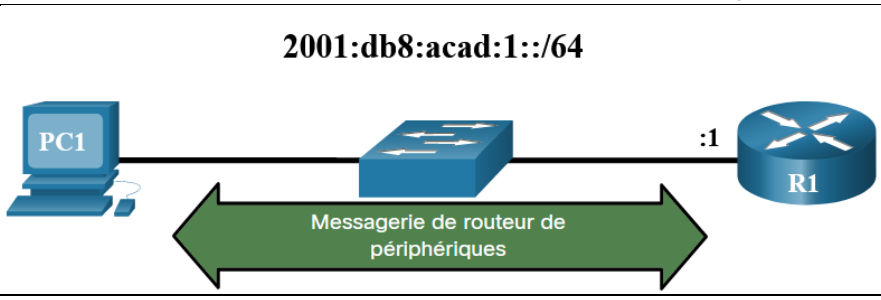
L'acteur de menace envoie une réponse ARP avec sa propre adresse MAC. Le récepteur de la réponse ARP ajoute la mauvaise adresse MAC à sa table ARP et envoie les paquets à l'acteur de la menace.

Exercice à faire – 9.2.10

3 – Découverte de voisins IPv6

Si votre réseau utilise le protocole de communication IPv6, c'est le protocole Neighbor Discovery, ou ND (ou NDP), qui remplace ARP.

Ce protocole dispose de cinq messages ICMPv6 pour effectuer ce service :

1 - Message de sollicitation de voisin 2 - Message d'annonce de voisin	
3 - Message de sollicitation de routeur (RS) 4 - Message d'annonce de routeur (RA) (utilisation de SLAAC)	

5 - Redirection du message : ce message de redirection est utilisé pour une meilleure sélection de tronçon suivant. Ces thèmes ne seront pas abordés dans ce cours.

Exercice à faire – 9.3.5

Travail personnel : Questionnaire 9.4.2

Module 10 : Configuration de base du routeur

Router >**enable**	Passage en mode d'exécution privilégié
Router # **configure terminal** Router (config)# **hostname R1**	Passage en mode de configuration globale et attribution du nom d'hôte du commutateur (débute par une lettre, pas d'espaces, se termine par une lettre ou un chiffre, ne comporte que des lettres, des chiffres ou des tirets et comportent moins de 64 caractères).
R1(config)# **enable secret toto**	Configuration de l'accès par mot de passe au commutateur
R1(config)# **no ip domain-lookup**	Empêchez les recherches DNS indésirables
R1(config)# **banner motd # L'acces au switch est interdite à toutes personnes non autorisées. #**	Configurez une bannière Message Of The Day de connexion. Le message est encadré entre deux # … #.
R1(config)# **line con 0** R1(config-line)# **password titi** R1(config-line)# **login** R1(config-line)# **exit**	Limitez l'accès au port de console.
R1(config)# **line vty 0 4** R1(config-line)# **password tata** R1(config-line)# **login** R1(config-line)# **exit**	Configurez la ligne de terminal virtuel (VTY) pour que le commutateur autorise l'accès Telnet ou SSH. Si vous ne configurez pas de mot de passe VTY, vous ne pourrez pas établir de connexion avec le commutateur.
R1(config)#**service password-encryption**	Permet de chiffrer les mots de passe dans le fichier de configuration
R1(config)#interface gigabitEthernet 0/0/0 R1(config-if)#description Lien vers le LAN Commercial R1(config-if)#ip address 192.168.0.1 255.255.255.0 R1(config-if)#ipv6 address 2001:db8:acad:10::1/64 R1(config-if)#no shutdown R1(config-if)#exit	Configuration de l'interface GigabitEthernet 0/0. Description du réseau (non obligatoire) @IP + masque de l'interface g0/0 (cela correspond à la passerelle du réseau 192.168.0.0/24). Idem pour l'adresse IPv6 Activation de l'interface.
R1(config)#int S0/0/0 R1(config-if)#ip address 192.168.1.1 255.255.255.0 R1(config-if)#no shutdown R1(config-if)#clock rate 128000 R1(config-if)#end R1#copy running-config startup-config	Configuration de l'interface Serial 0/0/0. @IP + masque de l'interface g0/0 (cela correspond à la passerelle du réseau 192.168.1.0/24). Activation de l'interface (comme une mise sous tension Si la ligne gère le DCE (DTE) alors il faut ajouter le débit (ici 128000 bit/s) Enregistrement de la configuration

Pour vérifier la configuration d'une interface on peut utiliser les commandes suivantes :

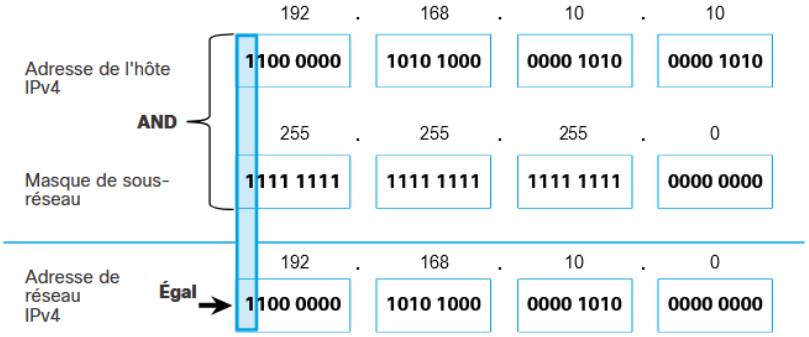
- **show ip interface brief**
- **show ip interfaces**
- **show ipv6 interface brief**
- **show ipv6 interfaces**

Travail personnel : Questionnaire 10.4.6

Module 11 : Adressage IPv4

1 – Structure de l'adresse IPv4

Pour identifier les parties réseau et hôte d'une adresse IPv4, chaque bit du masque de sous-réseau est comparé à l'adresse IPv4, de gauche à droite.



On utilise le masque de sous réseau pour repérer la partie réseau et la partie hôte.

Adresse réseau =

Adresse IP & masque de sous réseau

Longueur de préfixe (correspond au nombre de bits définis sur 1 dans le masque de sous-réseau)

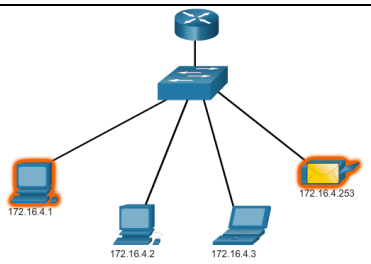
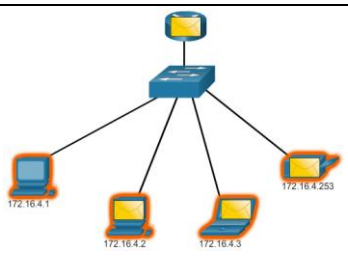
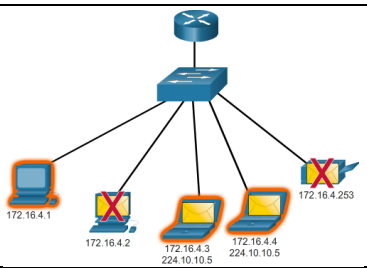
Masque de sous-réseau	Adresse 32 bits	Longueur de préfixe
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000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

Exercice à faire – 11.1.8

2 –Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

Attribution d'une adresse IPv4 à un hôte

- **Statique (manuelle)**
- **Dynamique : Utilisation d'un serveur (service) DHCP (Dynamic Host Configuration Protocol)**

		
Monodiffusion : envoyer des paquets d'un hôte à un autre.	**Diffusion** : envoyer des paquets d'un hôte à tous les hôtes du réseau	**Multidiffusion** : envoyer un paquet d'un hôte à un groupe d'hôtes en particulier, situés sur le même réseau ou sur des réseaux différents

Exercice à faire – 11.2.4

3 – Types d'adresses IPv4

Adresses privées (elles ne sont pas routables sur internet)

- **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

Adresses de bouclage : **127.0.0.0** /8 ou 127.0.0.1 à 127.255.255.254
Permet à un hôte de diriger le trafic vers lui-même

Adresses de liaison locale (link-local) ou adresses APIPA (Automatic Private IP Addressing) :
169.254.0.0 /16 ou 169.254.0.1 à 169.254.255.254
Ils sont utilisés par un client pour s'autoconfigurer dans le cas où aucun serveur DHCP n'est disponible.

Adressage par classe (Abandon de l'adressage par classe en 1990)

Classe	Bits de départ	Début	Fin	Notation CIDR par défaut	Masque de sous-réseau par défaut
Classe A	0	0.0.0.0	127.255.255.255[3]	/8	255.0.0.0
Classe B	10	128.0.0.0	191.255.255.255	/16	255.255.0.0
Classe C	110	192.0.0.0	223.255.255.255	/24	255.255.255.0
Classe D (multicast)	1110	224.0.0.0	239.255.255.255		non défini
Classe E (réservée)	1111	240.0.0.0	255.255.255.255		non défini

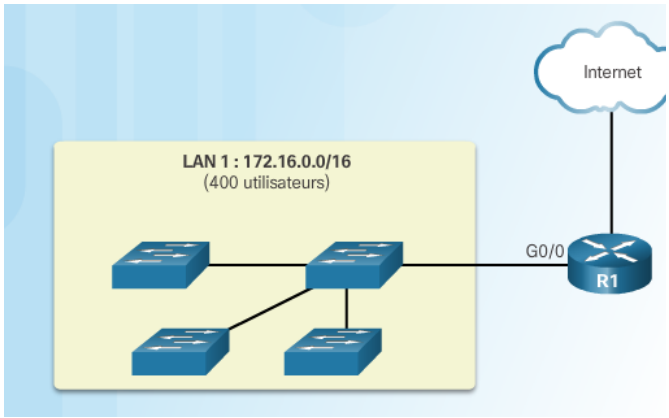
Adressage sans classe depuis 1990 (CIDR).

Attribution des adresses IP dans le monde
Pour que les entreprises ou organisations puissent prendre en charge les hôtes réseau (par exemple les serveurs web) accessibles depuis Internet, elles doivent disposer d'un bloc d'adresses publiques. L'utilisation des adresses publiques est régulée et dépend d'organisations :

- ARIN (Amériques du nord)
- RIPE (Europe, Asie centrale, Moyen Orient)
- APNIC (Asie - Pacifique)
- AFRINIC (Afrique)
- LACNIC (Amérique latine et certaines iles des Caraïbes)
- **IANA** (Gère les organismes précédents)

Exercice à faire – 11.3.3 et 11.3.8

4 – Pourquoi segmenter un réseau



Chaque interface de routeur connecte un domaine de diffusion.

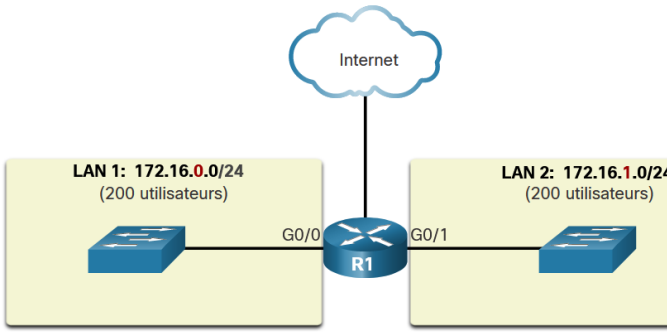
Les adresses de diffusion ne sont propagées que dans leur domaine de diffusion.

Ralentissement des opérations sur le réseau en raison d'une quantité importante de trafic de diffusion.

Solution

Réduire la taille du réseau en créant de plus petits domaines de diffusion.

Comme chaque domaine de diffusion se connecte à une interface de routeur différente, chaque domaine a besoin de son propre espace d'adressage réseau.

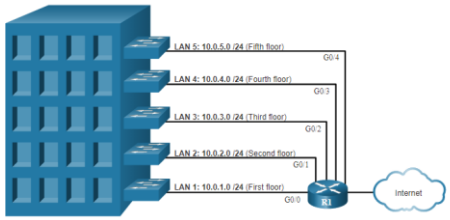
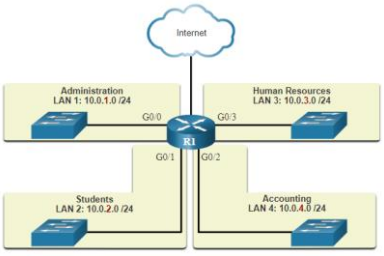
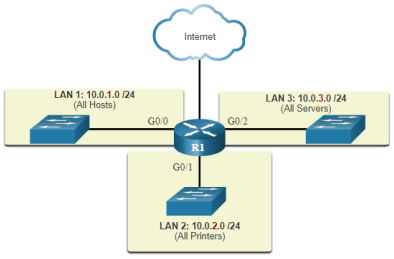


Avantages

Réduction du trafic global.

Mise en œuvre dune politique de sécurité.

