Chapitre 1: introduction

Réseau=ensemble d'équipements permettant l'envoie d'informations d'un émetteur à un ou n récepteurs.
L'administrateur doit notamment s'occuper des :

- Ordinateurs, utilisateurs et des périphériques
- performances des systèmes.
- La gestion des fichiers et des disques.
- Réseau et sécurité.

Les différentes tailles

- PAN (Personal Area Network)
- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)

Les différentes technologies de transmission = *La diffusion* et *Le point-à-point*

Les différentes topologies

1. La topologie physique **:** Arrangement spatial d'un réseau.
   - **Réseaux de diffusion** : Bus, Anneau
   - **Réseaux en mode point-à-point :** point-à-point, Etoile, maillée
2. La topologie logique : Manière de partage du support, IP et ports
3. Ethernet : Topologie de type bus linéaire Communication à l'aide du protocole CSMA/CD
4. Token Ring : Accès par jeton
5. FDDI : constitué de deux anneaux: le secondaire rattrape les erreurs du 1er

Mode de fonctionnement des réseaux
Périphériques connectés = périphériques finaux. Peuvent envoyer et recevoir un message sur le réseau et peuvent jouer le rôle de client, de serveur ou les deux.

- Les serveurs fournissent des informations
- Les clients demandent des informations et les affichent

On utilise un modèle client-serveur avec serveur passif qui répond aux demandes des clients ou le modèle P2P qui permet à un ordinateur d'être client et serveur
Avantages du P2P

- Facile à configurer
- Coût faible
- Pratique pour les petits réseaux

Désavantages du P2P

- Pas d'administration centralisée
- Peu sécurisé
- Non évolutif

Internet : Ensemble mondial de réseaux interconnectés qui échange des informations régi par des normes.
Intranet : Réseau LAN privé d'entreprise auquel peuvent accéder uniquement des gens autorisés.
Extranet : Utilisé lorsqu'une entreprise fournit un accès sécurisé aux personnes qui travaillent pour d'autres entreprises, mais qui ont besoin de données de l'entreprise en question.

Manières d'accéder à Internet

- Par câble : connexion haut débit.
- Par xDSL : Fonctionne sur une ligne téléphonique, divisée en trois (Tel, download et uplaod)
- ADSL : Exploite une autre bande fréquence, au-dessus de celle du téléphone
- VDSL : Permet d'atteindre un meilleur débit que les précédents
- VDSL 2 : Encore plus que le premier
- Par fibre : Plus est proche de l'utilisateur, plus la qualité sera meilleure. Derniers mètres en cuivre
- Par satellite : Idéal pour ceux sans accès DSL ou câble. Débits et frais d'installation élevés.
- Par cellulaire : performances limitées selon le téléphone et la station de base

Le WiMax (Worldwide Interoperabilityfor Microwave Access)
Technologie de transmission haut débit par ondes radio pour couvrir des zones importantes
Débit dépend de la distance, de la topographie des lieux et du nombre d'utilisateur

La segmentation et le multiplexage
La segmentation consiste à découper les données à envoyer en parties moins importantes
Le multiplexage consiste entremêler plusieurs conversations segmentées.

Le seul inconvénient est que ces techniques rendent les communications plus complexes car il va falloir étiqueter toutes les parties afin de les réassembler quand elles seront arrivées à destination.

L'architecture d'un réseau
Il y a 4 caractéristiques à prendre en compte:
- La tolérance aux pannes => redondance
- L'évolutivité => Utilisation d'un modèle hiérarchisé à plusieurs couches
- La qualité de service => Utilisation de niveaux de priorités
- La sécurité

BYOD (BringYourOwnDevice)
Consiste à offrir aux users la possibilité d'utiliser leurs propres device pour accéder aux réseau.

La virtualisation
Consiste à faire fonctionner plusieurs systèmes, serveurs ou applications sur le même serveur physique.
Moins coûteux, portabilité, administration simplifiée mais pannes généralisées et coût de mise en œuvre important.
- Hyperviseur type 1

Outil qui s'interpose entre la couche matérielle et logicielle.
Il a accès aux composants de la machine et possède son propre noyau.
- Hyperviseur type 2

Application installée sur un système d'exploitation.
Les performances sont réduites mais propose une parfaite étanchéité entre les systèmes.

Le cloud computing
Permet de stocker ou recevoir des fichiers sur des serveurs via Internet.
- Cloud personnalisé: Conçus pour répondre aux besoins d'un secteur spécifique
- Cloud public: Cloud dont les services et app. sont accessibles par tous. gratuits ou payant.
- Cloud privé: Cloud dont les services et app. destinés à une entreprise ou à une entité spécifique
- Cloud hybride: Cloud qui comporte au moins deux cloud.

Avantages
- Accès à tout moment via Internet
- Coûts d'infrastructure réduits,
- Permet de réagir rapidement aux besoins des clients

Le CPL (Courant Porteur de Ligne)
Permet la construction d'un réseau informatique sur le réseau électrique d'une habitation

Le Big Data
Solution pour permettre à tout le monde d'accéder en temps réel à des bases de données géantes

Règle des 3V:
- Volume des données considérables à traiter,
- Variété d'informations,
- Vélocité à atteindre = Fréquence de création, collecte et partage

Chapitre 2: Communication et protocoles réseaux

Protocole
Un protocole est une suite de règles qui veillent à ce qu'un message soit correctement transmis et compris.

Codage d'un message
Un message est d'abord codé en bits qui sont ensuite codé en impulsions électriques ou en ondes lumineuses selon le support

L'encapsulation et la désencapsulation

L'encapsulation est un processus permettant d'encapsuler un message dans un format spécifique appelé "trame", Avant d'être transmis sur le réseau.

Cette trame contiendra l'adresse source, l'adresse de destination ainsi que les données encapsulées (MAC)
La désencapsulation c'est l'inverse.

