Fiche Archi réseau partie 1

lundi 18 janvier 2016
17:41

Définitions

Réseaux :

- → Partage fichiers
- → Partage application
- → Partage ressources matérielles (imprimantes, disque, ..)
- → Téléchargement app et fichiers
- → Interaction utilisateur connectés (mail, visio, …)
- → Transfert de données
- → Transfert de parole (réseaux téléphoniques)
- → Transfert parole, vidéo données (réseaux num RNIS ou IP)

Session : un ou plusieurs flux de média sont établis entre deux points

Média : informations échangées par des partenaires qui communiquent

Trois type de média :

- → Voix
- → Vidéo
- → Texte

Média ≠ Médium de transmission (= autre nom canal de trans)

Connexion : allocation de ressources préalablement à l'échange de média (Pas sens conventionnel que l'on connaît)

Classification réseaux

Etendue

PAN (Personal Area Network) : faible portée (10m), débits de qq Kbps à Gbps. → équipements domestiques interconnectés, au sein même foyer.

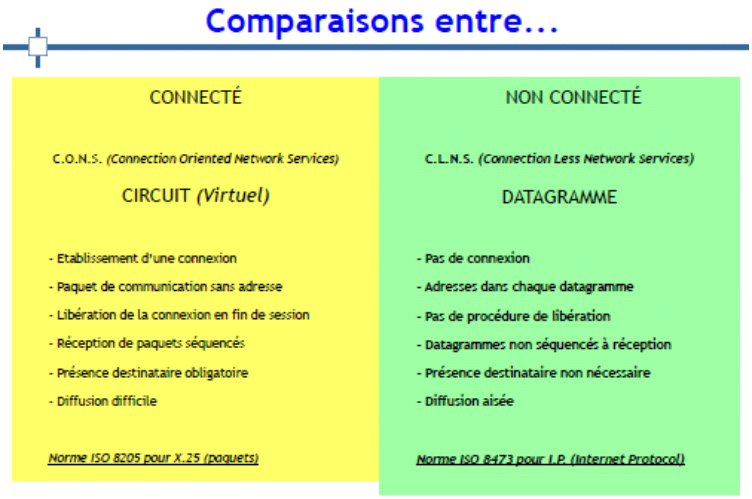
LAN (Local Area Network) : étendue limitée (circonscription géographique : bâtiment,…) débit de 10 à 100 Mbps → Ethernet

MAN (Metropolitan Area Network) : centaine de Kms, circonscritption géographique importante (campus), débit ordre de 100 Mbps) → GigaEthernet

WAN (Wide Area Network) : echelle pays, qq Kbps à dizaines Mbps → infrastructure filaires, sans fil ou marines : MPLS, ATM, RNIS, SDH, PDH, RTC, X.25…

Mode de connexion

→ Connecté
→ Non conncté



Nature du transfert

→ **Commutation :**

- **Commutation de circuits** :
  La commutation de circuit est un type de commutation dans lequel un circuit joignant deux interlocuteurs est établi à leur demande par la mise bout à bout de circuits partiels.
  ❑ Le circuit est désassemblé à la fin de la transmission.
  ❑ Il faut nécessairement une signalisation.
  ❑ La signalisation correspond à un passage de commandes, comme celles nécessaires à la mise en place d'un circuit à la demande d'un utilisateur.
  ❑ La signalisation spécifie les éléments à mettre en oeuvre dans un réseau de façon à assurer l'ouverture, la fermeture et le maintien des circuits.
  ❑ Le circuit est en général assez mal utilisé.

- **Commutation de messages** :
  Dans ce type de commutation, aucune réservation de lien "physique" n'est effectuée.
  ❑ Lorsqu'un message est reçu à un noeud et procède à la technique de type Store-and-forward :
  1. stocké,
  2. vérifié pour les erreurs
  3. et puis retransmis,
  ❑ Le message ne peut être relayé vers le prochain commutateur tant qu'il n'est pas complètement et correctement reçu par le noeud précédent.

