

# GENERALITE SUR LES RESEAUX

PRÉSENTÉ PAR : DR. **KATAKPE KOSSI KUMA** ENSEIGNANT  
CHERCHEUR À L'UNIVERSITÉ DE LABÉ (UL, GUINÉE),  
CONTACTS: [KOSSI.KATAKPE@IMSP-UAC.ORG](mailto:KOSSI.KATAKPE@IMSP-UAC.ORG),  
[KOSSI.KATAKPE@GMAIL.COM](mailto:KOSSI.KATAKPE@GMAIL.COM), [KOSSI.KATAKPE@UNIV-LABE.EDU.GN](mailto:KOSSI.KATAKPE@UNIV-LABE.EDU.GN)

# Partie I

# ROUTAGE

# Qu'est ce qu'un réseau?

- ▶ Ensemble d'équipements (nœud)
  - Reliés entre eux
  - Grâce à divers moyens matériels et logiciels
  - Pour échanger des données

# Découpage horizontal

- ▶ 3 couches
  - Infrastructures (supports)
    - ✓ Câbles, ondes radio, fibre optique, etc.
  - Fonctions de contrôle et de commande
    - ✓ Protocoles définissant comment sont échangées les données
    - ✓ Voir modèle TCP/IP et OSI
  - services
    - ✓ Rendus à l'utilisateur

# Echelle

- Intranet
  - ✓ Réseau interne d'une entité organisationnelle
- Extranet
  - ✓ Réseau externe d'une entité organisationnelle
- internet
  - ✓ Réseau des réseaux
  - ✓ Interconnectés à l'échelle de la planète

# Différents types de réseaux

## ➤ Introduction

- ✓ Il y'a plusieurs manières de classifier les réseaux
  - Par étendue (PAN, LAN, MAN, WAN)
  - Par relation fonctionnelle entre les composants
    - Client/serveur
    - p2p
  - Par topologie

# Différents types de réseaux

- Classification par étendue
  - ✓ PAN : Personal Area Network
  - ✓ LAN : Local Area Network
  - ✓ MAN : Metropolitan Area Network
  - ✓ WAN : Wide Area Network

# Personal Area Network

- Réseaux de très petite dimension
  - ✓ Généralement sur 10 m au moins
  - ✓ Pour une seule personne, ou un très petit nombre de personne
  - ✓ Et un très petit nombre d'éléments
    - Ex : un laptop + un smartphone + un appareil photo connecté.

# Personal Area Network

- ▶ le plus souvent via des technologies sans-fil (Wireless PAN)
  - IrDA
  - Wireless USB
  - Bluetooth
  - Z-Wave
  - ZigBee
- ▶ Peut être réalisé à proximité directe du corps humain (Body Area Network)

# Local Area Network

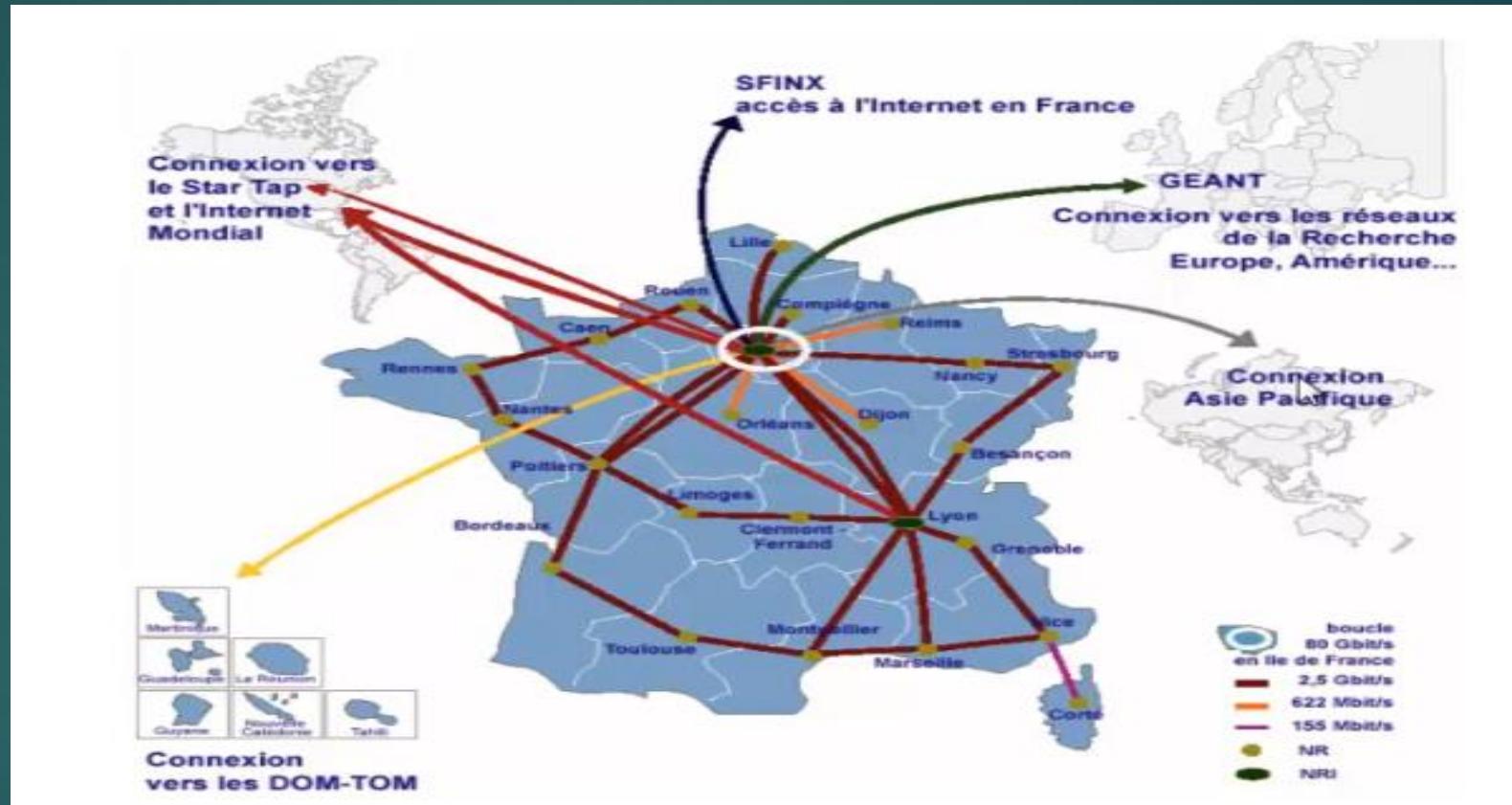
- ▶ réseau de petite dimension
  - A l'échelle d'un bâtiment ou d'une entreprise
  - Sur une distance comprise environnante entre 10 et 1 km
  - Généralement quelques centaines d'utilisateurs
- ▶ De 10 Mb/s (Ethernet) à 1 Gb/s (Gigabit Ethernet), voir 10 Gb/s

# Metropolitan Area Network

- ▶ à l'échelle d'un campus ou d'une ville
  - Prive ou public
  - Entre 5 et 50 km
- ▶ Généralement par fibre optique
  - Mais aussi
    - Par des médias identiques aux LAN
    - La paire téléphonique ( Ex : RNIS)
    - WiFi étendu
    - Wimax

# Wide Area Network

- ▶ très grande zone géographique
  - Pays, continent, voir planète
- ▶ Le plus grand et connu étant bien sur Internet
- ▶ Assure l'interconnexion entre LANs ou MANs
- ▶ Type de connexions hétérogène
  - En fonction du prix et de la distance
  - Jusqu'à 2 Tb/s sur fibre optiques
- ▶ Diverses topologies

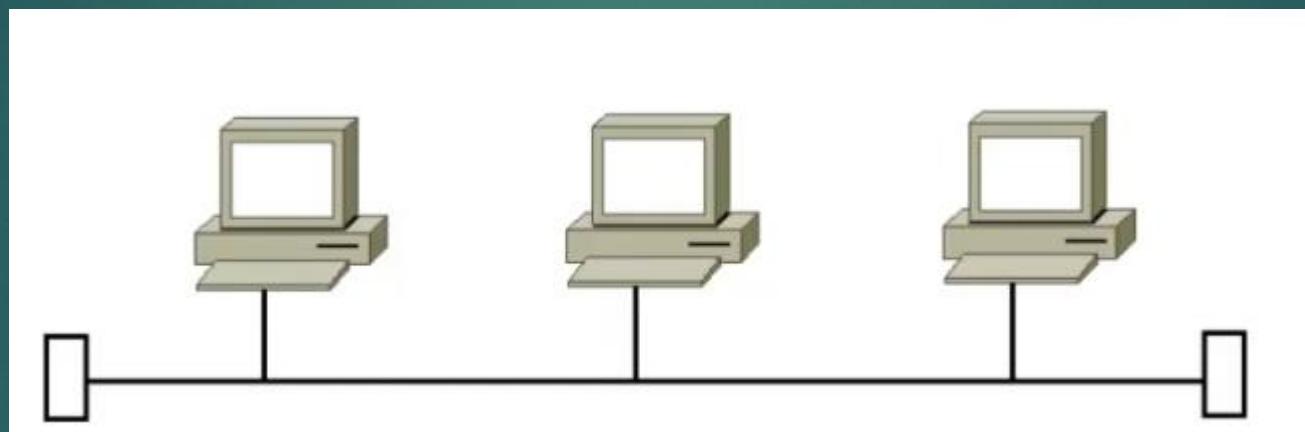


# Introduction

- ▶ Définie l'architecture d'un réseau
  - Relation entre composants
  - Via un ou plusieurs médias
  - Connections
  - hiérarchie

# Réseaux en bus

- ▶ Câblage unique
  - Liaison passive par dérivation (électrique ou optique)
  - Uni ou bidirectionnel
  - Termine à chaque extrémité par des 'bouchons'
    - Elimine les réflexions
- ▶ Quasi obsolète
- ▶ Avantages :
  - Simple
  - Economique
- ▶ Inconvénients
  - Panne totale en cas de dysfonctionnement du support
  - Bande passante partagée
  - Taux de collision élevé



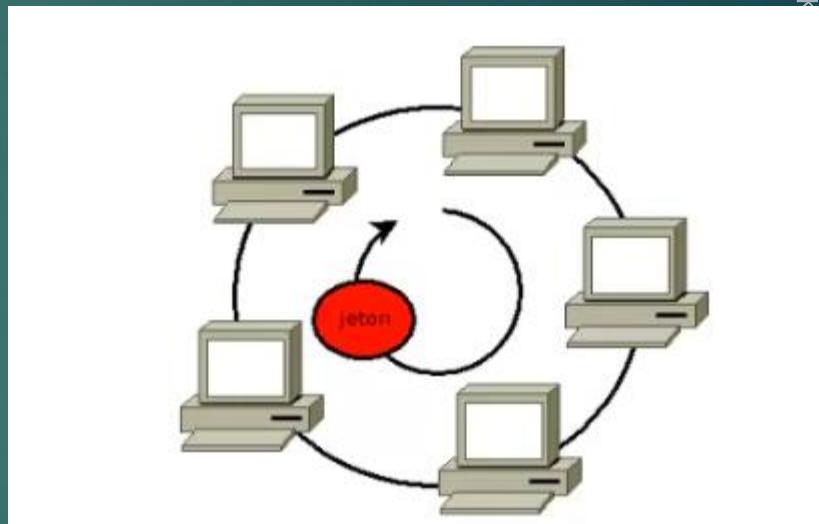
# Réseaux en bus

# Réseaux en anneaux (Token Ring, FDDI)

- ▶ Chaque station joue le rôle de station intermédiaire
  - Sur une connexion unique circulaire
  - Le plus souvent grâce à un répartiteur sur lequel sont connectés tous les éléments
- ▶ Sens unique
  - Souvent composé de deux anneaux à sens opposés
  - ▶ Avantage
    - Isolation de chaque nœud
      - Bande passante

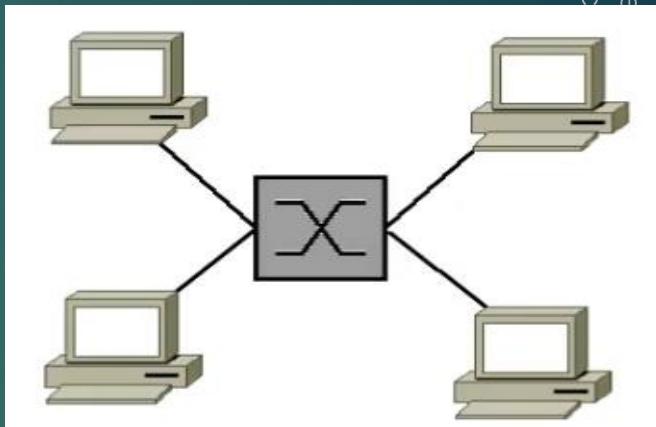
# Réseaux en anneaux (Token Ring, FDDI)

- ▶ inconvénients
  - Cout
  - Une défaillance d'un élément entraîne une panne de tout le système



# Réseaux en étoile

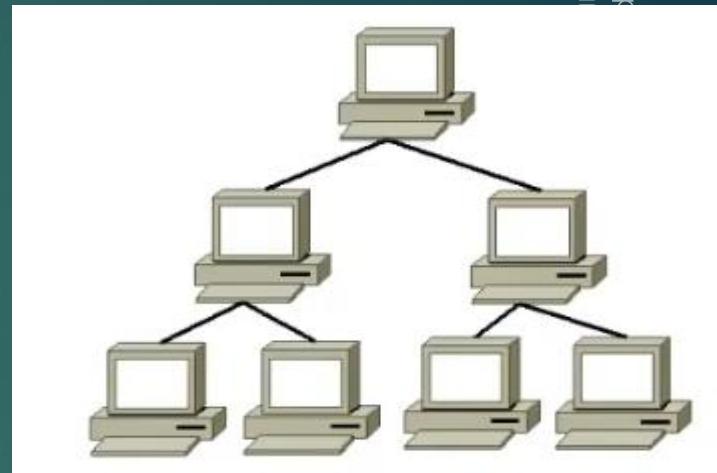
- ▶ Nœuds connectés grâce à un équipement d'interconnexion
  - Concentrateur (Hub) ou commutateur (switch)
  - Chaque nœud étant connecté à un équipement
- ▶ Topologie la plus courante
- ▶ Inconvénients
  - Coût d'évolution élevé



- ▶ Avantages
  - Pas de défaillance générale en cas de dysfonctionnement d'une liaison
  - Meilleur débit

# Réseaux hiérarchiques

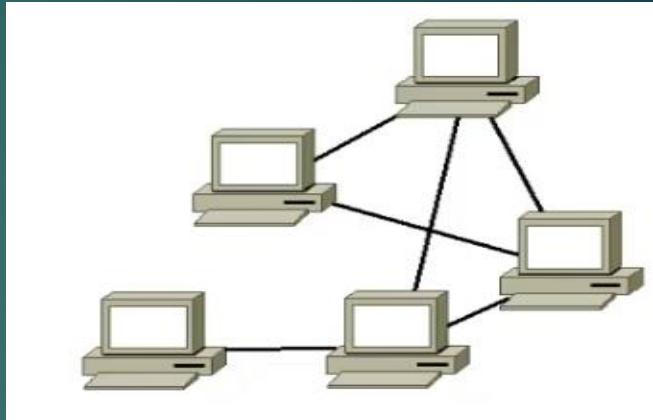
- ▶ Ou réseaux en arbre
- ▶ Au maximum 4 niveaux
- ▶ Souvent utiliser pour les LAN
- ▶ avantages
  - Très faible cout
  - flexibilité



