Communiquer avec TCP/IP °LAN°

EDF

Guillaume Lehmann

SEISO/ATI/PEX-T

Plan

- Introduction (5 min)
- Les modèles (20 min)
- Les couches basses (30 min)
- Les couches hautes (5 min)
- Le réseau ethernet (1h10)

pause 20 min

- Le réseau IP (1h10)
- Les protocoles de transport (1h30)

pause 20 min

- L'administration réseau (30 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, IP et TCP/UDP/SCTP. Comprendre la mise en œuvre qui en est faite à EDF.
- Posséder une base de connaissances solide sur les fonctionnalités des niveau 2, 3, 4, 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 détaillée des outils de supervision ou d'administration réseau.
- Le fonctionnement des réseaux radio, ATM, Frame Relay, RNIS, MPLS, X25, …
- Les détails superflus pour la compréhension du fonctionnement d'un protocole.
- Les cas particuliers des réseaux tels que le multicast, la VoIP ou encore la ToIP.
- L'existence des petits hommes verts.

Les modèles

- La pile OSI
- La pile TCP/IP
- La pile NetBEUI
- Parcourt de l’information

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, …

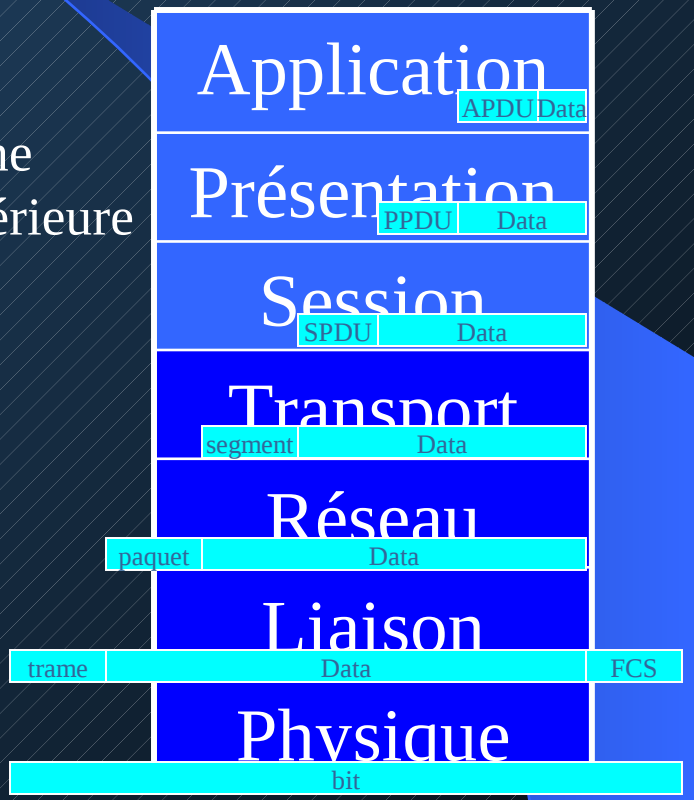
Session : ISO 8327 / CCITT X.225, rpc, NetBIOS, …

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 ancien que le modèle OSI (Department of Defense)
- 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, …

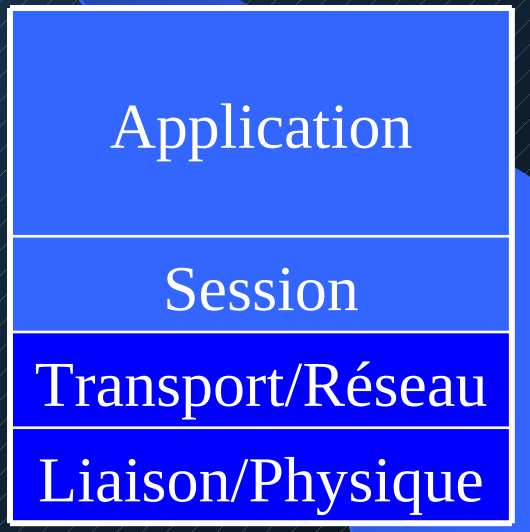
Réseau : ip, icmp (au-dessus d'ip), …

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*)