Taille des messages
Lorsqu'un message est trop long, il doit être segmenté en plusieurs trames

Synchronisation des messages
- Méthode d'accès (moment de la prise de parole)
- Contrôle de flux (débit de parole)
- Délai d'attente de la réponse => réagit en cas de non réponse

Option de remise des messages
- Monodiffusion => un émetteur, un récepteur
- Diffusion => un émetteur à tous les récepteurs
- Multidiffusion => un émetteur à un groupe de récepteurs

Protocole propriétaire
Cela signifie qu'une société ou qu'un fournisseur contrôle la définition du protocole et la manière dont il fonctionne

Acronymes des protocoles à connaître
Protocoles de la couche application :
- DNS : A pour rôle de traduire les noms de domaines en adresse IP
- DHCP : Attribue dynamiquement des adresses IP aux stations clientes au démarrage
- SMTP : Permet aux terminaux d'envoyer un mail à un serveur de messagerie
- POP : Permet aux clients de récupérer ou de télécharger des emails d'un serveur de messagerie
- IMAP : Permet aux clients d'accéder aux emails stockés sur un serveur de messagerie
- FTP : Permet à un hôte d'accéder et transférer des fichiers sur un autre hôte du réseau
- TFTP : Version simplifiée de FTP, pas d'authentification
- HTTP : Permet d'échanger du texte ou des fichiers multimédia sur le web

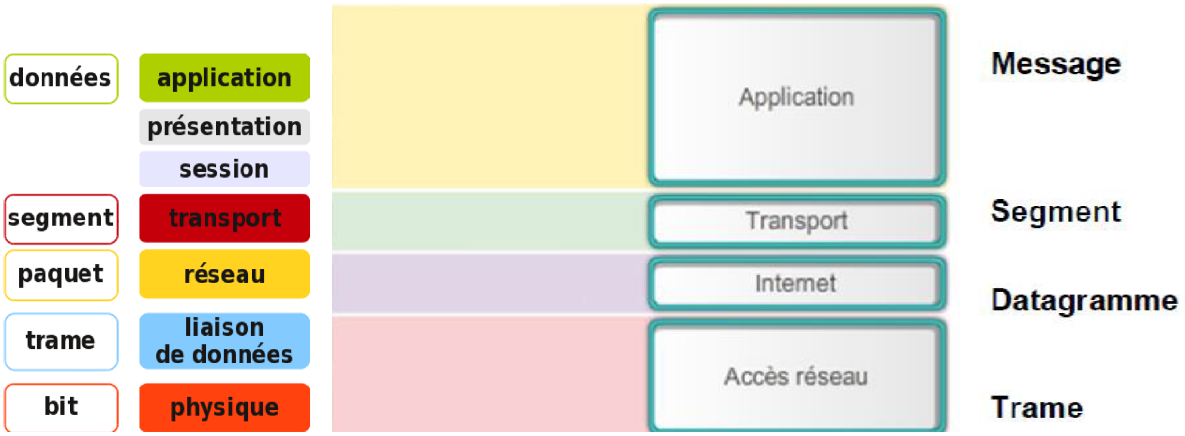
Protocoles de la couche transport :
- UDP : Permet d'envoyer des paquets sans confirmation de la transmission de datagrammes
- TCP : Au contraire d'UDP, permet une connexion fiable entre les processus des hôtes distincts

Protocoles de la couche internet :
- IP : Permet de recevoir des segments de message de la couche transport. Regroupe les messages en paquets et permet leur acheminement de bout en bout sur un interréseau
- NAT : Permet de convertir les adresses IP d'un réseau privé en adresses IP globales et publiques
- ICMP : Permet à l'hôte de destination de signaler à la source les erreurs de transmissions
- OSPF : Protocole de routage à états de liens permettant de faire du routage dynamique
- EIGR : Protocole de routage dynamique propriétaire à Cisco
- Protocoles de la couche réseau :
- ARP : Fournit un mappage dynamique entre une adresse logique (IP) et une physique (MAC)
- PPP : Permet d'encapsuler des paquets pour les transmettre via une connexion en série

Acronymes des sociétés
- Internet Society (ISOC) qui est chargée de promouvoir le développement, l'évolution et l'utilisation ouverte d'Internet dans le monde entier
- Internet Architecture Board (IAB) qui s'occupe de la gestion et du développement général des normes sur Internet
- Internet Engineering Task Force (IETF) qui a pour but de développer, de mettre à jour et d'assurer la maintenance d'Internet et des technologies T compose de différents groupes de travail qui constituent les principales entités de développement des spécifications et des recommandations de
- Internet ResearchTask Force (IRTF) qui se concentre sur la recherche à long terme liée à Internet, aux protocoles TCP/IP, aux applications, aux l'architecture
- L'Institute of Electronical and Electronics Engineers (IEEE) qui est une association américaine professionnelle s'adressant aux spécialistes du gén l'électronique qui souhaite se consacrer à l'innovation

- L'EIA (Electronic Industries Alliance) connue pour ses normes associées au câblage électrique, aux connecteurs et aux racks de 19 pouces utilisé l'équipement réseau.
- La TIA (TelecommunicationsIndustry Association) est responsable du développement des normes de communication dans un grand nombre de d
- L'ITU-T (secteur de la normalisation des télécommunications de l'Union Internationale des Télécommunications) définit des normes de compressi
- L'ICANN (Internet Corporation for AssignedNames and Numbers) est une association a but non lucratif basée aux états unis qui coordonne l'attri la gestion des noms de domaine utilisés par le protocole DNS et les identificateurs de protocole ou numéro de ports utilisés par les protocoles TC
- L'IANA (Internet AssignedNumbersAuthority) est une composante de l'ICANN chargée de superviser et de gérer l'affection des adresses IP, la ge domaines et les identificateurs pour le compte de l'ICANN.

OSI/TCP IP :



Adresse réseau et adresse liaison de données
Dans un paquet IP, on retrouve deux adresses logiques: l'IP source et l'IP destination
Dans une trame de liaison de données on retrouve deux adresses physiques: l'adresse MAC source et l'adresse MAC destination

Les adresses MAC sont formées de 48 bits et sont physiquement intégrées à la carte réseau.

Afin de déterminer l'adresse MAC d'un autre périphérique, on va utiliser le protocole ARP qui permet de déterminer l'adresse MAC d'une station à partir de son adresse IP en effectuant une diffusion.

Chapitre 3: Accès réseau

Les ≠ méthodes de codage

- Le codage NRZ (Non Return To Zero)

Le flux de bits est transmis en tant que série de valeurs de tension (0=bas et 1=haut)
Utilisé entre un ordinateur et ses périphériques.
Facile à mettre en œuvre mais une seule erreur et plus rien ne va.

- Le codage Manchester

Représente les valeurs binaires comme des transitions de tension. Codage synchrone. (0=bas vers le haut et 1= haut vers le bas mais ça peut être l'inverse aussi)
Utilisé pour les liaisons radio à courte distance, station météo domestique etc.
Mise en œuvre simple mais la limite haute de la bande passante occupée est doublée.