- ▶ inconvénient
  - Rôle centrale de l'élément et des liaisons de niveau 1

# Réseaux maille

- ▶ Réseau pair à pair
  - Sans aucun hiérarchie centrale
  - Chaque nœud doit recevoir, envoyer et relayer l'information
- ▶ Grand réseau de distribution
- ▶ Optimisé pour le sans fil
- ▶ Inconvénient
  - Nombre de liaisons
    - $N(N-1)/2$
    - Croissance rapide



- ▶ Avantages
  - Tolérance aux pannes et aux interférences
    - Issue de la recherche militaire
  - Déploiement rapide et simplifié
  - Grande évolutivité de la couverture

# Présentation du modèle OSI

- ▶ Standard de communication en réseau de tous les systèmes informatiques
  - OSI : Open Systems Interconnection
- ▶ Modèle basique de référence pour l'interconnexion des systèmes ouverts (OSI) : ISO 7498
  - Nécessaire face à la diversité des solutions à sa création (1984)
  - Définit un modèle universel pour les développeurs et les fabricants
- ▶ Détermine clairement le rôle de chaque élément et protocole
  - Par une décomposition en couches
  - Chaque couche servant de support à la couche supérieure

# Couches hautes

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
8 March 2025

Désignation	Description
7 Application	Point d'accès aux services réseau
6 Présentation	codage et conversion des données applicatives
5 Session	synchronisation des échanges et des transactions ouverture / fermeture
4 Transport	connexion bout à bout connectivité et contrôle de flux notion de ports

# Couches basses

Désignation	Description
3 Réseau	communication de proche en proche à travers des réseaux physiques différents parcours des données adressage logique
2 Liaison	communication entre deux hôtes reliés directement adressage physique
1 Physique	transmission de signaux sur le support physique binaire

# Mnémotechnique

- ▶ Physique Liaison Réseau Transport Session Présentation Application
  - PLRTSPA
    - Partout Le Roi Trouve S Place Assise
    - Pour Le Réseau Tout Se Passe Automatiquement
- ▶ Et dans l'ordre inverse
  - APSTRLP
    - Apres Plusieurs Semaines, Tout Respire La Paix

# Couches et protocoles

- ▶ Chaque couche fournie un ou plusieurs services
  - Implémenté (s) par des protocoles
- ▶ Chacun définissant une unité de donnée
  - PDU (Protocol Data Unit)
  - Compose de :
    - Une entête
    - Un champ de données
    - Et enfin d'une en-queue pour la couche liaison

Constituant l'élément à transmettre

# Types de données

	Désignation	Types de données
7	Application	Données
6	Présentation	
5	Session	
4	Transport	Segments
3	Réseau	Paquets/datagrammes
2	Liaison	trames
1	Physique	Bits

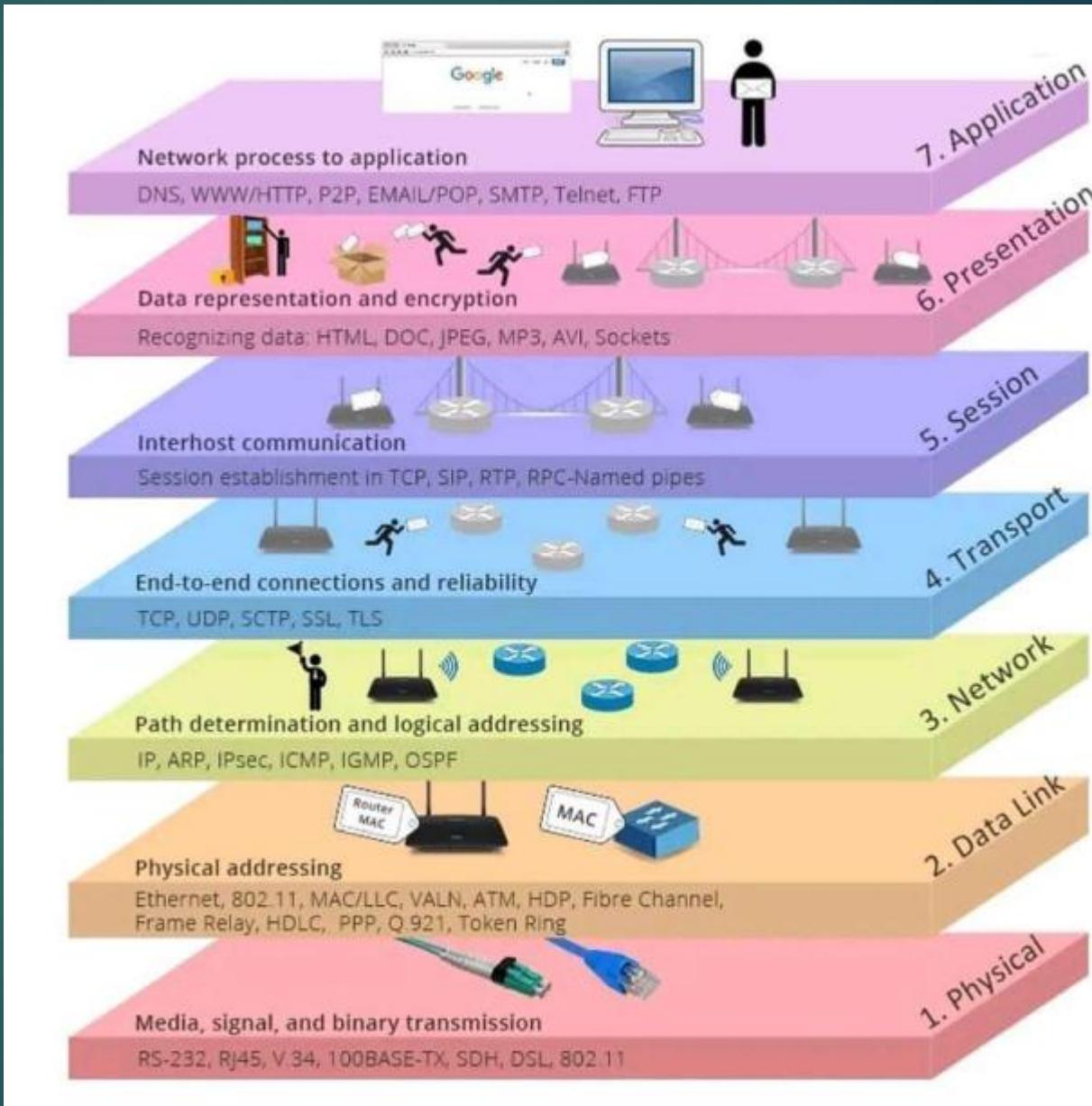
# Protocoles

28

Cours de CCNP : Networking & security  
Présenté par Katakpe Kossi Kuma  
18 March 2025

	désignation	Protocoles
7	Application	FTP, SMTP, Telnet, HTTP, DNS, DHCP
6	Présentation	HTML, MIME, ASCII, SMB, AFP
5	Session	SSH, L2TP, PPTP, Apple Talk, NetBIOS
4	Transport	TCP/UDP
3	Réseau	ICMP, IP, ARP, Service DHCP
2	Liaison	Ethernet, PPP, Wi-Fi
1	Physique	

# Protocoles



# Relations

- ▶ Chaque couche repose sur sa couche inférieure
  - Afin de pouvoir finalement, transmettre les informations sur le support physique (couche 1)
- ▶ Cela se fait grâce à l'encapsulation des PDUs
  - Chaque N-PDU contenant les données du (N+1)-PDU,
    - Plus une entête et éventuellement une en-queue
- ▶ L'émetteur envoie donc des données applicatives
  - Auxquelles sont ajoutées les en-tête des protocoles de chaque couche
- ▶ le receveur réutilisant ces en-tête pour analyser les données et les éléments du protocole
  - Afin de des-encapsuler l'information et l'utiliser

# Exemple : requête / réponse HTTPS

31

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
18 March 2025

Présenté par

Désignation	Protocoles	Requête	Réponse
7 Application	HTTP	GET	OK
6 Présentation	MIME	-	text/html
5 Session	SSL	<i>session ok</i>	<i>session ok</i>
4 Transport	TCP	established dport : 443	established sport : 443
3 Réseau	IPv4	s : 82.226.40.107 d : 82.165.81.167	s : 82.165.81.167 d : 82.226.40.107
2 Liaison	Ethernet	s : 8C-89-A5-08-D9-C2 d : 7D-82-4B-DD-32-42	s : 7D-82-4B-DD-32-42 d : 8C-89-A5-08-D9-C2
1 Physique	-	01000111101111...	001111000111...

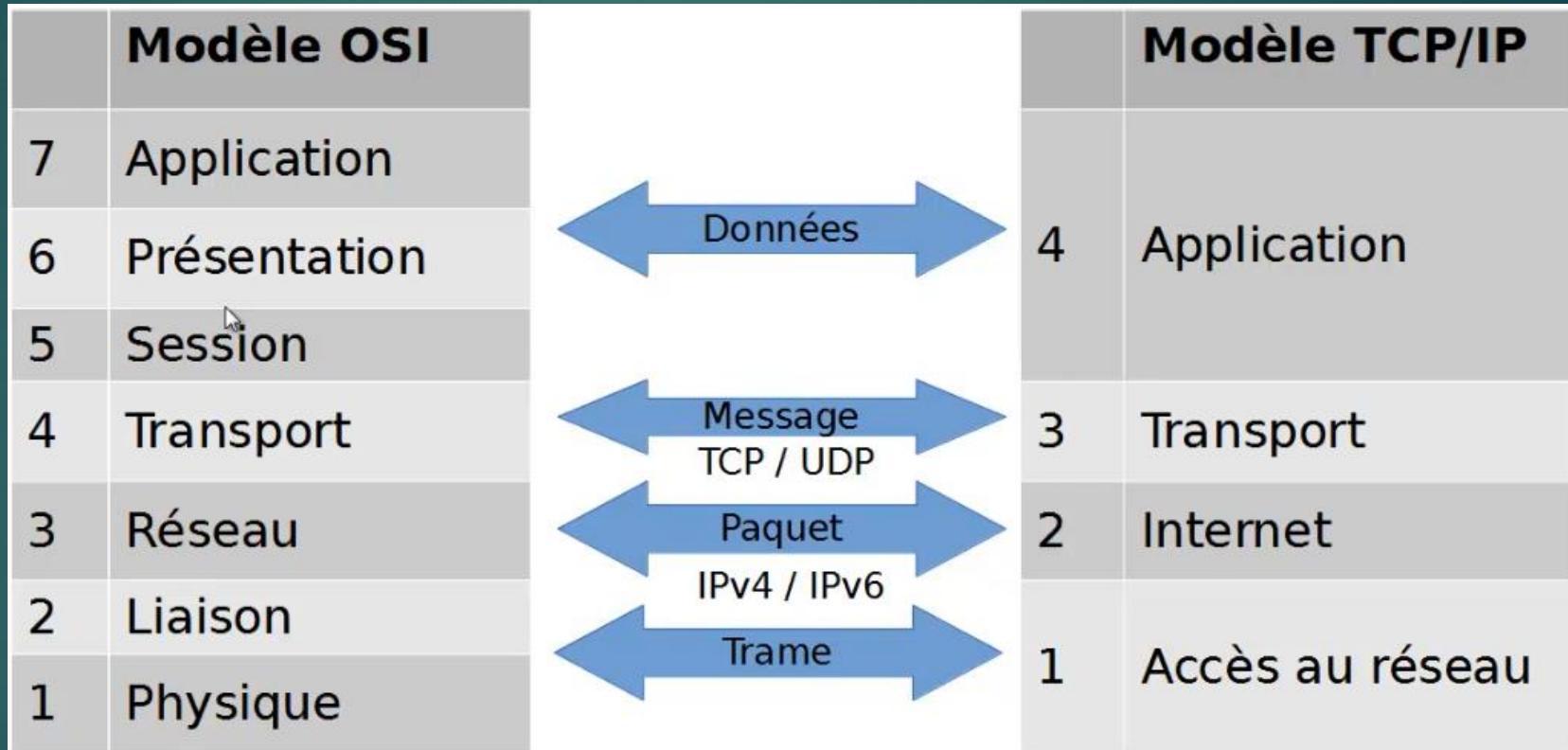
# Présentation du modèle TCP/IP

- ▶ Suite de protocoles TCP + IP
  - Adopté le 1<sup>er</sup> janvier 1983 par Arpanet
    - Fusionne avec le réseau de la National Science Foundation en 1984, donnant naissance à Internet
      - ✓ Le web, lui, n'étant apparu qu'en 1990
- ▶ Norme officielle d'internet depuis 1989 (RFC 1122)

# Comparaison avec le modèle OSI

- ▶ Plus pragmatique
  - Seulement 4 couches
    - Les protocoles internet ne se soucient pas de la liaison ni de la connexion physique
    - Ni de la séparation de protocoles applicatifs
      - ✓ Certains pouvant couvrir plusieurs couches
- ▶ Applications + TCP/UDP + IP + Réseaux
- ▶ Adopté sur la grande majorité des LAN, MAN et WAN aujourd'hui
  - Du fait du rôle central d'Internet

# Types de données



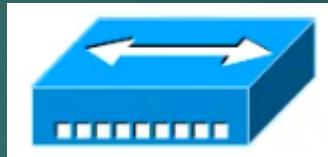
# Répéteur

- ▶ Combinaison de récepteur et d'émetteur
  - Permettant de retransmettre les signaux reçus
  - Permet d'augmenter la distance entre deux nœuds
    - Ex : portée WiFi (distance maximum AP -client)
- ▶ Fonctionnement binaire
  - Aucune interprétation du signal reçu
  - Couche 1 (physique) du modèle OSI

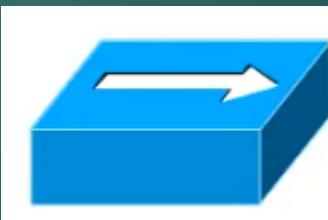
# Concentrateur (Hub)

- ▶ Amplifie et multiplie le signal vers plusieurs PCs
  - Forme de répéteur / multiprise
- ▶ Traitement binaire
  - Redistribution du signal sur tous les ports
  - Couche 1 du modèle OSI
    - Physique

- ▶ Petit concentrateur 10BaseT

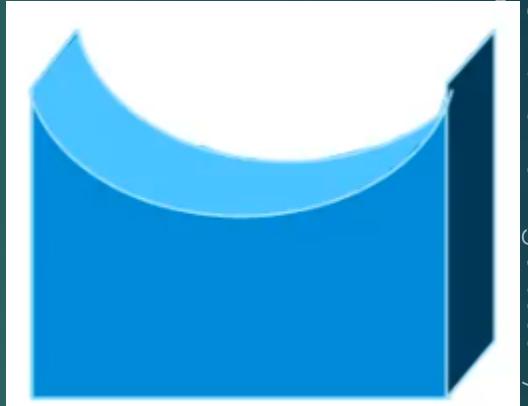


- ▶ Concentrateur 100BaseT



# Pont (Bridge)

- ▶ Assure la connexion entre réseaux distincts
  - De technologie semblables ou différentes
  - Plan d'adressage identique
- ▶ Filtre les collisions et évite de les transmettre
- ▶ Couche 2 (Liaison) du modèle OSI



# Commutateur (Switch)

- ▶ ‘hub intelligent’ et ‘pont multiport’
  - Aiguille les trames reçues vers le port / segment adéquat
    - ✓ Relativement à l’ adresse du destinataire
- ▶ Forte diminution (voir totale suppression) des collisions
- ▶ Niveau 2 (Liaison) du modèle OSI



# Routeur

- ▶ Niveau 3 (réseau) du modèle OSI
- ▶ Fait transiter des paquets d'une interface à une autre
  - Selon un ensemble de règles
- ▶ Permet d'interconnecter plusieurs réseaux
  - Le plus souvent via le protocole IP (adressage)
    - Plans d'adressage différents
- ▶ Routeur
- ▶ Logiciel de routage sur serveur applicatif