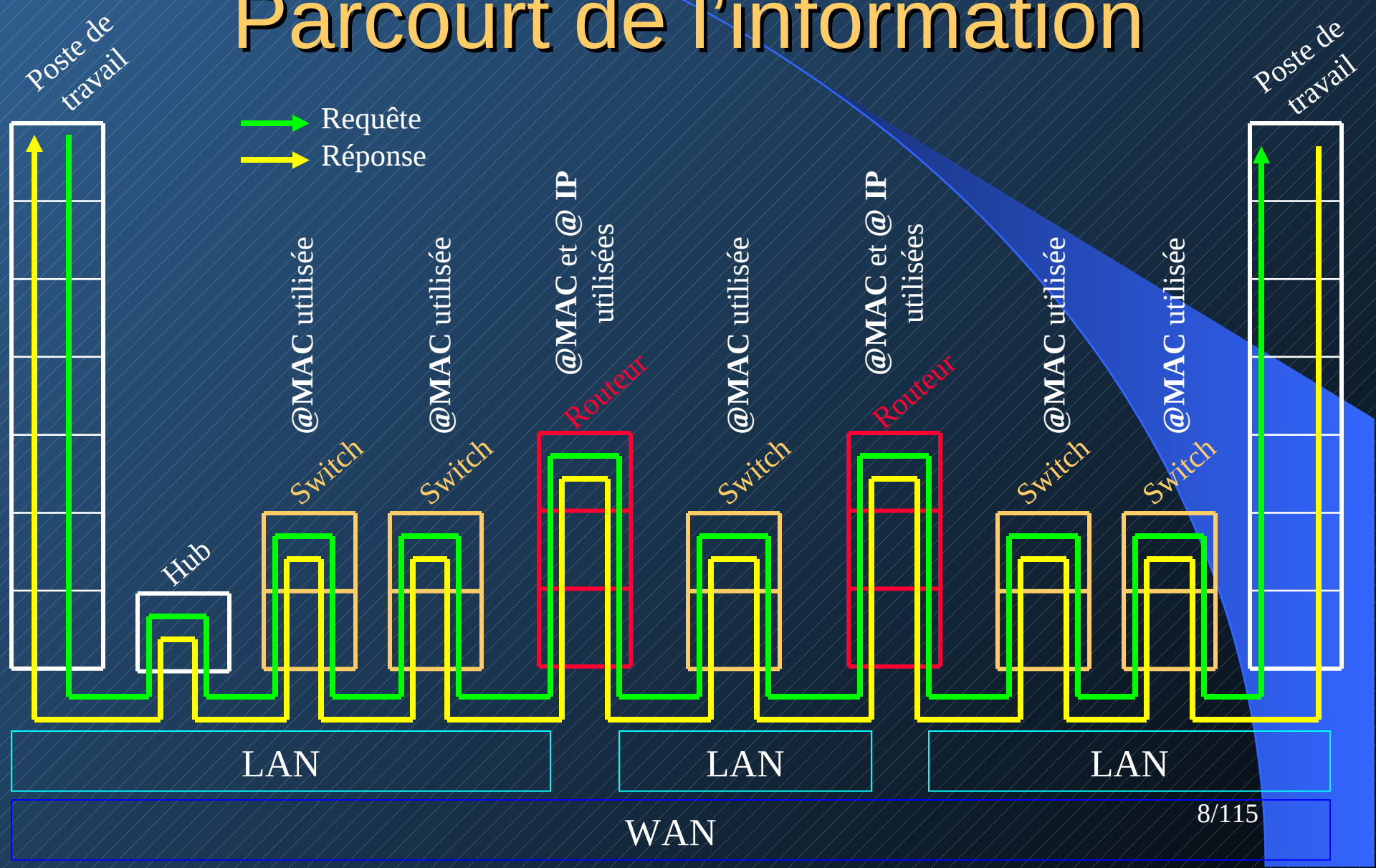
Session : NetBIOS (*Network Basic Input/Output System*)

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

NetBEUI (*NetBios Extented User Interface*)