Les ≠ types de transmissions (signalisation)

- Asynchrone

L'intervalle de temps entre les caractères ou les blocs de donnés peut être défini arbitrairement
--> Les trames doivent contenir des indicateurs de début et de fin.

- Synchrone

Les signaux de données sont envoyés synchronisé. Cela se fait à l'aide d'un signal d'horloge échangé entre les deux périphériques qui doivent communiquer.

Les ≠ types de supports physiques

1. Support de cuivre

Plus souvent utilisé car bon marché, facile à installer et présente une faible résistance au courant électrique. Limités par la distance et les interférences du signal.
Risque:

- Interférences électromagnétiques ou radioélectriques => blindage, mise à la terre
- Diaphonie => torsadé les paires de fils
- Catégorie 1 et 2 : correspondent à des types de câblages abandonnés.
- Catégorie 3 : bande passante de 16 MHz. en cours d'abandon
- Catégorie 4 : 20 MHz. fut principalement utilisé pour les réseaux Mbps ou les réseaux 10BASE-T.
- Catégorie 5 : 100 MHz. Permet du 100BASE-TX et du 1000BASE-T, téléphonie ou Token Ring
- Catégorie 5e : adaptation de la catégorie 5. vitesse allant jusqu'à 1 000 Mbits/s et une ban MHz.
- Catégorie 6 : 250 MHz.
- Catégorie 7 : 1 GHz et permet un débit allant jusqu'à 10 Gbit/s !

2. Câbles coaxiaux

Composé d'un conducteur de cuivre entouré d'une couche de matériau isolant flexible.
Sur ce matériau isolant, il y une torsade de cuivre ou une feuille métallique. La gaine enveloppe le tout.

Fibre optique

Il s'agit d'un fil en verre très pur, transparent, flexible et très fin. Les bits y sont codés sous forme d'impulsions lumineuses, le câble sert de guide d'ondes qui transmet de la lumière entre les deux extrémités Avec un minimum de perte de signal.

Elle peut fonctionner à des longueurs bien supérieures aux supports en cuivre sans régénération de signaux.
Désavantages: coût élevé, matériel différent, manipulation délicate.

Domaine d'application: réseaux d'entreprise, FTTH, réseaux longue distance, réseaux sous-marins
Composition: cœur => enveloppe => gaine intermédiaire => renforcement => gaine générale

Il en existe deux types:

- Monomode: Transporte un seul rayon lumineux émis par un laser, peut aller jusqu'à 100km, cœur de petit diamètre (8 à 10 microns), moins de dispersion
- Multimode: Transporte plusieurs rayon lumineux incohérents, la lumière émises des DEL entre selon différents angles, cœur + large (50 à 62,5 microns) +-

❖ Le connecteur ST (« Straight Tip ») est un connecteur à baïonnette très largement utilisé avec de la fibre optique multimode.
❖ Le connecteur SC (« Suscriber Connector ») est un connecteur utilisant un mécanisme de pousser-tirer, garantissant l'insertion dans le bon sens et largement utilisé avec de la fibre optique monomode.
❖ Le connecteur LC (« Lucent Connector ») est un petit connecteur utilisé avec de la fibre optique monomode et multimode (bidirectionnelle ou non).

Faire /!\ à l'alignement, l'écart à l'extrémité, finition de l'extrémité

Support sans fils

Utilisent les fréquences radio ou micro-ondes
On retrouve 3 normes courantes:

- IEEE 802.11: WLAN = Wi-Fi, utilise le CSMA/CA
- IEEE 802.15: WPAN = Bluetooth, utilise un processus de jumelage
- IEEE 802.16: WiMax accès à large bande sans-fil à l'aide d'une topologie point-à-multipoints
    - (802.1 = Réseaux locaux)
    - Dans le futur, le Li-Fi: peut atteindre 45mbit/s

Comment déterminer le type d'un câble

Shielded -> Blindage composé de tresses métalliques
Foiled => Blindage grâce à une feuille de métal (écran)

Si S/ devant => Tresses métalliques entourent le tout
Sinon => Tresses métalliques entourent chaque paire

La composition d'une trame

- Un en-tête
  - Indicateur de début de trame
    - Adresses
    - Type
    - Contrôle de flux
- Fin de trame
  - Détection d'erreur
    - Indicateur de fin de trame

Méthodes d'accès

- *Aloha*

Réseau hertzien qui a pour but de relier ses entités composé de:

- 1 station centrale (SC) + station secondaire (SS)
- 2 fréquences radio: une pour la diffusion SC -> SS et l'autre pour l'accès multiple SS -> SC

Lorsque SC veut transmettre une info, elle l'envoie et attend un ACK, s'il y a une collision il n'y a pas d'ACK donc les stations réémettent l'information après un délai d'attente aléatoire

- *CSMA (Carrier Sense Multiple Access)*

Amélioration de l'Aloha pour les réseaux câblés.
En l'absence d'informations à transmettre, la station écoute afin de recevoir les paquets qui circulent sur le media dans les deux sens. Quand la station a besoin d'émettre, elle vérifie que rien ne soit émis sur le media

- Si c'est le cas, elle commence à émettre
- Sinon elle attend la fin de la transmission en cours avant d'émettre

/!\ Ne supprime pas complètement les collisions

- *CSMA/CD (Collision Detection)*

Amélioration du CSMA grâce à la détection de collision.
Une station prête à émettre transmet et continue à écouter le canal. S'il y a une collision, elle interrompt sa transmission et envoie des signaux spéciaux "bits de bourrage" afin que Toutes les stations présentes sur le réseau soit prévenus de la collision.

Elle retentera une émission ultérieurement (après un délai aléatoire)

- *CSMA/CA (Collision Avoidance)*

Le périphérique examine le support pour établir si celui-ci comporte un signal.
Si le support est libre, le périphérique envoie une notif pour dire qu'il va transmettre ensuite il transmet ses données

- *La trame 802.11*

La norme IEEE 802.11 (communément appelée Wi-Fi) utilise une méthode d'accès au support de type CSMA/CA.
Les réseaux 802.11 utilisent également les accusés de réception de liaison de données pour confirmer la bonne réception d'une trame. Si la station de travail d'envoi ne détecte pas la trame d'accusé de réception, la trame est retransmise.