# Médias : Câble électriques

- ▶ Ligne de transmission
  - Elément conducteurs métalliques (cuivre le plus souvent)
  - Permettant d'acheminer un signal
    - D'un émetteur vers un récepteur

# Perturbations

- ▶ Sur une ligne de transmission
  - Les perturbations sont d'ordre électromagnétiques
    - D'origine intérieure ou extérieure
  - Ajoute une tension au signal à transmettre
    - Le transforme
- ▶ Ex : signal audio : 'friture'
- ▶ Dans le cadre d'un signal numérique
  - Changement d'état de certains bits
  - Fausse totalement le message

# Protection contre les perturbations

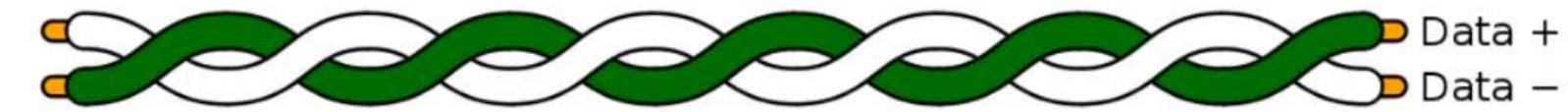
42

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
18 March  
2025

- ▶ Antiparasitage des sources de parasites
  - Obligation légale pour les constructeurs
- ▶ Eloigner la ligne de transmission de toute source potentielle
  - Micro-onde, moteur électriques, etc.
- ▶ Chemins de câbles métalliques
  - Cage de Faraday
- ▶ Blindage des câbles
- ▶ Transmission différentielle

# La paire torsadées

- enroulement en hélice de chaque paire de fils conducteur
  - diminue la diaphonie
    - perturbation du signal d'un fil par le chant magnétique du second
  - en maintenant constante la distance entre les fils
- Chaque paire étant caractérisé par un nombre moyen de torsade par mettre
  - augmenter le nombre de torsades permettant de diminuer les risques de diaphonie
- Un câble réseau pouvant être composé de plusieurs paires torsadées, il est important de varier leurs nombre moyen de torsades par mettre
  - pour éviter toute diaphonie entre les paires



# Catégorie obsolètes

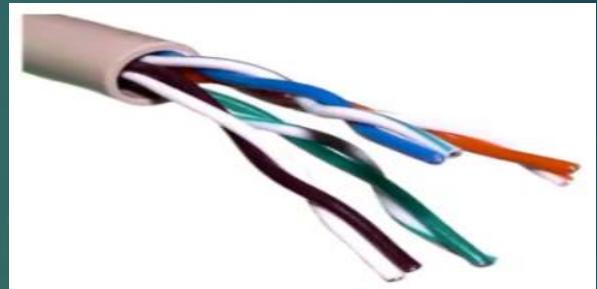
- ▶ Catégorie 1
  - Téléphonie
  - Abandonne au profit de la catégorie 5
- ▶ Catégorie 2
  - Anciennement utilise principalement pour du Token Ring
    - De faible débit : 4Mbts/s
  - Bande passante : 2Mhz

# Catégorie en voie de remplacement

- ▶ Catégorie 3
  - 4 paires torsadées
  - Bande passante 16Mhz
  - Utilise principalement en téléphonie
  - Progressivement remplace par la catégorie 5
- ▶ Catégorie 4
  - Non décrit dans la norme actuelle
  - 4 paires de cuivre
  - Bande passante : 20Mhz
  - Réseau Token Ring (16Mbps) / 10BASE-T

# Catégories actuelles

- ▶ Catégorie 5
  - Bande passante : 100Mhz
  - Téléphonie ou réseaux
    - FastEthernet (100Mbits/s)
  - Remplace par la cat5e /classe D
    - E pour enfance : 125Mhz
- ▶ Catégorie 6 / Classe E
  - 250Mhz et plus
  - Cat6a : 500Mhz
    - 10GBASE-T sur 90m



- ▶ Catégorie 7/ Classe F 600Mhz
  - Réseaux et télévision
    - VHF ou UHF
  - Cat7a : 1Ghz
    - Jusqu'à 10Gbits/s

# Blindage

- ▶ Limite les interférences
  - Pour chaque paire (autour de chacune)
  - Et/ou l'ensemble du câble
    - Place alors entre la gaine et les paires
  - En ajoutant le rôle de cage de faraday
    - Acheminement des parasites électriques vers la masse
- ▶ Type de blindage
  - F = foil shilling : blindage par feuillard
    - Feuille d'aluminium
      - ✓ Cout modéré
  - S = braided shielding : blindage par tresse
    - En cuivre étamé
    - Protection maximale pour un coup élevé.

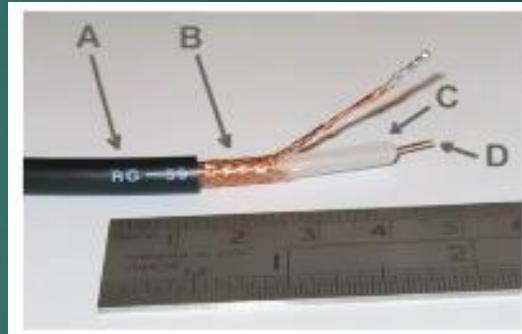
# Blindage

Dénomination courante	Dénomination officielle	Blindage du câble	Blindage des paires	Usage
UTP	U/UTP	-	-	coût minimal
STP	U/FTP	-	feuillard	
FTP	F/UTP	feuillard	-	le plus courant
FFTP	F/FTP	feuillard	feuillard	satellite, etc ...
SFTP	SF/UTP	feuillard et tresse	-	max pour cat5e
SSTP	S/FTP	tresse	feuillard	uniquement à partir de cat6

- TP = twisted pair : paire torsadée
- U = unshielded : non blindé

# Coaxiaux

- ▶ Un seul conducteur
  - Simple ou multibrin
  - Cuivre
  - Dit 'âme' du câble
- ▶ Isole de son blindage
  - Par un matériau diélectrique
  - PV ou TEFLON
- ▶ Débit important sur de longues distance
  - A faible cout
  - Ex : réseau câble urbain
- ▶ Fragile, instable et vulnérable aux interférences et aux écoutes



- ▶ A : gaine extérieure
  - Isolant plastique ou PVC
- ▶ B : blindage de cuivre tresse
- ▶ C : diélectrique (isolant)
- ▶ D : conducteur

# Fibre optique

- ▶ Très haut débit
  - Grace a des rayons optiques conduits par le "cœur" du câble
    - ✓ Entoure d'une gaine et d'une protection
- ▶ Unidirectionnel
- ▶ Insensible aux champs électromagnétiques
- ▶ 2 types
  - Monomode : 1 Gb/s/km
  - Multimode : 100Gb/s/km

# Fibre optique

- ▶ Avantages
  - Légèreté
  - Immunité au bruit
  - Faible atténuation
  - Très haut débit
  - Quasi impossibilité d'écoute
- ▶ Principalement utiliser pour
  - Des connections entre répartiteurs
  - Des connections très haut débit
- ▶ Ne convient pas aux LAN
- ▶ Inconvénients
  - Installation complexe
  - Cout élevé



# Sans fil (ondes électromagnétiques)

- ▶ Ondes radios (entre et 300GHz)
  - Règlementées suivant les régions du monde
  - Communication réseaux limitée a un espace de UHF
    - Ultra haute fréquence – 300MHz a 3GHz
      - ✓ PAN : Bluetooth, ZigBee, Wireless USB
      - ✓ LAN : WiFi, HiperLan 1 et 2
      - ✓ MAN : WiMax, HiperMan, hiperACCESS
      - ✓ WAN : 3G, 4G, GSM, UMTS, etc...
- ▶ Infra-rouge (300GHz a 100THz)
  - Voir IrDA (Infrared Data Association) pour le transfert de fichiers
  - Progressivement remplace par les technologies a ondes radios
- ▶ Champ lumineux visible (spectre optique – 384THz a 789THz)
  - Anecdotique
  - Voir LiFi

- ▶ Courant Porteur en Ligne
  - Transmission par réseau électrique
    - Ne nécessite aucune câblage supplémentaire.
  - Signal de plus haute fréquence et de faible énergie
    - Superposer au courant électrique alternatif
- ▶ Deux catégories
  - Haut débit : modulation multi-porteuses (type OFDM)
    - Bande de fréquence : de 1,6 à 30Mhz
    - Entre 14 et 500Mbps
  - Bas débit : une seule porteuse à la fois en modulation de fréquence
    - Bande de fréquence : entre 9 et 150khz en Europe
    - Entre 150 et 450khz aux USA
    - Principalement pour la domotique : de 2,4 à 20 Kbits/s
- ▶ Extrêmement sujet au bruit et aux atténuations
  - Contre par un mécanisme de redondance
  - Dépendant de la qualité du câblage électrique, n'étant pas destiné à transmettre des informations

# Ethernet

## ► Protocole réseau LAN

- Implémente la couche physique du modèle OSI
  - Sur réseau câblé (par paire torsades, coaxial et fibre optique)
    - ✓ A bande de base (par opposition aux large bandes types ADSL)
  - Ne s'applique pas au CPL, qui a ses propres normes
- Et la couche 2 (liaison) du modèle OSI
  - Adresse MAC, ...
  - Est généralement classe a ce niveau

## ► Norme IEEE 802.3

- A inspire la norme WiFi (802.11), dans la même famille de norme réseau 802
  - Quasi identique concernant la couche liaison
  - Avec ajout des caractéristiques spécifiques au sans fil
    - ✓ Identifiant réseau, découverte, association, etc.

# Adressage des pairs

- ▶ Adressage MAC (Media Access Point)
  - Identifiant dit physique
    - Stocker sur la carte ou l'interface réseau
  - Sous couche (dite couche MAC) de la couche liaison
    - Insertion et traitement de l'adresse MAC dans les trames
    - Utiliser par de nombreux protocoles de niveau 2
      - ✓ Ethernet, bien sur
      - ✓ Mais aussi WiFi, Bluetooth, ATM, Token Ring,ZigBee...
- ▶ 48 bits (6 Octets)
  - Généralement représenté sous forme hexadécimale
    - En séparant les octets par un double point (parfois un tiret)
    - Exemple : 5E:FF:56:A2:AF:15

- premier octet
  - bit 1 : bit I/G
    - 0 = unicast
      - paire (également A, C et E)
    - 1 = multicast ou broadcast
      - impaire (également B,D,F)
  - bit 2 : bit U/L
    - 0 = adresse universelle
      - conforme au format de l'IEEE
    - 1 = locale
- 22 bits réservés : adresse du constructeur
  - tout les bits à 0 pour une adresse locale
- 24 bits : adresse unique
  - permet de différencier les différentes cartes réseaux d'un même constructeur)

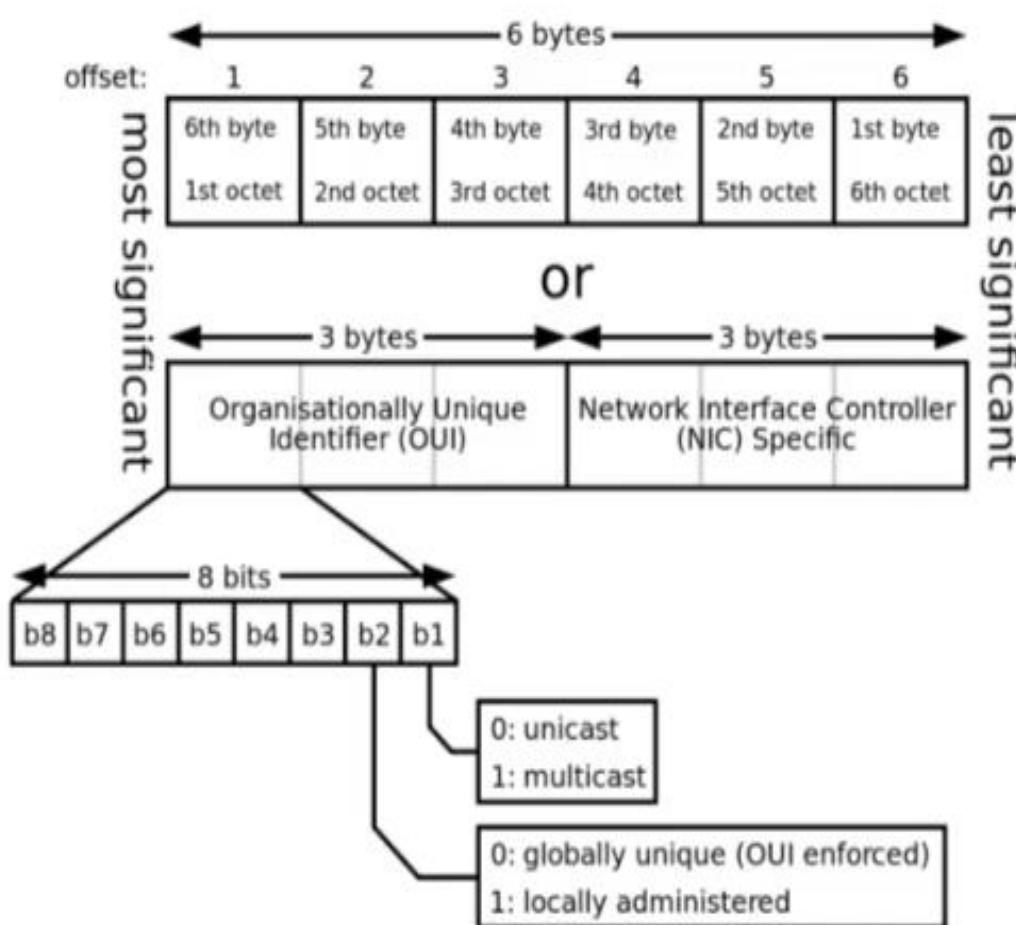


illustration [wikimedia commons CC-By-SA](#)

- PDU de la couche liaison
- EtherType : définition du protocole de couche supérieur utilisé
  - ex : 0x0800 = Internet Protocol version 4 (IPv4)
  - liste assez complète [ici](#)

0 ... 5	6 ... 11	12 et 13	14 ... 1513	1514 ... 1517
Adresse MAC Destination	Adresse MAC source	EtherType	Données	FCS/CRC
En-tête			Corps	En-pied

# Introduction à l'Internet Protocol

# Protocol IP

## Rôle

- ▶ Couche internet (2) du modèle TCP/IP
- ▶ Couche réseau (3) du modèle OSI
  - Elaboration et transport des paquets
  - Représentation, routage et expédition

## Versions

- ▶ Deux versions
  - IPv4
    - RFC 791 (Septembre 1981)
    - Limité : seulement à  $2^{32}$  (soit 4 294 967) d'adresses en théorie
      - En pratique seul un certain nombre en est utilisable
      - Limite en voie d'être atteinte sur internet
  - Encore le plus utilisé, aussi bien sur internet que sur les réseaux privés
  - IPv6
    - RFC 2460 (décembre 1998)
    - $2^{128}$  (soit environ  $3,4 \times 10^{38}$ ) adresses possibles

# Protocole IP

## version

- ▶ Ces versions sont incompatibles
  - Un hôte ne disposant pas d'adresse ipv4 ne peut communiquer avec un hôte ne disposant que d'une adresse ipv6
  - Transition toujours en cours, car complexe
    - Cf RFC 4966

## Adresse IPv4

- ▶ Codée sur 32 bits
  - Soit 4 octets
    - Représentés sous forme décimale (base 10)
      - ✓ Nombre entre 0 et 255
    - Séparés par des points
    - Notation dite « décimale pointée »
- ▶ Ex : 192.168.10.3
- ▶ Séparés en classes, en sous-réseaux, etc....