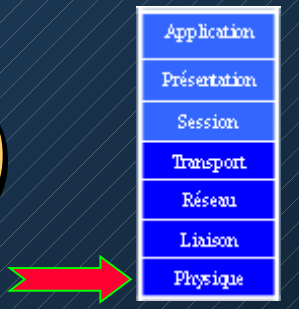
Liaison/Physique : Ethernet, token-ring, …

Parcourt de l'information



Les couches basses

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



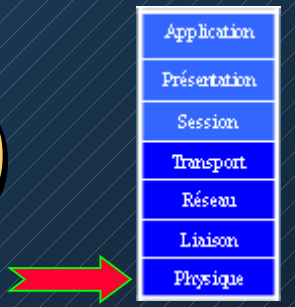
La couche physique (1/4)

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 => lasers, fibres optiques

Sont définis :

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



La couche physique (2/4)

RLE USSO

Fibres optiques monomodes ou multimodes :

- LC/SC/ST/MTRJ

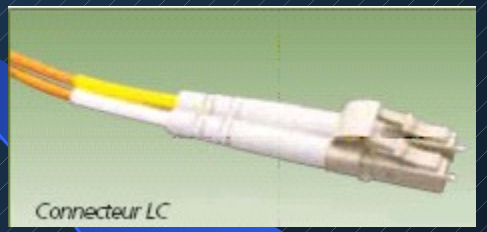
Câbles cuivres :

- RJ45 de catégorie 3 ou 5 ou 6

Matériel :

- Hubs 3Com PS40

(en voie d'extinction)


Connecteur LC


Connecteur SC sur EFE055


Connecteur MT-RJ sur EFE056


Connecteur ST sur EFE053

La couche physique (3/4)

Pour infos

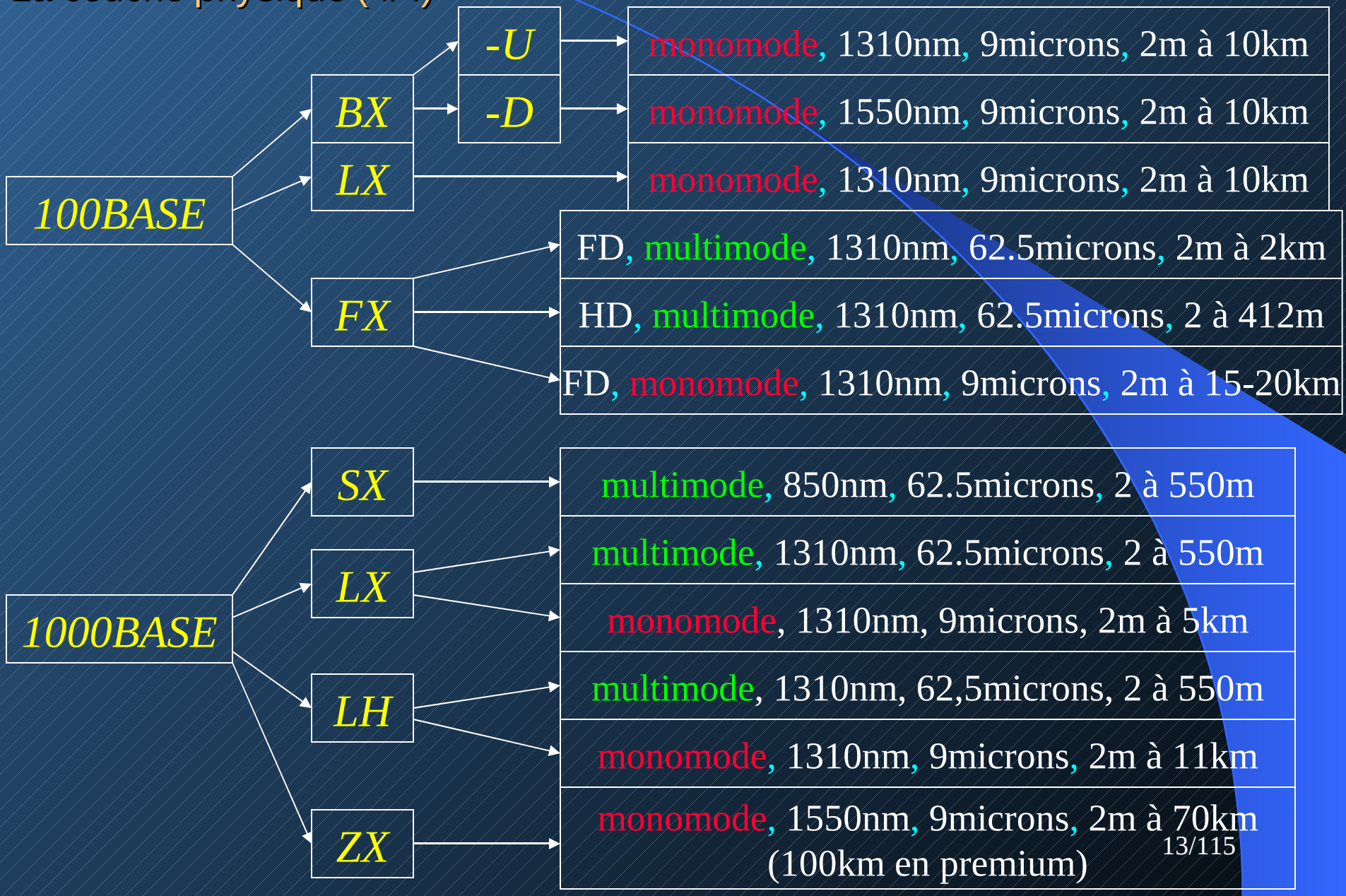
100BASETX : 100 ohms, 100m (90m Gbps), UTP (non blindé) ou STP(blindé)