Chapitre 4: Ethernet

Ethernet

Il s'agit de la technologie réseau local prédominante dans le monde

- Fonctionne au niveau de la couche liaison de donnée et de la couche physique
- Définie par les normes 802.2 et 802.3 de IEEE

Et prend en charge des bandes passantes de données de 10 Mbit/s, 100 Mbit/s, 1 Gbit/s (1 000 Mbit/s) ou 10 Gbit/s (10 000 Mbit/s).

La couche liaison de donnée

Séparée en deux parties

- Sous-couche LLC Ethernet (LLC = fait le lien entre la couche 3 et la couche MAC)

Gère la communication entre les couches supérieures et inférieures.

- Sous-couche MAC Ethernet

Elle encapsule les données et contrôle l'accès au support

Adresse MAC
Valeur binaire de 48 bits constituée de 12 chiffres hexadécimaux. Sont regroupés par 2 et séparés par ":" ou "-"
Elles sont uniques au monde.

Les 24 premiers octets sont la partie OUI qui est l'identifiant du constructeur (les autres c'est la partie NIC)
Elle est au départ stockée dans la mémoire morte et lorsque l'ordinateur démarre, elle est copiée dans la mémoire vive

Norme de taille d'une trame
Une trame doit avoir une taille minimale de 64 octets et maximale de 1522 octets, si elle fait plus (ou moins) elle est considérée comme un fragment de collision et est rejetée

Les types d'adresses MAC
- Monodiffusion

Adresse utilisée lorsqu'une trame est envoyée à partir d'un seul périphérique émetteur à un seul destinataire
- Diffusion

Ne comporte que des "F", tous les hôtes sur le réseau local recevront le paquet et le traiteront
- Multidiffusion

Commence par 01-00-5E, permet à un périphérique source d'envoyer un paquet à un groupe de périphériques

Protocole ARP
Il sert à récupérer l'adresse MAC d'un ordinateur à partir de son adresse IP.
Il met à jour une table ARP soit de manière statique ou de manière dynamique.
Il existe deux façons de le faire en dynamique:

I. Quand un nœud reçoit des trames en provenance d'un support, il enregistre les IP et MAC source dans sa table ARP
II. Le périphérique envoie une requête ARP à tous les périphériques du réseau local, la requête contient l'IP destination et une adresse mac de diffusion. Le périphérique concerné répond à la requête ARP en envoyant une trame de monodiff. contenant son adresse MAC

Les entrées de la table MAC, obtenues dynamiquement sont HORODATÉES, si cet horodatage expire, le périphérique est supprimé de la table ARP

Le concentrateur (HUB)
Matériel réseau le plus basique. Il utilise la première couche du modèle OSI et possède un certains nombres de ports (4, 8, 16 ou 32)
Il peut récupérer le signal arrivant sur un port, de le ré amplifier et de le diffuser.
Tout ce qui est lié (périph. finaux) à un HUB est considéré comme UN SEUL domaine de collision.

Le commutateur (SWITCH)
Dispositif permettant de relier des réseaux travaillant avec le même protocole. Il travaille sur les deux premières couches du modèle OSI.
Il analyse les trames arrivantes et filtres (par adresse MAC) les données afin de les aiguiller vers les ports adéquats en fonction de sa table de commutation

La table de commutation
Elle fait correspondre les adresses MAC de destination aux ports utilisés pour la connexion aux nœuds.
Pour chaque trame entrante, l'adresse MAC de destination dans son en-tête est comparée à la liste d'adresses.
Lorsqu'un port répertorié dans la table est mappé à une adresse MAC, il est utilisé comme port de sortie de la trame.

- L'apprentissage: Chaque fois qu'une trame entre dans le switch, celui-ci examine son adresse MAC source et l'ajoute dans sa table MAC si elle n'y est pas
- L'horodatage: Les entrées de la table de commutation acquises à l'aide de l'apprentissage sont horodatées. Une fois le compte à rebours à 0, l'entrée est supprimée
- L'inondation : Quand un commutateur ne sait pas sur quel port envoyer une trame, il fait une diffusion à l'exception du port d'arrivée. L'hôte possédant l'adresse correspondante va traiter la trame et lui répondre afin que le switch mette à jour sa table MAC

- Le réacheminement sélectif : Si une trame possède une adresse MAC source connue, le switch va acheminer la trame au port correspondant
- Le filtrage : Abandon de la transmission d'une trame lorsqu'elle est endommagée. Aussi, une trame n'est jamais envoyée à son port d'arrivée

Domaine de collisions et de diffusions

- Domaine de collision : Région du réseau au sein de laquelle les hôtes partagent l'accès au média (chaque câble sauf pour le hub c'est tout ce qu'il contient en 1 domaine)
- Domaine de diffusion : Zone logique où un ordinateur connecté au réseau peut transmettre à tous les autres ordinateurs du même domaine (chaque partie partant d'un routeur)

La fonction auto-MDIX

Lorsque vous activez cette fonction, le commutateur détecte le type de câble requis pour les connexions Ethernet cuivre, puis configure les interfaces avec les bons câbles.

Méthodes de transmission de trames

- Store and Forward

Lorsqu'un switch reçoit une trame, il stocke les données dans des mémoires tampons jusqu'à ce qu'il ait tout reçu, pendant ce temps il recherche dans la trame, des informations sur sa destination et procède à un contrôle d'erreur

- Cut-through

Le switch agit sur les données au fur et à mesure qu'il les reçoit, même si la transmission n'est pas finie. Il met une quantité suffisante en mémoire tampon afin de lire l'adresse MAC de destination et déterminer ainsi le port où il faut transmettre les données. Il n'y a pas de contrôle d'erreur donc plus rapide
Il en existe deux variantes:

  - Fast-Forward : Offre le niveau de latence le plus faible. Transmet un paquet immédiatement après la lecture de l'adresse de destination. Comme il envoie avant d'avoir tout reçu, les trames peuvent comporter des erreurs.
  - Fragment-Free : Le commutateur stocke les 64 premiers octets (car c'est là qu'il y a le plus souvent des erreurs) avant la transmission.

Mise en mémoire tampon

- Axée sur les ports

Les trames sont stockées dans des files d'attentes liées à des ports entrants et sortants. Une trame est transmise au port sortant uniquement si toutes les trames qui la précèdent dans la file d'attente ont correctement été transmises.

- Partagée

Le commutateur stocke toutes les trames dans une mémoire tampon commune à tous les ports du commutateur. La capacité est allouée dynamiquement. Les trames de la mémoire sont liées de manière dynamique au port de destination, ce qui permet de recevoir la trame sur un port et de la transmettre sans file d'attente.