Il existe plusieurs manières d'utiliser les sous-réseaux :

Lieu - Emplacement	Fonction	Type de périphériques
		

5 – Segmentation d'un réseau IPv4 en sous réseaux

Méthode 1 : Sous-réseau sur la limite d'octet (Exemple de segmentation du réseau 10.X.0.0 /16)

Adresse des sous-réseaux (256 sous-réseaux possibles)	Plage d'hôtes (65 534 hôtes possibles par sous-réseau)	Diffusion
10.0.0.0/16	10.0.0.1 - 10.0.255.254	10.0.255.255
10.1.0.0/16	10.1.0.1 - 10.1.255.254	10.1.255.255
10.2.0.0/16	10.2.0.1 - 10.2.255.254	10.2.255.255
10.3.0.0/16	10.3.0.1 - 10.3.255.254	10.3.255.255
10.4.0.0/16	10.4.0.1 - 10.4.255.254	10.4.255.255
10.5.0.0/16	10.5.0.1 - 10.5.255.254	10.5.255.255
10.6.0.0/16	10.6.0.1 - 10.6.255.254	10.6.255.255
10.7.0.0/16	10.7.0.1 - 10.7.255.254	10.7.255.255
...	...	...
10.255.0.0/16	10.255.0.1 - 10.255.255.254	10.255.255.255

On travaille sur des octets entiers (1 octet = 256 sous-réseaux)

Méthode 2 : Sous-réseau à l'intérieur d'une limite d'octet (on utilise quelques bits)

Exemple des différentes possibilités de segmentation d'un réseau /24

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

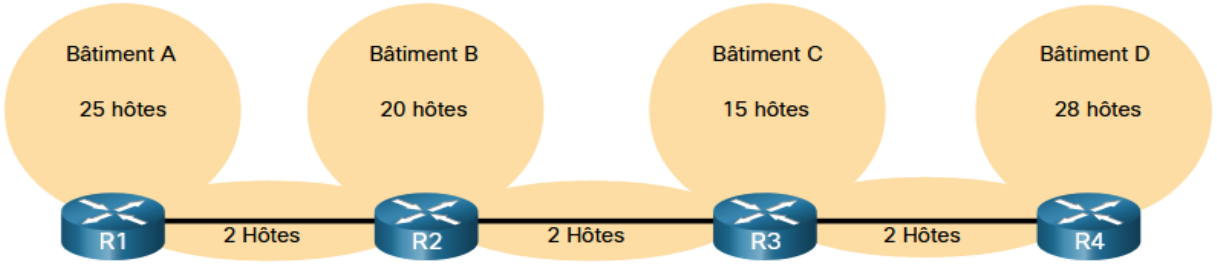
Nombre de sous réseaux = 2^n

n = nombre de bits empruntés pour créer les sous-réseaux.

Calcul du nombre d'hôtes = 2^h – 2

h = nombre de bits d'hôtes.

6 – Masque de sous réseaux de longueur variable VLSM

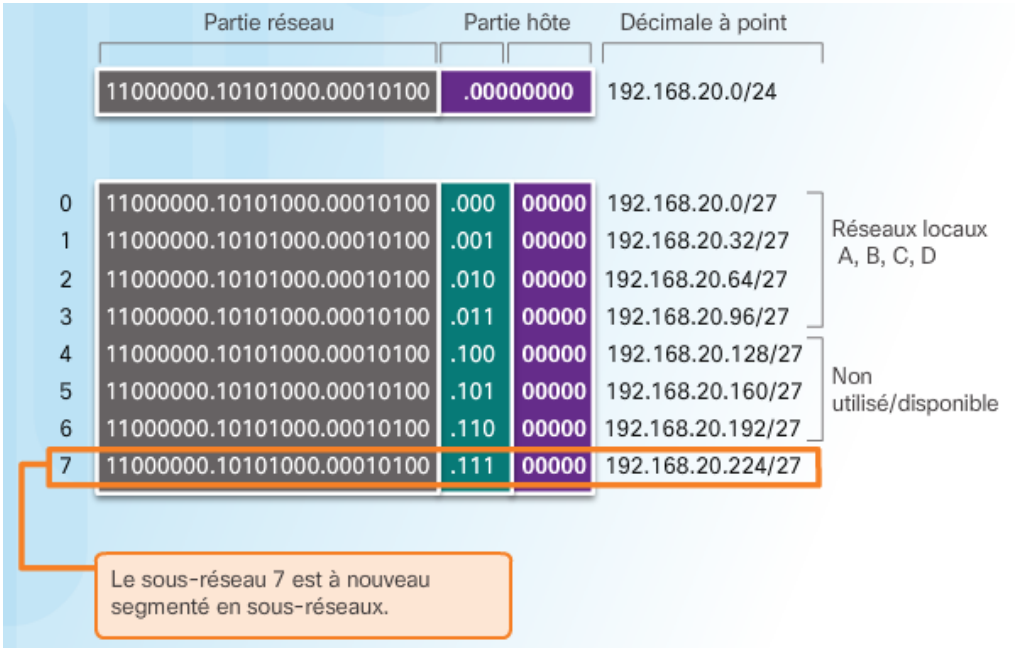


La méthode classique de segmentation en sous-réseaux n'est pas très flexible. Il en résulte un gaspillage des adresses.

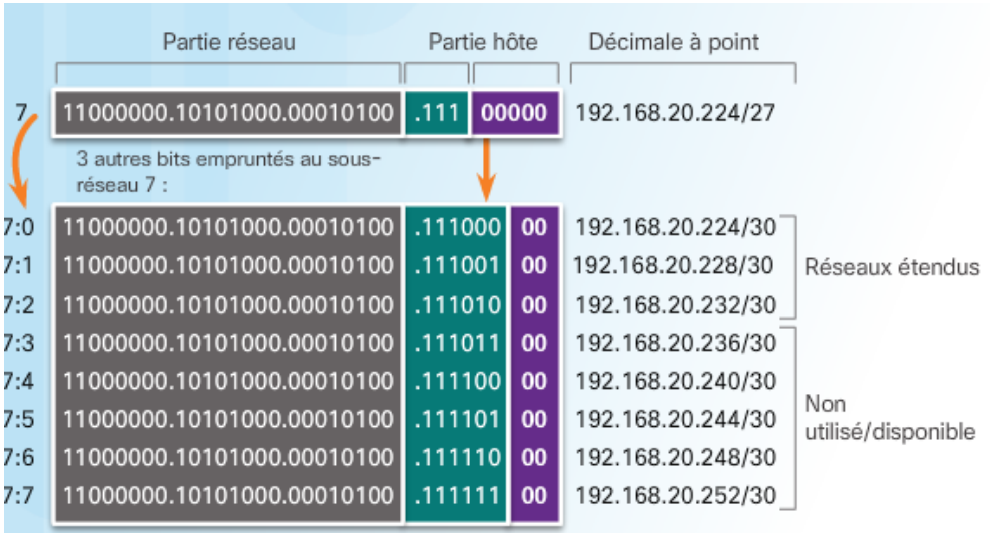
SOLUTION : Masques de sous-réseau de longueur variable.

En changeant le masque, un administrateur dispose d'un contrôle plus poussé. Moins de gaspillage.

Segmentation du réseau précédent avec une adresse réseau : 192.168.20.0 / 24



Changement de masque pour le sous-réseau n°7 puis segmentation.

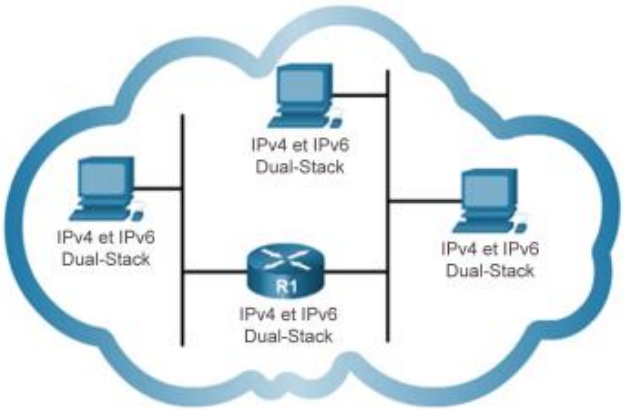


Travail personnel : Questionnaire 11.10.4

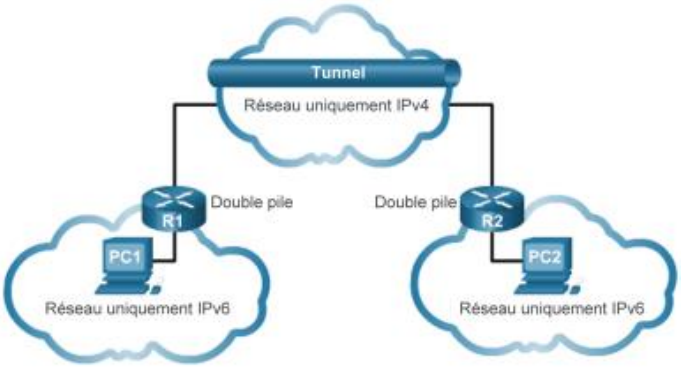
Module 12 : Adressage IPv6

1 – Problèmes liés au protocole IPv4

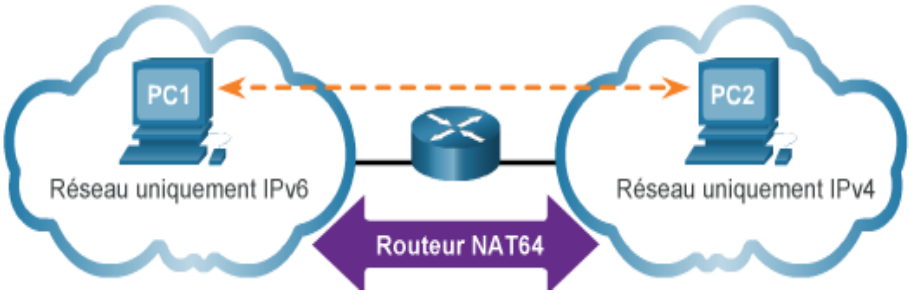
IPv6 est nécessaire car on a une pénurie d'espace d'adressage IPv4 (on est dans l'ère de l'Internet of Everything).



Double pile (dual-stack) :
IPv4 et IPv6 sur le même réseau



Tunnelisation (tunneling) : des paquets IPv6 dont encapsulés dans des paquets IPv4



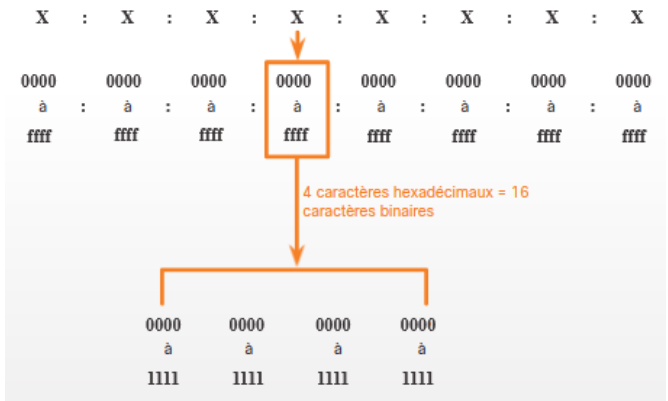
Traduction : un paquet IPv6 est traduit en un paquet IPv4, et inversement

Remarque : La tunnelisation et la traduction sont destinés à la transition vers IPv6 natif et ne doivent être utilisés qu'en cas de besoin

Exercice à faire – 12.1.3

2 – Représentation de l'adresse IPv6

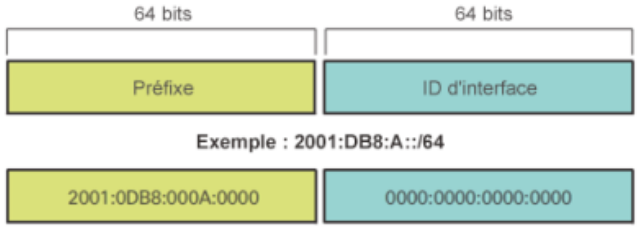
Représentation d'une adresse IPv6



Les adresses IPv6 ont une longueur de 128 bits et sont représentées par des valeurs hexadécimales.

Quatre bits peuvent être représentés par une seule valeur hexadécimale.

4 chiffres hexadécimaux = un hextet.



La longueur de préfixe est utilisée pour indiquer la partie réseau d'une adresse IPv6

La longueur de préfixe d'un LAN est généralement de /64.