# Adresse IPv6

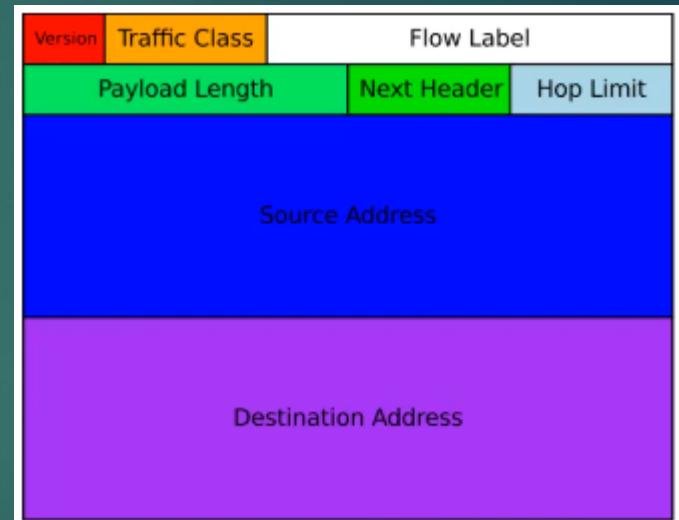
- ▶ Codée sur 128 bits
  - Soit 16 octets
    - 8 groupes de 2 octets
      - Représentés en hexadécimale (base 16) soit 39 caractères en notation complète
      - Séparés par des signes doubles points
- ▶ Ex : 2001:0db8:0000:85a3:0000:0000:ac1f:8001
- ▶ Représentation abrégée:
  - Omission de 1 à 3 chiffres zéro non significatifs
  - Et des groupes de valeur zéro
  - Ex : 2001: db8:0:85a3::ac1f:8001

# En-tête

► IPv4



► Ipv6



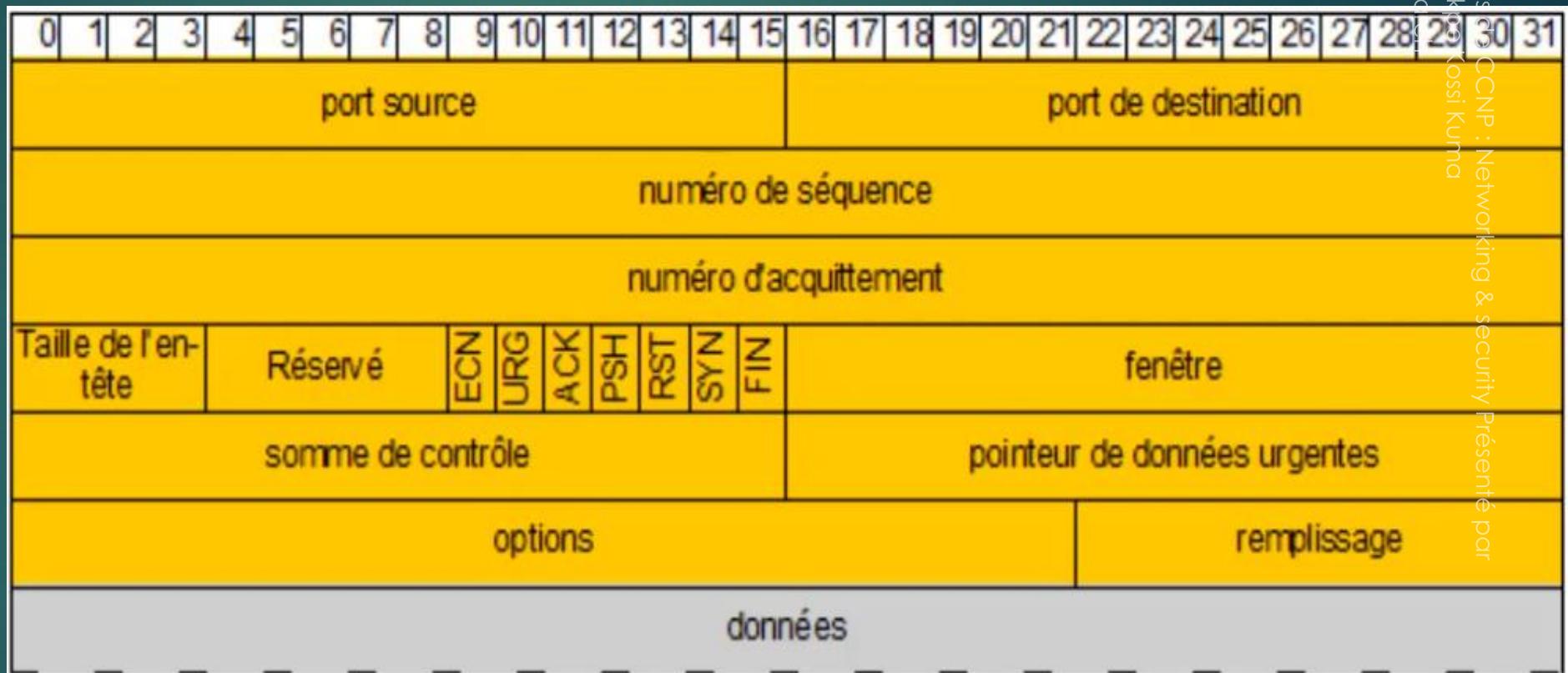
# TCP : Introduction

63

- ▶ Deux protocoles de couches transport dans le modèle TCP/IP
  - TCP : pour les communications nécessitant une fiabilité des données
    - Protocole de contrôle de transmission
  - UDP : pour les communications privilégiant le débit
- ▶ Permettent le dialogue entre applications
  - OSI niveau 2 (Liaison) : communication sur réseau local
  - OSI niveau 3 (Réseau) : communication entre réseaux
    - Entre machines distantes
  - OSI niveau 4 (Transport) : communication entre applications distantes

# Eléments

- ▶ Contrôle des données
  - Mode connecte
    - Etablissement d'une session de communication entre deux hôtes (applications)
    - A ne pas confondre avec la couche session du modèle OSI
- ▶ Régulation du débit
  - Par émission du message (segments) de taille variable
    - Par émission de messages (segments) de taille variable
- ▶ Multiplexage
  - Cohabitation sur une même ligne d'informations destinées à diverses applications
  - En les identifiant grâce à un numéro (de port)

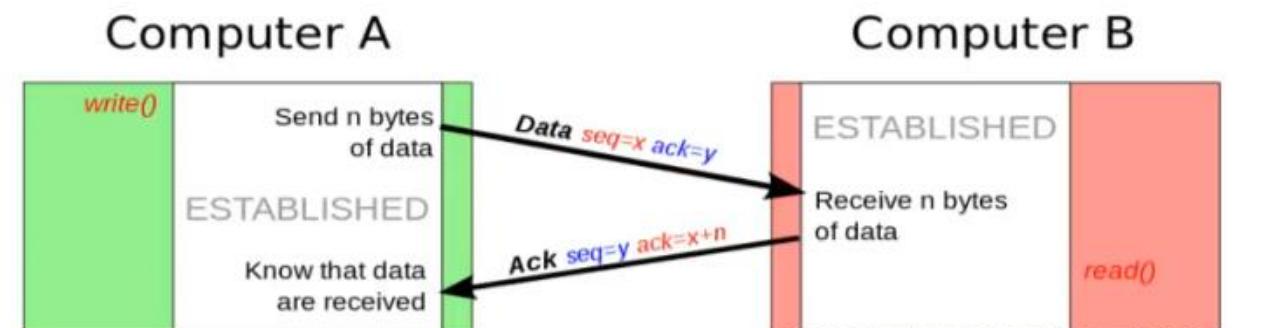


# Port TCP

2018 à ce jour

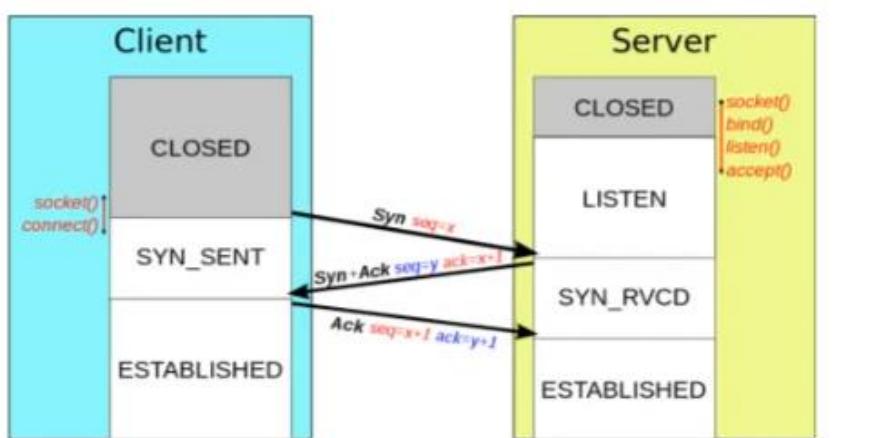
- stockés sur 2 octets
- défini l'application émettrice et l'application destinataire de l'information
- permettent le multiplexage
- 3 catégories :
  - ports "bien connus" (Well-known ports)
    - de 0 à 1023
    - assignés par l'IANA
      - Internet Assigned Numbers Authority
    - protocoles largement utilisés
      - exemples : FTP (21), SSH (22), HTTP (80)
      - voir liste officielle
  - ports enregistrés (Registered ports)
    - de 1024 à 49151
    - services
      - enregistrés par l'IANA (officiels)
        - exemples : OpenVPN (1194), IPSec (1293), Cisco X.25 over TCP (XOT) service (1998)
      - ou non officiels
        - exemple : Windows Live Messenger (1503)
  - ports dynamiques / privés
    - de 49152 à 65535
    - plus rarement utilisés

- **numéro de séquence**
  - associé à un paquet lors de son émission
- **après réception, un "accusé de réception" est envoyé**
  - paquet avec drapeaux ACK activé (à 1)
  - avec un numéro d'acquittement égal au numéro de séquence du paquet reçu + quantité de données (en octets) reçues
  - et un numéro de séquence égal au numéro d'acquittement du paquet reçu
- **en l'absence de réception de cet "accusé de réception" durant un temps imparti, le paquet est retransmis**
  - en cas de réception de deux paquets identiques (même numéro de séquence), la machine réceptrice ne considérera que le dernier paquet reçu



# Etablissement de connexion

- "synchronisation" des numéros de séquence
- Three-way handshake
- Deux drapeaux :
  - SYN : demande de connexion
  - ACK : acquittement
    - positionné ensuite pour tout les segments échangés sur une connexion établie



- 3 étapes :
  - demande de connexion
  - acquittement + demande de connexion
  - acquittement

# Autres drapeaux

- ▶ ECN : signale la présence de congestion
  - RFC 3168
- ▶ URG : données urgentes
- ▶ PSH : données à envoyer tout de suite (push)
- ▶ RST : rupture anormale de la connexion (reset)
- ▶ FIN : demande la FIN de la connexion
  
- ▶ Un espace de 5 bits est conservé avant ces drapeaux
  - Afin de prévoir des éventuels ajouts futurs

# Autres éléments

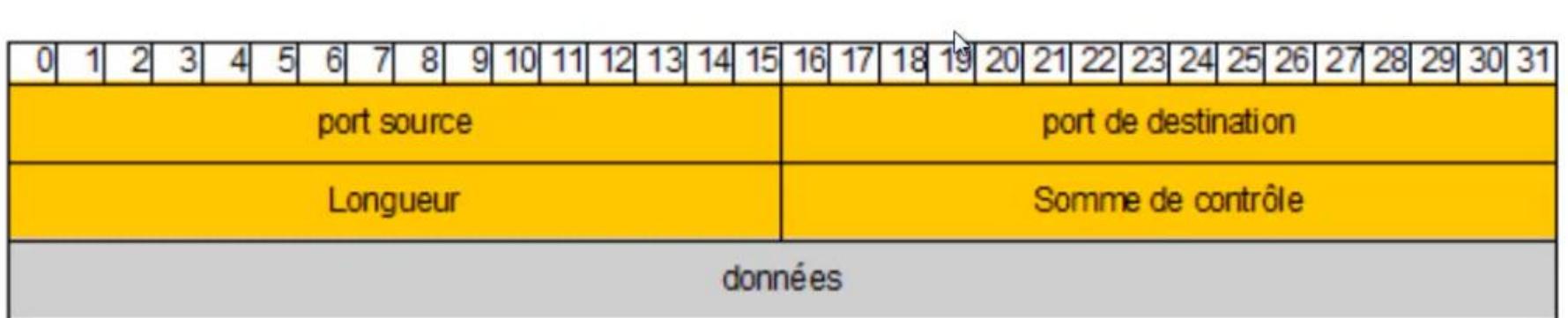
- ▶ Taille de l'en tête
  - Essentiel, car la taille de champs Options est variables
- ▶ Fenêtre
  - Nombre d'octets que le récepteur souhaite recevoir sans accuser de réception
- ▶ Somme de contrôle (checksum ou CRC)
  - Somme des champs de données de l'en tête
    - Afin de permettre de vérifier l'intégrité de l'en tête
- ▶ Pointeur de données urgentes
  - Numéro de séquence à partir duquel l'information devient urgente
- ▶ Option: divers options
- ▶ Remplissage par des zéros : afin d'obtenir une taille d'en tête multiple de 32 bits.

# Protocole UDP : Présentation

71

- ▶ Protocol de transport
  - Permet de répondre à certaines problématiques non couvertes par TCP
  - Services ne nécessitant pas de contrôle de la fiabilité de données
    - Permet un meilleur débit (transport immédiat des informations)
    - Streaming, VOIP, etc...
      - ✓ Un paquet peut être perdu
      - ✓ Mais l'essentiel est d'envoyer les informations en temps réel, le plus rapidement possible
- ▶ Bien plus simple que le TCP :  
aucune procédure de contrôle et donc de mode connecté
- ▶ Les services pourront utiliser le TCP ou UDP ou les deux
  - TCP uniquement : HTTP (port 80)
  - UDP uniquement (rare) : NTP (port 123), NFS (port 973)
  - Les deux (grande majorité des services) : SSH (port 22), IMAPv3 (port 220)

# Segment UDP



- Le plus simple possible
  - aucun mécanisme complexe
  - ports (source + destination)
    - idem que pour TCP
    - cf [https://fr.wikipedia.org/wiki/Liste\\_des\\_ports](https://fr.wikipedia.org/wiki/Liste_des_ports)
  - longueur du segment
  - somme de contrôle (pour l'intégrité)

- Nombreux termes → nombreuses confusions
  - paquet, segment, datagramme, trame
- Datagramme
  - pour les éléments envoyés sans contrôle de réception
  - IP mais aussi UDP
- Segment
  - division d'un message en plusieurs éléments de taille variable
  - pour optimiser le transfert
  - couche Transport : TCP / UDP
- Paquet
  - couche réseau uniquement ! (IP, ICMP)
  - souvent mal utilisé
    - ne s'applique pas aux couches supérieures (TCP/UDP) ni inférieures (Ethernet)
- Trame
  - dernière encapsulation avant transport sur le réseau
    - header + données + trailer
  - couche liaison uniquement ! (Ethernet, WiFi, PPP)

# Partie II

# Switching

# Rappel : qu'est ce qu'un commutateur?

- ▶ Elément de niveau 2 du modèle OSI
  - Agit donc au niveau de la liaison
    - Adresse MAC, CSMA/CD, etc...
- ▶ Nombreuses fonctionnalités supplémentaires
  - Par rapport aux hubs (composants de niveau 1)
    - Commutation (ire. aiguillage)
  - Et aux bridges (composants de niveau 2)
    - Multiport