Chapitre 5: Système d'exploitation de réseau

DLNA (Digital Living Network Alliance) est une alliance de plus de 250 fabricants d'appareils électroniques, informatiques, etc.

Périphériques intermédiaires

- Routeur => transfère les paquets de données vers Internet et reçoit des paquets depuis Internet
- Switch => Connecte des périphériques finaux à l'aide de câbles réseau
- Point d'accès sans fil => émetteur radio capable de connecter des périph. Finaux sans fil
- Pare-feu => Sécurise le trafic sortant et contrôle le trafic entrant

Cisco IOS (Internetwork Operating System)

Terme générique utilisé pour désigner l'ensemble des systèmes d'exploitation réseau utilisés sur les périphériques Cisco.
Lorsqu'un ordinateur est mis sous tensions, il charge le système dans la mémoire vive (RAM). La partie du code du système d'exploitation directement liée au matériel informatique s'appelle le noyau. La partie liée aux applications et à l'utilisateur s'appelle l'interpréteur de commande. (CLI)

Il est stocké dans la mémoire Flash (mémoire non volatile, ne se reset pas au reboot)

Accéder au CLI (Console-Line interface) :
- Via le port console (CTY)
- Via Telnet ou SSH (VTY)
- Via le port AUX (ligne téléphonique commutée)

Telnet et SSH permettent un accès distant, SSH est plus sécurisé

Modes d'exploitation Cisco IOS dans l'ordre croissant
- Mode d'exécution utilisateur (visualisation)
- Mode d'exécution privilégié (visualisation détaillée et accès à la configuration du périphérique)
- Mode de configuration globale (commandes de configuration globale sur l'équipement)
- Modes de configuration spécifiques (commandes de configuration d'un service ou d'une interface)

Chapitre 6: Couche réseau

La couche réseau
Elle fournit des services permettant aux périphériques finaux d'échanger des données sur le réseau.
Elle utilise pour cela, 4 processus de base:
- L'adressage

La couche réseau fournit un adressage qui permettra d'identifier de manière unique les périphériques sur le réseau afin d'acheminer des données
- L'encapsulation

Durant ce processus, la couche 3 reçoit l'unité de données de protocole de la couche 4 (segment ou datagramme) et ajoute un en-tête de co Pour créer l'unité de données de protocole de couche 3 (paquet)
- Le routage

Les paquets vont devoir traverser des périphériques intermédiaires connectant les réseaux (routeurs). Ils vont sélectionner les chemins afin de diriger les paquets vers leur destination. Chaque route empruntée par un paquet pour atteindre le périphérique suivant est appelée saut
- La désencapsulation

Si le paquet est bien adressé à l'hôte de destination, il va le décapsuler et l'unité de donnée de protocole couche 4 est transmise au service d

Les caractéristiques du protocole IP (Internet Protocol)
- Aucune connexion n'est établie avant l'envoi de paquets de données
- Acheminement non fiable: aucune surcharge n'est utilisée pour garantir la transmission des paquets
- Indépendant du support: fonctionne indépendamment du support transportant les données
- Il est qualifié de protocole "non fiable" car il ne sait pas gérer les paquets endommagés ou perdu
- Pas de champs requis pour la transmission fiable dans l'en-tête d'un paquet IP (- de surcharge)
- On ne sait pas si le destinataire est sur le réseau, si le paquet est bien arrivé et si le destinataire peut lire le paquet
- Le destinataire ne sait pas quand le paquet arrive

/!\ La taille maximale d'unité de données de protocole que chaque support peut transporter est déterminé au niveau de la couche de liaison de données et est transmise à la couche réseau. Donc la taille de création des paquets est déterminée.

Le protocole IPv4
Un paquet IPv4 comporte deux parties
- En-tête IP -> indique les caractéristiques du paquet
- Données utiles -> contient les infos. du segment de couche 4 et les données en elles-mêmes

Il possède un "Time To Live" qui contient une valeur pour limiter la durée de vie d'un paquet. Elle est indiquée en secondes mais généralement par sauts". Si cette valeur est dépassée, le routeur rejette le paquet et envoie un message de dépassement de délai ICMP à la source

Problèmes de l'IPv4
- Manque d'adresses IP => Il y en a 4 milliards mais ce n’est pas assez
- Croissance de la table de routage Internet => Ces routes IPv4 consomment beaucoup de mémoire et de ressources sur les routeurs Internes
- Manque de connectivité de bout en bout

Apparition de l'IPv6

Les problèmes de l'IPv4 ont conduit au développement de l'IPv6

- Espace d'adressage plus important (bcp + d'adresses IP, +- 67 milliards par cm^2 de surface terrestre)
- Traitement des paquets plus efficace => l'en-tête IPv6 a été simplifiée et comporte moins de champs
- Traduction d'adresses réseau non nécessaire => comme y'a beaucoup d'IP, plus besoin de NAT
- Sécurité intégrée => prend en charge les fonctions d'authentification et de confidentialité

Le routeur

Equipement intermédiaire opérant au niveau de la couche 3 du modèle OSI, il envoie et reçoit des paquets IP qui lui sont destinés. Chaque interface du routeur est un membre ou un hôte d'un réseau IP différent
/!\ Deux interfaces actives ne peuvent pas appartenir au même réseau. Ils nécessitent:

- Un OS
- Un processeur
- De la RAM => contient l'IOS, fichier de config, table de routage IP, Cache ARP, Mémoire tampon
- De la ROM => instructions de démarrage, le POST, une version limitée

La mémoire vive non volatile est utilisée par IOS comme stockage permanent pour le fichier startup-config
La mémoire Flash est une mémoire non volatile utilisée comme stockage permanent pour l'IOS et d'autres fichiers associés au système, il y est co. Flash vers la mémoire vive lors du démarrage
Etapes lors du démarrage:

- Exécution du POST et chargement du bootstrap (ROM)
- Localisation et chargement de l'IOS (Flash ou TFTP)
- Localisation et chargement du fichier de config initiale (NVRAM, TFTP ou Console)

Connexion et interfaces d'un routeur

Les connexions sur un routeur Cisco peuvent être regroupées en deux catégories:

- Ports de gestion: ports console et aux utilisés pour configurer, gérer et dépanner le routeur (pas de transfert de paquets)
- Interfaces de routeur: configurée via l'adressage IP pour transporter le trafic.