- Laser : distance maximale ~ 500m
- Fibre optique :
  - SX : short wavelength
  - LX : long wavelength
  - LH : long haul
  - FD : Full-Duplex
  - HD : Half-Duplex

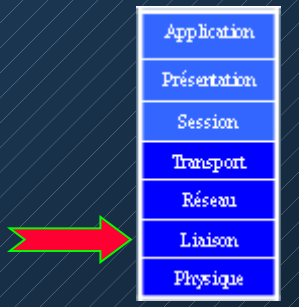
- 850 nm avec fibres multimodes 62,5/125 ou 50/125
- 1310 nm avec fibres multimodes 50/125 ou monomodes 9/125
- 1550 nm avec fibres monomode 9/125

Les couches basses

La couche physique (4/4)

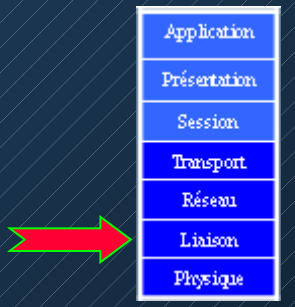


La couche liaison (1/2)



Transport des trames 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

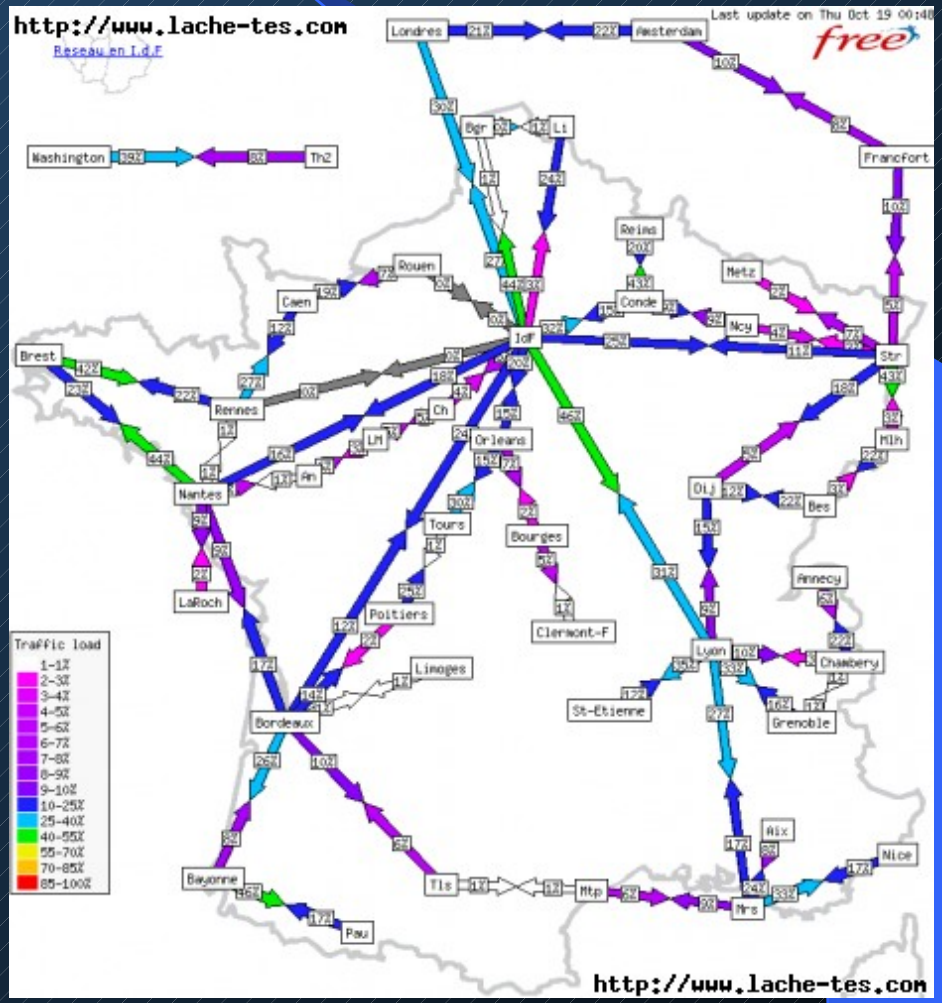
(p) : switchs de périphérie (empilables ?)
(cœ) : switchs de cœur de réseau empilables
(ch) : switchs de cœur de réseau, chassis

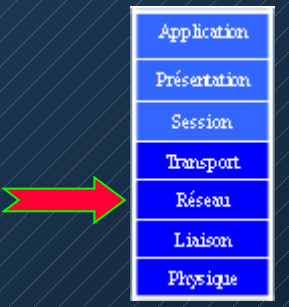
- Protocole :
  - ethernet
- Switchs ethernet 3Com :
  - SuperStack II : 1100/3300TX (p)
  - Superstack III : 3300FX (p), 4400 (p), 4050/4060/4070 (cœ), 4900/4950 (cœ)