- **Commutation de paquets** :
  ❑ Semblable à la commutation de messages excepté que les messages sont découpés en paquets de taille limitée.
  ❑ Les paquets sont envoyés indépendamment les uns des autres
  ❑ Les liaisons intermédiaires les prennent en compte pour

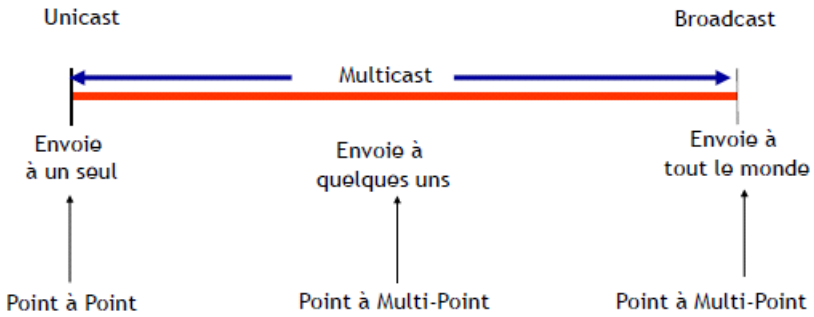
les émettre au fur et à mesure de leur arrivée dans le noeud
❑ Les paquets de plusieurs messages peuvent donc être multiplexés temporellement sur une même liaison

Ce type de commutation diminue le temps de transmission car les paquets sont de taille raisonnable.
❑ Le coût de communication dans les réseaux utilisant ce type de commutation est en fonction de la taille des paquets.
❑ Ce type de commutation nécessite des tampons pour stocker les paquets avant de les transmettre sur des lignes.
❑ Par rapport à la C.M, la CP est plus efficace surtout pour au niveau de la reprise sur erreurs
❑ La complexité surgit lors du processus de réassemblage de paquets, du même message, ayant empruntés des chemins différents

→ **Comparaison :**
Permet de recevoir de l'information d'un utilisateur quelconque parmi N et de la redistribuer a un autre utilisateur quelconque
❑ CIRCUITS
❑ Établissement d'une liaison durant toute la durée de la communication en fin.
❑ MESSAGE
❑ Réception, stockage, retransmission de noeud à noeud de volumes flux importants de données.
❑ PAQUET
❑ Message de taille réduite, à longueur maximale définie.
❑ Différences :
❑ Optimisation de l'utilisation des ressources
❑ Conversions au niveau de chaque noeud de commutation (vitesse, codage,…)
❑ Transparence vis-à-vis de l'information (contrôle de flux, la vitesse, le codage,..)
❑ Analogie entre la route et la voie ferrée

Types de transmission

❑ **Spectrum des Paradigmes**



Totale :
Broadcast :
→ Emettre message ensemble du réseau
→ même canal de com pour ttes les machines
→ Adresse spéciale

Sélective :
Multicast :

→ Emettre message vers sous-ensemble restreint de machines du réseau
→ Adresse spéciale pour la diff
→ Groupe de diffusion (ex ing1, ing2, …)

Point à point :

Unicast :

→ Emettre message vers une machine destinataire
→ Utilisation canal com par connexion pt à pt

Modèle OSI de l'ISO

Signifie Open System Interconnect (norme OSI 7498, publié en 1981)

❑ Défini par l'ISO : International Standard Organisation
❑ But : Définir les fonctions de la communication et les hiérarchiser en couches logicielles
❑ Pas de produit mais des spécifications et normes
❑ Exemple de normes
– ISO 8208 (X25 L3), ISO 7776 (X25 L2), ISO 8802 (V24)
– ISO 8326 (session), ISO 7478 (modèle de référence)
❑ Sévèrement concurrencé par le monde de l'Internet (Cf RFC's)

Définition système ouvert :

Composant Matériel ou Logiciel dont la description Fonctionnelle et Technique de l'interface avec son environnement externe est définie par des normes ou des standards publics et indépendant d'un seul fournisseur

Critères système ouvert :

→ La spécification est
– Publique et gratuite
– Développements multi-fournisseurs
– Non modifiable par un seul
– Implémentations multiples
– Disponible et supportée

→ Et a été validée par
– Tests de conformité
– Tests d'interopérabilité

OSI modèle de référence

Découpage en couches; les principes ayant conduit à ce découpage:

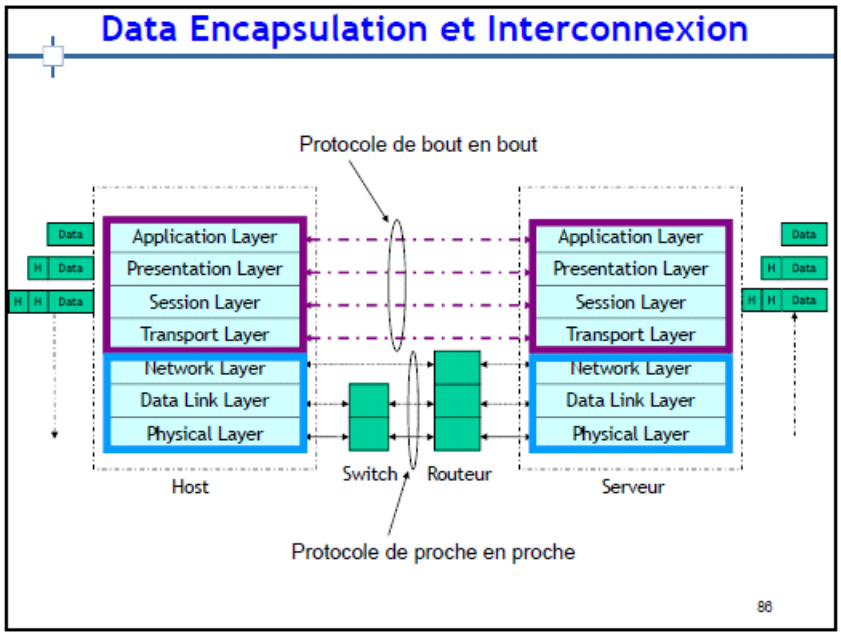
❑ Une couche définit un niveau d'abstraction,
❑ Chaque couche exerce une fonction bien définie,
❑ Les fonctions de chaque couche impliquent la définition de protocoles normalisés,
❑ Le choix des frontières entre couches doit minimiser le flux d'informations aux interfaces,
❑ Le nombre de couches doit permettre d'éviter la cohabitation de fonctions très diverses au sein d'une même couche.

❑ Une couche = un niveau d'abstraction

q Une couche n utilise les services de la couche n-1 et ses propres moyens pour offrir des services plus appropriés à la couche n+1.

- ❑ Relation entre les couches n et n-1
- ❑ n : utilisateur des services.
- ❑ n-1 : fournisseur des services.
- ❑ Nombre/nom/fonction des couches varie selon le réseau.

COUCHE :	Ensemble des moyens permettant à deux entités communicantes symétriques de même niveau d'échanger des unités de données
PROTOCOLE :	Règlement des échanges entre entités symétriques et correspondantes situées dans une même couche
SERVICE :	Ensemble des facilités offertes par une couche à celle immédiatement supérieure La prestation d'un service est faite par une entité
INTERFACE :	Point de passage obligé entre deux couches adjacentes



→ Couche Application : Offre aux processus applicatifs le moyen d'accéder à l'env. OSI

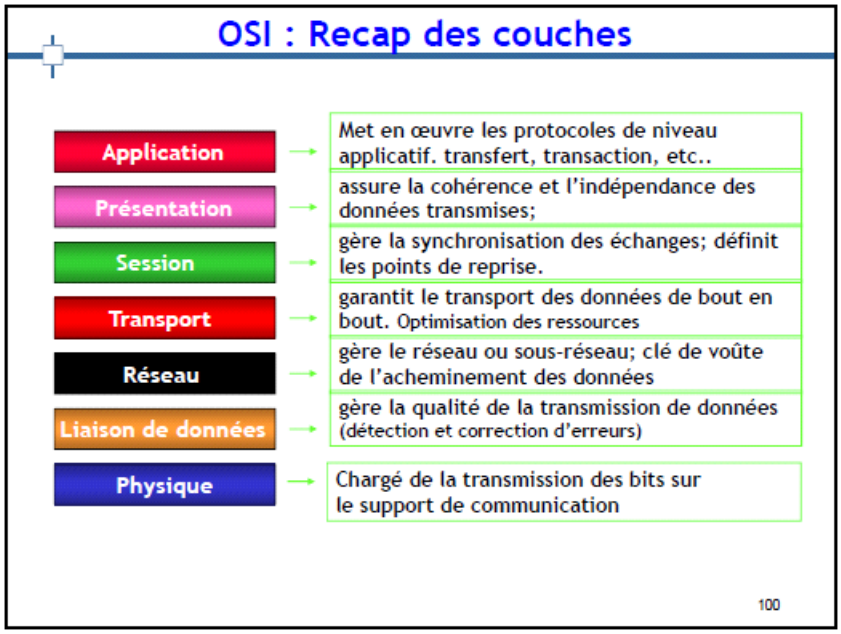
→ Couche présentation : représentation globale et unifiée de l'info, interprétation, cryptage, compression de données