Simplification des adresses IPv6

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

Règle n°2 : omettre les segments composés uniquement de zéros

Exercice à faire – 12.2.4

3 – Types d'adresses IPv6

Adresse de monodiffusion GUA (Global Unicast Address)
Adresses uniques routables sur Internet
Configurées de manière statique ou attribuées dynamiquement

Adresses de monodiffusion de liaison locale LLA (Link-Local Address) (gamme FE80::/10 à FEBF::/10)
Pour communiquer avec d'autres appareils IPv6 sur la même liaison (même sous réseau). Elle n'est pas routable sur un autre réseau. L'appareil crée sa propre adresse de liaison locale sans serveur DHCP

Adresses de monodiffusion de bouclage (::1/128)

Multidiffusion : une adresse de multidiffusion IPv6 est utilisée pour envoyer un seul paquet IPv6 vers plusieurs destinations. Exemple préfixe FF00::/8. Exemples adresses : FF02::1 ; FF02::2

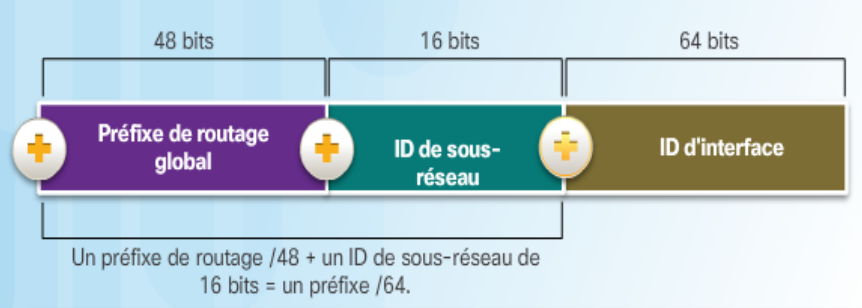
Anycast : une adresse anycast IPv6 est une adresse de monodiffusion IPv6 qui peut être attribuée à plusieurs périphériques. Un paquet envoyé à une adresse anycast est acheminé vers le périphérique le plus proche ayant cette adresse.

Attention : il n'y a pas d'adresse de diffusion en IPv6

Configurer les adresses de monodiffusion globale GUA.

L'adresse de monodiffusion globale IPv6 se compose en principe :

- d'un préfixe de routage global /48,
- d'un ID de sous-réseau 16 bits
- d'un ID d'interface 64 bits.



Exercice à faire – 12.3.8

4 – Configuration statique de GUA et LLA

Configuration statique (GUA) : configuration manuelle.
Exemple de configuration de l'interfaces G/0/0 d'un routeur avec l'adresse 2001:db8:acad:1::1/64

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
```

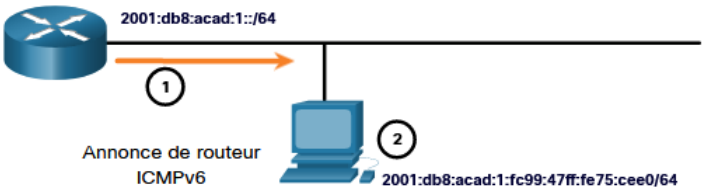
Configuration statique (LLA) : configuration manuelle.
Exemple de configuration de l'interfaces G/0/0 d'un routeur avec l'adresse fe80::1:1

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address fe80::1:1 link-local
R1(config-if)# exit
```

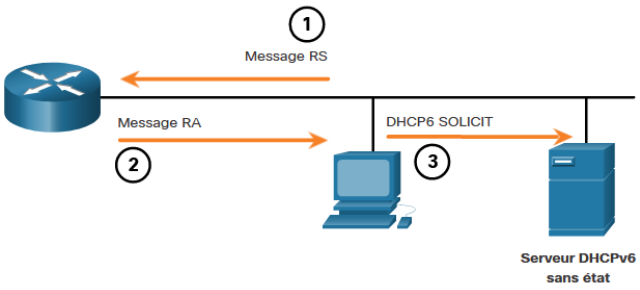
5 – Configuration dynamique des GUA

Les différentes méthodes :

1 - SLAAC : Le routeur envoie des annonces (RA – Routeur Annonce) toutes les 200 secondes (préfixe et longueur de préfixe, @ de la passerelle par défaut et @ DNS). Génération de l'@IPv6 à partir de ces infos (méthode EIU 64). Pas besoin de DHCPv6.



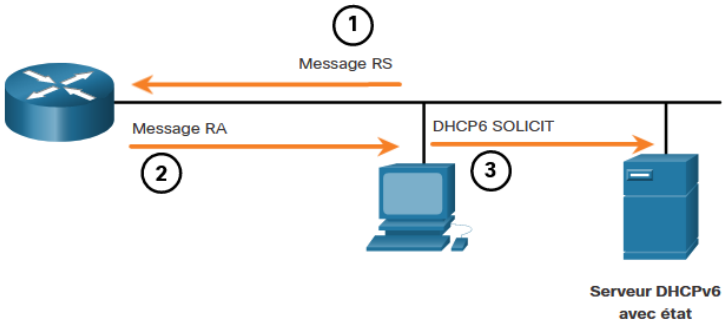
2 - SLAAC + DHCPv6 sans état : comme précédemment sauf que c'est le DHCPv6 qui donne le DNS et le nom de domaine.



RS = Message de Sollicitation (de l'hôte vers le Routeur)

RA = Message d'Annonce du Routeur (du Routeur vers les hôtes)

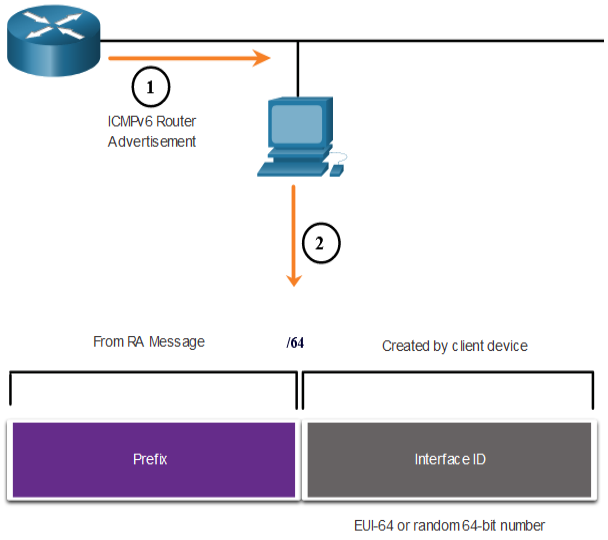
3 - Utilisation d'un DHCPv6 (avec état) : idem que DHCPv4. Tout est donnée par le DHCP.



Dans ce cas, le routeur envoie l'adresse de la passerelle, les autres infos seront fournies par le serveur DHCPv6 lorsque l'hôtes les lui demandera

Méthode EUI-64 et génération aléatoire

Lorsque le message d'annonce de routeur est la SLAAC seule ou la SLAAC avec DHCPv6 sans état, le client doit générer lui-même son ID d'interface (adresse IPv6).



L'IEEE a défini l'identifiant unique étendu (EUI), ou format EUI-64 modifié.

- Une valeur 16 bits de **fffe** (en hexadécimal) est insérée au milieu de l'adresse MAC Ethernet 48 bits du client.
- Le 7e bit de l'adresse MAC du client est inversé.

Exemple :

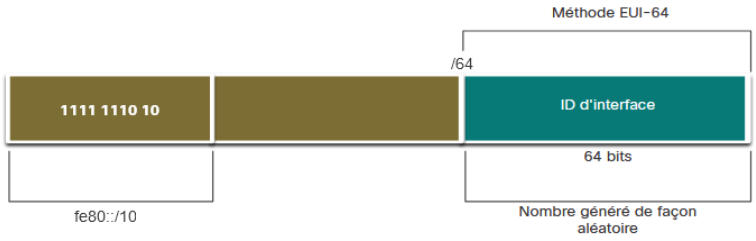
MAC 48 bits	fc:99:47:75:ce:e0
ID d'interface EUI-64	fe:99:47:ff:fe:75:ce:e0

À partir de la version Windows Vista, Windows utilise un ID d'interface généré aléatoirement au lieu d'un ID créé avec le processus EUI-64.

Exercice à faire – 12.5.8

6 – Configuration dynamique des LLA

- Toutes les interfaces IPv6 doivent avoir un IPv6 LLA.
- Comme les IPv6 GUA, les LLA peuvent être configurés dynamiquement.
- La figure montre que l'adresse link-local est créée dynamiquement à partir du préfixe FE80::/10 et de l'ID d'interface à l'aide de la méthode EUI-64 ou d'un nombre à 64 bits généré aléatoirement.



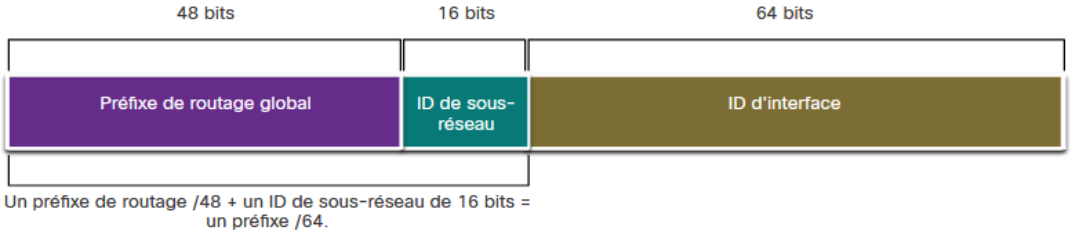
7 – Adresse de multidiffusion IPv6

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

- Les adresses de multidiffusion bien connues
  - **ff02::1 All-nodes multicast group** - Il s'agit d'un groupe de multidiffusion que tous les appareils compatibles IPv6 rejoignent. Un paquet envoyé à ce groupe est reçu et traité par toutes les interfaces IPv6 situées sur la liaison ou le réseau.
  - **ff02::2 All-routers multicast group** - Il s'agit d'un groupe multicast que tous les routeurs IPv6 rejoignent. Un routeur devient un membre de ce groupe lorsqu'il est activé en tant que routeur IPv6 avec la commande de configuration globale **ipv6 unicast-routing** .
- Adresses de multidiffusion de nœud sollicité : vous choisissez l'adresse (autre que les deux précédentes) dans la plage FF00/8

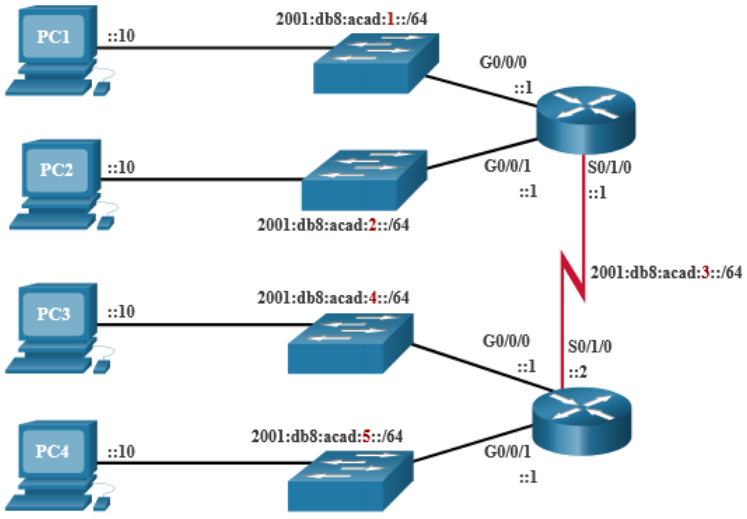
8 – Segmenter un réseau IPv6 en sous-réseau

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



- **ID de sous-réseau 16 bits** - Crée jusqu'à 65536 sous-réseaux.
- **LID de l'interface 64-bit** - prendre en charge jusqu'à 18 quintillions d'adresses IPv6 d'hôte par sous-réseau (i.e., 18,000,000,000,000,000,000).

Segmentation du réseau en sous-réseaux à l'aide de l'ID de sous-réseau



L'ID de sous-réseau prend en charge de nombreux sous-réseaux et hôtes sur un seul sous-réseau.

L'ID de sous-réseau à lui seul permet de créer jusqu'à 65 536 sous-réseaux /64.

Attribution de sous-réseaux IPv6

Le gaspillage d'adresses n'est pas un problème avec IPv6.

Les administrateurs peuvent se concentrer sur la conception d'un schéma logique pour le réseau.

Exercice à faire – 12.8.5

Travail personnel : Questionnaire 12.9.4

Module 13 : **ICMP**

1 – Messages ICMP (IPv4 ou IPv6)

Ces messages ont pour objectif de fournir des commentaires sur les problèmes liés au traitement de paquets IP dans certaines circonstances. Les messages ICMP ne sont pas obligatoires et sont souvent interdits sur les réseaux pour des raisons de sécurité.

Les messages ICMP les plus utilisés sont :

- **Accessibilité 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. Utilisé pour la commande **ping**.

- **Destination or Service Unreachable** (destination ou service inaccessible)

  Codes de Destination Inaccessible pour l'ICMPv4 :
  - 0 - Réseau inaccessible
  - 1 - Hôte inaccessible
  - 2 - Protocole inaccessible
  - 3 - Port inaccessible

  Codes de Destination Inaccessible pour l'ICMPv6 :
  - 0 - Pas de route vers la destination
  - 1 - La communication avec la destination est interdite administrativement (par exemple lorsque l'on rencontre un pare-feu qui bloque l'accès)
  - 2 - Au-delà de la portée de l'adresse source
  - 3 - Adresse inaccessible
  - 4 - Port inaccessible

- **Time exceeded (Délai dépassé)**
  Lorsque le champ Durée de vie (TTL) d'un paquet est décrémenté à 0, un message ICMPv4 Délai dépassé est envoyé à l'hôte source.
  ICMPv6 envoie également un message Délai dépassé. Au lieu du champ TTL IPv4, ICMPv6 utilise le champ Hop Limit IPv6 pour déterminer si le paquet a expiré.