  - Core Builder : 4007 (ch)
- Switchs ethernet Nortel :
  - Bay Stack 450 (p)
  - Accelar 1200 (ch)
- Switchs ethernet Enterasys :
  - A2, B2 (p)
  - C2 (cœ)
- Switchs ethernet Cisco :
  - Catalyst 2940/2960 (p)
  - Catalyst 3750 (cœ)

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
  - Enterasys : C2
  - Cisco : Catalyst 3750
- Routeurs :
  - Cisco (propriété et gestion par France Telecom / 9Cégetel)

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 perte 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

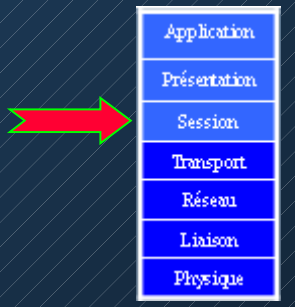
- Utilisé pour :
  - Déterminer les flux (notion de ports TCP/UDP)
  - Mettre en place de la QoS

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

Les couches hautes

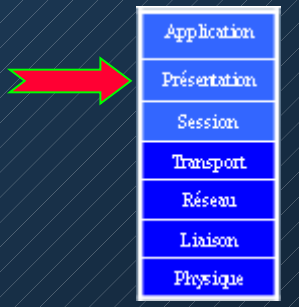
- La couche session
- La couche présentation
- La couche application

