Communiquer avec TCP/IP °LAN°

EDF

Guillaume Lehmann

DT/PTR || DT/PTO

Plan

- Introduction (5 min)
- Les modèles (10 min)
- Les couches basses (30 min)
- Les couches hautes (10 min)
- Le réseau ethernet (1 h)

pause 15 min

- Le réseau IP (1h)
- TCP et UDP (??)
- L'administration réseau (20 min)
- La sécurité (25 min)
- Conclusion (5 min)

But de cette formation

- Apprendre les principes de bases des réseaux et la logique qui les lie tous.
- Comprendre le fonctionnement des couches basses et plus particulièrement des réseaux ethernet et IP. Comprendre la mise en œuvre qui en est faite à EDF.
- Posséder une base de connaissance solide sur les fonctionnalités de niveau 2, sur les fonctionnalités de niveau 3, sur l'administration réseau et sur le monitoring.
- Posséder des connaissances générales sur la sécurité réseaux (orienté protection contre les actes malveillants).

Ne seront pas abordés

- La configuration détaillés des équipements réseaux.
- L'utilisation détaillées des outils de supervision ou d'administration réseau.
- Le fonctionnement des réseaux radio, ATM, Frame Relay, RNIS, MPLS, X25, …
- Les détails superflu sur les protocoles (taille des en-têtes, les flags TCP, …).
- Les cas particuliers des réseaux tels que le multicast, la VoIP ou encore la ToIP.

Les modèles

- La pile OSI
- La pile TCP/IP
- La pile NetBEUI

La pile OSI

- Modèle théorique sur la communication entre 2 entités.
- 7 couches utilisant le service rendu par la couche inférieure pour rendre un service à la couche supérieure => encapsulation/désencapsulation.

Application : http, smtp, snmp, telnet, nfs, …

Présentation : xdr, ASN.1, smb, aft, …

Session : ISO 8327 / CCITT X.225, rpc, NetBIOS, …

Transport : tcp, udp, rtp, spx, atp, …

Réseau : ip, icmp, igmp, X.25, arp, ospf, rip, ipx, …

Liaison : ethernet, ppp, hdlc, Frame Relay, rnis, atm, …

Physique : laser, fibre optique, câble UTP cat. 3/5/6/7, codage, radio, …

La pile TCP/IP

- Standard de fait, plus récent que le modèle OSI.
- Pile Internet
- Les couches basses des 2 modèles correspondent plus ou moins.
- Les couches hautes de la pile OSI sont regroupées en une seule couche Application.

Application : http, ftp, pop, smtp, telnet, snmp, dns, …

Transport : tcp, udp, rtp, …

Routage : ip, icmp (au-dessus d'ip), …

Liaison : ethernet, token-ring, wifi, wimax, atm, …

Physique : fibre optique monomode/multimode, câbles UTP cat. 3/5/6/7, codage, laser, radio, …

La pile de NetBEUI

- Pile utilisée par Microsoft Windows
- Conçue à l'origine pour des petits réseaux locaux
- NetBEUI disparaît avec MS Windows 2000

Application : WINS, SMB (*Server Message Block*), NCB (*Network Control Block*), RPC (*Remote Procedure Control*)

Session : NetBIOS (*Network Basic Input/Output System*)

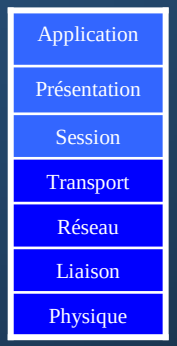
Transport/Réseau : NetBT (*NetBios over Tcp/ip*),

NetBEUI (*NetBios Extented User Interface*)

Liaison/Physique : Ethernet, token-ring, …

Les couches basses

- La couche physique
- La couche liaison
- La couche réseau
- La couche transport



La couche physique (1/3)

Émission et réception de signaux :

- Par voie hertzienne => radio (FM, AM, OOK, FSK, PSK, ASK/PAM)
- Par voie électronique => câbles coaxiaux, paires de cuivres.
- Par voie lumineuse => laser, fibres optiques

Sont définis :

- Type de médium
- Les connecteurs
- Les niveaux et puissances des signaux
- Le codage/modulation/longueurs d'ondes
- La synchronisation (horloge)
- Les distances maximales

La couche physique (2/3)

RLE USSO

Fibres optiques monomodes ou multimodes :

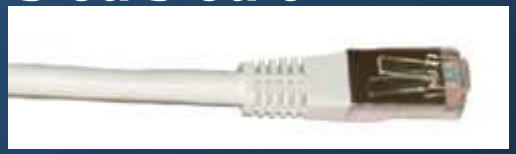
- LC/SC/ST/MTRJ

Câbles cuivres :

- RJ45 de catégorie 3 ou 5 ou 6

Matériel :

- Hubs 3Com PS40

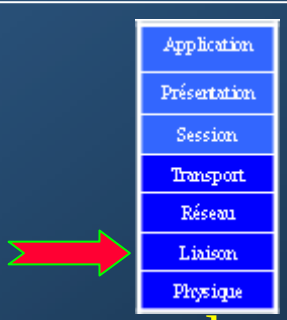


La couche physique (3/3)

Pour infos

- 100BASETX : 100ohms, 100m (90m Gbps), UTP (non blindé) ou STP(blindé)
- Laser : distance maximale ~ 500m
- Fibre optique :
  - *100BASEFX-FD*, multimode, 1300nm, 62.5microns, 2 à 2000m
  - *100BASEFX-HD*, multimode, 1300nm, 62.5microns, 2 à 412m
  - *1000BASESX-FD*, multimode, 850nm, 62.5microns, 2 à 275m
  - *1000BASELX-FD*, multimode, 1300nm, 62.5microns, 2 à 550m
  - *1000BASELX-FD*, monomode, 1300nm, 9microns, 2 à 11000m

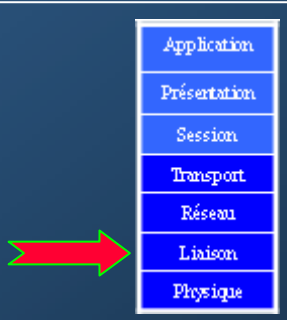
La couche liaison (1/2)



Comment les paquets sont transportés d'un nœud vers un autre noeud

- Le tramage (séquences de bits qui marquent le début et la fin des trames).
- Transmission entre deux nœuds physiques sur une zone restreinte : LAN (Local Area Network).
- Adressage physique des nœuds (en-tête).
- Contrôle d'erreur.
- Couche parfois subdivisée en :
  - MAC
  - LLC (au-dessus de MAC)
- QoS possible mais rarement utilisée.

La couche liaison (2/2)



RLE USSO

- Protocole :
  - ethernet
- Switchs ethernet 3Com :
  - SuperStack II : 1100/3300TX (p)
  - Superstack III : 3300FX (p), 4400 (p), 4050/4060/4070 (cœ), 4900/4950 (cœ)
  - Core Builder : 4007 (ch)
- Switchs ethernet Nortel :
  - Bay Stack 450 (p)
  - Accelar 1200 (ch)

(p) : switchs de périphérie

(cœ) : switchs de cœur de réseau empilables

(ch) : chassis

La couche réseau (1/2)

Acheminement des paquets à travers un ou plusieurs réseaux

- Un protocole d'adressage
- Un protocole de transmission de diagnostics
- Un protocole de gestion des transmissions multicasts
- QoS possible

La couche réseau (2/2)

RLE USSO

- Protocoles :
  - IP, ICMP, ARP pour le RLE
  - RIP, OSPF, IP, X.25 pour le RIH
- Switchs :
  - 3Com Superstack III : 4050/4060/4070, 4900/4950
- Routeurs :
  - Cisco (propriété et gestion par France Telecom / Cégetel)

La couche transport (1/2)

Fiabiliser le transport des paquets et les ordonner

- Vérifier que les données sont intègres.
- Vérifier qu'il n'y a pas duplication ou manque de paquets.
- Vérifier que les paquets sont présentés dans le bon ordre à la couche supérieure (seulement en mode connecté).

- Mode connecté et mode non connecté.
- Dans la pile TCP/IP, cette couche détermine aussi à quelle application les paquets doivent être envoyés.
- Retransmission en cas de perte.
- La QoS (Quality of Services) influe sur cette couche.
- Notion de flux.