Exercice à faire – 13.1.6

2 – Test à l'aide des commandes ping et traceroute

Le protocole ICMP sert à tester la connectivité réseau (ping, traceroute, tracert).

Confirmation de l'hôte
Destination ou service inaccessible
Dépassement du délai (TTL = 0)
Redirection du routeur

La commande **ping**
Pour tester la connectivité à un autre hôte sur un réseau, une demande d'écho est envoyée à l'adresse de l'hôte à l'aide de la commande **ping**. Si l'hôte à l'adresse spécifiée reçoit une requête d'écho, il répond en envoyant une réponse d'écho. Au fur et à mesure de la réception de chaque réponse, **ping** fournit un retour d'information sur le

temps écoulé entre l'envoi de la demande et la réception de la réponse. Cela peut être utilisé pour mesurer les performances réseau.
Exemple d'utilisation de la commande ping :

- 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

La commande **traceroute** : tester le chemin
Si les données parviennent à destination, la commande affiche la liste des interfaces de tous les routeurs situés entre les hôtes. Si les données restent bloquées au niveau d'un tronçon, l'adresse du dernier routeur ayant répondu à la commande peut fournir une indication sur l'endroit où se situe le problème ou sur d'éventuelles restrictions de sécurité.
L'utilisation de traceroute fournit le temps aller-retour pour chaque saut le long du chemin et indique si un saut ne répond pas.

Travail personnel : Questionnaire 13.3.4

Module 14 : Couche transport

1 – Transport des données

La couche transport est chargée de l'établissement d'une session de communication temporaire entre deux applications et de l'acheminement des données entre elles.
La couche de transport comprend deux protocoles :

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

Rôle de la couche transport

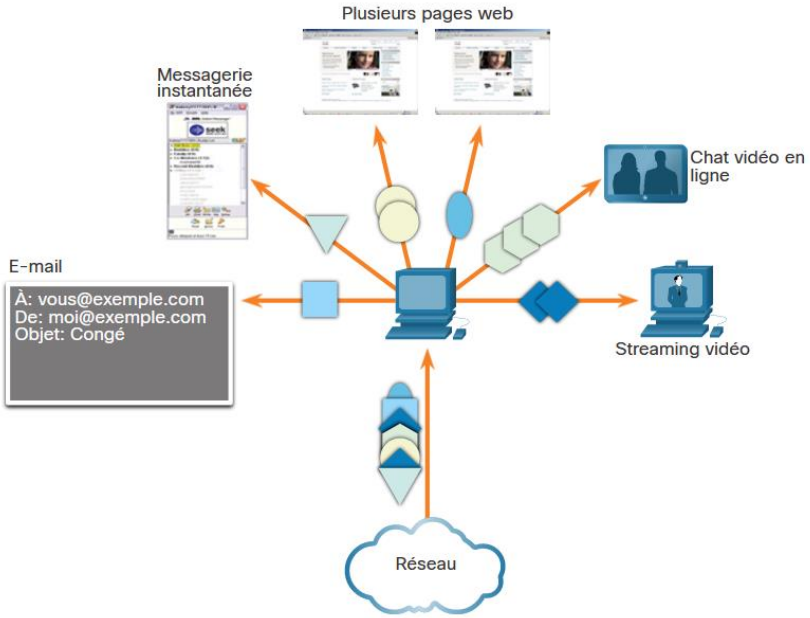
-Suivi des conversations individuelles

- Segmentation des données et reconstitution des segments.

- Ajouter des infos d'entête.

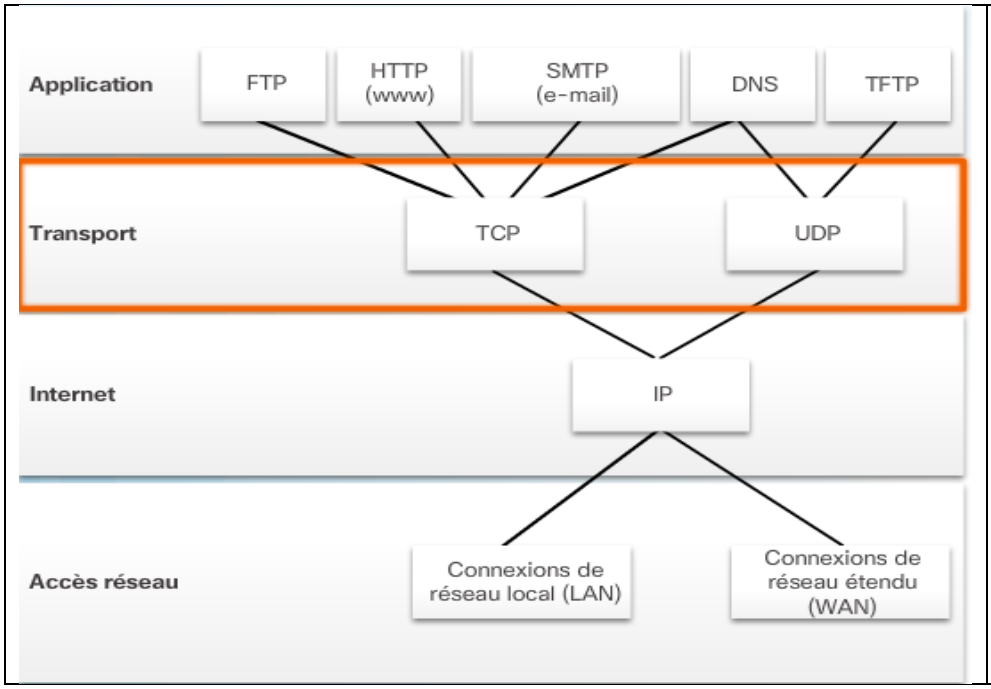
- Identification des applications (port).

- Multiplexage de conversations



2 – Fiabilité de la couche transport

TCP et UDP sont deux protocoles de la couche transport



Le protocole TCP est plus adapté aux bases de données, aux navigateurs, aux clients de messagerie, etc.

Le protocole UDP est plus adapté à la diffusion audio ou vidéo en flux continu en direct, à la VoIP, etc.

TCP prend en charge la fiabilité, contrairement à UDP.

TCP est fiable => en-tête plus complexe, taille paquet plus grande, retard car paquet plus grand.
- Numérotation et suivi des segments de données.

- Accusé de réception des données reçues.
- Si pas d'accusé alors renvoie des données.

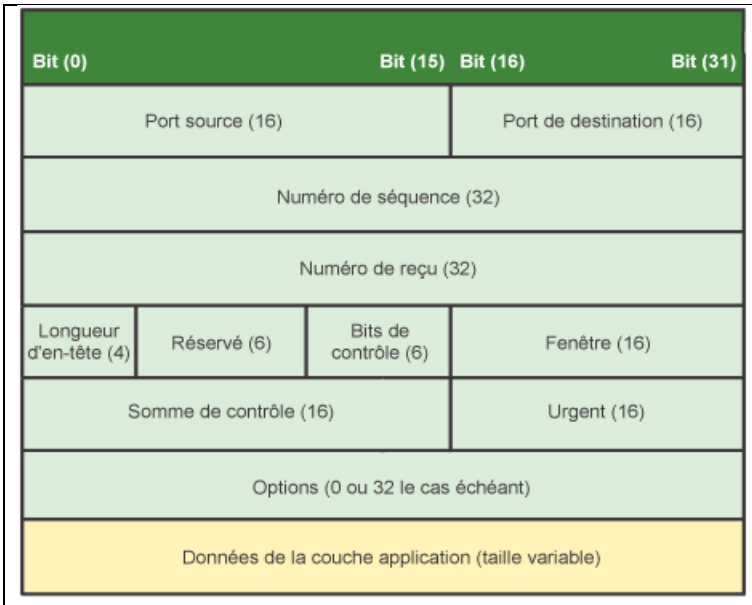
UDP est peu fiable mais plus rapide. C'est un protocole d'acheminement au mieux. Pas d'accusé de réception. Pas de renvoie des données perdues.

Exercice à faire – 14.1.7

3 – Protocole TCP

Les services du protocole TCP (surcharge de 20 octets)

L'établissement d'une session permet de s'assurer que l'application est prête à recevoir les données.
L'acheminement fiable signifie que les segments perdus sont renvoyés afin que les données soient reçues dans leur intégralité.
La livraison dans un ordre défini permet de s'assurer que les segments sont remis dans le bon ordre.
Le contrôle de flux permet de s'assurer que le récepteur est capable de traiter les données reçues.



Port source : Champ 16 bits utilisé pour identifier l'application source par le numéro de port. Ports privés et/ou dynamiques (49152 à 65535).

Port de destination permet d'identifier une application sur le serveur (destination).
Ports réservés (0 à 1023).
Ports inscrits (Attribués par l'IANA sur demande) (1024 à 49151).

Numéro d'ordre (32 bits) : utilisé à des fins de réassemblage de données.

Numéro d'accusé de réception (32 bits) : Champ 32 bits utilisé pour indiquer que les données ont été reçues et que le prochain octet est attendu de la source.

Longueur d'en-tête (4 bits) : Indique la longueur de l'en-tête du segment TCP.

Réservé (6bits) : réservé pour une utilisation future.

Bits de contrôle (6 bits) : comprennent des codes de bits, ou indicateurs, indiquant l'objectif et la fonction du segment TCP.

Taille de fenêtre (16 bits) : indique le nombre de segments pouvant être acceptés en même temps.

Somme de contrôle (16 bits) : utilisée pour le contrôle des erreurs dans l'en-tête et les données de segment.

Urgent (16 bits) : indique si les données sont urgentes.

Exemples d'applications qui utilisent le protocole **TCP : DNS, FTP, http, SMTP, SSH**, …)

Interface de connexion = @IPsource + port source + @IP destination + port destination.

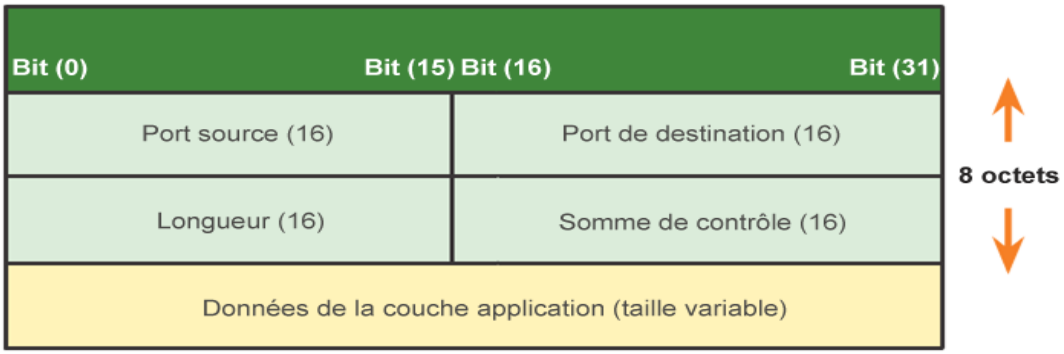
Exercice à faire – 14.2.5

4 – Protocole UDP

Les services du protocole UDP (surcharge de 8 octets)

Simplicité et rapidité.