La couche session



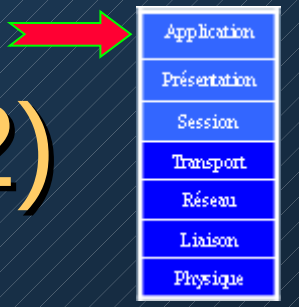
Placement de points de synchronisation, gestion des procédures d'ajournement, de fin ou de redémarrage de connexion et gestion de la continuité du service rendue aux couches supérieures

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



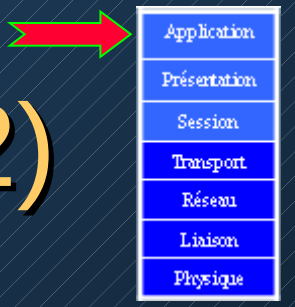
La couche présentation

Mettre en forme les données pour qu'elles 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

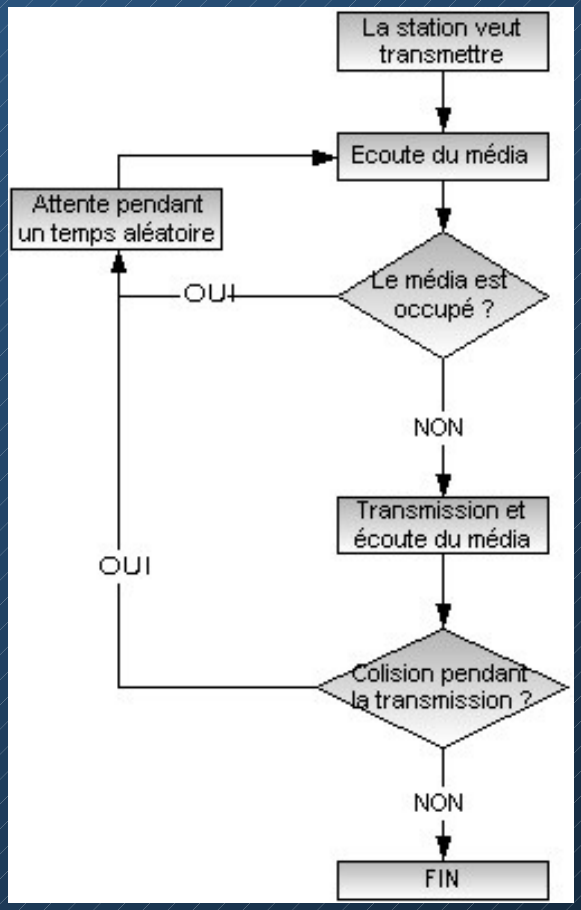
- Mail/partageDeDocuments => Lotus Notes
- Gestion de réseau Microsoft Windows
- Partage de fichiers à travers Microsoft Windows
- SNMP
- http/https
- ftp
- telnet
- ssh