La couche transport (2/2)

RLE USSO

- Protocoles :
  - TCP (Transmission Control Protocol) : mode connecté
  - UDP (User Datagram Protocol) : mode non connecté

- Utilisé pour :
  - Déterminer les flux (notion de ports TCP/UDP)
  - Mettre en place de la QoS

Utilisée dans le domaine des réseaux car lié à la couche réseau

Les couches hautes

- La couche session
- La couche présentation
- La couche application

La couche session

Placement de points de synchronisation, gestion des procédures d'ajournement, de fin ou de redémarrage de connexion et gestion de la continuité du service rendu aux couches supérieures

Gestion groupée d'infos provenant de plusieurs flux
=> Utilisée essentiellement dans le multimédia

La couche présentation

Mettre en forme les données pour qu'elle puissent être interprétées par la couche application

La couche application (1/2)

Programmes réseaux délivrant ou consultant un service

La couche application (2/2)

RLE USSO

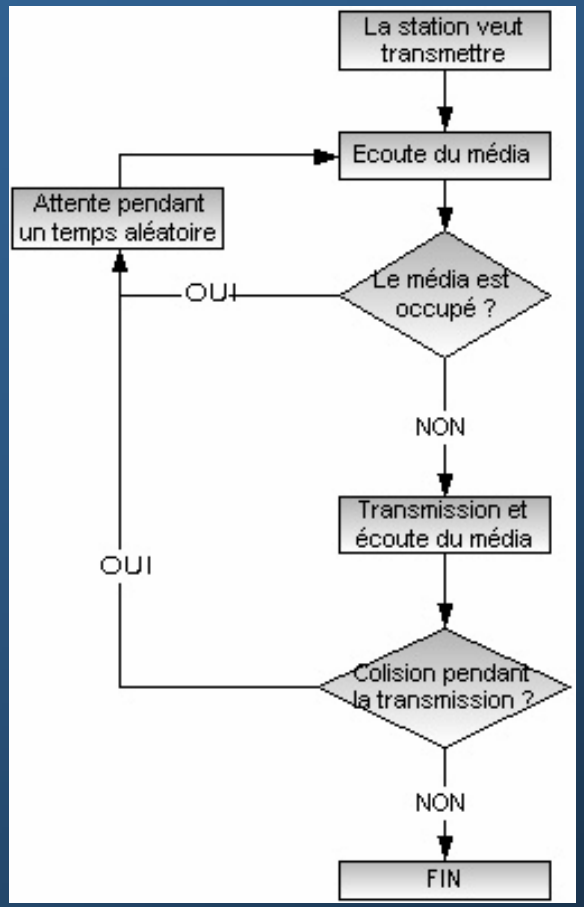
- Mail/partageDeDocuments => Lotus Notes
- Gestion de réseau Microsoft Windows
- Partage de fichiers à travers Microsoft Windows
- SNMP
- http/https
- Telnet

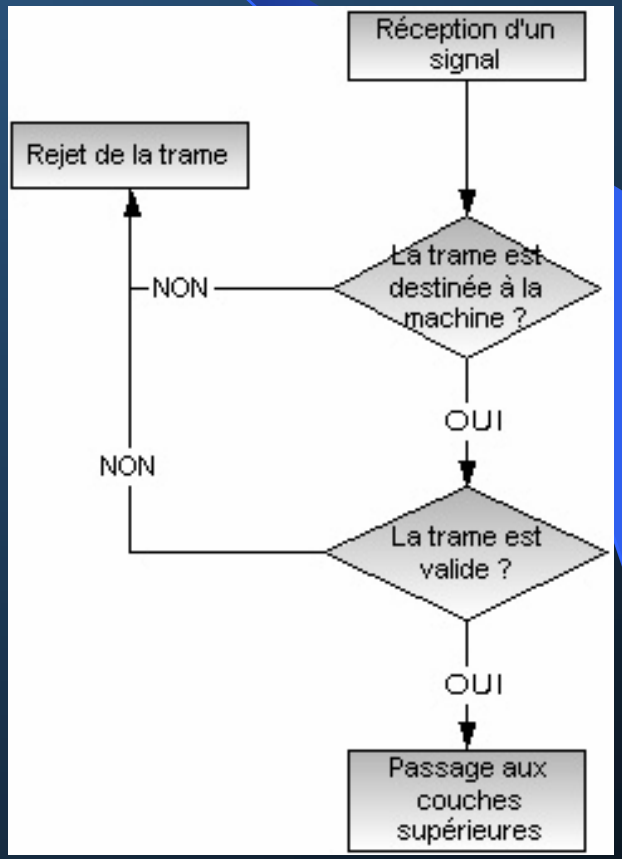
Le réseau ethernet

- Le fonctionnement
- L’adressage
- Les équipements
- Les fonctionnalités de base
- Les fonctionnalités évoluées

Le fonctionnement

CSMA/CD : Carrier Sense Multiple Access/Colision Detection





L'adressage

- La norme ethernet spécifie l'utilisation d'adresses physiques liées aux cartes réseau : les adresses MAC.
- Une carte ne prend en compte que les trames qui lui sont destinées et les transmets au protocole de niveau 3 trouvé dans le champ « Type » (0x0800 pour IP). Exception pour :
  - Les trames de broadcasts
  - Les adresses multicasts qui lui ont été configurées
  - Les cartes en mode promiscuité
- Une adresse MAC sous forme hexadécimale est constituée :
  - Du bit I/G : adresse unicast (0) ou multicast (1)
  - Du bit U/L : adresse universelle attribuée par l'IEEE (0) ou adresse locale (1)
  - De l'adresse du constructeur sur 22 bits
  - De l'adresse affectée par le fabricant sur 24 bits

I/G	U/L	@constructeur	@fabricant
0/1	0/1	-0f-23	-2c-14-34

Les équipements (1/2)

- **Hubs :**
  - Niveau 1 : La trame est répliquée sur tous les ports sauf celui d'arrivée de la trame
  - Même domaine de collisions de part et d'autre du hub
  - Débit : 10 Mbps, parfois 100 Mbps.
  - Technologie : Composants électroniques, avec un ou plusieurs bus ethernets.

Les équipements (2/2)

- **Switchs :**
  - 3 grandes familles de switchs :
    - *Stand alone* (bon marché) => *périphérie* ;
    - *Empilables* (extension aisée) => *périphérie* ou *cœur de réseau* ;
    - *Châssis* (redondance, remplacement à chaud des composants, modulaire, fonctionnalités plus nombreuses) => *cœur de réseau*.
  - Niveau 2 : La trame est envoyée uniquement sur le bon port (une table MAC par port) sauf si l'adresse est inconnue par le switch.
  - Niveau 3 : Fonctions de routage ajoutées par les constructeurs. Hors normalisation du 802.3.
  - Débits : 10/100/1000/10000 Mbps.
  - Technologie : ASIC et processeur RISC, matrice de commutation.
  - Domaines de collisions séparés par le switch, mais pas les domaines de broadcasts IP.

Les fonctionnalités de base

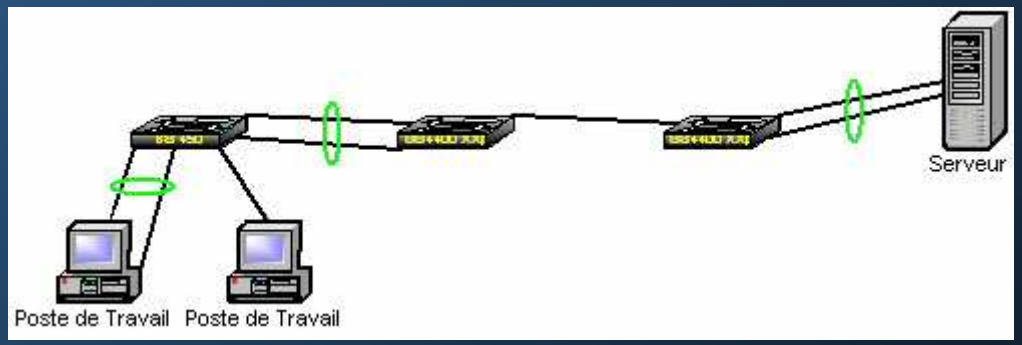
- Vitesse des ports et mode de fonctionnement :
  - Autonégociation ;
  - Autosense.
- Croisement logiciel du câble RJ45 :
  - (Auto-)MDIX.

Les fonctionnalités évoluées (1/4)

- Administration et supervision :
  - Accès en telnet, web, client propriétaire, …
  - Supervision par SNMP (MIB implémentée plus ou moins complète) et RMON.
- (Rapid) Spanning Tree Protocol : Désactivation automatique des ports impliqués dans un boucle.
  - STP => v1 ; RSTP => v2 ;
  - Communication entre les switchs (Bridge Protocol Data Unit) pour détecter les boucles ;
  - Élection d'un switch root et notion de coûts pour chaque liaison.

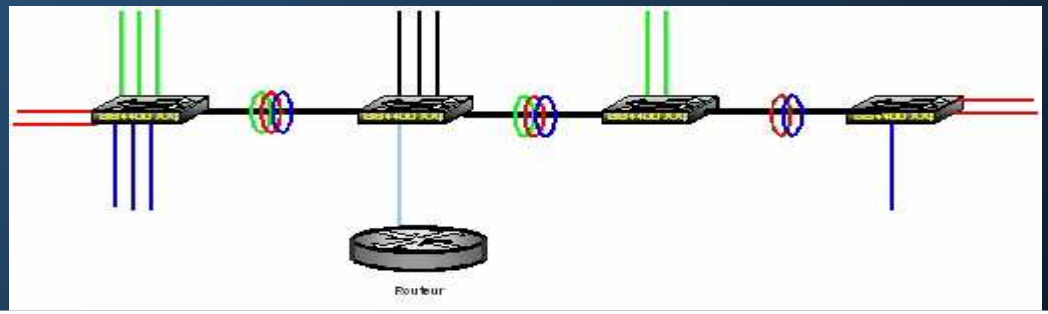
Les fonctionnalités évoluées (2/4)

- Agrégation de liens (802.3ad) : Lier plusieurs liens physiques hôte à hôte comme un seul lien logique. Répartition de charge (par « session » MAC) :
  - Montée en charge en parallèle des liens agrégés ;
  - Basculement de la charge sur un autre lien de l'agrégation une fois le premier lien arrivé à pleine charge ;
  - Basculement de la charge sur un autre lien de l'agrégation si le premier lien est hors-service.