# Commutation

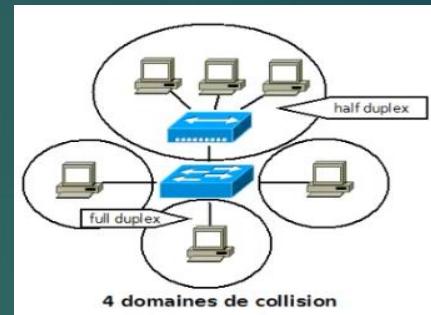
- ▶ Un commutateur est un composant multiports
  - Une ou plusieurs machines pourront donc être reliées à chacun
  - Ce qui va permettre de déterminer de manière intelligente où envoyer chaque trame.
    - En fonction de son adresse MAC de destination
      - ✓ Un port étant associé à chaque adresse MAC
    - C'est ce qu'on appellera la commutation
      - ✓ A ne pas confondre avec le routage
- ▶ Le commutateur va établir ces correspondances port/Adresse MAC Grace à une table CAM (Content Addressable Memory)

# Apprentissage

- ▶ Au départ, la table CAM du commutateur est vide
  - Aucune correspondance MAC / port
- ▶ Celle-ci va donc être remplie de manière dynamique et intelligente
- ▶ A la réception d'une trame le commutateur va :
  - Associer l'adresse MAC source au port par lequel est parvenue cette trame
  - Puis envoyer le paquet à tout le monde (ire sur tous les ports)
  - Quand la machine de destination répondra à cette trame, il pourra alors associer son adresse MAC au port par lequel est parvenu cette réponse

# Domaine de collision

- ▶ Zone logique du réseau dans laquelle les collisions sont possibles
  - Toute portions constituée uniquement de composants de niveau 1
- ▶ Un commutateur stocke les trames avant envoi
  - Afin de ne les envoyer que si le media est libre
  - Evite donc les collisions
  - Permet de ne plus utiliser le CSMA/CA
    - C'est ce qu'on appelle le flux duplex, utiliser avec les hub et les câbles coaxiaux
    - Utilisation déterminer automatiquement par la carte réseau



# Première approche de la CLI

- ▶ CLI : Command Line Interface
  - Interface de configuration en ligne de commande
  - L'administrateur rentre une ligne de commande
    - Appuyer sur enterrée envoie cette commande au switch, qui agit en conséquent.
- ▶ IOS : Internetwork Operating System
  - Système d'exploitation pour la connexion des réseaux
  - Système d'exploitation de la plupart des équipes Cisco
  - Beaucoup de commandes vues dans ce chapitre seront donc applicable aux routeurs
  - Utilise TCL (Tool Command Languages)

# Accéder à la CLI

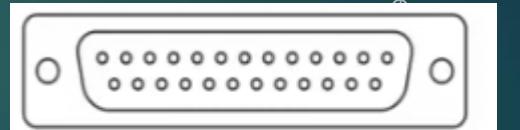
- ▶ 3 méthodes
  - Console
    - Port physique
  - Par le réseau IP
    - Telnet
    - SSH
- ▶ Il est également possible d'utiliser un outil graphique
  - Cisco Security Device Manager (SDM)
  - Ou son successeur Cisco Configuration Program (CCP)

# Port console

- ▶ Port Rj-45
  - Clairement indique ('console')
  - Connecte au PC via un câble UTP rollover
  - Via le port série (RS232 – DB25)
    - Il est possible d'utiliser un adaptateur série USB pour les PC récents
    - Ou un câble Rj-45 to DE-9
      - ✓ Souvent désigné à tort comme port DB9
- ▶ Nécessite un émulateur de terminal
  - Minimum : libre, pour les systèmes Unix
  - Teratem : libre, pour Windows
    - Bonne alternative pour HyperTerminal, supprime de Windows a partir de visita
    - Putty : libre, très complet, compatible Windows et Unix



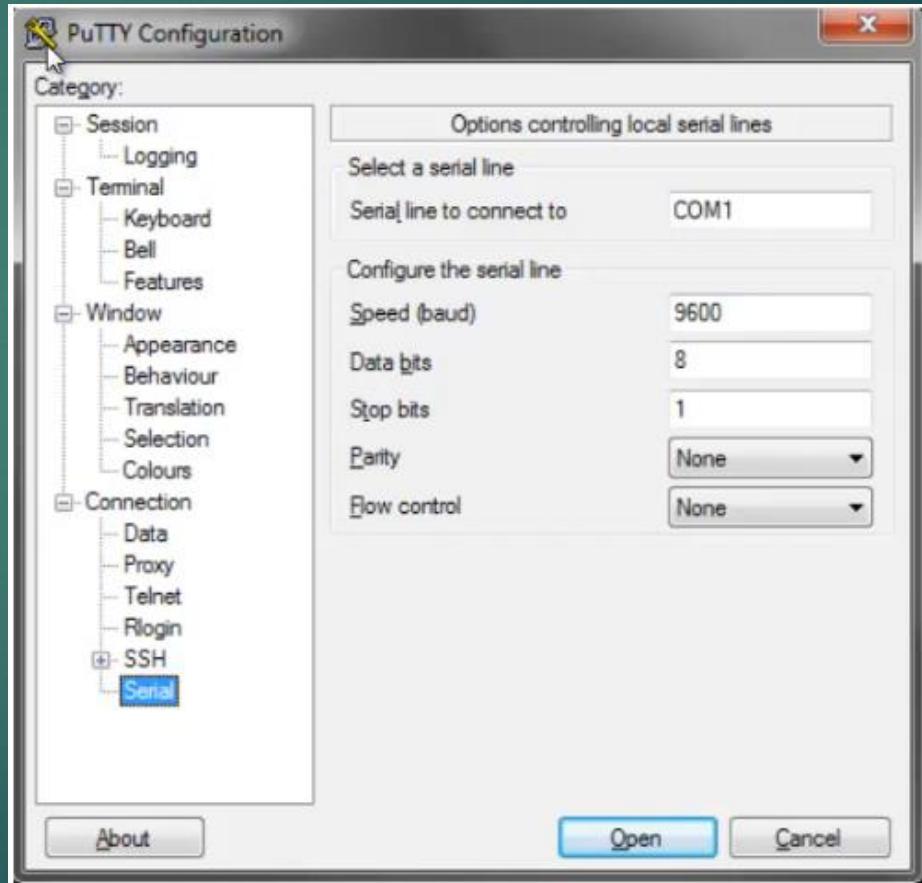
connecteur mâle DE-9



connecteur DB25

# Paramètres

- ▶ Paramètres à respecter :
  - 9600 bits/s
  - Aucun contrôle de flux matériel
  - 8-bit ASCII
  - Pas de bit de parité
  - 1 bit stop
- ▶ Voir plus loin pour établir la connexion avec Putty



# Telnet et SSH

- ▶ Deux protocoles clients serveur
  - Telnet
  - Non sécurisé
    - Toute communication transmise en clair, mot de passe compris
  - Port TCP/UDP 23
- ▶ SSH (Secure Shell)
  - Sécurisé
    - Toute communication est authentifiée et chiffrée
  - Port TCP/UDP 22
- ▶ Se connecter via le réseau
  - Nécessite un client Telnet ou SSH
  - Clients basiques
    - Commande ssh (openssh-client) ou Telnet des systèmes Unix
    - Disponible via Cygwin sous Windows
  - Putty
    - Client graphique complet
    - SSH, Telnet, mais aussi Rlogin, TCP brut et connexion directe

# Modes

- ▶ Dans le terminal, les commandes seront interprétées suivant le 'mode' actuel
- ▶ Le prompt indiquera systématiquement le mode actuel
  - Exemple : en mode « configuration d'une ligne' »  
Switch (config-line)#
- ▶ Nous verront au fur et à mesure les commandes permettant de passer dans chaque 'mode'

## modes "utilisateur" et "privilégié"

Par défaut, suite à votre connexion, le mode "user EXEC" est utilisé

- ce qui implique qu'il est impossible d'effectuer des commandes nécessitant certains priviléges
  - ex : redémarrer le switch grâce à la commande reload
- ceci est indiqué par le prompt ">"

Pour exécuter ces commandes, il vous faudra passer en mode "privilégié"

- "Enable mode", "privileged mode" ou encore "privileged EXEC mode"
- grâce à la commande enable
  - nécessite un mot de passe
- indiqué par le prompt "#"

# Running config et startup config

85

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
18 March  
2025

- deux espaces distincts pour stocker la configuration
  - mémoire vive (RAM)
    - running-config
    - configuration actuellement utilisée
    - perdues après redémarrage
  - mémoire non volatile (NVRAM)
    - startup-config
    - configuration chargée au démarrage
- pour afficher la configuration

```
# show running-config
```

```
# show startup-config
```

- pour enregistrer la configuration actuelle (running-config)

```
# write
```

- ou

```
# copy running-config startup-config
```

# Configuration d'interface

- mode Interface

```
(config)# interface type number  
(config-if)#
```

- Exemple

```
(config)# interface FastEthernet 0/1
```

- Il est possible de configurer en une seule fois un ensemble d'interfaces

- Exemple

```
(config)# interface range FastEthernet 0/10 - 20  
(config-if-range)#
```

# Configuration IP

- nécessaire pour accéder au commutateur via le réseau
  - telnet, ssh, interface web ...
- hors, un commutateur n'est pas fait pour, normalement, agir sur la couche 3
  - on va donc utiliser une interface virtuelle VLAN1 (cf cours suivants)
    - dans le VLAN par défaut

```
(config)#interface vlan 1
```

- nous configurons ensuite l'adresse ip
  - statique

```
(config-if)#ip address 192.168.1.200 255.255.255.0
```

- ou dynamique

```
(config-if)#ip address dhcp
```

- puis on active l'interface

```
(config-if)#no shutdown
```

# Configuration des interfaces de commutation

- Par défaut, la vitesse et le mode duplex d'une interface sont négociés automatiquement avec le périphérique connecté
  - il est cependant possible de forcer ces valeurs

```
(config)#interface fastEthernet 0/1
(config-if)#speed 10
(config-if)#duplex half
(config-if)#end
```

- Pour plus de clarté, il est également possible de renseigner une description pour chaque interface

```
(config-if)#description votre description ici
```

# Sécurité

- ▶ Par défaut, votre commutateur est 'convenablement' sécurisé
  - Du moment qu'il reste inaccessible physiquement
    - Enfermer dans une salle appropriée
  - Seul un accès console est autorisé par défaut
    - Aucune authentification requise
    - Accès complet à toutes les commandes
      - ✓ Pas de mot de passe pour le mode Enable
- ▶ Il peut cependant être nécessaire de mettre en place un mot de passe pour la connexion
  - Et d'activer le Telnet et le SSH

# Mot de passe

- deux types
  - console
  - Virtual Terminal - vty (pour le telnet)
    - de 0 à 15 (ou de 0 à 4 pour les modèles les plus anciens)
- aucun nom d'utilisateur
- Exemples de configuration :
  - nécessite de passer en mode configuration à partir du terminal

```
> enable  
# configure terminal
```

- Port console 0
- Tout les vty

```
(config)# line console 0  
(config-line)# password faith  
(config-line)# login
```

```
(config)# line vty 0 15  
(config-line)# password love  
(config-line)# login
```

- nécessite l'usage de noms d'utilisateurs locaux

```
(config)#line vty 0 15
(config-line)#login local
```

- activer le ssh en plus du telnet
  - seul le telnet est activé par défaut

```
(config-line)#transport input telnet ssh
```

- ajout d'une ou plusieurs paire(s) utilisateur / mot de passe

```
(config)#username name password pwd
```

- configurer un nom de domaine

```
(config)#ip domain-name example.com
```

- générer une paire clé publique / privée ainsi qu'une clé de chiffrement partagée

```
(config)#crypto key generate rsa
```

# Sécurité des ports

- évite l'intrusion d'un attaquant sur le réseau
  - en explicitant la machine prévue pour se connecter au port
- pas à pas
  - passer en mode de configuration de l'interface

```
(config)#interface FastEthernet 0/1
```
  - passer l'interface en mode "access"

```
(config-if)#switchport mode access
```
  - activer la sécurisation de port sur cette interface

```
(config-if)#switchport port-security
```

# Sécurisation des ports : configuration

- indiquer le nombre maximum d'adresses MACs sécurisées sur cette interface
  - Optionnel - 1 par défaut

```
(config-if)#switchport port-security maximum nombre
```

- indiquer l'action à réaliser à la réception d'une trame non conforme
  - Optionnel - shutdown par défaut

```
(config-if)#switchport port-security violation {protect | restrict | shutdown}
```

- protect : blocage des trames sans message d'avertissement.
- restrict : blocage des trames avec avertissement
  - message syslog, trap snmp et incrémentation du compteur d'erreur
- shutdown : désactivation de l'interface
  - avec blocage des trames et avertissement

# Sécurisation des ports : adresses

- 3 possibilités :
  - configuration manuelle (explicite)
  - apprentissage dynamique
    - ne peuvent être enregistrées
  - sticky : adresses apprises dynamiquement et enregistrées dans la running-config
    - peuvent alors être enregistrées dans la startup-config
    - mode désactivé par défaut
    - lors de l'activation de ce mode, toute adresse apprise dynamiquement est convertie en adresse "sticky"
- spécifier explicitement une nouvelle adresse MAC autorisée
  - si il reste un certain nombre d'adresses MAC autorisées possible non définies, celles-ci seront apprises dynamiquement

```
(config-if)#switchport port-security mac-address adresse-mac
```

- activer le mode "sticky"

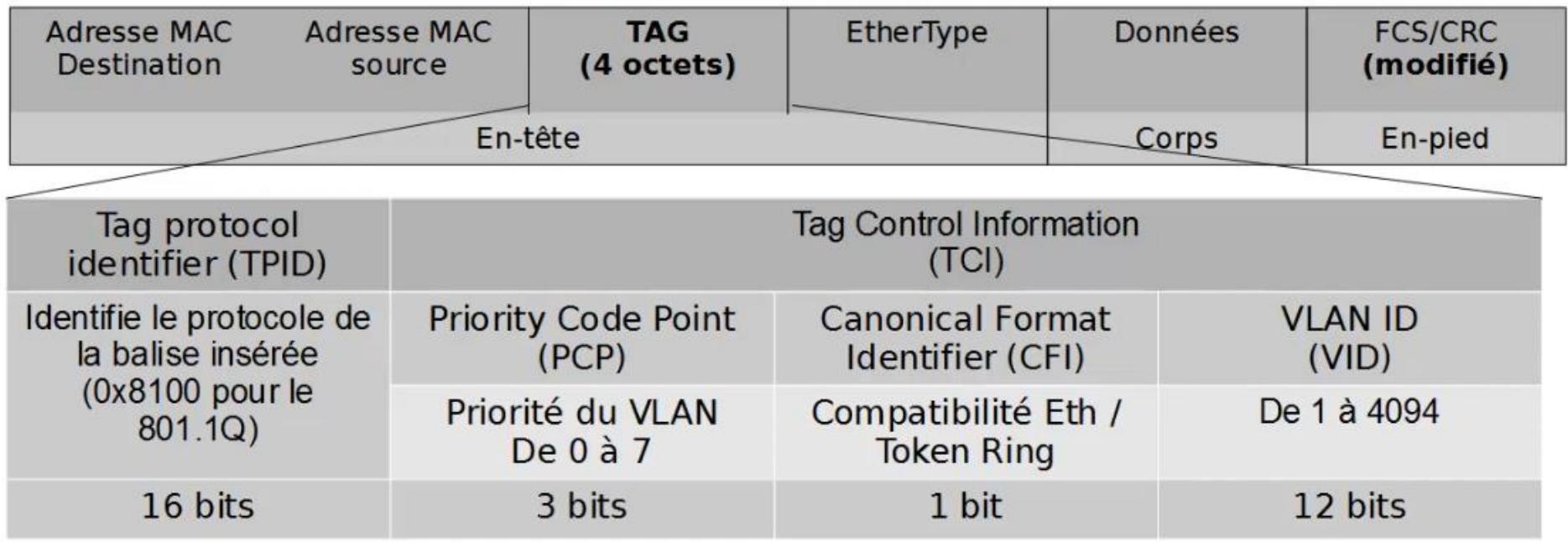
```
(config-if)# switchport port-security mac-address sticky
```