On peut y accéder avec le port console, Telnet ou SSH, le port AUX (comme le switch)

Le routage

Le rôle principal du routeur c'est d'effectuer la fonction de routage (Et oui, Jamy) c'est à dire de diriger les paquets entre les hôtes
Un hôte peut envoyer un paquet à:

- Lui (via 127.0.0.1 qui est une interface de bouclage)
- Un hôte local
- Un hôte distant => le routeur sera une "passerelle par défaut"

La passerelle par défaut, dans un réseau domestique, est souvent utilisée pour connecter un réseau local à internet.

La table de routage

Fichier de donnée stocké dans la mémoire vive qui contient des informations de route sur le réseau connecté ainsi que les entrées de réseaux dits périphérique a découvertes. Le routeur utilise ces infos pour trouver le meilleur chemin.
Les routes possèdent trois caractéristiques principales:

- Le réseau de destination
- Le tronçon suivant ou la passerelle permettant d'atteindre le réseau de destination
- La métrique associée au réseau de destination

Fonctionnement

- Le routeur lit l'adresse de destination dans l'en-tête IP et regarde dans sa table de routage s'il connait une route à cette adresse
- Il transfère le paquet au prochain routeur en fonction du tronçon suivant spécifié par cette route.

Un routeur peut être configuré pour posséder une route par défaut.
Il s'agit d'une route qui correspond à tous les réseaux de destination.
Dans les réseaux IPv4 l'adresse 0.0.0.0 avec le masque 0.0.0.0 est utilisée à cet effet.
La route par défaut est utilisée pour transférer les paquets pour lesquels aucune entrée ne figure dans la table de routage pour le réseau de destination.
Quand un routeur reçoit des infos sur des nouvelles routes ou des routes modifiées, il met à jour sa propre table de routage et transmet ces infos aux autres routeurs.
C'est donc du routage dynamique et l'inconvénient est que l'échange d'infos afin d'avoir les routes correctement à jour impose une surcharge de la… ?

Les protocoles de routage sont:

- RIP (Routing Information Protocol)

Chaque route est associée à une métrique (et nombre de sauts limité à 15)
Chaque routeur envoie à ses voisins ses infos de routage (toutes les 30 sec)
Il va calculer les meilleures routes et déduire sa table de routage selon la métrique calculée

- EIGRP (Enhanced Interior Gateway Routing Protocol) que pour Cisco

Calcule les métriques sur base d'une formule composée du délai, de la bande passante, de la fiabilité et de la charge.
Au niveau du réseau, chaque routeur envoie un paquet "Hello" à ses voisins toutes les 5sec afin de dire qu'il est actif et que ses routes sont ok
Au niveau de l'échange d'infos une mise à jour concernant une table de routage n'est envoyée que lorsque celle-ci est modifiée. Cette màj des routes modifiées et sera envoyée qu'aux routeurs concernés

- OSPF (Open Shortest Path First)

Permet d'avoir des routes de plus de 15 sauts
Utilise une métrique plus compliquée (prenant compte des débits)

Chapitre 7: Couche transport

Introduction

La couche transport est chargée de l'établissement d'une session de communication temporaire entre deux applications et de l'acheminement des paquets
La plupart de ses protocoles ont des fonctions essentielles communes:

- Segmentation et reconstitution => diviser un bloc de données en des sous-blocs plus petit et va les reconstituer à la réception
- Multiplexage de conversions => à l'aide du port de l'application ou du service, la couche transport va déterminer à qui les données se rapportent

Dans le cadre du TCP/IP la segmentation et la réorganisation peuvent être fait à l'aide des protocoles TCP et UDP

Objectifs de la couche transport

- Effectuer un suivi des communications individuelles entre les applications résidant sur les hôtes source et de destination
- Segmenter les données et gérer chaque bloc individuel
- Réassembler les segments en flux de données d'application
- Identifier les différentes applications en leur affectant un numéro de port

Fiabilité de la couche transport

Elle est basée sur 3 opérations de base:

- Effectuer le suivi des données transmises
- Accuser la réception des données
- Retransmettre toute donnée n'ayant pas fait l'objet d'un accusé de réception

Les protocoles TCP et UDP

1. TCP (Transmission Control Protocol)

Protocole de couche transport fiable et complet, garantit que toutes les données arrivent à destination.
Il segmente un message en partie numérotées à une destination, s'il ne reçoit pas d'accusé de réception, il renvoie tout en supposant que ça a échoué. En-tête TCP = 20 octets

2. UDP (User Datagram Protocol)

Protocole de couche transport très simple qui ne permet pas de garantir la fiabilité
Il fournit des fonctions de base permettant d'acheminer des segments entre les applications appropriées avec peu de surcharge. En-tête UDP = 8 octets
Donc TCP > UDP

Les numéros de port classé par l'IANA

- Ports réservés (0 à 1023) : Ils sont réservés à des services ou applications
- Ports inscrits (1024 à 49151) : Affecté à des processus ou applications d'utilisateurs
- Ports privés ou dynamiques (49152 à 65535) : Appelés port éphémères, affectés de façon dynamique à des applications clientes lors d'une connexion

Exemple de ports réservés:

- 69 TFTP
- 21 FTP

- 23 Telnet
- 80 HTTP
- 53 DNS

Etablissement d'une connexion TCP

1. Le client demande l'établissement d'une session client-serveur avec le serveur
   Envoi d'une demande de synchronisation avec numéro de séquence SEQ
2. Le serveur accuse réception de la session et demande l'établissement d'une session serveur-client.
   Réponse du serveur avec ACK égal au numéro d'ordre reçu +1 et son numéro d'ordre de synchronisation
3. Le client accuse réception de la session serveur-client
4. Connexion établie, le client répond avec un ACK égal au numéro d'ordre reçu + 1.

Fermeture d'une connexion TCP

1. Le client n'a plus rien à envoyer, il envoie un segment pour demander la fin de la connexion (FIN)
2. Le serveur envoie un ACK disant qu'il a bien reçu le segment FIN, afin de fermer la session client-serveur
3. Le serveur envoie un segment FIN au client pour mettre fin à la session serveur-client
4. Le client envoie un ACK pour dire qu'il a bien reçu le segment FIN

La taille de fenêtre

La quantité de données qu'une source peut transmettre avant qu'un accusé de réception soit reçu est la "taille de fenêtre". Cette taille est définie lors du démarrage de la session.
Le protocole TCP peut réduire la taille de la fenêtre afin de mieux contrôler le flux de données (envoie d'ACK plus fréquent, évite les pertes)

Gestion des pertes de segments du TCP

Quand le protocole TCP source envoie des segments de données, il va placer une copie du segment dans une file d'attente de retransmission et va déclencher en même temps un timer. S'il ne reçoit pas d'ACK avant la fin du timer, il va retransmettre à partir du dernier numéro d'accusé de réception.