Les fonctionnalités évoluées (3/4)

- Virtual Local Area Network (802.1q) : séparer virtuellement des réseaux physiquement identiques :
  - Affectation du VLAN par *port*, ou VLAN de niveau 1 ;
  - Affectation du VLAN par *adresse MAC* ou VLAN de niveau 2 ;
  - Affectation du VLAN par *adresse IP* ou VLAN de niveau 3 ;
  - Séparation de réseaux IP => nécessité de passer par un routeur pour aller d'un VLAN à l'autre ;
  - Tag/marquage d'un port lorsqu'il est nécessaire de faire passer le trafic de plusieurs VLAN par un même port (généralement pour l'interconnexion de 2 switchs).
  - Séparation des domaines de collisions, de broadcasts et de multicasts.



Les fonctionnalités évoluées (4/4)

- Quality of Services (802.1p inclus dans 802.1q) : Définition de priorités selon 7 classes de services (champ de 3 bits) (les constructeurs regroupent parfois plusieurs classes de services !) :
  - 0 = Best effort
  - 1 = Background
  - 2 = Réservé (spare)
  - 3 = Excellent effort (business critical)
  - 4 = Application à contrôle de charge (streaming multimedia)
  - 5 = Vidéo (interactive media), moins de 100ms de latence et jitter
  - 6 = Voix (interactive media), moins de 10ms de latence et jitter
  - 7 = Network control reserved traffic
- Roving analysis : recopie de ports (attention toutes les données ne sont pas toujours recopiées !).
- Power over Ethernet : alimentation des périphériques connectés au switch par le câble réseau (en plus de la transmission des données).

Le réseau IP

- L’adressage
- ARP/RARP
- DHCP/BOOTP
- La translation d’adresse
- Les équipements
- Le routage

L’adressage (1/4)

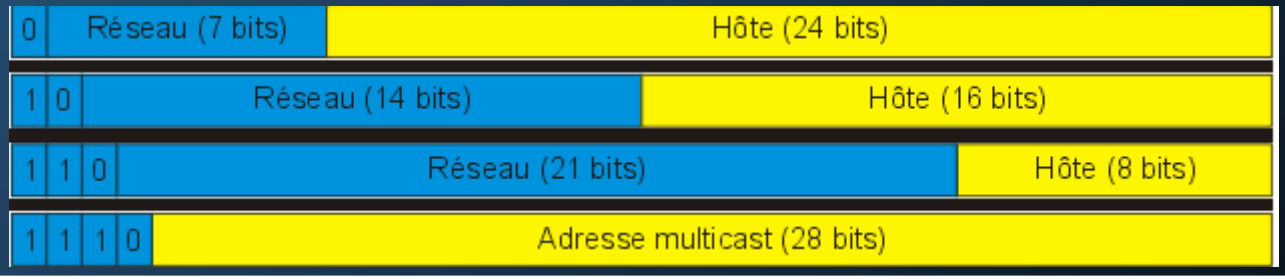
- Internet Protocol : actuellement en version 4. L’utilisation de IP a fortement évoluée !
- 32 bits utilisés, écriture en 4 fois 8 bits.

  11000000.10101000.00001020.10000010 = 192.168.10.130
- L’adressage d’une machine/d’un réseau = @ IP + masque sous-réseau (exception avec la notion de *classes*).
- 1 réseau IP = 1 plage IP constituée (exception pour le multicast) :
  - d’une adresse définissant le réseau (première adresse de la plage).
  - d’une adresse définissant le broadcast réseau (la dernière adresse de la plage).
  - d’adresses des hôtes uniques (toutes les autres adresses).
- Plusieurs méthodes de découpage des plages d’adresses :
  - Classes.
  - VLSM (*Variable Length Subnetwork Mask*), sorte de CIDR local à l’entreprise.
  - CIDR (*Classless Inter-Domain Routing*).
- Il existe des exceptions : des plages IP réservées et d’autres à ne pas router.

L'adressage (2/4)

Classes

- Les bits les plus lourds définissent la classe :
  - Classe A : réseaux de 16777214 machines max (de 0.0.0.0 à 127.255.255.255)
  - Classe B : réseaux 65534 machines max (de 128.0.0.0 à 191.255.255.255)
  - Classe C : réseaux de 254 machines max (de 192.0.0.0 à 223.0.0.0)
  - Classe D : adresses multicasts
  - Classe E : réservée à des usages expérimentaux



L'adressage (3/4)

CIDR

- Le masque sous-réseau permet de créer des sous-réseaux ou sur-réseaux qui ne respectent plus le découpage en classes A, B, C.
- C'est le masque sous-réseau qui définit la limite des bits d'adressage du réseau, des bits d'adressage de la machine :

192.168.10.5/255.255.255.0 ou 192.168.10.5/24 ← 24 bits Rx sur 32

→ 192.168.10.0 → 192.168.10.255

192.168.10.5/255.255.255.128 ou 192.168.10.5/25 ← 25 bits Rx sur 32

→ 192.168.10.0 → 192.168.10.127

192.168.10.5/255.255.252.0 ou 192.168.10.5/22 ← 22 bits Rx sur 32

→ 192.168.8.0 → 192.168.11.0

L’adressage (4/4)

Exceptions

Les plages IP à ne pas router par défaut

- 10.0.0.0/8 à 10.255.255.255/8
- 172.16.0.0/16 à 172.31.255.255/16
- 192.168.0.0/16 à 192.168.255.255/16

Les plages IP réservées

- 0.0.0.0 => utilisée par l’hôte quand l’adresse réseau est inconnue
- 255.255.255.255 => diffusion limitée à tous les hôtes du sous-réseau.
- 0.x.x.x
- 127.x.x.x => boucle locale/loopback
- 128.0.x.x
- 191.255.x.x
- 192.0.0.x
- 223.255.255.x
- 224.0.0.0 => diffusion multipoint (multicast)

ARP/RARP

- Correspondance entre l'adresse MAC (@ physique de la machine) et l'adresse IP (adresse logique).

ARP (*Address Resolution Protocol*)

Depuis l'@IP on recherche l'@ MAC

RARP (*Reverse Address Resolution Protocol*)

Depuis l'@MAC on recherche l'@IP

Exemple : permettre à des stations sans disque dur local connaissant leur adresse MAC de se voir attribuer une IP.

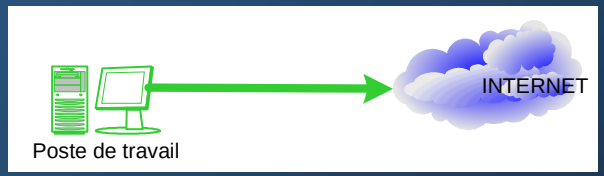
DHCP/BOOTP

- BOOTP (*BOOTstrap Protocol*): Ce protocole permet à un équipement de récupérer son adresse IP au démarrage.
- DHCP (*Dynamic Host Configuration Protocol*) : Remplaçant de BOOTP, il permet l'obtention dynamique d'une configuration IP plus ou moins complète.

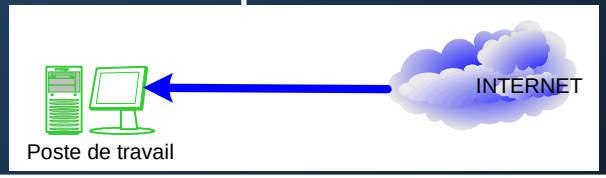
La translation d'adresse (1/3)

2 types de NAT (Network Address Translation)

- **Le SNAT (Source NAT) :**
  - Changer l'adresse IP et/ou le port de la source.
  - Le masquerading est un cas particulier de SNAT.



- **Le DNAT (Destination NAT) :**
  - Changer l'adresse IP et/ou le port de la destination.
  - La redirection est un cas particulier du DNAT.



La translation d'adresse (2/3)

- **NAT statique :**
  - @IP A1 sera toujours translatée en @IP B1
  - @IP A2 sera toujours translatée en @IP B2
  - …
- **NAT dynamique**
  - {A1, A2, …} translatée en {B1, B2 , …} ➔ pas de lien prédéfini entre une adresse An et Bm.

Version (4 bits)	Longueur de l'en-tête (4 bits)	Type de service (8 bits)	Longueur totale (16 bits)
Identification (16 bits)		Drapeau (3 bits)	Décalage fragments (13 bits)
Durée de vie (8 bits)	Protocole (8 bits)	Somme de contrôle en-tête (16 bits)	
Adresse IP source (32 bits)			
Adresse IP Destination (32 bits)			
Données			