# VLAN : Intérêts

- ▶ Du concept de VLAN lui-même
  - Segmentation
  - Sécurité : nécessite l'utilisation du routeur pour communiquer entre VLANs
  - Optimisation de la bande passante
- ▶ De l'usage de VLANs plutôt que de nombreux Switchs séparés
  - Diminution des couts
    - Un gros switch de 256 ports revient moins cher que 5 Switchs de 48
  - Centralisation de la configuration
  - Modification simplifiées
    - Le passage d'une machine d'une VLAN à une autre peu se faire par simple configuration

# fonctionnement

- norme IEEE 802.1Q
  - successeur de Cisco ISL (Cisco Inter-Switch Link)
- ajout d'un tag aux trames ethernet



# Configuration VLAN : Administration des VLANs

- pour passer en mode de configuration d'un VLAN

```
(config)# vlan 2  
(config-vlan)#
```

- il est également possible de configurer plusieurs VLANs à la fois

```
(config)# vlan 2,3,4  
(config-vlan)#
```

- si la VLAN n'existe pas encore, elle est automatiquement créée
- pour la supprimer, utiliser la commande no

```
(config)# no vlan 2
```

# Configuration des ports

- 2 modes
  - access (par défaut)
    - connexion terminale d'un périphérique
    - n'appartient qu'à un seul VLAN
  - trunk
    - connexion faisant transiter les trames de plusieurs VLAN
    - particulièrement utile pour les connexions entre switchs

- Mise en œuvre

- mode access

```
(config-if)#switchport mode access
```

- mode trunk

```
(config-if)#switchport mode trunk
```

- si plusieurs protocoles d'encapsulation sont disponibles (isl ou dot1q), il peut-être nécessaire de spécifier celui à utiliser au préalable

```
(config-if)#switchport trunk encapsulation dot1q
```

# Affectation d'un port à un VLAN

- en mode de configuration de l'interface
  - fonctionne aussi avec un groupe d'interface (if-range)

```
(config-if)#switchport access vlan 2
```

- Autoriser des VLANs

```
(config-if)#switchport trunk allowed vlan add 2,3,10
```

- Interdire un VLAN

```
(config-if)#switchport trunk allowed vlan remove 3
```

- Annuler le filtrage

```
(config-if)#no switchport trunk allowed vlan
```

# Classes d'adressage IPv4 : introduction

- ▶ Au départ, seul le premier octet servait à désigner le réseau
  - Les 3 autres octets désignant les machines
  - Soit seulement 256 réseaux de 16 millions d'adresses
- ▶ Nécessité de permettre plus de réseaux
  - Première proposition de : IEN 46 – juin 1978
    - Aggregation des réseaux en régions
  - RFC 790 – Septembre 1981
    - Solution présentée dans ce cours
    - Obsolète depuis Septembre 1993!
      - ✓ Et l'apparition du CIDR (Classless Inter-Domain Routing)
      - ✓ RFC 1518

# Concept

- ▶ Séparation des adresses en deux parties
  - Net id : adresse réseau
  - Host id : adresse de l'hôte
- ▶ 5 classes d'adresses
  - Identifiées par une lettre de A à E
  - Différentes tailles de réseaux
- ▶ Les adresses réseaux sont générées au niveau mondial (pour Internet)
  - Par l'IANA
  - Par d'autres organisations (Apple, MIT, etc...)
  - Ou par des registres internet régionaux

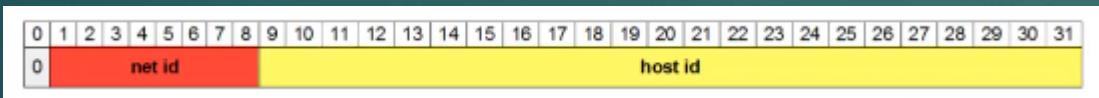
# Classes

Classes	Début	Fin	Net id sur :
A	0.0.0.0	127.255.255.255	Le premier octet
B	128.0.0.0	191.255.255.255	Les deux premiers octets
C	192.0.0.0	233.255.255.255	Les trois premiers octets
D	224.0.0.0	239.255.255.255	NA (multicast)
E	240.0.0.0	255.255.255.255	NA (réservée)

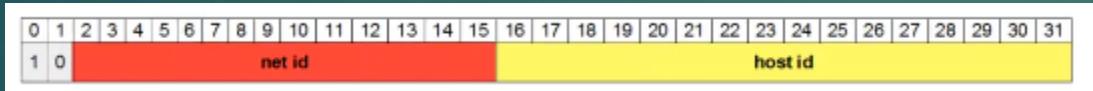
# Classes

Classe	Adresses privées
A	$10.x.y.z$ , où $0 \leq x \leq 255$ $0 \leq y \leq 255$ et $0 \leq z \leq 255$
B	$172.x.y.z$ , où $16 \leq x \leq 31$ $0 \leq y \leq 255$ et $0 \leq z \leq 255$
C	$192.168.x.y$ , où $0 \leq x \leq 255$ et $0 \leq y \leq 255$

- ▶ Réseaux de très grande dimension
  - Nombreuses adresses réservées a des organisations
    - Ex : 018.rrr.rrr.rrr pour le MIT
  - Cas particulier : boucle locale (réseau 127.0.0.0)
- ▶ Nombre de réseaux possibles : 128
- ▶ Nombre de postes maximum par réseau : plus de 16 millions
- ▶ Premier octet : de 0 à 127
- ▶ Masque par défaut : 255.0.0.0 - /8



- ▶ Réseau de 'moyenne' dimension
- ▶ Nombre de réseaux possibles : 16 384
- ▶ Nombre de postes maximum par réseau : 65 534
- ▶ Premier octet : de 128 à 191
- ▶ Masque par défaut : 255.255.0.0 - /16



- ▶ Réseau de petite dimension
- ▶ Nombre de réseaux possibles : 2 097 152
- ▶ Nombre de postes maximum par réseau : 254
- ▶ Premier octet : de 192 à 223
- ▶ Masque par défaut : 255.255.255.0 - /24



# Classe D et E

- ▶ Adresses uniques (pas de Net id)
- ▶ Classe D
  - Destinées au multicast
  - Bits de départ : 1110
  - Premier octet : 224 à 239
- ▶ Classe E
  - Réservées par l'IANA pour usage futur
  - Bits de départ : 1111
  - Premier octet : 240 à 255
- ▶ Et l'IPv6?
  - IPv6 est représenté en 1998
    - Soit bien après le CIDR (1993) et l'abandon du concept de classe
  - Il n'y'a donc aucun concept de classe
    - IPv6 étant pleinement orienté CIDR

# introduction

- ▶ Le concept de classe est très limité
  - Ne permet que peu de réseaux
- ▶ Pour pallier à cela, un nouveau concept est introduit en 1984
  - RFC 917 (Internet Subnets)
  - Sous réseaux
- ▶ Permet la subdivision logique des réseaux de taille plus importante
  - Relativement aux classes d'adresses

# Fonctionnement

- ▶ Ajout d'un troisième champ
  - Entre le net id et le host id
  - Permettant de designer un sous-réseaux
- ▶ La taille de ce champ étant variable, la division entre adresse de sous réseaux et d'hôtes est faite grâce a un masque
  - Adresses IPv4 dont tous les bits correspond a une adresse de reseau qui ont une valeur de 1
  - Ex : 18 premiers bits = 255.255.192.0
  - Donne le sous-réseau d'un hôte par un ET logique sur son adresse
- ▶ Le nombre de sous-réseaux possible est déterminé par la formule suivante :
  - $S = 2^n - 1$  car l'adresse de broadcast (tous à 1) n'est pas utilisable
    - Ou  $n$  est le nombre de bits masques en plus de ceux de net id
- ▶ Le nombre d'hotes possibles est déterminé par la formule suivante :
  - $S = 2^{n-2}$  car ni l'adresse de broadcast ni l'adresse de réseau ne sont utilisables
    - Ou  $n$  est le nombre de bits restant pour le host id

# Exemple

- Un administrateur souhaite diviser le réseau 192.52.61.0 dont il a la charge en 4 sous-réseaux
  - réseau de classe C : 8 bits disponibles
  - $3 = 2^2 - 1 < 4 \leq 2^3 - 1 = 7$ 
    - il aura donc besoin de 3 bits pour le sous-réseau
  - soit un masque de 27 bits



- Les adresses de sous-réseaux seront donc celles dont le dernier octet est égale à une addition de  $2^5$  (32) ou  $2^6$  (64) ou  $2^7$  (128)
  - ex : l'adresse IPv4 d'hôte 192.52.61.112 = **11000000.00110100.00111101.01110000**
    - ET le masque : 255.255.255.224 = **11111111.11111111.11111111.11100000**
    - donnent l'adresse de sous-réseau : **11000000.00110100.00111101.01100000** = 192.52.61.96
- Chaque sous-réseau pourra donc avoir maximum 16 hôtes

# VLSM et CIDR

# Introduction

- ▶ Le concept de classe implique de nombreuses adresses inutilees
  - Ex : un organisme gérant une adresse de classe A mais n'utilisant que un million d'adresses = plus de 15 millions d'adresses inutilisables
- ▶ Son abandon est donc propose en juin 1992 (RFC 1338)
  - Et adopté en Septembre 1993 (RFCs 1518 et 1519)
    - CIDR : Classless Inter-Domain Routing
      - ✓ Remplace le concept de classe par celui de supernetting
    - On parle alors d'adresse Classless

# Variable Length Subnet Mask

- ▶ Mentionné dès Aout 1985 (RFC 950)
- ▶ Permet de diviser un réseau en sous-réseaux de taille variables et non plus fixe
  - Optimisation de l'adressage
  - En établissant des sous-réseaux de sous-réseaux
- ▶ Très peu supporté sur les réseaux de classful
  - Extrêmement répandu aujourd'hui
- ▶ Bonnes pratiques
  - Partir du plus grand au plus petit (en nombre d'hôtes)
- Toujours prendre la valeur de masque offrant le nombre d'hôtes le plus proche de (et supérieur à) celui escompté
  - A une exception près : prévoir la croissance (modeste) des sous-réseaux (ne pas prendre exactement le nombre escompté)
- ▶ Exemple le RFC 1875, relative au VLSM de décembre 1995 permet de passer outre la RFC1860 voulant qu'une adresse de réseau (tous les bits à 0) ne soit jamais utiliser pour désigner un de ses sous-réseaux
  - De même pour l'adresse de sous-réseaux avec tous les bits à 1 non utilisable normalement
    - Le nombre de sous-réseaux pourra donc être de  $2^n$  et non  $2^{n-1}$

# Exemple

- subdiviser 192.168.56.0/25 au mieux
  - plage d'adresses :
    - de 192.168.56.0 0000001 /25
    - à 192.168.56.0 1111110 = 126 /25
  - en 3 réseaux :
    - N1 : 28 machines → 5 bits (30 hôtes max) → /27
    - N2 : 10 machines → 4 bits (14 hôtes max) → /28
    - N3 : 4 machines → 3 bits (6 hôtes max) → /29
- 192.168.56. 0 00 00000  
/25 /27 hôtes ou sous-réseaux (5 bits)
- une sous division à netmask fixe sur 2 bits (/27) donne 3 (éventuellement 4) sous-réseaux de 30 hôtes max
  - nous "gâcherions" donc  $30-4+30-10+30-28 = 47$  adresses
  - et nous n'aurions aucun autre sous-réseau disponible pour un usage futur

# Exemple

- On prend le premier sous réseau /27 pour N1
  - soit le 192.168.56.0/27
    - de 192.168.56.0 **00** 00001 /27 à 192.168.56.0 **00** 11110 = 31 /27
- Puis on prend le second (192.168.56.0 **01** 00000 = 32 /27)
  - qu'on peu diviser en deux sous-réseaux en /27 de 14 hôtes max
    - on prend le premier pour N2 (192.168.56.32/28)
      - de 192.168.56.0 **010** 0001 = 33 /28 à 192.168.56.0 **010** 1110 = 46 /28
    - et on peu à nouveau diviser le second en 2 sous-réseaux en /29 (6 hôtes max)
      - on prend le premier pour N3 (192.168.56.48/29)
        - de 192.168.56.0 **0110** 001 = 49 /29 à 192.168.56.0 **0110** 110 = 54 /29
      - et le second reste disponible pour un usage futur

# Exemple : conclusion

- ▶ Nous avons donc ‘gâché’  $30-28+14-10+6-4=8$  adresses
  - Qui seront bien utiles en cas de croissance de ces sous-réseaux
- ▶ Et il nous reste de disponible pour un usage futur :
  - Le sous-réseau 192.168.56.64/27 soit 30 machines
- ▶ Remarque : gardez a l'esprit de toujours prévoir la croissance de vos sous-réseaux
  - Donc de conserver un nombre d'adresses disponible suffisant pour chacun
    - Ne pas prendre forcément le nombre de bits le plus proche, mais le plus adapté.

# CIDR et le supernetting

117

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
18 March  
2025

- ▶ CIDR implique l'absence de classe
  - Donc de net id prédéfini pour designer l'ensemble de nos sous-réseaux
- ▶ De plus, VLSM implique qu'un réseau peut être subneté à plusieurs niveaux
  - Nous avons donc besoin d'une adresse permettant de designer l'ensemble des sous-réseaux pour chaque niveau
    - Ainsi le routeur connectant ces réseaux ne devra propager qu'une table de routage au lieu d'une par sous-réseau
    - Et ainsi économiser ressource mémoire et processeur
- ▶ Cela s'appelle le supernetting
  - Opération inverse du subnetting
  - Agréger des sous-réseaux en un seul

# Suite de l'exemple précédent

- Nous avons donc 3 sous-réseaux :
  - N1 : 192.168.56.0/27 soit 0 00 00000
  - N2 : 192.168.56.32/28 soit 0 010 0000
  - N3 : 192.168.56.48/29 soit 0 0110 000
- Quel est donc l'adresse permettant d'un réseau englobant ces 3 sous-réseaux ?
  - il nous faut donc un réseau englobant les adresses :
    - de 192.168.56.0 soit 0 00 00000
      - masque /27 soit 255.255.255.1 0000000
    - à 192.168.56.55 soit 0 0110 111
      - masque /29 soit 255.255.255.11111 000
  - le réseaux le plus proche de cette plage d'adresse est donc
    - de 192.168.56.0 à 192.168.56.00 0 111111 = 63
    - donc le réseau 192.168.56.0 0 000000 /26
      - masque : 255.255.255.11 000000 soit 255.255.255.192
    - qui est bien un sous-réseau de 192.168.56.0/25

# Adresse IPv6

# Introduction

120

- ▶ Même si la migration de l'IPv4 à l'IPv6 n'a, clairement, toujours pas réellement eu lieu
  - Elle devient de plus en plus nécessaire
  - Face à la pénurie d'adresses IPv4
- ▶ Même si la notation hexadécimale peu paraître complexe
  - Comprendre l'IPv6 n'est pas bien plus difficile que pour l'IPv4
- ▶ Donc, même si nous n'en rencontrons encore que peu
  - Nous allons en rencontrer de plus en plus
  - Et il est plus que nécessaire de s'y préparer
    - D'autant plus que cela ne représente que peu de temps d'apprentissage