Protocole de la couche application utilisant UDP

UDP c'est quand même pas de la merde, c'est utile pour certains protocoles

- DNS
- DHCP
- TFTP
- RIP
- VoIP

Il n'y a pas de numéro d'ordre dans le protocole UDP, donc il ne sait pas réordonner les datagrammes => Il les réassemble dans l'ordre qu'il les a reçu.

Chapitre 8: Adressage IP

Adressage IPv4

Une IP est le numéro qui identifie chaque ordinateur connecté à Internet, ou plus précisément, l'interface avec le réseau de tout matériel informatique Internet.
Elle a un format de 4 octets (32 bits) présentable en binaire ou en décimal
Elle contient deux parties:

- ID de réseau : Adresse réseau logique du sous réseau auquel l'ordinateur se rattache
- ID d'hôte : Adresse logique du périphérique logique identifiant chaque ordinateur sur un sous réseau

Les ≠ classes d'adresses

A: 8 bits partie réseau, 24 partie hôte premier BIT est fixé a "0"
B: 16 bits réseau, 16 bits hôtes deux premiers bits fixé a "10"
C: 24 bits réseau, 8 hôtes
D: Réservées pour le multicast, TOUJOURS UNE ADRESSE DE DESTINATION
E: Réservées à la recherche ou à des usages futurs

La classe A de l'adresse IP 0.0.0.0 à 126.255.255.255
La classe B de l'adresse IP128.0.0.0 à 191.255.255.255
La classe C de l'adresse IP 192.0.0.0 à223.255.255.255
La classe D de l'adresse IP 224.0.0.0 à 239.255.255.255(Adresses de multicast).
La classe E de l'adresse IP 240.0.0.0 à 255.255.255.255 (adresses réservées par l'IETF).

Les adresses privées de la classe A : 10.0.0.0 à 10.255.255.255/8 (10.0.0.0 /8)
Les adresses privées de la classe B : 172.16.0.0 à 172.31.255.255/12 (172.16.0/12)
Les adresses privées de la classe C : 192.168.1 .0 à 192.168.255.255 192.168.0/16)

Le réseau 127.0.0.0 est réservé pour les tests de boucle locale avec notamment l'adresse IP 127.0.0.1 qui est l'adresse « local host » c'est-à-dire de boucle locale de votre PC.
Le réseau 0.0.0.0 est lui aussi réservé (et utilisé notamment pour définir une route par défaut sur un routeur).
Les adresses du bloc 168.254.0.0/16 sont des adresses link-local (c'est du réseau local)
Les adresses TEST-NET du bloc 192.0.2.0/24 sont réservées à des fins pédagogiques
Les adresses expérimentales du bloc 240.0.0.0 à 255.255.255.254 sont réservées pour une utilisation future

Solution pour pallier aux problèmes de l'IPv4

- Le CIDR (Classless Inter-Domain Routing)

Permet une diffusion plus efficace de l'espace d'adressage IPv4 et retarde la croissance des tables de routages donc la pénurie d'adresses

- Utilisation du NAT

Permet à un ensemble d'hôtes présents sur un réseau local, d'avoir accès à internet en utilisant une adresse IP unique => retarde la pénurie d'adresses

Technique calcul IP réseau/diffusion/hôtes

CIDR	32	31	30	29	28	27	26	25	24	23	22	21
Hosts	1	2	4	8	16	32	64	128	256	512	1024	2048

1. Trier les réseaux à faire par ordre de grandeur
2. Trouvez l'adresse réseau
3. Adapter le CIDR
    a. Voir tableau : on prend le premier multiple strictement plus grand que le nombre d'hosts voulu
4. Trouver l'adresse du réseau suivant
    a. On considère que i=0
    b. On ajoute à l'IP le nombre d'hosts donné par notre CIDR suivant les 2 choix suivants :
        i. Si CIDR < 25
            1. CIDR + 8 et i+1
                a. Ex : CIDR 24< 25 => 24+8 = 32
            2. On trouve la valeur correspondante dans le tableau
                a. Ex : CIDR 32 = 1
            3. On ajoute 1 à la valeur de l'octet (i=1) soit : 48 + 1 = 49
        ii. Si CIDR = 25 ou +
            1. Ajouter simplement le nombre d'hosts à l'octet i=0
5. Pour trouver la 1ère adresse ajouter simplement 1 à votre adresse réseau
6. Pour trouver la broadcast soustrayez 1 à l'adresse de réseau suivant
7. Recommencer à l'étape b) pour le réseau suivant jusqu'à complétion de votre table d'adressage.

Coexistence IPv4 et IPv6

- Techniques de migration vers l'IPv6
    1. Double pile

Permet à l'IPv4 et à l'IPv6 de coexister sur le même réseau.
Les périphériques exécutent les piles de protocoles IPv4 et v6 simultanément

    2. Tunneling

Méthode de transport des paquets IPv6 via un réseau IPv4. Les paquets IPv6 sont encapsulés dans les paquets IPv4

    3. Traduction

Un paquet IPv6 est traduit en paquet IPv4 et inversement

Adressage IPv6

Une adresse IPv6 est longue de 128 bits (16 octets)
La notation décimale a été abandonnée au profit d'une notation hexadécimale où les 8 groupes de deux octets sont séparés par un signe ":"

- Règles
    - On peut supprimer les 0 de gauche: 01AB devient 1AB et 00CD devient CD /!\ 0000 devient 0 !