- **Version** (4 bits) : il s'agit de la version du protocole IP que l'on utilise (actuellement on utilise la version 4 *IPv4*) afin de vérifier la validité du datagramme. Elle est codée sur 4 bits.
- **Longueur d'en-tête**, ou *IHL* pour *Internet Header Length* (4 bits) : il s'agit du nombre de mots de 32 bits constituant l'en-tête (nota : la valeur minimale est 5). Ce champ est codé sur 4 bits.
- **Type de service** (8 bits) : il indique la façon selon laquelle le datagramme doit être traité.
- **Longueur totale** (16 bits) : indique la taille totale du datagramme en octets. La taille de ce champ étant de 2 octets, la taille totale du datagramme ne peut dépasser 65536 octets. Utilisé conjointement avec la taille de l'en-tête, ce champ permet de déterminer où sont situées les données.
- **Identification, drapeaux (flags)** et **déplacement de fragment** sont des champs qui permettent la fragmentation des datagrammes, ils sont expliqués plus bas.
- **Durée de vie** appelée aussi **TTL**, pour *Time To Live* (8 bits) : ce champ indique le nombre maximal de routeurs à travers lesquels le datagramme peut passer. Ainsi ce champ est décrémenté à chaque passage dans un routeur, lorsque celui-ci atteint la valeur critique de 0, le routeur détruit le datagramme. Cela évite l'encombrement du réseau par les datagrammes perdus.
- **Protocole** (8 bits) : ce champ, en notation décimale, permet de savoir de quel protocole est issu le datagramme
- **Somme de contrôle de l'en-tête, ou en anglais *header checksum* (16 bits)** : ce champ contient une valeur codée sur 16 bits qui permet de contrôler l'intégrité de l'en-tête afin de déterminer si celui-ci n'a pas été altéré pendant la transmission. La somme de contrôle est le complément à un de tous les mots de 16 bits de l'en-tête (champ *somme de contrôle* exclu). Celle-ci est en fait telle que lorsque l'on fait la somme des champs de l'en-tête (somme de contrôle incluse), on obtient un nombre avec tous les bits positionnés à 1
- **Adresse IP source** (32 bits) : Ce champ représente l'adresse IP de la machine émettrice, il permet au destinataire de répondre
- **Adresse IP destination** (32 bits) : adresse IP du destinataire du message

La translation d'adresse (3/3)

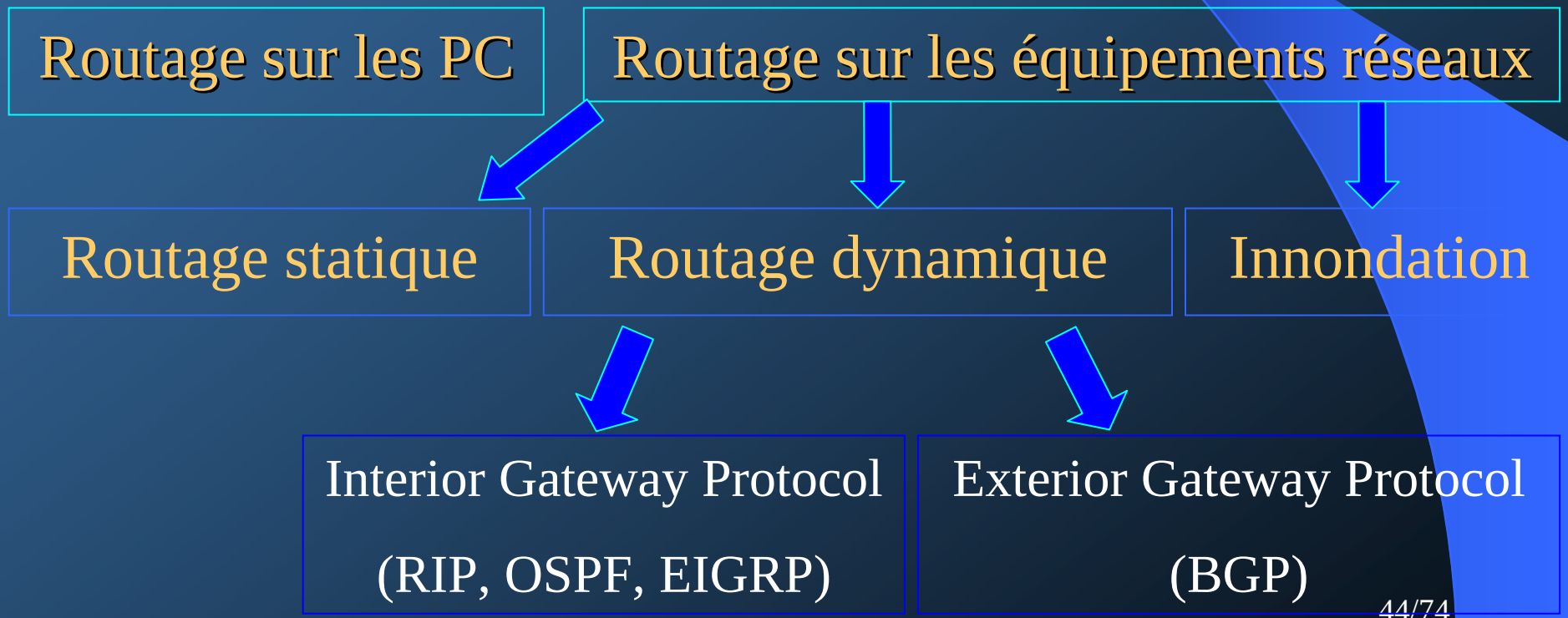
- **Overloading**
  - @IP A1 translatée en @IP B(port x)
  - @IP A2 translatée en @IP B(port x+1)
  - @IP A3 translatée en @IP B(port x+2)
  - …
- **Overlapping**
  - Utilisé quand l'adresse utilisée dans le LAN est dans une plage IP déjà existante sur un autre site et qui, depuis l'extérieur, apparaît comme un doublon. Le routeur joue alors de relais en faisant croire au client que la machine extérieure à une autre adresse IP.

Les équipements

- Niveau 3 :
  - Switchs de niveau 3 → commutation.
  - Routeur → routage.
- Débit : très variable (de quelques Ko à plusieurs Go).
- Technologie : Matériel dédié avec une partie logicielle. Table de routage.
- Séparation des domaines de collisions, et coupure des broadcasts IP.

Le routage (1/7)

Le routage permet d'acheminer les paquets d'un réseau à un autre, en passant par plusieurs autres réseaux, et à priori en ne connaissant pas le chemin à emprunter.



Le routage (2/7)

- Le routage statique :
  - Simple à mettre en place ;
  - Adapté à un faible nombre de réseaux IP ;
  - Permet de gérer les exceptions.
- Le routage dynamique :
  - Plus complexe à mettre en place ;
  - Seule solution viable sur un réseau comprenant de nombreux réseaux IP ;
  - Communication entre les routeurs par un protocole de routage.

Le routage (3/7)

- RIP (v1 et v2) : le meilleur chemin est celui ayant le moins de sauts. Vecteur de distance (Bellman-Ford)
- OSPF : le meilleur chemin est celui proposant les meilleures bande-passantes. Arbre du plus court chemin (Dijkstra).
- EIGRP : protocole propriétaire Cisco, combinant le routage par saut, par bande-passante, et par charge réseau.

Le routage (4/7)

RIP *(Routing Information Protocol)*

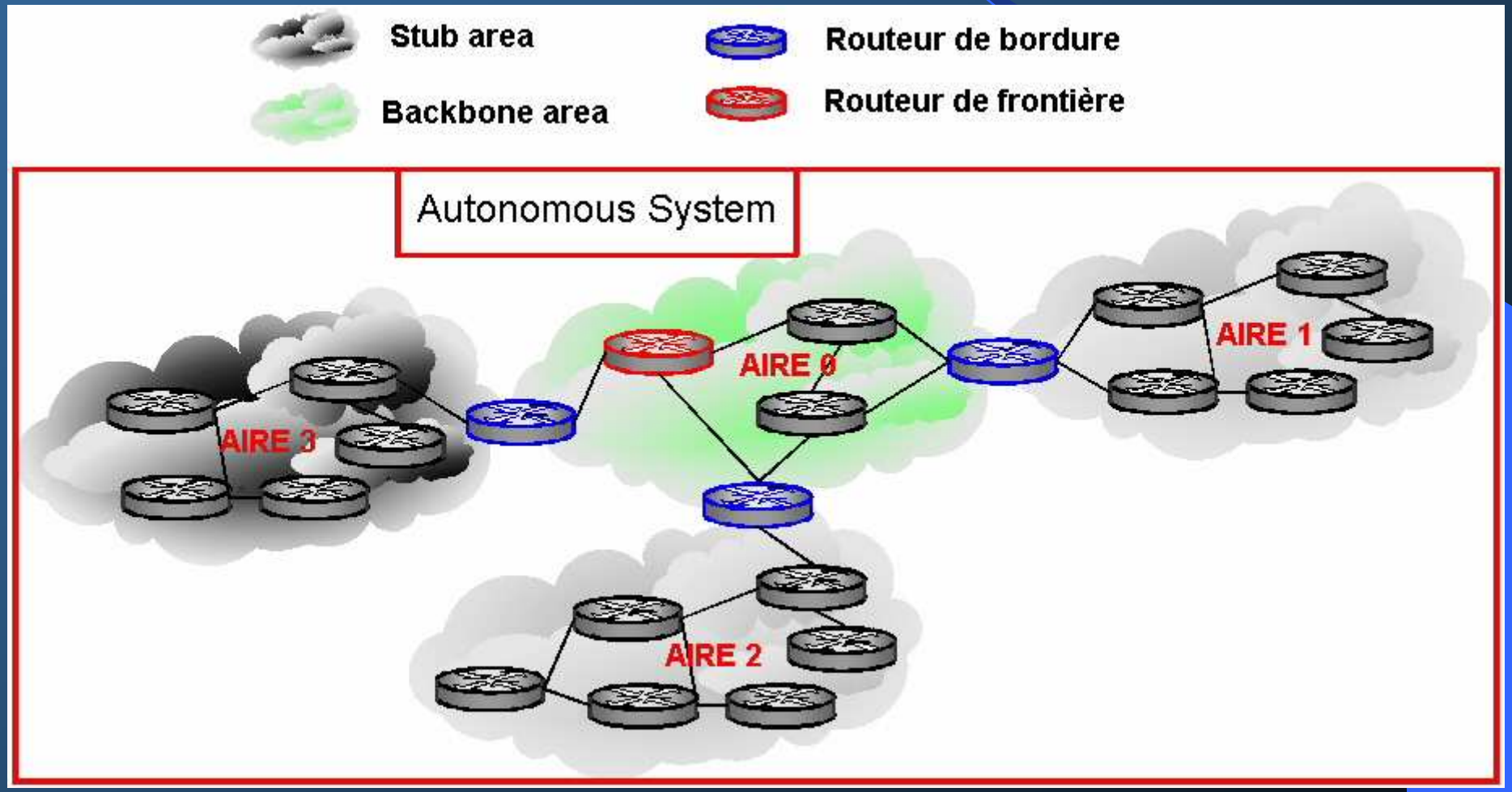
- 15 sauts maximum. Une route de 16 sauts est considérée comme coupée.
- Par défaut, 1 saut = 1 routeur.
- Protocole dépassé, mais encore présent de part sa simplicité de mise en œuvre et de compréhension.