# Rappels

- ▶ Une adresse IPv6 est codée sur 128 bits
  - Soit en théorie  $3,4 \times 10^{38} = 340$  sextillions d'adresses
    - Soit 340 milliards de milliards de milliards de milliards!
    - Soit 48 quadrilliards ( $10^{27}$ ) d'adresses par personnes dans le monde
      - ✓ Soit de quoi changer 17 billards ( $10^{15}$ ) de fois d'IP par seconde en 85 ans pour une personne possédant 1 milliard de machines
- ▶ Tout cela ne reste que de la théorie
  - Car bien entendu, de 'très' nombreuses ne sont pas utilisables
- ▶ Mais on pourrait donc tout de même établir des adresses uniques mondialement pour chaque machine!
  - Résolution du problème de pénurie du nombre d'adresses IPv4

- ▶ Unicast
  - Adresse désignant une seule interface d'un hôte
- ▶ Anycast
  - Nouveau concept
  - 'le plus proche' / 'le plus efficace'
  - Adresse d'un nœud parmi un groupe de nœuds
    - Désigne 'n'importe quel' membre ce nœud
- ▶ Multicast
  - Abandon des adresses de broadcast
  - Désigne un groupe d'interfaces
  - Chaque interface étant libre de s'abonner à un groupe et de le quitter, à tout moment
    - Moins pénalisant que le Broad casting IPv4

# Types d'adresses unicast

- ▶ Adresse de boucle locale (Loopback)
  - ::1/128
  - Limite à une utilisation interne pour un hôte
- ▶ Adresse de liaison (Link-local)
  - Unique sur un lien donné
  - Purement locales (adresses locales de lien)
    - Non routables
  - Ou uniques (mondialement)
    - RFC 4193
- ▶ Adresse globales
  - Unique dans le monde
- ▶ Sous-réseaux
  - Même système que pour l'IPv4 Classless
    - Notation CIDR du masque
- ▶ Exemple :
  - 2001:db8:1:1a0::/59
    - De 2001:db8:1:1a0:0:0:0:0 à 2001:db8:1:1bf:ffff:ffff:ffff:ffff

# Adresses locales de lien

124

Cours de CCNP : Networks  
Katakpe Kossi Kuma  
18 March  
2025

- adresses fe80 ::/10
    - masque en /64
  - purement locales
    - non routables
    - uniquement utilisables sur les réseaux de niveau 2 (segment réseau : lien ou domaine de broadcast)
  - allouée automatiquement (le plus souvent à partir de l'adresse MAC) ou manuellement
    - requis sur toute interface sur lesquelles IPv6 est activé
    - pour d'autres protocoles liés à IPv6 (NDP, DHCPv6, etc ...)
  - uniques sur un lien uniquement
    - ce qui permet à un hôte d'utiliser éventuellement la même adresse pour plusieurs interfaces
  - aucun sous-réseau
    - toutes les machines appartiennent au réseau fe80::/64

0 1 2 3 4 5 6 7 8 9	10 ... 64	65 ... 128
<b>préfixe</b>	<b>zéros</b>	<b>interface</b>
1 1 1 1 1 1 1 0 1 0		
10	54	64

# Adresses locales unique

- fc00::/7 (pour Internet)
  - et fd00::/8+ (pour L=1, pour les réseaux locaux)
- ne sont routables que sur les sites qui le souhaitent
  - pas sur Internet
  - équivalent des plages d'adresses privées (RFC 1918) IPv4

0	1	2	3	4	5	6	7	8	...	48	49	64	65	...	128
préfixe		L	ID Globale				Sous-réseau				interface				
1	1	1	1	1	1	0	1	7	1	40	16	64	65	...	128

- ID Globale : identifiant unique de l'organisation
  - choisi pseudo-aléatoirement
- L : 1 si l'ID Globale est assigné localement

# Adresses globales unicastes

- 2000 ::/3
  - soit 1000 0000 0000 0000 ::/3
- 1/8ème de l'espace total d'adressage IPv6 utilisé seulement (la plupart en 2001::/16)
  - afin de limiter la taille des tables de routage
  - assignées par blocs de /23 à /22 par les Registres Internet Régionaux (cf IANA)
    - exemple : SFR détient le bloc 2001:4c18::/32
    - routables sur Internet
- moins d'un autre 1/8ème est réservé
  - ex : 2002::/16 : adresses 6to4
    - permettent d'acheminer le trafic IPv6 via un ou plusieurs réseaux IPv4
- Toutes les autres adresses routables (plus des trois quarts) sont actuellement réservées pour usage ultérieur

0	...	47	48	64	65	...	128
préfixe		Sous-réseau			interface		
48		16			64		

# Multicast

- ff00::/8
- propres à l'application
- exemple : ff02::1:ff00:0/104
  - pour découvrir l'adresse MAC d'un hôte dont l'adresse IPv6 est connue
  - avec NDP (Neighbor Discovery Protocol)



- Drapeau : 3 bits définis par la RFC 4291
  - le bit le plus significatif étant réservé à un usage ultérieur
- Scope : domaine de validité de l'adresse

# Méthodes et protocoles de routages : Qu'est ce le routage?

128

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
18 March  
2025

- ▶ Permet d'interconnecter plusieurs réseaux
  - Via des routeurs
    - Composants de couche réseaux (3)
    - Toute machine compatible IP peut agir en tant que routeur, grâce à un logiciel de routage
      - ✓ En relayant les paquets qui ne sont 'pas pour lui'
      - ✓ En désencapsulant le paquet IP de la trame Ethernet
      - ✓ Et en le réencapsulant avec une nouvelle adresse MAC de destination
- ▶ Grace a un ensemble de règles
  - Déterminant qui peut communiquer avec qui et comment
    - C'est-à-dire 'en empruntant quel chemin' / 'en passant par qui'
    - Enregistre dans des 'tables de routage'
- ▶ Remarque : un routeur permet également de connecter les VLANs
  - Par exemple pour communiquer avec des ressources partagées (comme le DHCP)
  - Le subnetting se fera entre des réseaux physiques différents (séparés par des routeurs) alors que les VLANs seront sur un même réseau physique (via des Switchs)
    - En pratique, on cumulera souvent les deux

# Table de routage

- ▶ Le routage est un processus décentralisé
  - Chaque routage possède des informations sur son voisinage
  - Détermine à qui doivent être envoyés les paquets destinés à un réseau particulier
    - Routeur voisin ou réseau directement connecté
- ▶ Associe une adresse réseau à une passerelle (un routeur)
- ▶ Trois types de routes
  - Statique : configuration manuelle par l'administrateur
    - Chaque entrée est donnée explicitement
  - Dynamique : apprentissage par le routeur lui-même
    - Grâce à des protocoles de routage spécifique
  - Connectée : réseau directement connecté au routeur
    - Appel à un Protocol de niveau 2 (Ethernet)
- ▶ A cela s'ajoute une route par défaut, qui peut être statique ou dynamique

# Systèmes Autonomes

- ▶ AS pour Autonomous System
- ▶ Zone particulière (sous ensemble) d'un très grand réseau
  - Compose de nombreux réseaux IP, LAN, WAN, stc.
  - Administre par une même entité
  - Ex: réseaux grand compte d'envergure mondiale, backbone internet (réseau d'opérateur de large envergure)
- ▶ Deux types de routeurs en son sein
  - De bordure : permettent d'entrer et sortir de l'AS
    - Par exemple, pour joindre internet (d'un réseau d'opérateur vers les autres)
  - Internes : assurent la communication entre réseaux de l'AS.
- ▶ Chaque AS est identifiée par un numéro ASN unique au sein d'un même réseau
  - Sur internet ceux-ci sont délivrés par les registres internet régionaux

# Protocoles de routage

- ▶ Pour employer des algorithmes de routage efficaces, un routeur a besoin de connaître au moins une partie de la typologie du réseau
  - Il est donc nécessaire de diffuser les tables de routage
    - Il faut échanger les informations entre routeurs
- ▶ On utilise pour cela un protocole de routage
  - De deux types :
    - Internes : Interior Gateway Protocols (IGP) entre routeurs internes d'un même AS:RIP, OSPF, les seules concernées par la CCENT
    - Ou externes : Exterior Gateway Protocols (EGP)
      - ✓ Entre routeurs de bordure d'AS différents : BGP

# Quelques exemples de protocoles de routage interne

- ▶ RIP et RIP-2 : Routing Information Protocol
  - Le plus ancien et le plus simple
  - Très limité
- ▶ OSPF : Open Shortest First
  - Ecrit pour remplacer RIP en palliant à ses limites
  - Complet et performant
  - Habituellement réservé aux grands réseaux
  - Recommandé comme IGP pour Internet (RFC 1371)
- ▶ IGRP : Interior Gateway Routing Protocol
  - Propriétaire Cisco
- ▶ IS-IS : Interior System to Interior System
  - Norme ISO/IEC 10589:2002 de l'OSI : extrêmement stable

# Protocoles de routage externe

133

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
18 March  
2025

- ▶ EGP : Exterior Gateway Protocol
  - Le premier
  - Très peu performant
  - Quasi abandonné
- ▶ BGP : Border Gateway Protocol
  - Le plus efficace et donc le plus utilisé
  - Utilisé pour Internet
- ▶ ES-IS : Exterior System to Interior System
  - Unique EGP normalisé OSI
  - Très peu utilisé

# CONFIGURATION BASIQUE DES ROUTEURS :

## Introduction

- ▶ La grande majorité des commandes vues pour les Switchs reste applicable
  - Modes (user et ensable) et mot de passe
  - Mode de configuration
  - Configuration console Telnet, et ssh
  - Nom d'hote et configuration d'interface
  - Configuration des interfaces (speed, duplex)
  - Activation et désactivation des interfaces (Shutdown)
  - Aide et raccourcis
  - Startup et running config (copy et setup)
- ▶ Seules diffèrent
  - La configuration IP
  - Les questions posées en mode setup, la présence du port AUX, absent des Switchs
    - Accès a la CLI par ligne téléphonique

# Commandes d'information

135

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
18 March  
2025

- ▶ Rappel : Adresse IP d'une interface

- afficher les protocoles configurés

```
# show protocols
```

- afficher la table de routage

```
# show ip route
```

- affichage des statistiques IP

```
# show ip traffic
```

- afficher l'état des protocoles de routage actifs

```
# show ip protocols
```

- configuration statique

```
(config-if)#ip address 10.1.1.1 255.255.255.0
```

- configuration par dhcp

```
(config-if)#ip address dhcp
```

- synthèse rapide de la configuration des interfaces

```
#show ip interface brief
```

# Routes statiques

136

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
18 March  
2025

- syntaxe générale

```
(config-if)#ip route adresse-réseau masque passerelle
```

```
(config-if)#ip route adresse-réseau masque interface
```

- route par défaut

```
(config-if)#ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

- exemples de routes statiques

```
(config-if)#ip route 192.168.1.0 255.255.255.0 FastEthernet 1/0
```

```
(config-if)#ip route 192.168.1.0 255.255.255.0 192.168.1.1
```

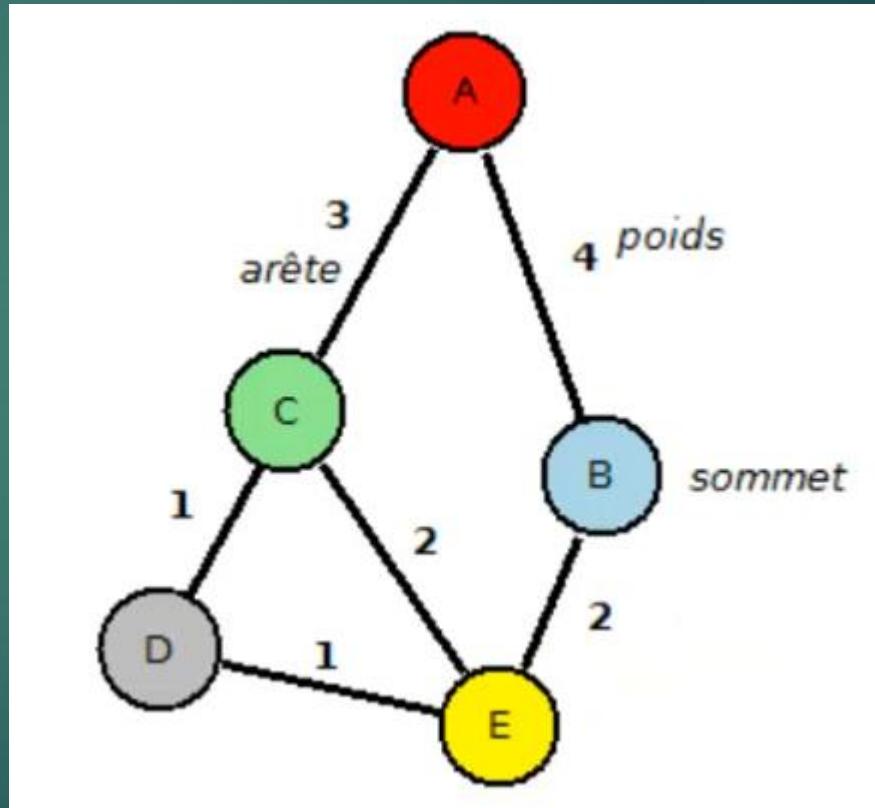
# Le protocole OSPF

# Problème du plus court chemin

138

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
18 March  
2025

- ▶ Problème classique de théorie des graphes
  - Trouver le chemin optimal entre les sommets d'un graphe
  - Particulièrement dans le cadre des réseaux
- ▶ De nombreux algorithmes existent pour résoudre ce problème
  - Plus ou moins efficaces suivant les contextes
  - Algorithme de Dijkstra
  - Algorithme de Bellman-Ford



# Limitations de RIP

139

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
18 March  
2025

- ▶ Protocole à vecteur de distances
  - Aucune vision globale du réseau
    - Diffusion des routes de proche en proche
  - Grande consommation de la bande passante
    - Particulièrement pour les grands réseaux
    - Du fait de l'envoie périodique de toutes les tables de routage en broadcast
  - Sensible aux boucles de routage
    - Limite de 15 sauts
      - ✓ Tout réseau au delà de 15 routeurs est considéré comme inaccessible
- ▶ Ne se base que sur le nombre de 'sauts' permettant d'atteindre le routeur voisin
  - Aucune prise en compte de la bande passante des liaisons pour choisir le meilleur chemin possible, ou d'autres informations (fiabilité, charge, délai, etc.)

# Open Shortest First (OSPF)

- ▶ Protocole à état de lien
  - Connaissance de l'intégralité de la topologie du réseau
    - Élimine les boucles de routage
  - Collecte de l'ensemble des couts de liens
    - En terme de temps
    - En continue
  - Plus grande consommation de ressources processeur
    - Nécessite des routeurs performants
- ▶ Fonctionnement
  - Analyse en continue des connexions vers les éléments proches
    - Message hello envoyé à intervalles réguliers
  - Calcul du plus court chemin vers les routeurs voisins
  - Diffusion de la liste des routes connectées et des états de liens
    - Propage de proche en proche
    - Toutes les 30 minutes (intégralité des LSAs)

# Open Shortest First (OSPF)

- Et à chaque changement (LSA modifiées uniquement)
- LSA (Link-State Advertisement)
  - ✓ L'ensemble des LSAs d'une aire formant la LSDB (Link-State Data Base)
- Détermine enfin la route la plus courte pour chaque réseau de la LSDB.
- ▶ Area
  - Sous-ensemble de routeurs
    - En bordure duquel un résumé de la LSDB peut être fait
    - Chaque sous-réseau appartenant à une seule aire
  - Permet d'éviter de propager l'intégralité de la LSDB
- Identifie par des nombres entiers de 32 bits
  - Souvent note en notation décimale pointée
    - ✓ A la manière des adresses IPv4
- La configuration d'OSPF devient complexe quand plusieurs aires sont mises en place
  - Heureusement il ne vous est demandé que de savoir le configurer dans une aire unique dans le cadre de la CCENT

# Activation