→ Couche Session : ne gère pas les pb de dépl d'info mais fournit les moyens nécessaires pour organiser et synchroniser mes dialogues et les échanges de données

→ Couche physique : fournit les moyens mécaniques, électriques, fonctionnels et procéduraux nécessaire à l'activation, le maintien et la désactivation des connexions physiques destinées à la transmission de bits entre deux entités de liaison de données

→ Couche liaison de données :
Fournit les moyens fonctionnels et procéduraux nécessaires à l'établissement, le maintien et la libération des connexions de liaison de données entre deux entités du réseau

→ Couche transport : chargée de régler définitivement tous les problèmes relevant du déplacement d'information et qui n'auraient pas été réglés par les couches inférieures



Fiche Archi réseau partie 2

lundi 18 janvier 2016
18:40

TCP-IP

→ Transmission Control Protocol/Internet Protocol :
– La suite de protocoles réseaux qui ont servi pour construire l'internet global.
– Egalement appelé la suite DoD ou ARPANET car son développement initial était financé par le Advanced Research Projects Agency (ARPA) du Department of Defense (DoD) Américain.

→ TCP-IP est la pile protocolaire qui permet aux ordinateurs de communiquer entre eux sans se soucier du système d'exploitation ou du vendeur

Couche Internet

→ C'est la couche clé de toute l'architecture équivalente à la couche réseau du modèle OSI.
→ Contient le protocole IP, chargé de communiquer avec d'autres machines en commutation de paquets, et sans connexion
- Si un paquet se perd, il appartiendra aux couches supérieures de faire le nécessaire pour récupérer le paquet perdu : La couche Internet est donc non-fiable : best effort

→ Le protocole IP sera également amené à éventuellement découper les datagrammes pour les adapter au type de réseau traversé.

La couche Internet doit permettre :
– L'adressage des paquets : le protocole IP
– La résolution d'adresses : les protocoles ARP/RARP
– Injection de paquets dans n'importe quel réseau : fragmentation (MTU)
– La prise en charge des messages de contrôle : le protocole ICMP
– et leur acheminement indépendamment les uns des autres jusqu'à leur destination : les Protocoles de routage RIP,OSPF, ...

Le protocole IP : Adressage

→ Une adresse IP est un identificateur de machines dans l'internet

→ **Adresse IP** : 4 octets, pas plus de 255 par octets → 256.qqc pas possible

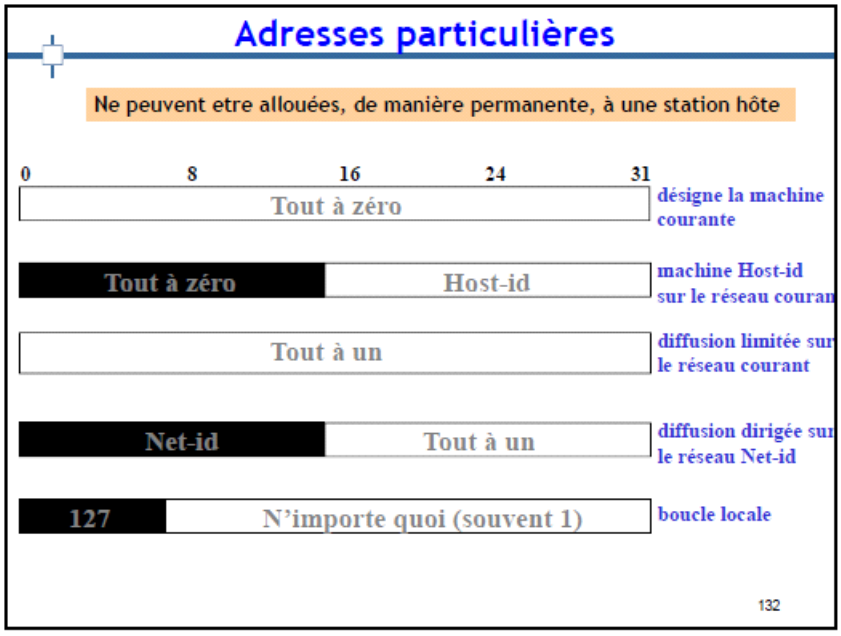
→ **3 classes d'adresse IP** : (ici adresse IP représentée par a.b.c.d)
- **Classe A** : a est le net_id, b.c.d le host_id
- **Classe B** : a.b net_id, c.d host_id
- **Classe C** : a.b.c net_id, d host_id
- **Classe D** : multicast (ex : 239.255.255.255)
- **Classe E** : adresses expérimentales