Le routage (5/7)

OSPF *(Open Shortest Path First)*

- Découpage par aire :
  - Aire 0 (backbone area) : aire au centre de toutes les autres.
  - Les autres aires, doivent être contiguës à l'aire 0, physiquement ou par utilisation d'un lien virtuel.
  - Stub area : aire qui n'échange pas de route avec les autres aires.
- Routeur désigné (Designated Router) et Routeur désigné de secours (Backup Designated Router) pour synchroniser l'échange entre les bases de données.

Le routage (6/7)



Le routage (7/7)

- VRRP (*Virtual Router Redundancy Protocol*) :

Une adresse IP et une adresse MAC virtuelles sont utilisées comme passerelle par défaut. Un groupe de routeurs se surveille pour qu'un seul d'entre eux ait ces adresses (éviter les conflits d'adresse) et que ces adresses soit toujours affectées à un routeur valide (gateway toujours disponible vu des PC).

- HSRP (*Hot Standby Router Protocol*) : propriétaire Cisco, ancêtre de VRRP.
- CARP (*Common Address Redundancy Protocol*) : travail d'OpenBSD. Non reconnaissance par les organismes de normalisation malgré la valeur technique. Implémentation existante sous d'autres plateformes (cf. UCARP).

TCP et UDP

- TCP
- UDP

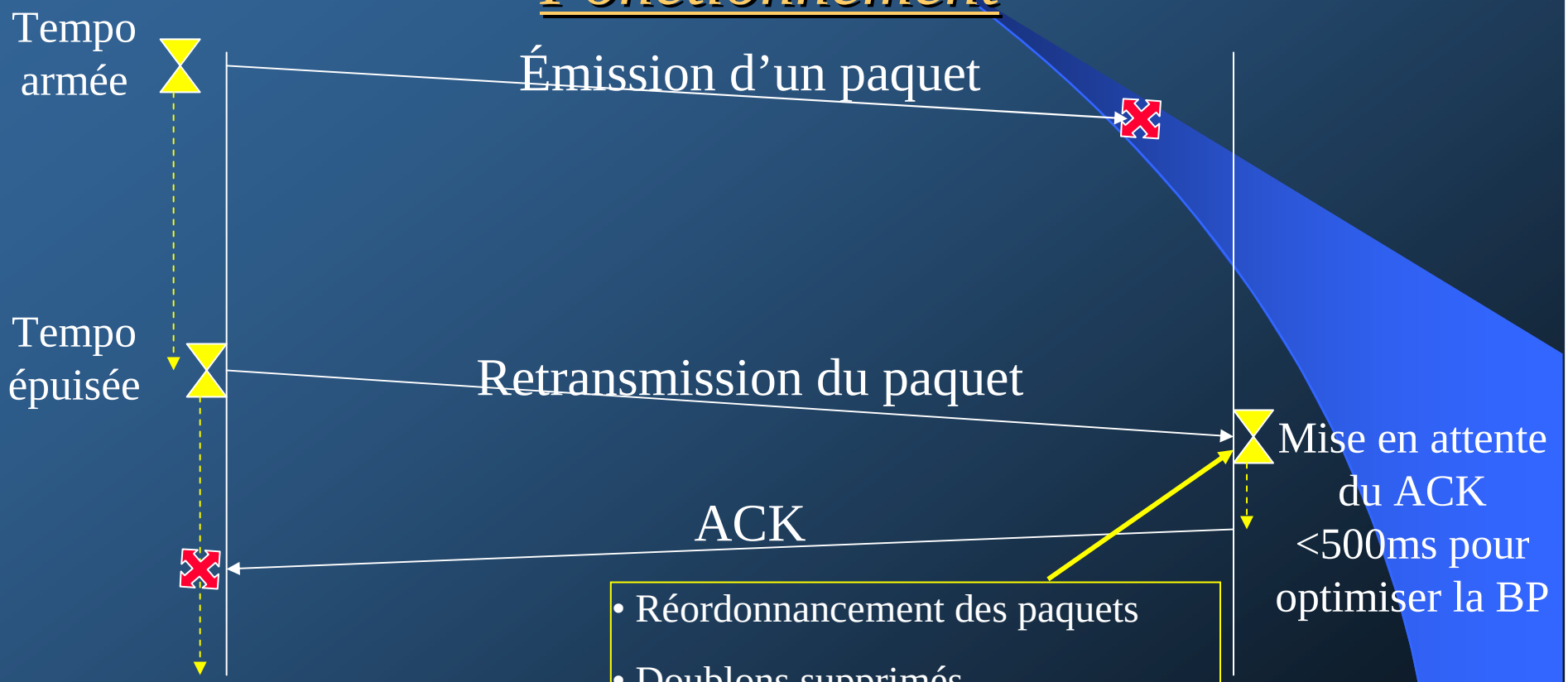
TCP (1/5)

Transmission Control Protocol

- Protocole de niveau 4 assurant un transfert :
  - Bidirectionnel ;
  - Fiable ;
  - Sans erreur ;
  - Avec contrôle d'intégrité ;
  - avec retransmission des données si des paquets sont perdus.
- Grâce à :
  - La notion de port source et destination ;
  - Un checksum ;
  - L'émission d'un ACK ;
  - Suivi d'un numéro de séquence des données.
- Protocole en mode connecté.

TCP (2/5)

Fonctionnement



- Réordonnancement des paquets
- Doublons supprimés
- Si checksum invalide, paquet détruit (émetteur détectera alors une perte de paquet et reémettra le paquet)

TCP (3/5)

Les flags TCP

Plusieurs peuvent être positionnés dans un même segment TCP.

- PSH (*push*) : Envoyer les données contenues dans le tampon d'émission même si celui-ci n'est pas plein.
- URG (*urgent*) : associé au pointeur « urgent » définit une zone de donnée spéciale dans la zone de données du segment TCP.
- SYN (*synchronisation*) : utilisé lors de l'établissement de la connexion.
- RST (*reset*) : réinitialisation de la connexion.
- FIN (*finalize*) : terminer la connexion.

TCP (4/5)

Adaptation du débit

Un mécanisme adaptatif de débit grâce à l'algorithme de Nagle

Retarder l'envoi de paquets pour les agréger en un seul segment TCP → désactivé si trafic intéractif nécessitant des temps de réponses < 200ms.

2 modes de fonctionnement de TCP

- Slow-start (démarrage progressif) : découverte de la qualité de la liaison.
- Congestion-avoidance (protection contre la congestion) : moins agressif.

TCP (5/5)

- Détection de paquets et retransmission :
  - Alarme RTO (Retransmit Time Out) : timer à l'émission épuisé.
  - Duplication des ACK : l'émetteur reçoit les segments n et n+2 → il envoie 3 fois le ACK pour n.
  - → comportements de l'émetteur différent, car types de pertes différentes dans chacun des cas.
  - Dans le premier cas, il y a un reroutage ou un changement de topologie entre les 2 extrémités. Qualité de la liaison à redécouvrir.
  - Dans le second cas, c'est une congestion (un routeur intermédiaire supprime des paquets) → l'émetteur réduit le débit

A mettre en forme

UDP

User Datagram Protocol

- Protocole en mode déconnecté :
  - Fragmentation et réassemblage géré par la couche IP
  - Pas de détection de perte de paquet
  - Pas de gestion des retransmissions
  - Pas de QoS
- UDP apporte :

A mettre en forme

  - La notion de port source et destination
  - Un champ longueur des données
  - Un checksum

L’administration réseau

- Les activités
- La boîte à outil
- La supervision réseau avec SNMP et ICMP
- Le monitoring

Les activités (1/2)

- La supervision réseau
- Le monitoring
- Le maintien en condition opérationnelle (MCO) :
  - Suivre les évolutions matérielles et logicielles
  - Étudier les optimisations en fonctions des nouveaux besoins
- Assurer la continuité de service :
  - Programmer des interventions de maintenance en dehors des heures de bureau
  - Réactivité et définition de procédures pour minimiser les impacts d’un incident réseau.