```
# router ospf process-id  
(config-router)#{
```

- lancement d'un processus de routage OSPF
  - permet d'activer l'OSPF sur le routeur (aucun par défaut)
  - ou de passer en mode de configuration de ce processus de routage si déjà actif
- process-id : identifiant interne du processus de routage
  - n'importe quel entier supérieur ou égal à 1

## ► Définition du routeur-ID

- Optionnel
  - généralement généré automatiquement à partir des adresses IP du routeur au lancement d'OSPF
- Valeur explicite
  - (config-router)# router router-id
- ou par configuration de la plus haute adresse IP de l'interface de loopback

```
(config)#interface loopback 0  
(config-if)#ip address 172.16.0.1 255.255.255.0
```

# Activation

## ▶ Activation de l'OSPF sur une interface

- De manière implicite
  - relativement à une adresse réseau

```
(config-router)# network ip-address wildcard-mask area area-id
```

- Exemple

```
(config)#router ospf 100
(config-router)#network 10.0.3.0 0.0.0.255 area 0
(config-router)#network 10.0.0.0 0.0.0.255 area 0
```

## ▶ Le passive interface

- Par défaut, un routeur sur lequel OSPF est activé continuera de chercher régulièrement ses "voisins" sur ses interfaces
  - par envoi de messages hello à intervalles réguliers
- Hors cela peut-être un gâchis de ressources quand il n'y a aucun voisin sur celle-ci
  - il est donc possible de mettre une interface en mode passif
  - afin qu'elle n'envoie plus de message hello
- en mode de configuration du processus de routage

```
(config-router)# passive-interface type number
```

- ou en mode de configuration de l'interface

```
(config-if)# ip ospf passive-interface
```

# Routage Inter-VLAN

# 3 Solutions

## ▶ Via un routeur

- Avec une interface connectée à chaque VLAN
  - Très rarement employé
- Avec une interface trunk vers un Switch
  - Routeur on a stick (ROAS)
    - ✓ Routage inter-vlan à l'aide d'un routeur dédié
  - Solution la plus courante
  - Présentée dans ce cours
- Via un Switch de couche 3

## ▶ Rappel : Trunking

- permet de faire transiter les trames de plusieurs VLANs sur une interface

```
Switch(config)# interface FastEthernet 0/0
Switch(config-if)# switchport mode trunk
```

- à activer avant toute chose sur l'interface connectée du switch

# Sous interfaces

- Pour effectuer le routage interVLAN, il est nécessaire de disposer d'une adresse IP sur chaque VLAN
  - hors, avec un ROAS, seule une interface réelle est connectée en mode trunk
  - les sous-interfaces vont donc permettre, sur une même interface trunk, de créer virtuellement une interface par VLANs
    - Autant d'interface logique qu'il existe de VLAN à router
- Exemple

```
(config)# interface FastEthernet 0/0.1
(config-subif)#

```

- sur chaque sous-interface
  - activation du 802.1Q
  - association à un VLAN
  - configuration IP (adresse et masque)
- Exemple
  - association de la sous-interface FastEthernet 0/0.1 au VLAN 1

```
(config)# interface FastEthernet 0/0.1
(config-subif)# encapsulation dot1Q 1
(config-subif)# ip address 192.168.1.254 255.255.255.0

```

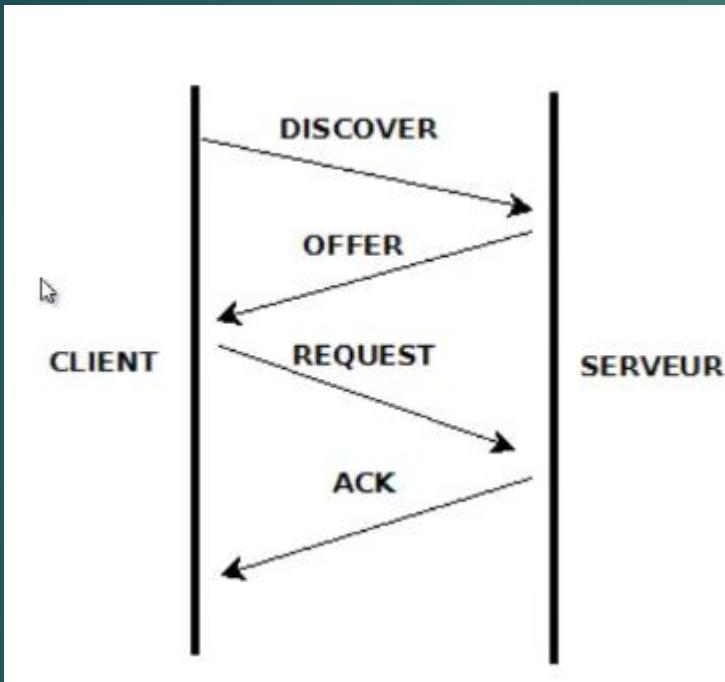
# DHCP : Dynamic Host Configuration Protocol

- ▶ Octobre 1993 : première définition (RFC 1531)
  - Comme extension de BOOTP (bootstrap Protocol)
    - Couvre l'ensemble des configurations IP
      - ✓ Adresse IP, masque, passerelle par défaut
      - ✓ Adresses de serveurs de noms (DNS et NBNS (WINS))
- ▶ Modifie et complète par la [RFC 2131](#) (Mars 1997) : référence ipv4 actuelle
- ▶ Adapte à l'ipv6 depuis juillet 2003 ([RFC 3315](#))
- ▶ DHCP DISCOVER
  - Broadcast (255.255.255.255)
  - Port 67
- ▶ DHCP OFFER
  - Réponse du serveur ayant reçu la requête
    - Proposant une adresse IP et un masque
    - Et indiquant l'adresse IP du serveur
  - Port 68
- ▶ DHCP REQUEST
  - Demande d'assignation de l'adresse proposée
    - Et l'envoie des valeurs des paramètres
- ▶ DHCP ACK : accuse de réception, assigne l'adresse ip pour une durée définie
  - Ainsi que d'autres paramètres éventuels (passerelle par défaut, UNIS, WINS)

# DHCP

## ► Agent relais DHCP

- Les datagrammes DHCP sont limités à un domaine de broadcast
  - Nécessite donc des serveurs DHCP ou des serveurs relais sur chaque segment
  - Transforme les requêtes multicast en de l'unicast
- Défini par la [RFC 1542](#)



```
(config-if)# ip address dhcp
```

# IOS DHCP Server : mise en place

149

Cours de CCNP : Network  
Katakpe Kossi Kuma  
18 March  
2025

## ▶ IOS DHCP Server : paramètres

- création d'un pool d'adresses

```
(config)# ip dhcp pool pool-ID  
(dhcp-config)#
```

- pool-ID : chaîne de caractères identifiant le pool d'adresses

↳

- définition du sous-réseau supporté

```
(dhcp-config)# network 192.168.2.0 255.255.255.0
```

- définition de la durée de bail

```
(dhcp-config)# lease days hours minutes
```

- définition du/des routeur(s) par défaut

```
(dhcp-config)# default-router adresse1 adresse2 ...
```

- adresses du/des serveur(s) DNS

```
(dhcp-config)# dns-server adresse1 adresse2 ...
```

- nom de domaine DNS

```
(dhcp-config)# domain-name name
```

# Commandes d'information

150

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
18 March  
2025

- informations d'état de chacun des baux alloués

```
# show ip dhcp binding
```

- statistiques et intervalles d'adresse d'un pool d'adresses

```
# show ip dhcp pool [poolname]
```

- statistiques du serveur DHCP

```
# show ip dhcp server statistics
```

- afficher les conflits

```
# show ip dhcp conflict
```

# Les ACLs

# Introduction

152

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
18 March  
2025

- ▶ Filtrer les accès
  - Aux réseaux
  - Au routeur lui-même
- ▶ Relativement à :
  - Adresse IP
    - Source
    - Destination
  - Protocole
  - Numéro de port
- ▶ Sur un trafic entrant ou sortant
- ▶ Analysées de manière séquentielle
  - L'ordre des ACLs est donc important
  - Du plus précis au plus générique
- ▶ Tout trafic est interdit par défaut.

- uniquement sur les adresses IP source

```
(config)# access-list number {permit|deny} {host|source source-wildcard|any}
```

- number : entre 1 et 99 ou 1300 et 1999

- Exemple

- interdire l'accès seulement à tout les membres du réseau 192.168.1.0/24 ainsi qu'à l'hôte 192.168.2.10

```
(config)# access-list 1 deny 192.168.1.0 0.0.0.255
```

```
(config)# access-list 1 deny host 192.168.2.10
```

```
(config)# access-list 1 permit any
```

# Les ACLs étendues

- sur les adresses IP source, de destination, le protocole ou le numéro de port

```
(config)# access-list number {deny|permit} protocole source masque-source
[opérateur [port]] destination masque-destination
[opérateur [port [established]][log]
```

- opérateurs :
  - eq : égal à
  - neq : différent de
  - gt : plus grand que
  - lt : plus petit que
- number : entre 100 et 199 ou 2000 et 2699

# Exemples

- interdire tout paquet IP à destination de l'hôte 192.168.2.10

```
(config)# access-list 101 deny ip any host 192.168.2.10
```

- interdire tout segment TCP de port source supérieur à 1023 et à destination du port 23 de l'hôte 192.168.2.10

```
(config)# access-list 101 deny tcp any gt 1023 host 192.168.2.10 eq 23
```

- interdire tout segment TCP à destination du port 80 et en provenance du réseau 192.168.10.0/24

```
(config)# access-list 101 deny tcp 192.168.10.0 0.0.0.255 any eq http
```

- Il est possible de définir une description d'ACL pour plus de clarté

```
(config)# access-list 101 remark Description de l'ACL
```

# ACLs nommées

- Les ACLs numérotées sont complexe à administrer dès que leur nombre devient important et qu'elles deviennent complexes
  - il est impossible de les modifier
  - la seule solution étant de la supprimer et de la réécrire
- Une ACL nommée est en revanche modifiable

```
(config)# ip access-list extended nom
(config-ext-nacl)# {deny|permit} protocole source masque-source ...
```

- pour ajouter une règle, il suffit d'utiliser la syntaxe des ACLs étendues numérotées, sans "access-list number"
  - et d'utiliser la commande "no" pour la supprimer

# Appliquer une ACL à une interface

157

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
18 March  
2025

```
(config-if)# ip access-group {number|name} {in|out}
```

- utiliser la commande "no" pour désactiver l'ACL sur l'interface
- afficher une ACL

```
# show access-lists [number|name]
```

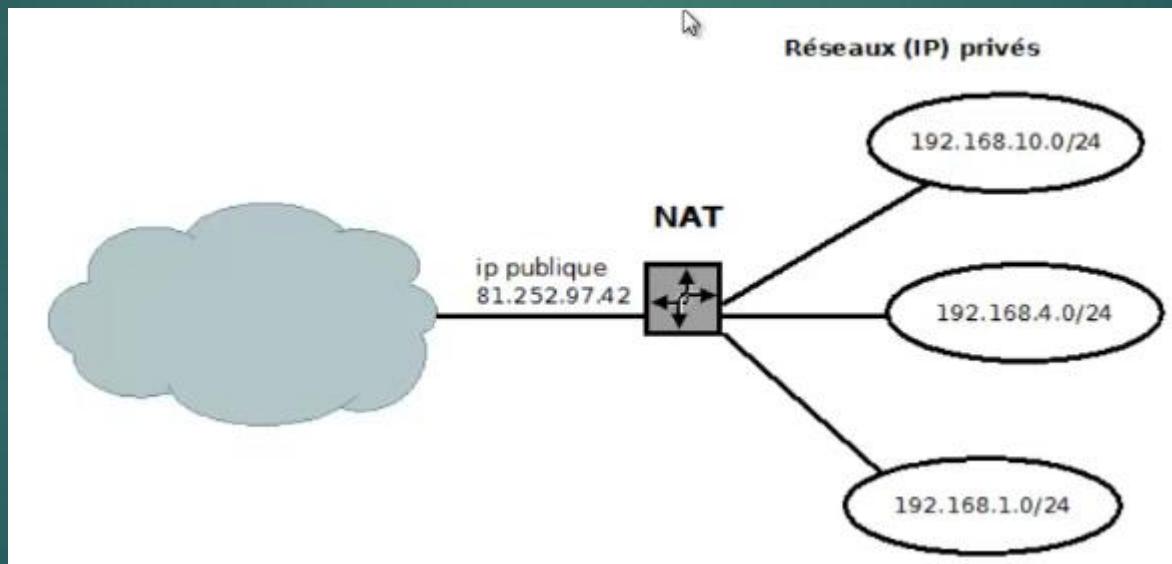
- afficher la configuration d'une interface

```
# show run interface FastEthernet 0/0
```

# NAT

# Introduction

- ▶ Traduction d'adresse IP (Network Address Translation)
  - Faire correspondre une adresse publique unique pour un réseau privé
  - Le nombre d'adresses publiques étant limite
    - Démarche de demande de bloc d'IP au RIPE NCC via OVH
- ▶ RFC 1631 – mai 1994



# Types de Nating

- ▶ Statique
  - Faire correspondre une adresse publique à une adresse privée
- ▶ Dynamique
  - Cree dynamiquement les translations dans un pool d'adresses publiques
- ▶ PAT
  - Translation basée sur les ports TCP/UDP
- ▶ Réseau Prive/publique
  - Première étape de tout type de nating
    - Le NAT ne prenant effet que quand un paquet est route de "l'intérieur" vers "l'extérieur", ou inversement
    - Il est donc nécessaire de définir cet "intérieur" et cet "extérieur"
  - Par interface

```
(config-if)# ip nat {inside|outside}
```

# NAT statique

- Faire correspondre une adresse publique à une adresse privée

```
(config)# ip nat inside source static 192.168.1.10 201.55.4.8
```

## ► NAT dynamique

- Les adresses publiques sont automatiquement choisies dans un pool d'adresses

- création du pool d'adresses

```
(config)# ip nat pool POOL-NAT-LAN1 201.55.4.1 201.49.10.10 netmask 255.255.255.240
```

- création de l'ACL

```
(config)# access-list 1 deny 192.168.1.10
(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

- activation du NAT

```
(config)# ip nat inside source list 1 pool POOL-NAT-LAN1
```

# NAT dynamique PAT

- ▶ Nécessaire si le nombre d'adresses publique est plus faible que celui d'adresses privées
  - Translation du port source, afin d'identifier le client
- ▶ Ajouter seulement "Over Load" à la configuration précédente.
- ▶ NAT dynamique PAT pour adresse publique unique
  - Configuration la plus courante sur les réseaux de plus petite dimension
    - Une seule adresse IP fixe sur internet par exemple
  - Définir un pool d'adresse n'est donc plus adapté
    - Il suffira alors de se baser sur l'adresse de l'interface " outside "

```
(config)# ip nat inside source list 1 pool POOL-NAT-LAN1 overload
```

```
(config)#ip nat inside source list 1 interface serial 0/0 overload
```

# Commandes d'informations

163

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
18 March  
2025  
Présenté par

- Afficher la table de translations
  - translations effectuées en accord avec les règles établies

```
# show ip nat translations
```

- Vérifier l'adresse des paquets reçus sur un routeur

```
# debug ip paquet
```

- ▶ Service IP: le Protocole NTP (Network time Protocol)
  - ▶ Synchronisation des horloges sur le réseau
  - ▶ Présenter pour la première fois en septembre 1985
    - ▶ RFC 958
  - ▶ Dernière version : NTPv4
    - ▶ RFC 5905 – juin 2010
  - ▶ Indispensable pour une bonne lecture des logs
    - ▶ Et donc un trouble shooting simple

# NTP

- nécessite de spécifier un serveur NTP
  - ainsi qu'une version du protocole

```
(config)# ntp server 172.16.2.2 version 4
```

- Vérifier si l'horloge est synchronisée

```
# show ntp status
```

- Vérifier l'association à un serveur de temps

```
# show ntp associations
```