→ Plages d'id de réseau (pour le premier octet a) :
- Classe A : de 1 à 126
- Classe B : de 128 à 191

- Classe C de 192 à 223

=> Permet de reconnaître les classes !!!

→



Masque sous-réseau

→ Adresse de 32 bits
→ Permet de distinguer net_id à partir d'une IP
→ Permet de savoir si 2 adr ϵ même réseau

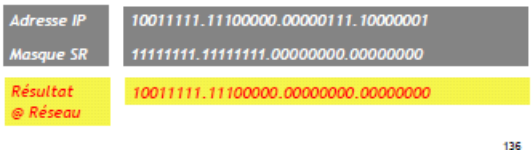
Tous les bits net_id mis à 1, tous les bits host_id mis à 0

- Le masque sous réseau permet de déterminer l'@ IP du réseau auquel appartient un hôte
- Pour cela, il suffit de procéder à une opération ET logique entre l'@IP du hôte et celle du masque sous réseau

⇒ @IP du hôte ET Masque sous réseau = @IP du réseau

- Rappel :

1 ET 1 = 1; 1 ET 0 = 0; 0 ET 1 = 0; 0 ET 0 = 0



Fiche Archi réseau cours 2 partie 1

mardi 19 janvier 2016
13:12

MTU (Maximum Transfer Unit)

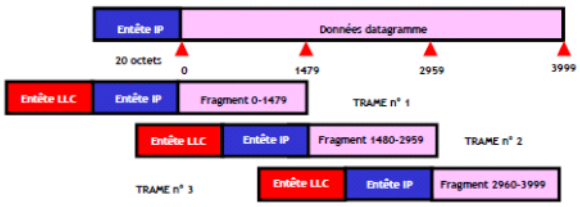
→ Tous réseaux taille de trame limitée qui circule : **MTU**
- ❖ Réseaux Ethernet : 1500 octets
- ❖ Réseaux FDDI : 4470 octets

→ Pour déterminer taille datagramme IP, on aurait pu adopter MTU la + faible mais injecter petits paquets avec MTU grande : moins efficace
- ⇒ IP doit s'adapter à cet état de fait

→ IP possède un mécanisme de fragmentation pour voyager dans réseaux sous-jacent
- ⇒ Ce mécanisme s'accompagne méthode pour reconstituer datagramme fragmenter. Routeur d'entrée qui fragmentent.

Découpage du datagramme IP pour portage dans plusieurs trames de niveau LIAISON, avec reprise de l 'entête IP dans chaque fragment.

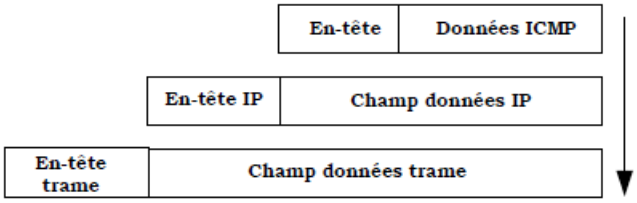
Exemple : un datagramme IP de 4.000 octets dans trois trames LLC
(Longueur maximale champ de données = 1.500 octets, entête IP= 20 octets)



ICMP (Internet Control Message Protocol)

Mécanisme d'échange de msg d'erreur et supervision pour permettre aux routeurs de rendre compte **erreurs** ou fournir **circonstances exceptionnelles** : protocole **ICMP** = module obligatoire protocole IP

⇒ Messages ICMP deux lvl encapsulation : champs de données datagramme IP, placé dans chps de données trame.