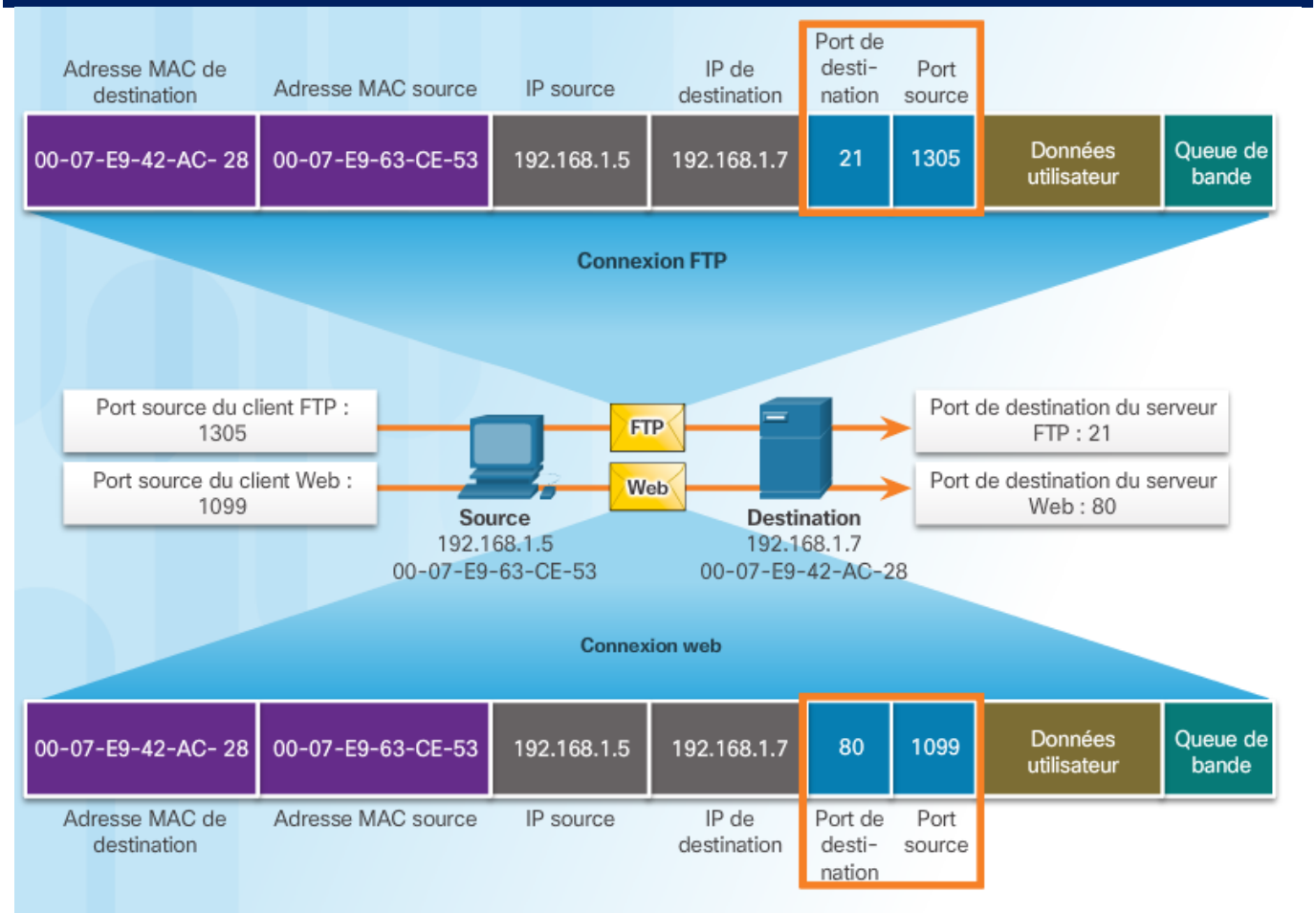
- Le protocole UDP est un protocole stateless ou « sans état ».
- Les données sont reconstituées selon l'ordre de réception.
- Les segments perdus ne sont pas renvoyés.
- Pas d'établissement de session.
- L'expéditeur n'est pas informé de la disponibilité des ressources. Les blocs de communications utilisés dans le protocole UDP sont appelés des datagrammes.



Exemples d'applications qui utilisent le protocole **UDP : DNS, DHCP, TFTP, VoIP, Vidéoconférence**, …)

Exercice à faire – 14.3.5

5 – Ports de communication



Numéros de ports connus

Numéro de port	Protocole	Application
20	TCP	FTP (File Transfer Protocol) - Données
21	TCP	FTP (File Transfer Protocol) - 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	Protocole DHCP (Dynamic Host Configuration Protocol) (client)
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	Simple Network Management Protocol (SNMP)
443	TCP	Protocole HTTPS (Hypertext Transfer Protocol Secure)

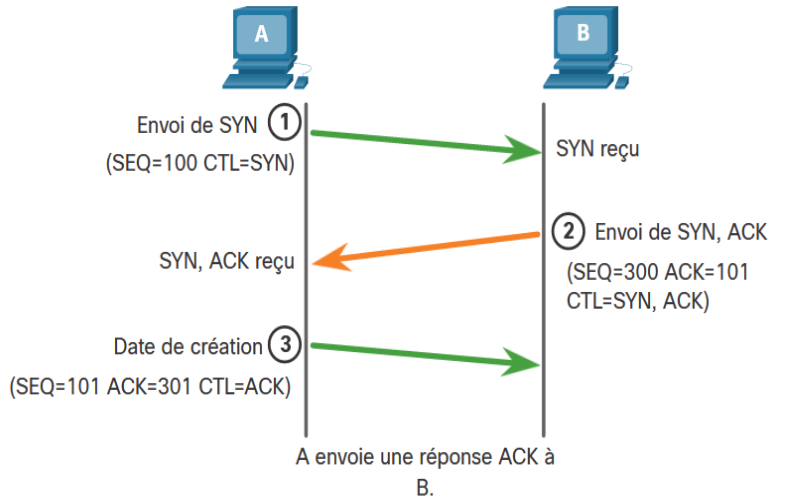
```
C:\> netstat
Active Connections
Proto Local Address Foreign Address State
TCP 192.168.1.124:3126 192.168.0.2:netbios-ssn ESTABLISHED
TCP 192.168.1.124:3158 207.138.126.152:http ESTABLISHED
TCP 192.168.1.124:3159 207.138.126.169:http ESTABLISHED
TCP 192.168.1.124:3160 207.138.126.169:http ESTABLISHED
TCP 192.168.1.124:3161 sc.msn.com:http ESTABLISHED
TCP 192.168.1.124:3166 www.cisco.com:http ESTABLISHED
```

La commande **netstat** permet de connaitre les ports utilisés sur votre machine et l'adresse du destinataire.

Exercice à faire – 14.4.5

6 – Processus de communication TCP

Établissement d'une connexion TCP



Une connexion TCP est établie en trois étapes

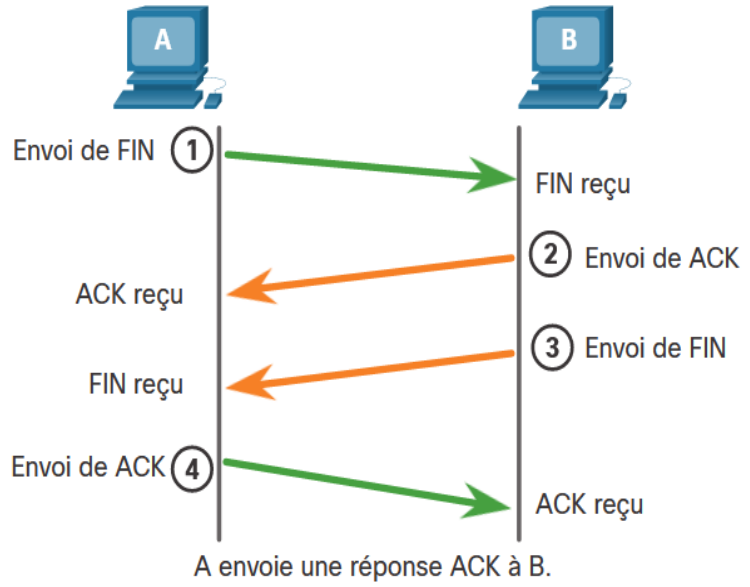
1 - Le client demande l'établissement d'une session de communication client-serveur avec le serveur.

2 - Le serveur accuse réception de la session de communication client-serveur et demande l'établissement d'une session de communication serveur-client.

3 - Le client accuse réception de la session de communication serveur-client.

Les six indicateurs de bits de contrôle sont les suivants :

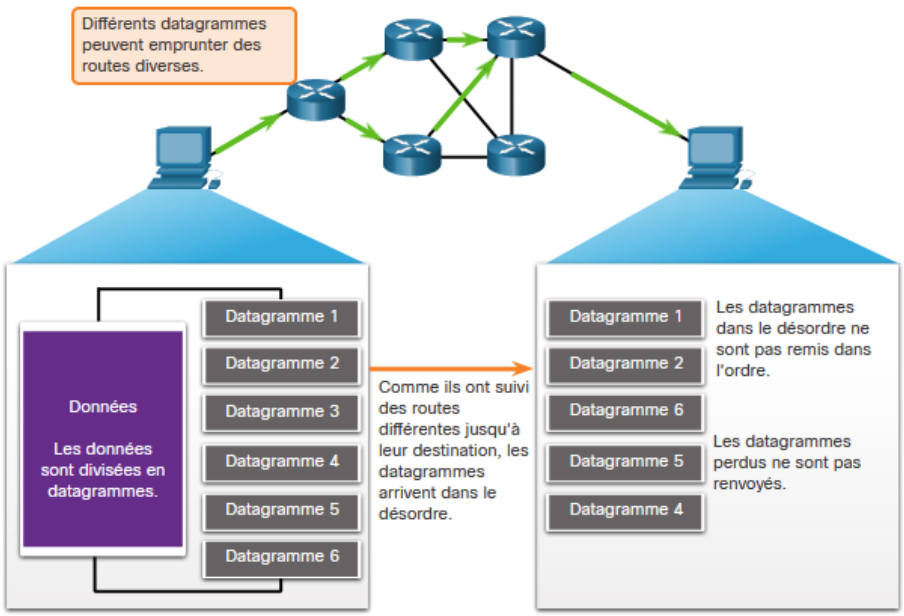
- **URG** - Champ de pointeur urgent significatif (Urgent pointer field significant)
- **ACK** - Indicateur d'accusé de réception utilisé dans l'établissement de la connexion et la fin de la session
- **PSH** - Fonction push (Push function)
- **RST** - Réinitialisation de la connexion en cas d'erreur ou de dépassement de délai
- **SYN** - Synchroniser les numéros de séquence utilisés dans l'établissement de connexion
- **FIN** - Plus de données de l'expéditeur et utilisées dans la fin de session

Fermeture d'une session TCP	
	L'indicateur FIN TCP permet de mettre fin à une connexion TCP. Quand le client n'a plus de données à envoyer dans le flux, il envoie un segment dont l'indicateur FIN est défini. Le serveur envoie un segment ACK pour informer de la bonne réception du segment FIN afin de fermer la session du client au serveur. Le serveur envoie un segment FIN au client pour mettre fin à la session du serveur au client. Le client répond à l'aide d'un segment ACK pour accuser réception du segment FIN envoyé par le serveur. Quand la réception de tous les segments a été confirmée, la session est fermée.

TCP gère le contrôle de flux en ajustant la vitesse des flux de données entre la source et la destination pour une session donnée.
Cette fonction de contrôle de flux TCP dépend d'un champ d'en-tête TCP de 16 bits appelé taille de fenêtre. 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.
La source et la destination TCP conviennent d'une taille de fenêtre initiale lors de l'établissement de la session TCP.

Exercice à faire – 14.5.6 et 14.6.8

6 – Communication UDP



Le protocole UDP n'effectue pas de suivi des numéros d'ordre comme le fait le protocole TCP.

Il n'a en effet aucun moyen de réordonnancer les datagrammes pour leur faire retrouver leur ordre de transmission d'origine.

Le protocole UDP se contente donc de réassembler les données dans l'ordre dans lequel elles ont été reçues, puis de les transmettre à l'application.

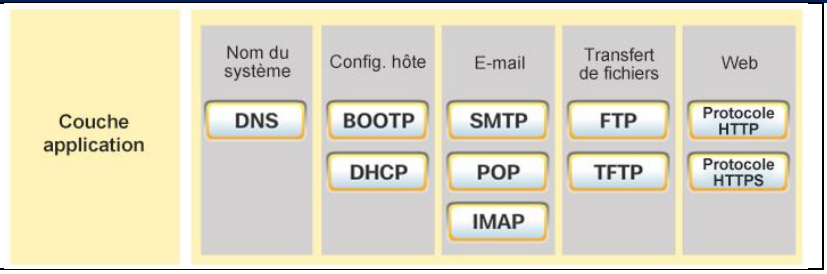
Exercice à faire – 14.7.5

Travail personnel : Questionnaire 14.8.3

Module 15 : Couche application

1 – Application, Présentation et Session

Couche application
- facilitent l'échange en fournissant l'interface entre les applications utilisées pour communiquer,
- Les protocoles courants de la couche application sont les suivants : HTTP, FTP, TFTP, DNS.



Couche présentation
Mise en forme (format identique entre la source et le destinataire),
Compression des données,
Chiffrement des données.
Exemples de formats d'images graphiques : GIF, JPEG et PNG.

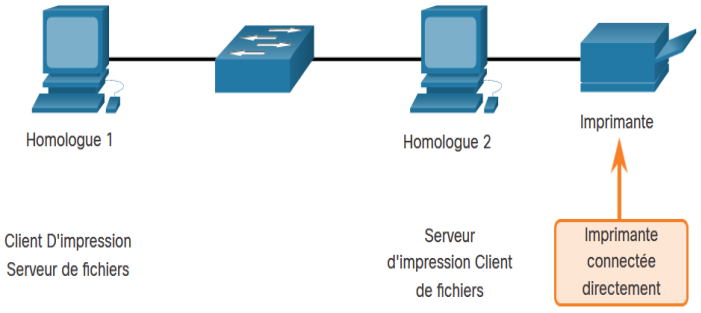
Couche session
La couche session crée et gère les communications entre les applications source et de destination.
La couche session traite l'échange des informations pour commencer un dialogue, le maintenir actif et redémarrer les sessions interrompues ou inactives.