- Une (ou plusieurs) suite de groupe de quatre 0 peut être compressée en "::" (une seule fois)
  - ex: 2001:DB8:0:1111::200 => 2001:0DB8:0000:1111:0000:0000:0000:0200

La longueur de préfixe est utilisée pour indiquer la partie réseau d'une adresse IPv6, elle peut aller de 0 à 128
Si elle vaut 64, il y a 64 bits réseau et 64 bits hôtes

Adresse anycast

Adresse de monodiffusion IPv6 qui peut être attribuée à plusieurs périphériques. Le périphérique le plus proche reçoit le paquet.
Il n'y a pas d'adresse de diffusion en IPv6 mais on peut faire une multi-diffusion à tous les nœuds donc ça revient au même

Adresse de monodiffusion

Il existe 6 types mais voici les plus importants:

- Adresse de monodiffusion globale: idem qu'IPv4, un hôte à un destinataire 48 bits.
- Adresse link-local: utilisées pour communiquer avec d'autres périphériques sur la même liaison locale, uniquement utilisable en local

Chapitre 9: Découpage réseau

Certains réseaux sont tellement grands qu'il en devient difficile d'y acheminer les paquets ou encore d'y faire des diffusions. Pour éviter cela il faut diviser ce réseau en différents sous-réseaux.
On divise un réseau selon les critères suivants:

- Taille
- Nombre d'hôtes par sous réseau
- Méthode d'attribution des adresses d'hôte
- Hôtes nécessitant des adresses IP statiques
- Hôtes pouvant utiliser le protocole DHCP

L'attribution des adresses ne doit pas être laissée au hasard, trois critères sont à prendre en compte:

- Eviter les doublons
- Assurer et contrôler l'accès
- Surveiller la sécurité et les performances

Pour communiquer entre eux les sous-réseaux doivent passer par un routeur comme passerelle par défaut

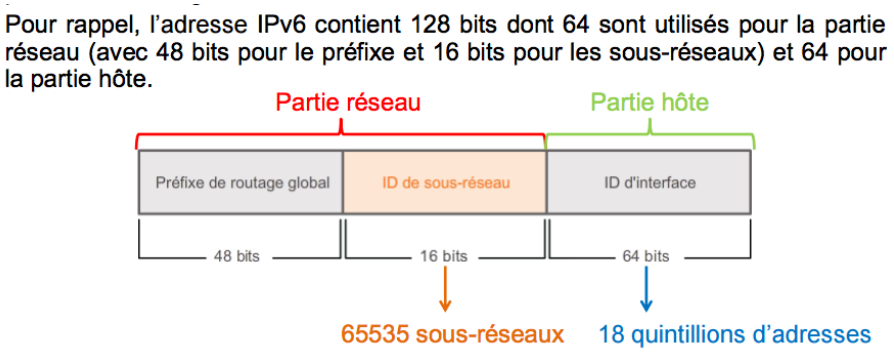
Comment découper un réseau correctement

- Toujours commencer par décomposer les réseaux en affectant les plages d'adresses les plus grandes en premier
- Quand on place un réseau plus grand que le précédent dans une plage, il faut sauter une certaine plage d'adresses

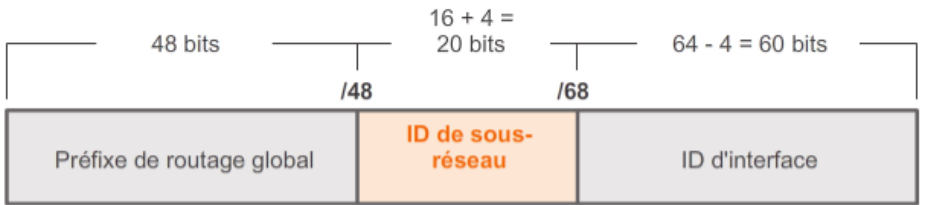
On rassemble ce qui doit être rassemblé (même IP) et on remet dans l'ordre

Segmentation IPv6

- 1 ère solution



- 2 ème solution



Chapitre 10: La couche application

Introduction

Couche la plus proche de l'utilisateur final, elle sert d'interface entre les applications et le réseau sous-jacent
Elle possède trois fonctionnalités principales:

- Met en forme ou présente les données d'un hôte dans un format compatible pour la réception par le périph. Destinataire
- Compresse les données afin qu'elles puissent être décompressées à l'arrivée
- S'occupe du chiffrement/déchiffrement des données en vue de leur transmission

La couche session a pour rôle de créer et gérer les dialogues entre les app source et destination

Le protocole HTTP

- Lancement d'une requête HTTP client-serveur
- Le serveur envoie au client le code HTML de la page web
- Le client décode à l'aide du navigateur le code HTML

Il s'agit du protocole d'application les plus utilisés.
Il existe trois types de message courant:

- GET => requête cliente pour obtenir des données
- POST
- PUT

Servent à uploader des fichiers de données vers le serveur Web
/!\ il n'est pas sécurisé => tout est envoyé en texte brut
HTTPS est sécurisé, il chiffre et déchiffre le trafic mais est plus lent à cause de ça

Caractéristiques du protocole HTTP

- Utilise TCP au port 80
- Stateless: le serveur ne maintient aucune info sur les requêtes des clients
- Non sécurisé => pas de chiffrement

Il y a eu HTTP 1.0 et 1.1, pas de keep-alive dans 1.0 (connexion persistante)

Codes de statut

- 1xx: info
- 2xx: succès
- 3xx: redirection
- 4xx: erreurs du client
- 5xx: erreurs du serveur

Le cache

Lorsqu'une page ne subit pas de modification, elle est mise en cache

- Réduit le temps d'attente
- Réduit le trafic des réseaux

Il y a le cache navigateur => permet au navigateur de fournir immédiatement les objets présents dans son cache sans devoir faire de requête et le cache mandataire (proxy server) => les clients utilisant un proxy vont disposer de son cache

Les cookies

Permettent au serveur de mémoriser des données du côté client

Les protocoles Email

1. SMTP :

Permet de transférer les e-mails de manière fiable et efficace.
Port: 25 sans chiffrement, d'autres avec chiffrement

2. POP3

Port: 110, Permet à ordinateur de récupérer des e-mails à partir d'un serveur de messagerie. L'email est téléchargé du serveur au client puis supprimé du serveur

3. IMAP

Port : 143 ou 220 selon la version, Des copies des messages sont téléchargées vers l'application cliente. Les messages originaux sont conservés sur le serveur jusqu'à ce qu'ils soient supprimés manuellement.

4. DNS => Associe un domaine à une IP

Service de nom de domaine, associe les noms des ressources à l'adresse réseau numérique requise.

5. DHCP

Port: Serveur 67, Client 68
Permet aux périphériques d'un réseau d'obtenir d'un serveur DHCP des adresses IP et d'autres infos
Généralement, on utilise les adresses statiques pour des périphériques réseaux et le serveur DHCP attribue des IP aux autres (périph. finaux)

6. FTP

Permet le transfert de données entre un client et un serveur, port 20 et 21. Existe en version simplifiée appelée TFTP, (pas sécurisé), port 69