Principales fct ICMP

→ Commande ping s'appuie sur demande d'écho

→ Demande de redirection ICMP importantes car à l'origine de la modif de la table de routage d'une machine donnée

- Dans rsx, **routeurs** seules machines sensées connaître bonnes routes
- Si erreur empêche délivrer datagramme > message ICMP > détruit datagramme
- Si durée de vie dg = 0, fait de même => empêche dg de tourner indef dans rsx.

Couche internet (Routage)

Mode de routage

→ Définit processus permettant routeur de prendre des décision acheminement unité données

⇒ Mode routage Statique
⇒ Mode routage Dynamique

Routage Statique

→ Gérer manuellement table de routage
→ Mise à jour à chaque ajout ou suppression d'un réseau
⇒ Consomme temps et ressources, est source d'erreur

→ Config de 3 elmt : adresse IP dest, masque associé, adresse IP routeur suivant

Recommandé pour station.

Routage Dynamique

→ Méthodes automatiques, routeurs utilisent protocoles assurant :
- Calcul accessibilité réseau
- Détection topologie
- Construction table de routage

Deux classes de protocoles :
- Protocole "Distance Vector" (ex: Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP))
- Protocole "Link State" (ex: OSPF (Open Shortest Path First))

Fiche Archi réseau cours 2 partie 2

mardi 19 janvier 2016
12:50

Service DHCP

→ Très recommandé sur réseaux grde taille ou réseaux dont utilisateurs changent fréquemment
→ Nvx utilisateurs avec ordi portable peuvent se présenter
→ Nvlles stations de travail peuvent être connectées
→ Adresse IP attribuées automatiquement plutôt que par l'admin réseau => plus efficace

Protocole DHCP

DHCP = Dynamic Host Configuration Protocol

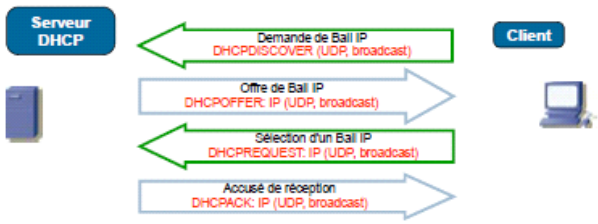
→ Extension du protocole BOOTP qui permet à client sans disque dur de démarrer et configurer automatiquement TCP/IP
→ Client obtient dynamiquement une adresse IP auprès serveur DHCP
→ Automatisation affectation adresse IP, masque sous-réseau, passerelle et autre param IP

Fonctionnement: DHCP contacté et adresse demandée

→ Choisit adresse dans une plage définie (pool)
→ Attribue temporairement adresse au client DHCP pour durée définie (bail)

4 étapes :

- **Demande de bail IP par le client**
- **Offre de bail par serveur**
- **Sélection offre par client**
- **Accusé réception bail IP par serveur**



A 50% de l'utilisation du bail, le client envoie un message DHCPREQUEST pour le renouvellement de son bail.

→ Si elle est accordée, le client continue avec un nouveau bail et éventuellement de nouveaux paramètres (DhcpAck).
→ Si le serveur est absent, le bail reste donc valide pendant 50% de la valeur initiale

A 87.5% du bail, si le serveur est indisponible, le client envoie un message DHCPDISCOVER.