Exercice à faire – 15.1.4

2 – Modèles client / serveur et Peer To Peer

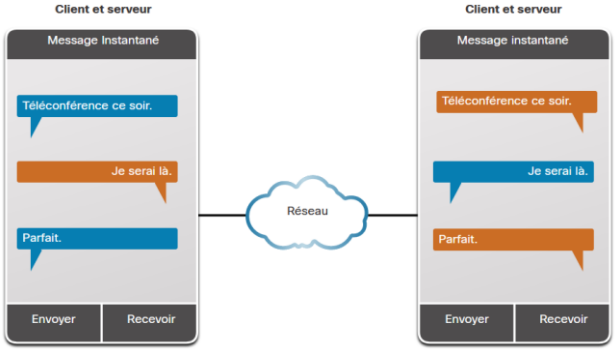
Modèle client-serveur
- Les clients demandent des informations et les serveurs les fournissent.
- Les processus client et serveur sont considérés comme faisant partie de la couche application.
- Le contenu des données échangées dépend de l'application utilisée.
- La messagerie électronique est un exemple d'interaction client-serveur.

Réseaux peer to peer



Les données sont accessibles sans l'intervention d'un serveur dédié.
Deux ordinateurs ou plus peuvent être connectés à un réseau P2P pour partager des ressources.
Chaque périphérique connecté (« peer » ou « homologue ») peut faire office de serveur ou de client.
Les rôles du client et du serveur sont définis en fonction de chaque requête.

Applications peer to peer

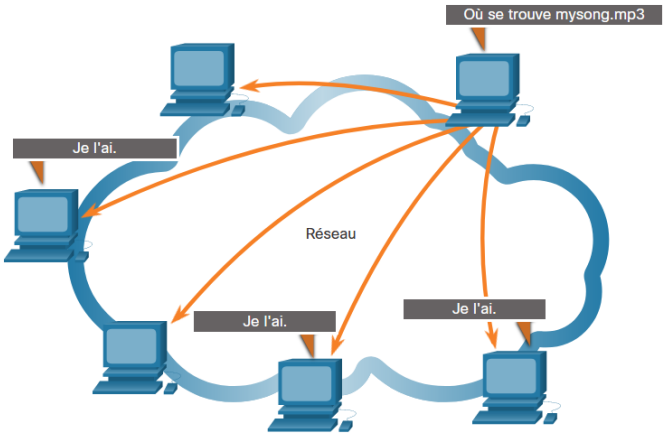


Certaines applications P2P utilisent un système hybride, où le partage des ressources est décentralisé.

Les index qui pointent vers les emplacements des ressources sont stockés dans un répertoire centralisé.

Dans un système hybride, chaque homologue accède à un serveur d'index pour obtenir l'emplacement d'une ressource stockée chez un autre homologue.

Applications P2P courantes



De nombreuses applications P2P permettent aux utilisateurs de partager simultanément des parties de plusieurs fichiers (BitTorrent, Direct Connect, eDonkey, Freenet).
Certaines applications P2P sont basées sur le protocole Gnutella qui permet aux utilisateurs de partager des fichiers avec d'autres personnes. Un petit fichier torrent contient des informations sur l'emplacement des autres utilisateurs et des ordinateurs dits « trackers ».
Les trackers sont des ordinateurs qui effectuent le suivi des fichiers hébergés par les utilisateurs.
Cette technologie s'appelle BitTorrent.

Exercice à faire – 15.2.5

3 – Protocoles WEB et messagerie

HTTP (Hypertext Transfer Protocol)

Une URL est une référence à un serveur Web.

L'URL est le nom que la plupart des utilisateurs associent aux adresses Web.

L'URL contient le protocole, le nom du serveur et le nom de fichier demandé.

Exemple http://www.mon-site.fr/index.html

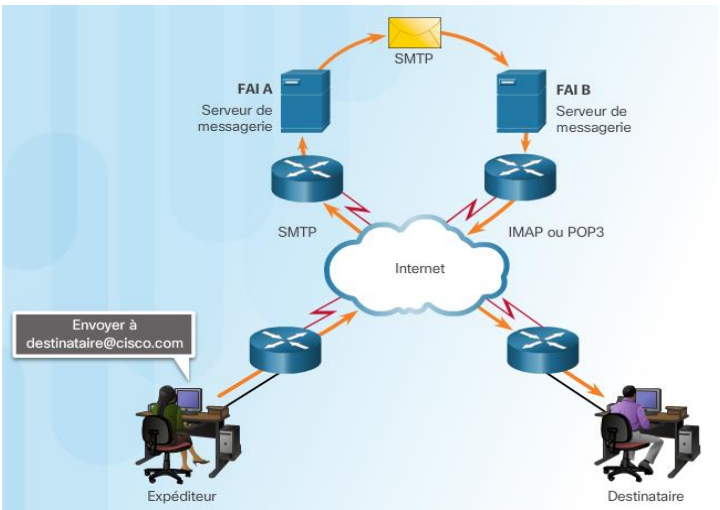
1. http (protocole ou schéma) ;
2. www.mon-site.com (nom du serveur)
3. index.html (nom du fichier demandé)

DNS traduit la partie nom du serveur de l'URL en adresse IP valide, pour pouvoir contacter le serveur.

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

- **GET** est une requête cliente visant à obtenir des données. Un client (navigateur web) envoie le message GET au serveur web pour demander des pages HTML.
- **POST** télécharge des fichiers de données vers le serveur web, comme des données de formulaires.
- **PUT** télécharge des ressources ou du contenu vers le serveur web, comme une image.

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.



Protocoles de messagerie

Les e-mails sont stockés sur des serveurs de messagerie.

Les clients de messagerie communiquent avec les serveurs de messagerie pour envoyer et recevoir des messages.

Les serveurs de messagerie communiquent avec d'autres serveurs de messagerie pour acheminer les messages d'un domaine à un autre.

La messagerie fonctionne avec trois protocoles : **SMTP, POP** et **IMAP**.

SMTP

L'en-tête doit comporter l'adresse e-mail du destinataire et celle de l'expéditeur.
Un client SMTP envoie un e-mail en se connectant à un serveur SMTP sur le port 25.
Le serveur reçoit le message et le stocke ou le relaie à un autre serveur de messagerie.

POP

Les clients de messagerie dirigent leurs requêtes POP jusqu'aux serveurs sur le port TCP 110.
Le protocole POP permet de télécharger les e-mails sur l'appareil du client (ordinateur ou téléphone) et de les supprimer du serveur.

IMAP

Les e-mails s'affichent à l'intention de l'utilisateur, mais ils ne sont pas téléchargés.
Les e-mails d'origine restent sur le serveur jusqu'à ce qu'ils soient manuellement supprimés par l'utilisateur.
Les utilisateurs affichent des copies des messages dans leur logiciel de messagerie.

Exercice à faire – 15.3.5

4 – Le service DNS

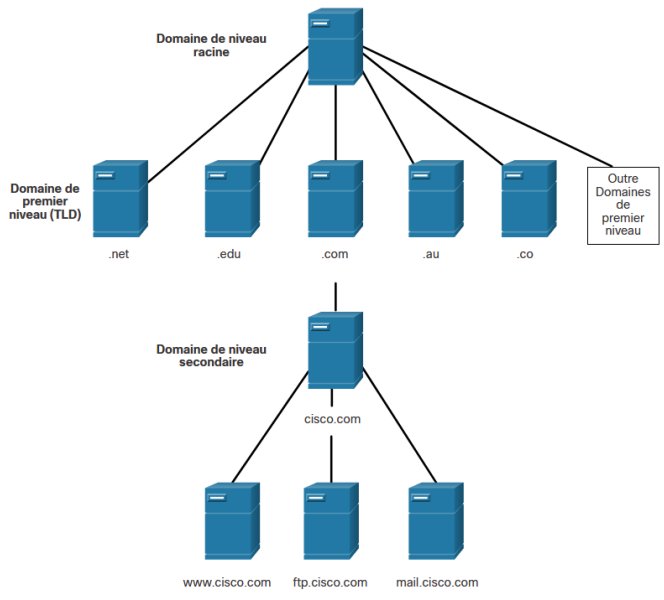
Domain Name Service (service de noms de domaines)

- Il n'est pas facile de mémoriser les adresses IP.
- Il a donc fallu créer des noms de domaine pour nous faciliter les choses.
- Les ordinateurs ont toujours besoin de l'adresse numérique pour pouvoir communiquer.
- Le protocole DNS assure la conversion dynamique du nom de domaine en adresse IP valide.

Format du message DNS

- Les serveurs DNS recherchent d'abord dans leurs propres dossiers, puis relaient la demande du client aux autres serveurs s'ils ne peuvent pas y répondre.
- La réponse est ensuite transmise au client.
- Le client stocke souvent les résolutions de noms précédentes. Utilisez la commande **ipconfig /displaydns** pour afficher les entrées DNS mises en cache sous Windows.

Hiérarchie DNS



Le protocole DNS utilise un système hiérarchique.

La structure d'attribution de noms est divisée en petites zones gérables.

Chaque serveur DNS gère uniquement les mappages entre noms et adresses IP dans une petite partie de la structure DNS.

Les requêtes pour des zones qui ne sont pas stockées sur un serveur DNS précis sont transmises à d'autres serveurs où elles sont traduites.

Les domaines de premier niveau représentent le type de domaine ou le pays d'origine.

.com, .org, **.au** et **.co** sont des exemples de domaines de premier niveau.

Commande nslookup

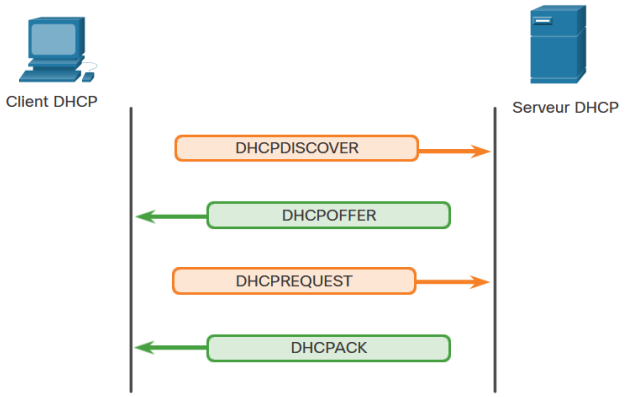
Utilisez la commande nslookup pour envoyer des requêtes DNS (Utile pour le dépannage DNS).

5 – Le service DHCP

Les ordinateurs ont besoin d'informations IP pour communiquer sur un réseau.
Ces informations IP incluent **les adresses de l'hôte et de la passerelle, le masque et le serveur DNS.**
Le protocole DHCP assure la distribution automatisée et évolutive des informations IP.
Les adresses DHCP distribuées sont affectées pour une période de temps définie.
Les adresses sont renvoyées au pool pour y être recyclées si elles ne sont plus utilisées.

Pour l'IPv6 on a DHCPv6

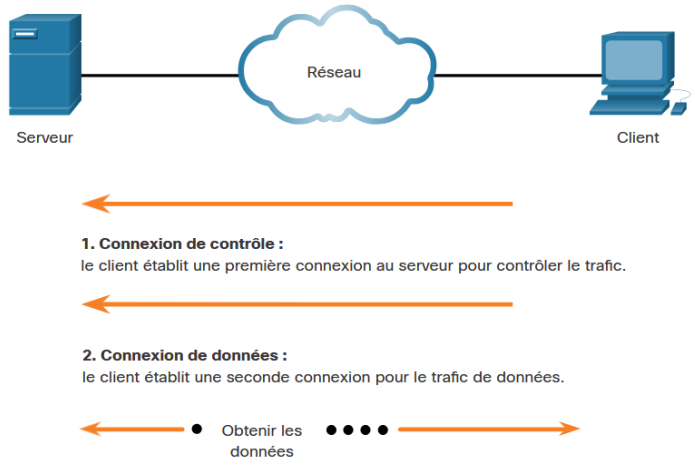
1 - Le client diffuse une requête DHCPDISCOVER.
2 - Un serveur DHCP répond en envoyant un message DHCPOFFER.
3 - Le client envoie un message DHCPREQUEST au serveur qu'il veut utiliser (dans le cas de plusieurs offres). Un client peut également demander une adresse que le serveur lui a déjà attribuée précédemment.
4 - Le serveur renvoie un message DHCPACK pour confirmer que le bail a été finalisé.



Pour retenir plus facilement – « DORA l'exploratrice » – **D**étection, **O**ffre, **R**equête, **A**ccusé de réception.

Exercice à faire – 15.4.9

6 – Le service FTP



Le protocole FTP a été développé pour permettre le transfert de fichiers sur le réseau.

Le protocole FTP nécessite deux connexions entre le client et le serveur : l'une pour les commandes et les réponses, l'autre pour le transfert de fichiers.

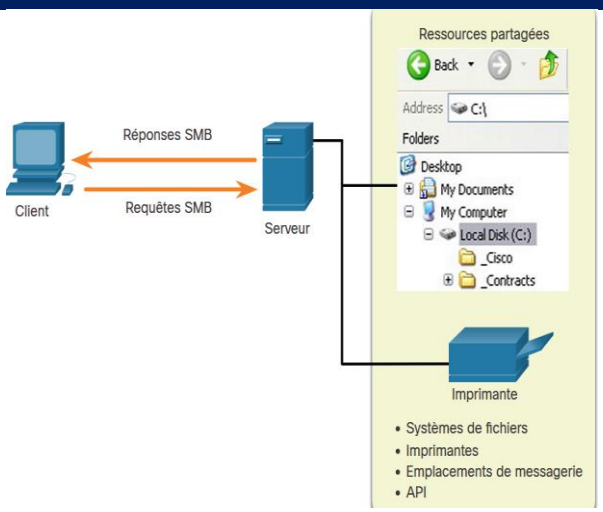
Le client initie et établit la première connexion au serveur pour contrôler le trafic sur le **port TCP 21**.