Les activités (2/2)

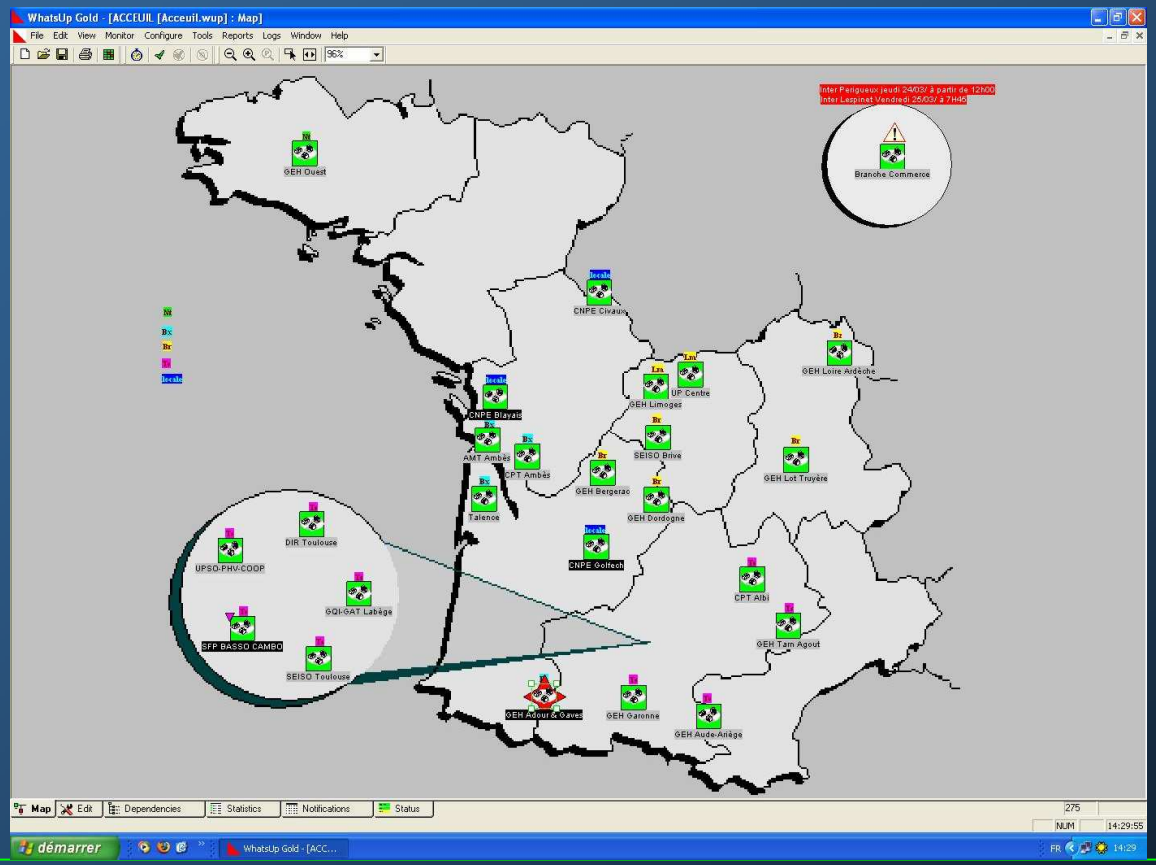
- La gestion du matériel réseau
  - Pour la gestion des stocks de réserve
  - Pour la gestion du matériel en production
  - Pour la gestion des garanties
- La documentation (attention aux extrêmes !)
  - Procédures d’interventions sur incidents
  - Procédures d’interventions programmées
  - Documentations techniques
  - Schémathèque
- Audits

La boîte à outils

- Test de la connectivité : ping
- Test de l’itinéraire : traceroute
- Remontée d’informations d’un PC sous MS Windows : nbtstat –A
- Étudier les données qui transitent sur un réseau : analyseur réseau
- Surveiller l’état du réseau : station de supervision (snmp et icmp), outils des opérateurs
- Suivi des incidents : tickets d’incidents
- Administrer les équipements : telnet, web, client propriétaire, accès par port console, tftp

La supervision réseau avec SNMP et ICMP (1/4)

Elle s’appuie essentiellement sur icmp et SNMP

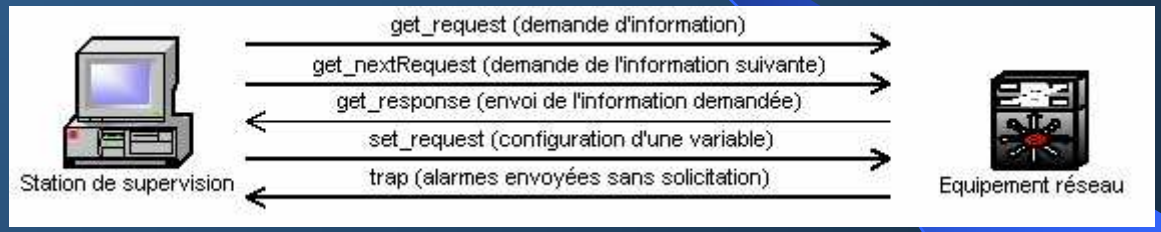


La station de supervision est l’outil principal

La supervision réseau avec SNMP et ICMP (2/4)

SNMP (Simple Network Management Protocol)

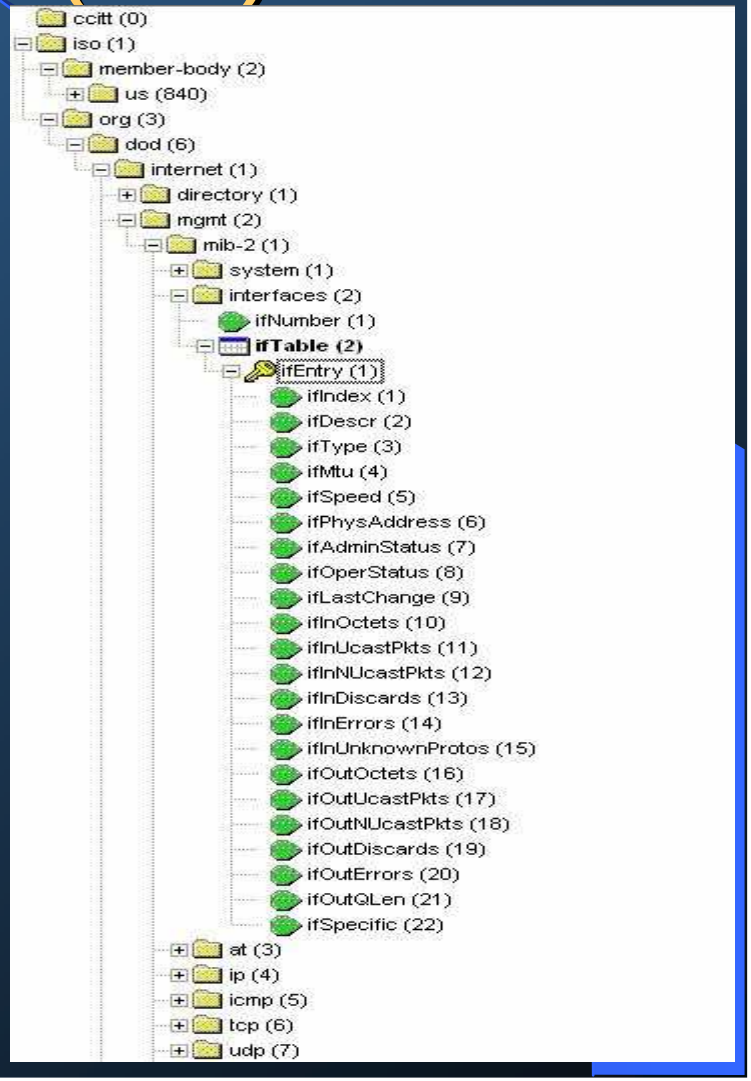
- 5 types de trames :



- Architecture client/serveur : station de supervision / agent SNMP
- Supervision selon 3 approches :
  - Polling : get_request/get_response
  - Remontée d'alarmes : trap
  - Combinaison des 2 premières méthodes
- Identification par l'utilisation d'une communauté SNMP identique.

La supervision réseau avec SNMP et ICMP (3/4)

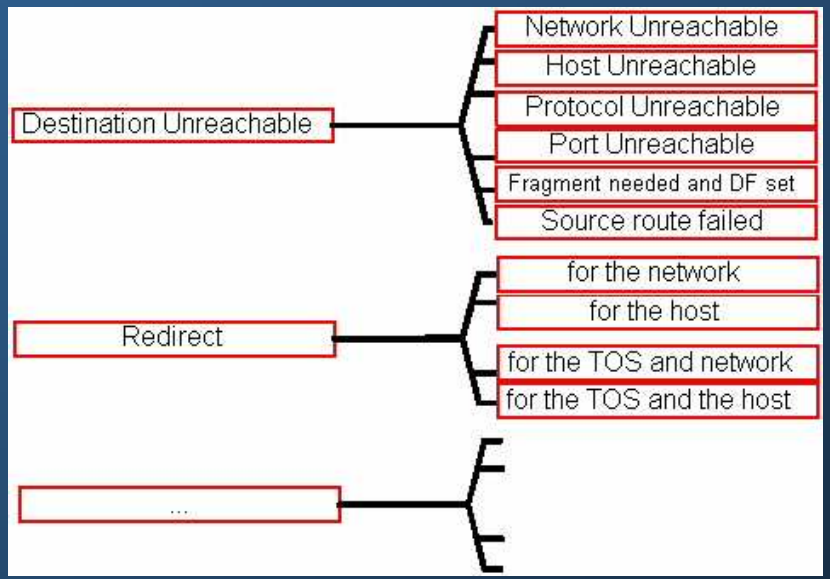
- SNMP s’appuie sur la MIB (Management Information Base) pour se référer à une variable.
- La supervision permet grâce à la consultation de ces variables de :
  - Détecter la panne d’un matériel
  - Détecter les bagottements
  - Tracer les incidents
  - Remonter des alertes