→ Cette fois la demande est adressée à tous les serveurs (diffusion).
1. Un serveur peut répondre en proposant un nouveau bail (DhcpAck)
2. Mais peut également répondre avec un message DhcpNack qui oblige le client à se réinitialiser (reprise de la procédure d'obtention d'un bail)

Messages DHCP

- DHCPDISCOVER : Requête de Localisation des serveurs DHCP disponibles
- DHCPOFFER : Réponse d'un serveur à un paquet DHCPDISCOVER, contenant les premiers paramètres DHCP
- DHCPREQUEST : Requête du client pour annoncer qu'il a accepté une offre ou pour prolonger son bail
- DHCPACK : Réponse du serveur contenant des paramètres supplémentaires en plus de l'adresse IP du client
- DHCPNAK : Réponse du serveur pour signaler au client que son bail est expiré ou si le client annonce une mauvaise configuration réseau
- DHCPDECLINE : le client annonce au serveur que l'adresse est déjà utilisée
- DHCPRELEASE : le client libère son adresse IP
- DHCPINFORM : le client demande des paramètres locaux de configuration si il a obtenu une adresse réseau grâce à d'autres moyens (ex. configuration manuelle)

Cours 3 Partie 1

lundi 25 avril 2016
14:38

Service DNS

La technologie de base (TCP/IP) permet d'atteindre les machines par leurs adresses IP
Il est pratiquement devenu impossible aux utilisateurs de connaître les adresses (IP) des machines auxquelles ils veulent accéder.
Pour cette raison, des noms de domaine ont été créés pour convertir les adresses numériques en noms simples et explicites.
Le système DNS permet d'identifier une machine par un (des) nom(s) représentatif(s) de la machine et du (des) réseau(x) sur le(les)quel(s) elle se trouve ;

- www.enseeiht.fr identifie la machine www sur le réseau enseeiht.fr

Le système est mis en oeuvre par une base de données distribuée au niveau mondial

Protocole DNS

Pour acheminer la requête vers la destination, l'application cliente requiert la traduction du nom de domaine auprès d'un serveur de nom (DNS) : cette opération s'appelle la résolution de nom.

Serveur DNS

Un serveur DNS effectue la résolution des noms à l'aide du démon de nom, souvent appelé named (name daemon).

1. Lorsqu'un client effectue une demande,
2. le processus de démon de nom du serveur examine d'abord ses propres enregistrements pour voir s'il peut résoudre le nom.
3. s'il ne peut pas résoudre le nom à l'aide de ses enregistrements stockés, il contacte d'autres serveurs pour résoudre le nom.

Domaines (Zones)

Les domaines définissent différents niveaux d'autorité à l'intérieur d'une structure hiérarchisée.

→ Le plus haut domaine est appelé le domaine racine.
→ Les domaines de niveau supérieur peuvent contenir des hôtes et des domaines de second niveau.
→ Les domaines de second niveau peuvent contenir à la fois des hôtes et d'autres domaines.

Les noms d'hôtes sont ajoutés au début du nom de domaine.

On appelle « nom de domaine » chaque nœud de l'arbre.

→ L'extrémité d'une branche est appelée hôte, et correspond à une machine ou une entité du réseau.
→ Le nom d'hôte qui lui est attribué doit être unique dans le domaine considéré, ou le cas échéant dans le sous-domaine.
→ A titre d'exemple le serveur web d'un domaine porte ainsi généralement le nom www.

Nslookup

→ Le système d'exploitation des ordinateurs comprend également un utilitaire nommé nslookup
→ Nslookup permet à l'utilisateur d'envoyer une requête manuellement les serveurs de noms, afin de convertir un nom d'hôte donné.
→ Cet utilitaire permet également de résoudre les problèmes de résolution de noms et de vérifier l'état actuel des serveurs de noms.

Cours 3 partie 2

mardi 26 avril 2016
21:46

Couche transport

- Son rôle est de permettre aux entités paires sur les ordinateurs source et destination de soutenir une conversation comme s'ils étaient reliés par une liaison point à point : s'occuper de la qualité de transport
- Deux protocoles de bout en bout ont été définis pour cette couche :
  – TCP : Transmission Control Protocol
  – UDP : User Datagram Protocol

Elle doit s'assurer au minimum que les données transmises à son interlocuteur sont bien dirigées vers la bonne application.

Principe de communication inter-applications

A chaque démon présent dans un système donné correspond un numéro de port

La couche transport doit donc indiquer à quel démon elle doit envoyer les données.

La « localisation » du démon dans le système s'appelle un port et il est identifié par un numéro.