Il établit une seconde connexion au serveur pour effectuer le transfert de données sur le **port TCP 20**.

Le client peut télécharger des données à partir du serveur ou en direction du serveur.

7 – Le service SMB (Server Message Block)

SMB est un protocole de partage de fichiers entre clients et serveurs.
Tous les messages SMB partagent un format commun.
Le partage de fichiers et les services d'impression SMB sont devenus la base des réseaux Microsoft Windows.
Les produits Microsoft prennent désormais en charge les protocoles TCP/IP pour assurer le partage direct de ressources SMB.
Une fois la connexion établie, l'utilisateur du client peut accéder aux ressources résidant sur le serveur comme si elles étaient situées localement sur l'hôte client.
Les systèmes d'exploitation LINUX et UNIX fournissent également une méthode de partage des ressources avec les réseaux Microsoft à l'aide d'une version de SMB nommée SAMBA.



Exercice à faire – 15.5.3

Travail personnel : Questionnaire 15.6.2

Module 16 :
Fondamentaux de la sécurité des réseaux

1 – Menaces et vulnérabilités de la sécurité

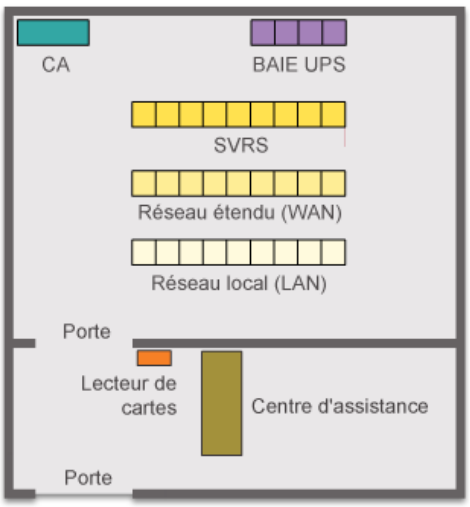
Les menaces : on en distingue quatre types.

- Vol d'informations
- Perte et manipulation de données
- Usurpation d'identité
- Interruption de service

Les vulnérabilités (degré de faiblesse d'un réseau ou d'un périphérique) **:** on en distingue trois types.

- **Les vulnérabilités technologiques** peuvent inclure des faiblesses du protocole TCP/IP, des faiblesses du système d'exploitation et des faiblesses de l'équipement réseau.
- **Les vulnérabilités de configuration** peuvent inclure des comptes d'utilisateur non sécurisés, des comptes système avec des mots de passe faciles à deviner, des services internet mal configurés, des paramètres par défaut non sécurisés et un équipement réseau mal configuré.
- **Les vulnérabilités de la politique de sécurité** peuvent inclure l'absence d'une politique de sécurité écrite, la politique, le manque de continuité de l'authentification, les contrôles d'accès logiques non appliqués, l'installation et les modifications de logiciels et de matériel ne respectant pas la politique, et un plan de reprise après sinistre inexistant.

2 – Sécurité physique



Sécuriser les locaux informatiques

Planification de la sécurité physique
pour limiter les dégâts aux équipements

Verrouiller les équipements et empêcher l'accès non autorisé par les portes, les plafonds, les planchers surélevés, les fenêtres, les conduits et les bouches d'aération.

Contrôler et surveiller l'accès aux armoires électriques à l'aide de journaux électroniques

Utiliser des caméras de sécurité

Menaces matérielles : entraînant des dommages physiques aux serveurs, routeurs, commutateurs, installations de câblage et stations de travail.

Menaces environnementales : dues aux variations extrêmes de la température ou du taux d'humidité.
Menaces électriques : telles que des pics de tension, une tension insuffisante, une alimentation inappropriée (bruit) et une panne totale de courant.

Menaces liées à la maintenance : mauvaise manipulation des composants électroniques principaux (décharges électrostatiques), absence de pièces de rechange essentielles, câblage de mauvaise qualité et étiquetage peu efficace.

Exercice à faire – 16.1.4

3 – Attaques réseau

Un « malware » désigne un programme malveillant (virus, cheval de Troie, un vers). Il s'agit de code ou d'un logiciel spécialement conçu pour endommager, perturber ou effectuer une action illégitime sur des données, des hôtes ou des réseaux.

Un virus informatique est un type de programme malveillant qui se propage en insérant une copie de lui-même dans un autre programme. Lorsque le code hôte est exécuté, le code viral l'est également.

Les vers informatiques sont semblables aux virus en ce sens qu'ils reproduisent des copies fonctionnelles d'eux-mêmes et peuvent provoquer le même type de dommages. Contrairement aux virus, qui nécessitent la diffusion d'un fichier hôte infecté, les vers sont des logiciels autonomes et ne requièrent pas de programme d'accueil ou d'intervention humaine pour se propager.

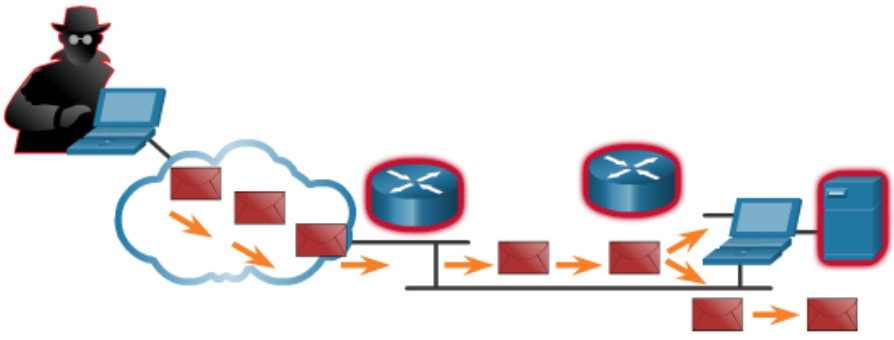
Un cheval de Troie est un autre type de programme malveillant. Il s'agit d'une partie de code qui présente une apparence tout à fait légitime. Les utilisateurs sont généralement trompés en les chargeant et en les exécutant sur leurs systèmes. Une fois activé, il peut réaliser un certain nombre d'attaques contre l'hôte. Contrairement aux virus et aux vers, les chevaux de Troie ne se reproduisent pas

Attaques de reconnaissance : mappage de systèmes et de services, détection des vulnérabilités, lecture des ports, renifleurs de paquets.

Attaques par accès :

- Attaque de mot de passe,
- Redirection des ports,
- Exploitation de la confiance
- L'homme du milieu.

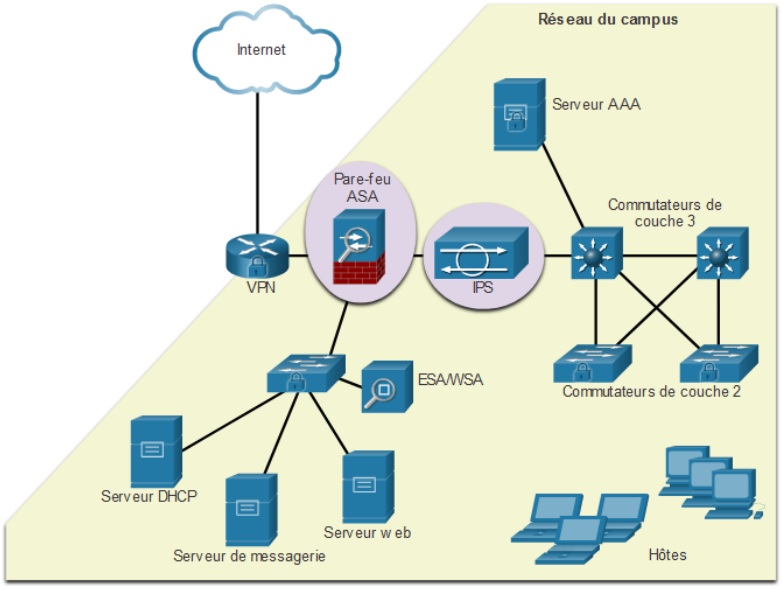
Attaques par déni de service (DoS) : empêchent les personnes autorisées d'utiliser un service en épuisant les ressources du système (ping fatal, attaque par inondation SYN, attaque Smurf).



Exercice à faire – 16.2.5

4 – Atténuation des attaques du réseau

Techniques pour atténuer les risques.



- VPN

- Pare-feu ASA : bloque le trafic externe non identifié.

- IPS : Recherche de logiciels malveillants, d'attaque réseau, …

- ESA : Sécurisation de la messagerie (spams, emails suspects).

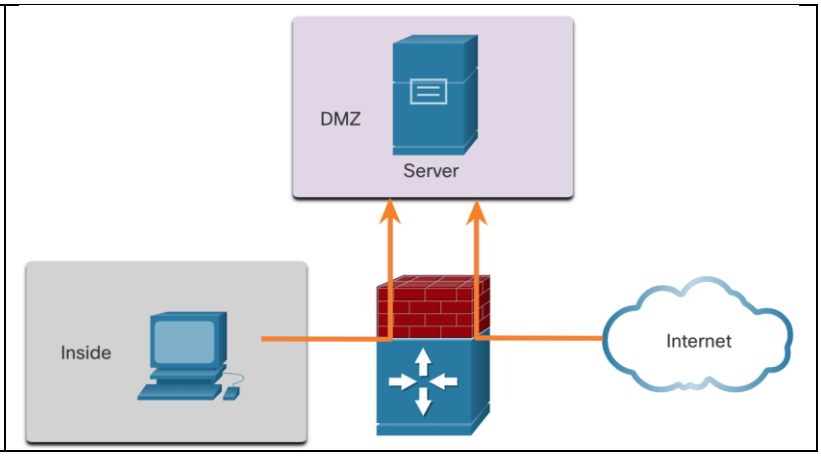
- WSA : Sécurisation du web, filtrage des sites web suspets (malwares)

- **Sauvegarde, mise à jour, mise à niveau et correctif.**

- Serveur AAA : Base de données sécurisée de qui est autorisé à accéder et à gérer les périphériques réseau.

Principe du pare-feu

Un pare-feu permet aux utilisateurs externes de contrôler l'accès à des services spécifiques. Par exemple, les serveurs accessibles aux utilisateurs extérieurs sont généralement situés sur un réseau spécial appelé zone démilitarisée (DMZ). La DMZ permet à un administrateur de réseau d'appliquer des politiques spécifiques pour les hôtes connectés à ce réseau.



Sur un pare-feu on peu faire :

- **Filtrage des paquets** - Empêche ou autorise l'accès sur la base d'adresses IP ou MAC
- **Filtrage des applications** - Empêche ou autorise l'accès à des types d'applications spécifiques en fonction des numéros de port
- **Filtrage des URL** - Empêche ou permet l'accès à des sites web basés sur des URL ou des mots clés spécifiques
- **Inspection minutieuse des paquets (SPI)** - Les paquets entrants doivent être des réponses légitimes aux demandes des hôtes internes. Les paquets non sollicités sont bloqués, sauf s'ils sont expressément autorisés. Le SPI peut également inclure la capacité de reconnaître et de filtrer des types d'attaques spécifiques, comme le déni de service (DoS).

5 – Sécurité des périphériques

- Protéger les périphériques en utilisant des mots de passe forts.
- Cryptage tous les mots de passe en texte clair.
- Définition d'une longueur de mot de passe minimale acceptable.
- Empêcher les attaques par force de deviner les mots de passe.
- Désactivation d'un accès en mode EXEC privilégié inactif après une durée spécifiée.
- Activation de SSH.
- Désactiver les services inutilisés.

Travail personnel : Questionnaire 15.5.4

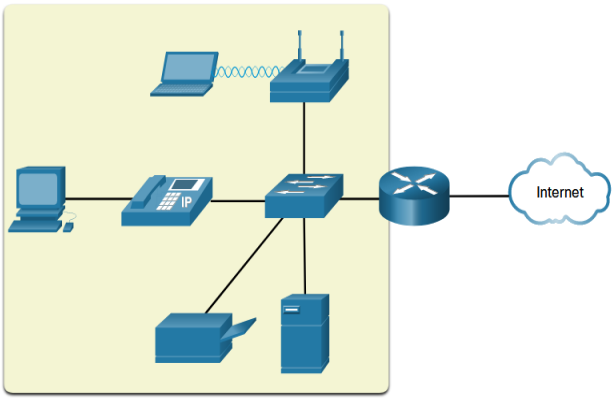
Module 17 :
Conception d'un réseau de petite taille

1 – Périphériques d'un petit réseau

Identification des équipements entrant dans la conception d'un petit réseau.