La supervision réseau avec SNMP et ICMP (4/4)

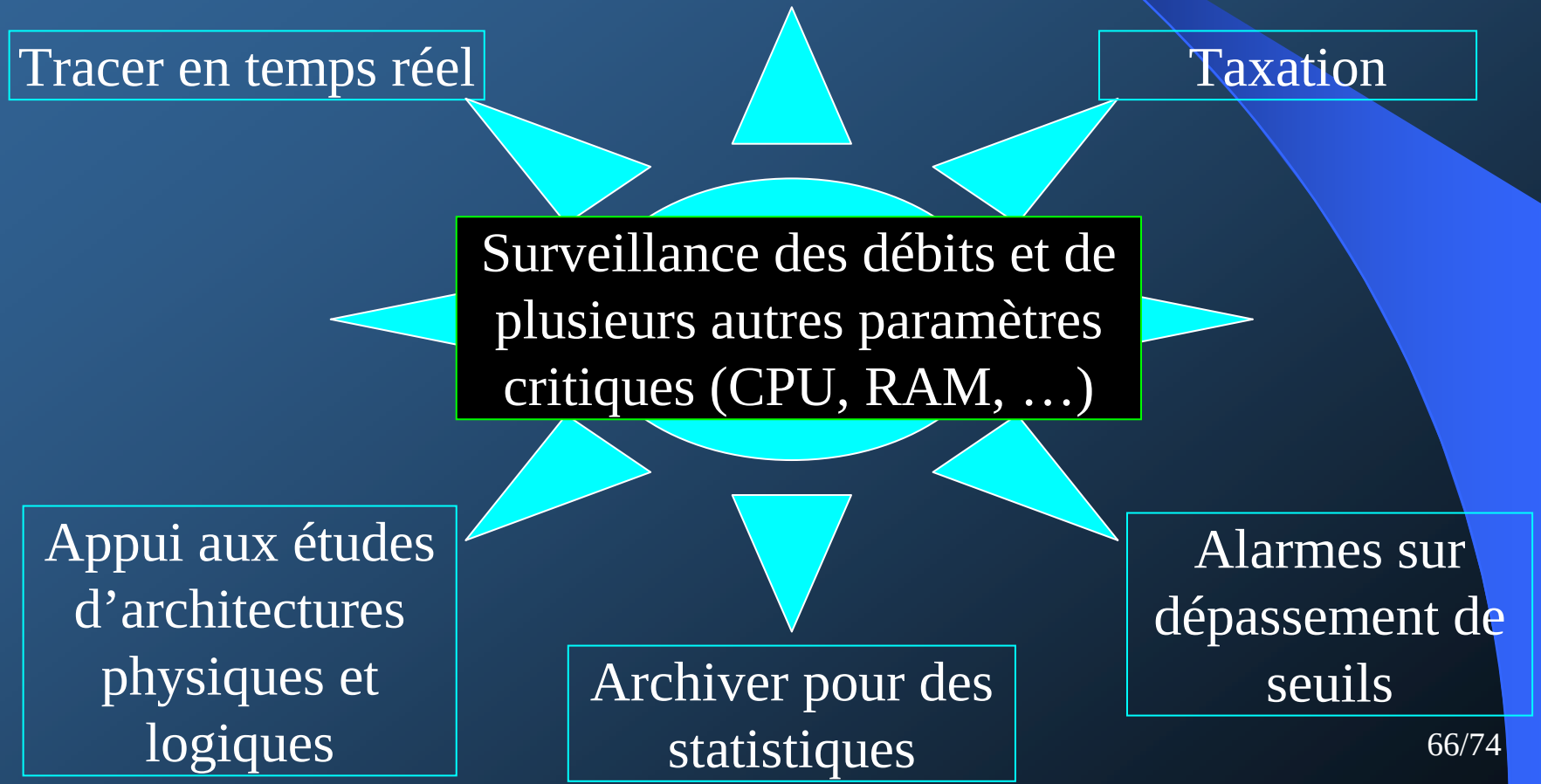
ICMP (Internet Control Message Protocol)

- Utilisé pour scanner un réseau (avant d’utiliser SNMP ou un autre protocole pour recueillir des informations sur l’hôte scanné)
- Utilisé pour savoir si l’équipement est accessible à l’instant t.

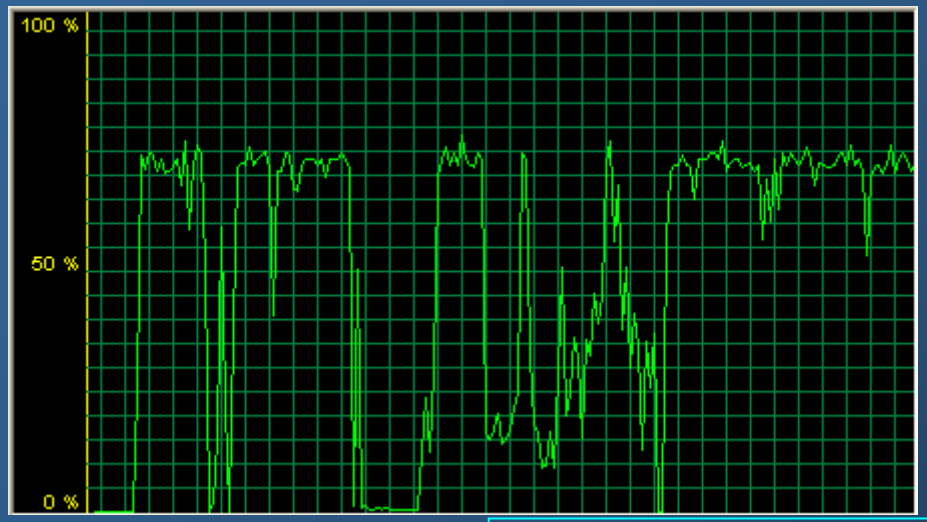


- Le ping (echo_request/echo_reply) est l’aspect le plus connu du protocole, mais il en existe beaucoup d’autres !

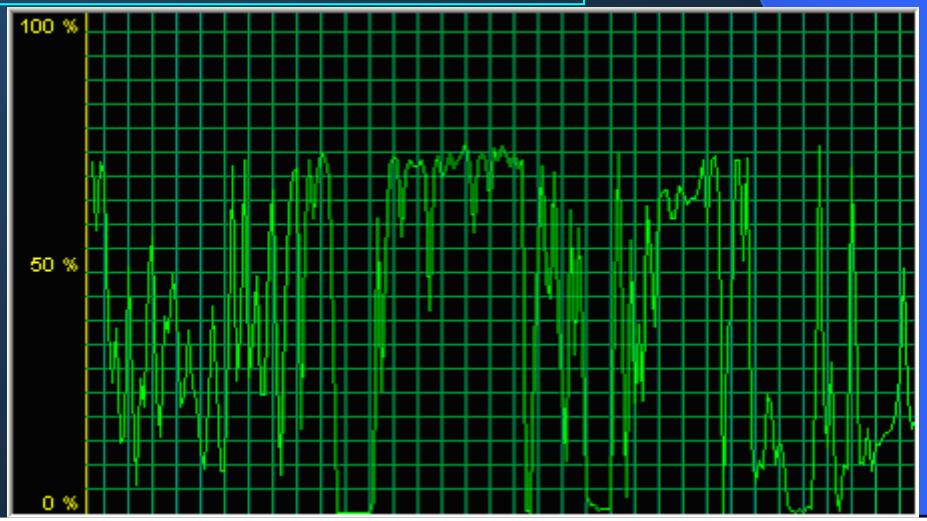
Le monitoring (1/3)



Le monitoring (2/3)

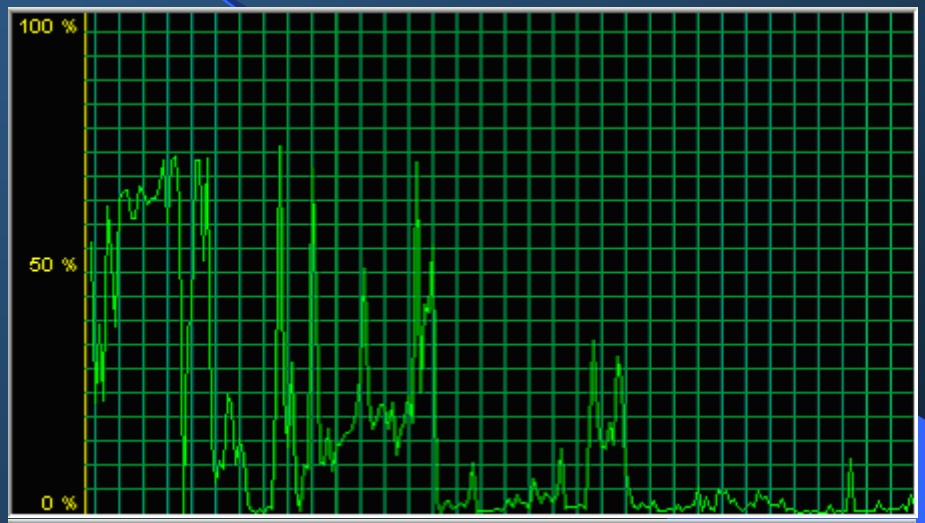


Trafic oscillant ou trafic normal ?