C'est la couche transport qui attribue le numéro de port à une connexion

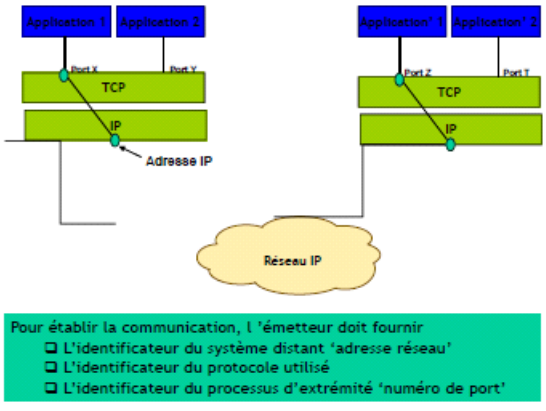
Socket

La combinaison adresse IP/numéro de port est parfois appelée une
socket.

Une socket décrit une connexion entre deux machines.

En général, les processus serveurs sont identifiés par leur numéro de port bien connu compris entre 1 et 1023.

La partie client possède un numéro de port éphémère.
Ces numéros de port sont compris entre 1024 et 5000 et changent à chaque connexion.



L'association : {protocole, @IP destination, port source, @IP source} est
désigné sous le terme SOCKET

Protocole TCP

Protocole TCP :

– Protocole responsable de l'adressage de niveau 4
– Protocole de transport en mode connecté qui résout tous les problèmes résiduels du déplacement de l'information
– Il garantit donc plusieurs choses :

1. Le séquencement des paquets.
2. Le contrôle de pertes : la destination devra recevoir tous les paquets envoyés.
3. Le contrôle des doublons (c'est à dire que le destinataire ne doit pas recevoir deux fois le même paquet).
4. Le contrôle de flux afin d'éviter la saturation et la congestion du destinataire.
5. La gestion d'un circuit virtuel qui en fait un protocole orienté connexion.

- TCP préférera couper une connexion plutôt que de violer une des trois premières garanties.
- La contrepartie à ces garanties est un temps d'acheminement nettement plus long qu'UDP.

TCP est

– Un protocole en mode connecté de bout en bout
– Avec contrôle de flux et de congestion
– Assure l'intégrité des données (checksum)
– Assure la transmission (détection des pertes et retransmission)
– Une connexion TCP est identifiée de manière unique par: adresse IP source, adresse IP destination, port TCP source, port TCP destination

- TCP est utilisé pour sa robustesse:
  – Émulation de terminal, transfert de fichier, web, e-mail…
  – Client serveur

La couche Transport : UDP

Protocole UDP :

– Protocole responsable de l'adressage de niveau 4
– Protocole de transport en mode non connecté qui vise la rapidité et non pas la résolution des problèmes résiduels du déplacement de l'information
• Les protocoles de niveau supérieurs doivent se charger de la résolution des problèmes
  – Ex : TFTP va corriger les erreurs

- UDP est un protocole simple de transport qui n'offre aucune garantie du point de vue de la fiabilité. UDP travaille sans connexion.

UDP reçoit des messages en provenance de diverses applications et les passe à la couche IP.

❑ A la réception, UDP récupère des datagrammes destinés à diverses applications et se charge de les distribuer.

❑ Chaque programme a un numéro de port local et un numéro de port distant avant de pouvoir envoyer des informations au protocole UDP.

❑ Lorsque UDP reçoit un datagramme, il vérifie le numéro de port dst. Un message d'erreur peut-être envoyé à la src du datagr par l'intermédiaire du protocole appelé ICMP (à venir).

❑ UDP multiplexe et démultiplexe les paquets en provenance et à

destination des programmes du système d'exploitation.

UDP	TCP
Service sans connexion ; aucune connexion n'est établie entre les hôtes.	Service orienté connexion ; une connexion est établie entre les hôtes.
UDP ne garantit ou n'accuse pas réception des données de livraison ou de séquence.	TCP garantit la livraison à l'aide des accusés de réception et la livraison de données en séquence
Les programmes qui utilisent le protocole UDP doivent fournir une stabilité nécessaire pour le transport des données	Les programmes qui utilisent TCP sont assurés de la fiabilité du transport des données.
UDP est rapide, présente des exigences de faible délai et peut facilement prendre en charge des communications point à point et point à multipoint.	TCP est plus lent, présente des exigences de délai plus élevé et ne peut prendre en charge facilement que les communications point à point.