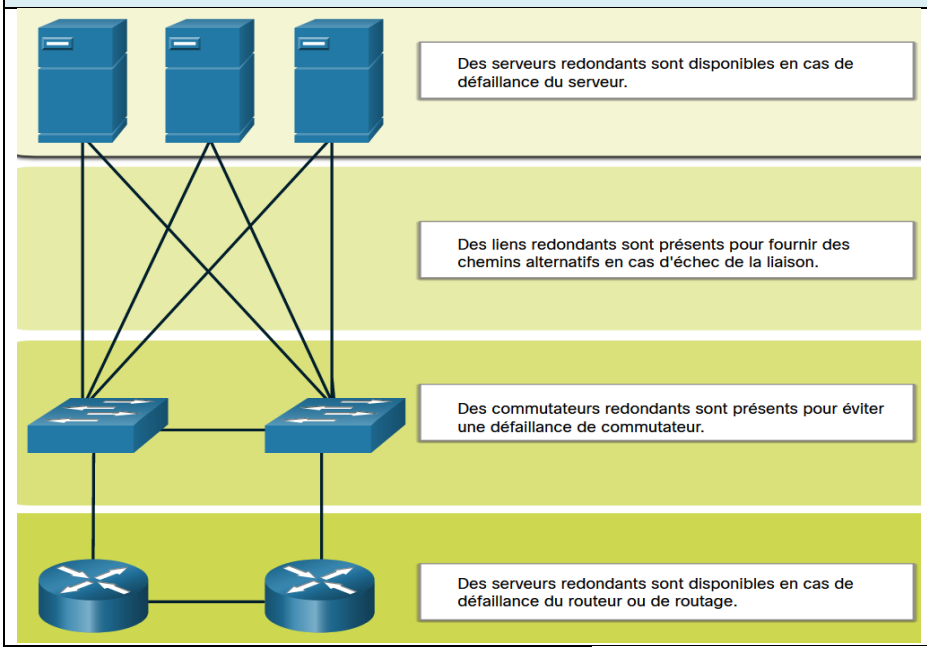
Un routeur, quelques commutateurs (en général un), un point d'accès, de la téléphonie IP, une imprimante et des PC pour les employés.
L'utilisateur accède à Internet par une liaison WAN unique, par câble ou par DSL.
Les facteurs qui doivent être pris en compte lors de la sélection des périphériques réseau sont les suivants :

- Coût
- Vitesse et types de port/d'interface
- Évolutivité
- Caractéristiques et services du système d'exploitation



Il est recommandé de planifier, documenter et gérer un système d'adressage IP basé sur le type de périphérique. L'utilisation d'un système d'adressage IP planifié facilite l'identification d'un type de périphérique et la résolution des problèmes.

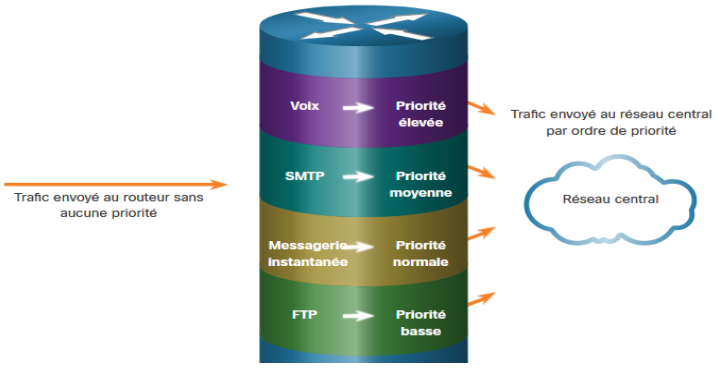
Redondance dans un petit réseau



Les petits réseaux offrent en général un seul point de sortie vers Internet via une ou plusieurs passerelles par défaut. En cas de panne du routeur, c'est tout le réseau qui est déconnecté à l'internet. Par conséquent, il est conseillé aux petites entreprises de prendre un second fournisseur d'accès par mesure de sécurité

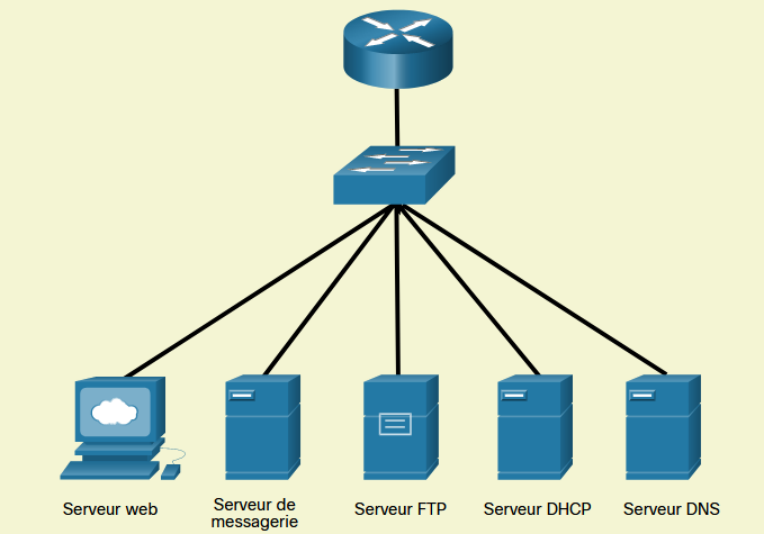
Gestion du trafic

Dans un réseau de petite taille, les routeurs et les commutateurs doivent être configurés pour prendre en charge le trafic en temps réel, comme la voix et la vidéo, et ce, séparément du trafic des autres données. En fait, une bonne conception de réseau mettra en œuvre la qualité de service (QoS) pour classer soigneusement le trafic en fonction des priorités.



Exercice à faire – 17.1.6

2 – Applications et protocoles des réseaux de petite taille



Un réseau de petite taille doit prendre en compte un certain nombre d'applications et de protocoles :

SSH, http, https, SMTP, POP, IMAP, FTP, SFTP, DHCP et DNS.

Exercice à faire – 17.2.4

3 – Evolution vers de plus grands réseaux

Pour faire évoluer un réseau, plusieurs éléments sont nécessaires :

- **Documentation réseau** - Topologie physique et logique
- **Inventaire des équipements** - liste des périphériques qui utilisent ou constituent le réseau
- **Budget** - Budget informatique détaillé, y compris les achats d'équipements pour l'année fiscale
- **Analyse du trafic** - les protocoles, les applications et les services, ainsi que leurs besoins respectifs en termes de trafic doivent être documentés.

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

Pour déterminer des modèles de flux de trafic, il est recommandé d'effectuer les points suivants :

- Capturer le trafic pendant les périodes de pointe pour obtenir une représentation juste des différents types de trafic.
- Effectuer la capture sur différents segments du réseau et périphériques tel que certaines parties du trafic pouvant être locales sur un segment spécifique.
- Les informations collectées par l'analyseur de protocole sont évaluées en fonction de la source et de la destination du trafic, ainsi que du type de trafic envoyé.
- L'analyse peut ensuite être utilisée pour déterminer comment améliorer la gestion du trafic.

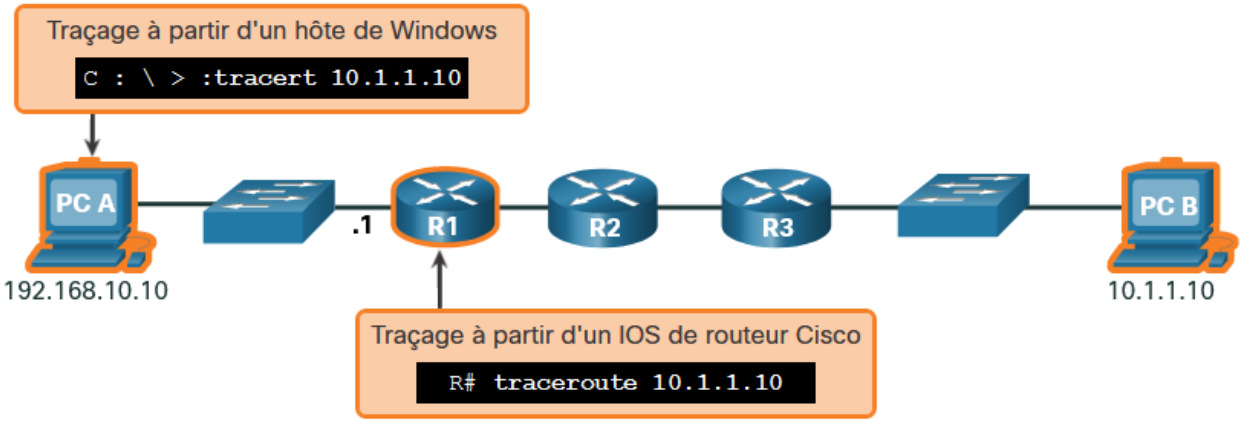
Exercice à faire – 17.3.4

4 – Vérification de la connectivité

- La commande ping, disponible sur la plupart des systèmes d'exploitation, est le moyen le plus efficace de tester rapidement la connectivité de couche 3 entre une adresse IP source et de destination.

- La commande ping utilise les messages d'écho ICMP (Internet Control Message Protocol) (ICMP Type 8) et de réponse d'écho (ICMP Type 0).
  - **!** : Indique la réception réussie d'une réponse d'écho ICMP.
  - **.** : Indique l'expiration du délai d'attente d'une réponse d'écho ICMP (Timeout).
  - **U** : indique qu'un des routeurs distants a dit "unreachable"(réseau injoignable).

Traceroute peut aider à localiser les zones problématiques de couche 3 dans un réseau. Cette commande renvoie une liste des sauts effectués par un paquet acheminé à travers un réseau.
La syntaxe de la commande trace varie d'un système d'exploitation à l'autre.



Exemple de réponse :

```
C:\Users\PC-A> tracert 10.1.1.10
Tracing route to 10.1.10 over a maximum of 30 hops:
  1     2 ms     2 ms     2 ms  192.168.10.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
^C
C:\Users\PC-A>
```

5 – Commandes d'hôtes et IOS

Commande **ipconfig** (Windows) ou **ifconfig** (linux - Mac).

La commande **arp -a** répertorie tous les appareils actuellement présents dans le cache ARP de l'hôte (adresse IP et adresse MAC).

Commandes show pour vérifier la configuration et l'état des périphériques réseau.
Les commandes show servent à afficher les fichiers de configuration, à vérifier l'état des interfaces et des processus des appareils, et à consulter l'état de fonctionnement de l'appareil.

Commande	Description
show running-config	Vérifie la configuration et les paramètres actuels
show interfaces	Vérifie l'état de l'interface et affiche les messages d'erreur
show ip interface	Vérifie les informations de couche 3 d'une interface
show arp	Vérifie la liste des hôtes connus sur les réseaux locaux Ethernet locaux
show ip route	Vérifie les informations de routage de couche 3
show protocols	Vérifie quels protocoles sont opérationnels
show version	Vérifie la mémoire, les interfaces et les licences du périphérique
show ip interface brief	Affiche un résumé des informations clés pour toutes les interfaces
show cdp neighbors	Affiche les informations concernant chaque périphérique CDP voisin

6 – Méthodologies de dépannage

Étape	Description
Étape 1. Identifier le problème	La première étape de la procédure de dépannage. Bien que les outils puissent être utilisés dans cette étape, une conversation avec l' utilisateur est souvent très utile.
Étape 2. Élaborer une théorie des causes probables	Une fois le problème identifié, essayez d'établir une théorie des causes probables. Cette étape fait généralement naître plusieurs causes probables.
Étape 3. Tester la théorie pour déterminer la cause	En fonction des causes probables, testez vos théories afin de dégager la véritable cause du problème. Un technicien peut alors appliquer une rapide procédure et voir si cela permet de résoudre le problème. Si une procédure rapide ne permet pas de résoudre le problème, il peut être nécessaire d'effectuer des recherches complémentaires en vue de déterminer la cause exacte.
Étape 4. Établir un plan d'action pour résoudre le problème et implémenter la solution	Après avoir déterminé la cause exacte du problème, établissez un plan d'action en vue de le résoudre en implémentant la solution.
Étape 5. Vérifier la solution et mettre en œuvre des mesures préventives	Après avoir corrigé le problème, vérifiez la fonctionnalité complète. Le cas échéant, mettre en œuvre des mesures préventives.
Étape 6. Documenter les résultats des recherches et des actions entreprises	Au cours de la dernière étape du processus de dépannage, vous devez documenter les résultats de vos recherches ainsi que les actions entreprises. Cette étape est très importante pour référence ultérieure.

Exercice à faire – 17.6.5

7 – Scénarios de dépannage

Résoudre les problèmes liés aux interfaces et aux câbles : Vérifier le mode (duplex, full duplex, …)

Résoudre les problèmes de connectivité du client liés au service DNS.
Vérification de l'affectation manuelle ou automatique de l'IP (DHCP), adresse en 169.x.x.x, problème de DNS (adresse non renseignée), problème de passerelle.

Travail personnel : Questionnaire 17.8.5