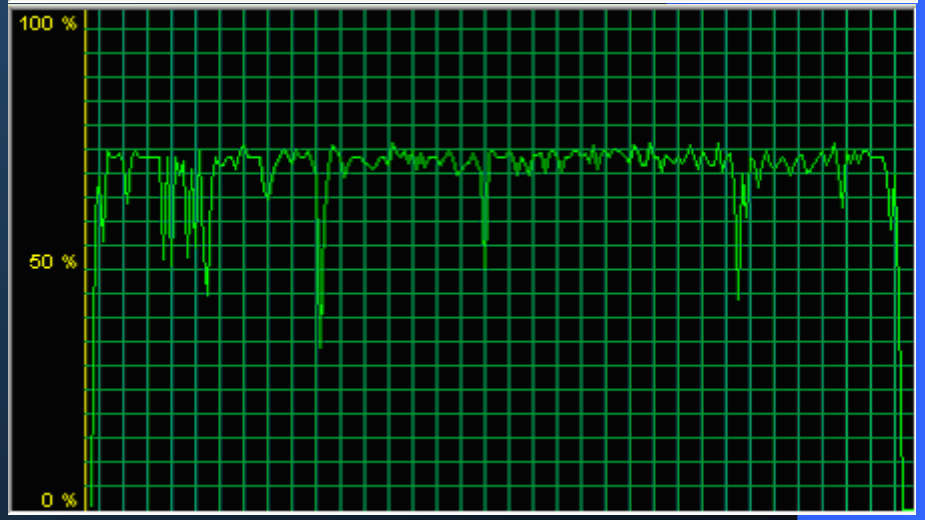


Le monitoring (3/3)

Trafic faible ou transfert de nombreux petits fichiers ?



Trafic optimum ou saturation réseau ?



Saturation émetteur ou récepteur ?

La sécurité réseau

- Les firewalls
- Les systèmes de détection d'intrusions réseaux (NIDS)
- Les réseaux privés virtuels (VPN)
- Les antivirus
- L'authentification
- Administration/supervision

Les firewalls (1/2)

Plusieurs types de firewalls existent :

- Filtrage de niveau 2 : adresses MAC ➔ identification d'une carte réseau.
- Filtrage de niveau 3 : adresses IP ➔ identification de la machine + prise en compte basique des en-têtes TCP/UDP.
- Filtrage de niveau 4 : suivi d'état ➔ prise en compte de la globalité de la communication pour effectuer le filtrage.
- Filtrage de niveau 7 : filtrage applicatif ➔ analyse des données contenues dans la trame pour identifier le protocole applicatif utilisé et sa validité.
- Firewalls authentifiants ➔ un logiciel client est présent sur le PC de l'utilisateur.
- Firewalls couplés à un IPS ➔ modification automatique des règles de filtrage suivant les remontées d'un IPS.

Les firewalls (2/2)

- Avantages.
  - Fonctionne comme un équipement réseau ➔ facile à installer.
  - Bloque un très grand nombre d'attaques.
  - Possibilité de gestion et de configuration à distance et centralisées.
  - Solution bon marché au vu de son efficacité.
- Inconvénients.
  - Problèmes avec les trafics légitimes mais exotiques.
  - Nécessite de répertorier de manière exhaustive tous les flux à autoriser.
  - De nombreuses solutions sur le marché.
  - Combiner au-moins le filtrage de niveau 3 et 4 pour être efficace.
  - Pour effectuer le filtrage, ne se base que sur les en-têtes des trames, non sur les données (sauf niveau 7).

Les systèmes de détection d'intrusions réseaux (NIDS) (1/2)

- Le NIDS est une sonde transparente dédiée à la sécurité → à différencier des sondes de monitoring.
- Analyse du trafic et étude de correspondances avec des scénarios d'attaques pré-enregistrés.
- Analyse du trafic et alarme si un comportement est « déviant ».
- Pas de contre-mesures si une attaque est détectée → voir les IPS pour une protection active.

Les systèmes de détection d'intrusions réseaux (NIDS) (2/2)

- Avantages.
  - Analyse le contenu des trames.
  - Son fonctionnement transparent peut en faire un point d'analyse réseau de choix (monitoring, …).
  - Centralisation des logs et gestion à distance souvent facilité par une console d'administration.
  - Configuration affinée au fur et à mesure du temps, sans gêne pour les utilisateurs.
- Inconvénients.
  - Étude de l'emplacement des sondes complexe.
  - Solution complexe à mettre en place.
  - Solution souvent vendue trop chère par rapport à ses fonctionnalités.
  - Administration très lourde (faux-positifs, faux-négatifs, lecture des logs).
  - L'efficacité de la solution repose sur la réactivité de l'administrateur, et sur la base de scénarios d'attaques connus par la sonde.

Les réseaux privés virtuels (VPN) (1/2)

Le VPN utilise le chiffrement des communications pour relier :

- 2 machines par l'intermédiaire d'un réseau non-sûr.
- 1 machine et un réseau sûrs, par l'intermédiaire d'un réseau non-sûr.
- 2 réseaux sûrs par l'intermédiaire d'un réseau non-sûr.

Le VPN établit une liaison entre :

- 2 réseaux IP différents par l'intermédiaire d'un troisième (répandu).
- 2 réseaux IP identiques par l'intermédiaire d'un réseau IP différent (moins répandu).
- 2 groupes de machines d'un même réseau IP (peu répandu).

Le VPN simule le comportement d'une liaison dédiée en assurant l'authentification des extrémités du VPN et l'intégrité des données.

La mise en place du VPN relève d'une étude réseau au même titre que n'importe quel ajout d'interconnexion de 2 réseaux.

Les réseaux privés virtuels (VPN) (2/2)

- Avantages.
  - Des produits pas chers et efficaces.
  - Assurance de l'intégrité, de l'identification, de l'authentification, à la fois de l'émetteur et du récepteur.
  - On peut attacher l'authentification à une machine, mais aussi à une personne, quel que soit la machine utilisée.
- Inconvénients.
  - Gamme de prix très large (de nombreux pièges).
  - De nombreuses approches ➔ compétences indispensables en cryptographie et en réseau.
  - La sécurité de cette solution repose aussi sur la bonne gestion des clefs de chiffrements.

Les antivirus (1/2)

Il existe plusieurs types de virus dont :

- Les vers : ils s'auto-propagent en utilisant le réseau.
- Les troyens : l'attaque est menée à distance par une personne malveillante qui accède à la machine par le réseau.
- Les « espions » : keylogeurs, …

Même si l'IDS détecte les attaques, l'antivirus est indispensable car il bloque le virus ***avant*** qu'il ne s'installe.

Cette protection est efficace lorsqu'elle est mise à jour très régulièrement.

Les antivirus (2/2)

- Avantages.
  - Très efficaces contre la plupart des types de virus.
  - Intervient avant même que le virus effectue son action illicite.
  - Certains produits proposent une gestion centralisée des mises à jour des postes de travail.
- Inconvénients.
  - Gamme de produits très large.
  - L'efficacité de la solution s'appuie beaucoup sur la rigueur des mises à jour des signatures.
  - Antivirus inefficace si l'attaque lui est inconnue.

L'authentification (1/2)

Identification : « dire qui on est ».

Authentification : « le prouver ».

- Par ce que l'on sait (mot de passe, pass-phrase, réponse à une question donnée, …).
- Par ce que l'on est (forme du visage, voix, empreinte rétinienne, …).
- Par ce que l'on a (badge magnétique, clef de chiffrement, tocken, …).
- Par ce que l'on sait faire (utiliser un logiciel, répondre à un évènement imprévu, …).

L’authentification (2/2)

- Avantages.
  - Non répudiation.
  - Authentification.
  - Permet d’attacher des droits d’accès à un profil, une personne, une machine, ou encore à un programme.
- Inconvénients.
  - De nombreuses solutions existent, de la plus simple (login/mdp) aux plus complexes (authentification forte).
  - L’authentification n’est généralement qu’un sous-ensemble d’une solution de sécurité.

Administration/supervision (1/2)

Les outils de sécurité, les applications, les systèmes d'exploitation remontent une quantité importante d'évènements dans les journaux systèmes.

L'administration c'est d'abord de lire ces journaux → certains outils permettent de faciliter le travail des administrateurs.

Vue globale : Homogénéisation des solutions et de la configuration → évite les sur-coûts et optimise l'administration.

Il est intéressant de compléter l'administration réseau par la supervision → réactivité, surtout en cas de panne matérielle.

Administration/supervision (2/2)

- Avantages.
  - Réactivité face à un problème.
  - Adapter une résolution d'incident au mélange « causes / effets / risques / contraintes ».
  - Vision globale de la problématique.
- Inconvénients.
  - Recherche constante des informations.
  - Bien définir la répartition des compétences et des activités pour être efficace.
  - La qualité de travail dépend fortement de la qualification de l'administrateur.

Conclusion

- Euh … qu'est-ce que je pourrais encore rajouter ?
- Évolution niveau 1 : « multiplexage optique ».
- Évolutions niveau 2 : augmentation des débits en WIFI, arrivée du WIMAX, 10 Gbps ethernet, ethernet à la conquête du MAN, CPL, mobilité.
- Évolution niveau 3 : IPv6, mobilité.
- Évolutions couches hautes : le tout IP (téléphonie, TV) et multimédia de plus en plus présent.

Questions

Bouh !