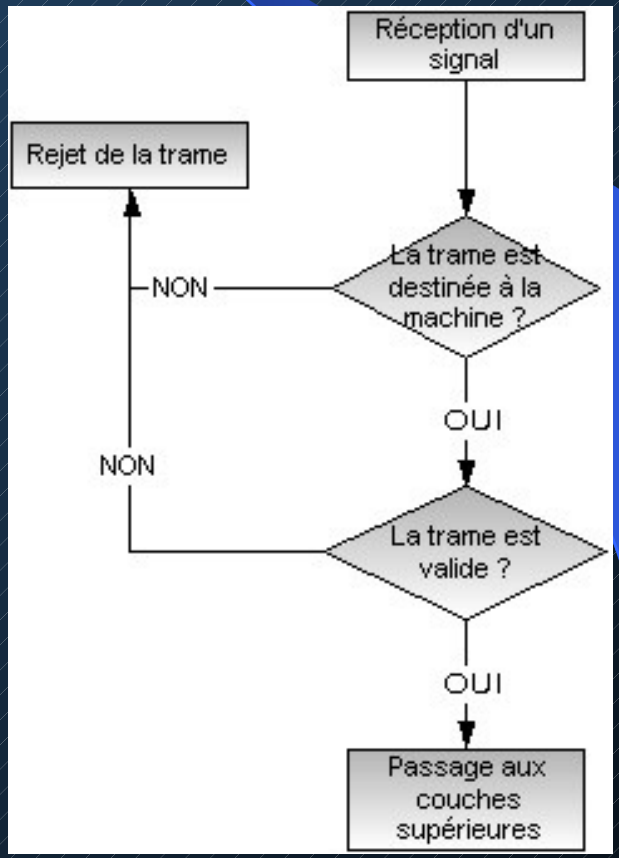
Le réseau ethernet

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

Le fonctionnement

CSMA/CD : Carrier Sense Multiple Access/Colision Detection





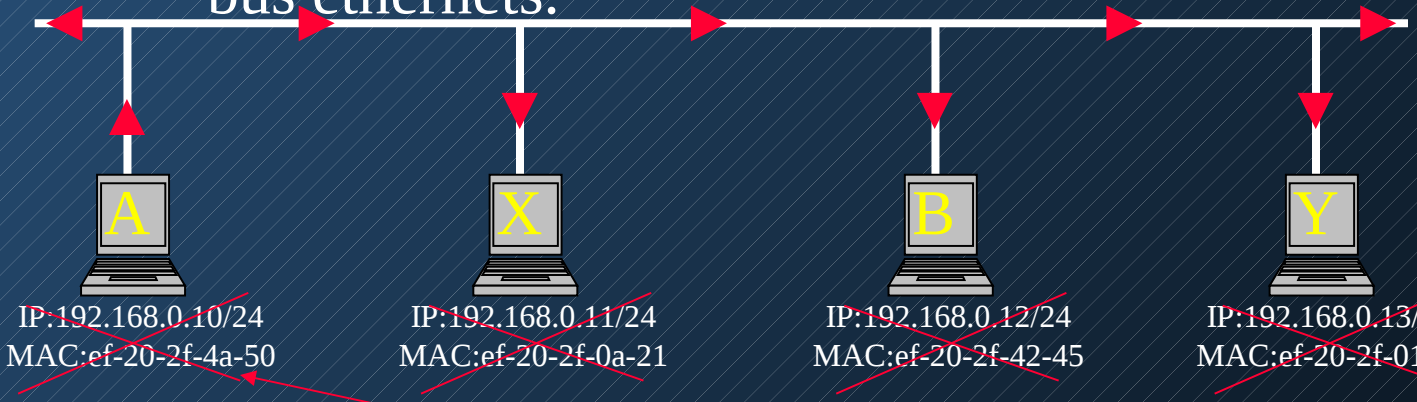
L'adressage

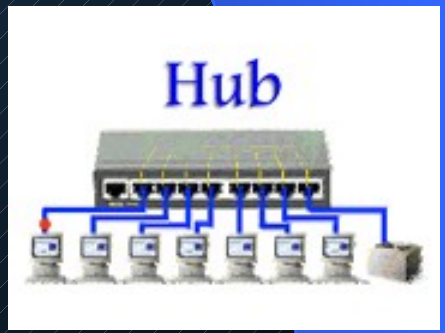
- La norme ethernet spécifie l'utilisation d'adresses physiques liées aux cartes réseaux : les adresses MAC.
- Une carte ne prend en compte que les trames qui lui sont destinées et les transmet au protocole de niveau 3 indiqué dans le champ « Type » (0x0800 pour IP). Exception pour :
  - Les trames de broadcasts
  - Les adresses multicasts qui lui ont été configurées
  - Les cartes en mode promiscuité
- Une adresse MAC sous forme hexadécimale est constituée :
  - Du bit U/L : adresse universelle attribuée par l'IEEE (0000 0000) ou adresse locale (0000 0010)
  - Du bit I/G : adresse unicast (0000 0000) ou multicast (0000 0001)
  - De l'adresse du constructeur sur 22 bits (comprend les 6 premiers bits à 0)
  - De l'adresse affectée par le fabricant sur 24 bits

@constructeur (part 1)	U/L	I/G	@constructeur (part 2)	@fabricant
6 bits à 0	0/1	0/1	-0f-23	-2c-14-34

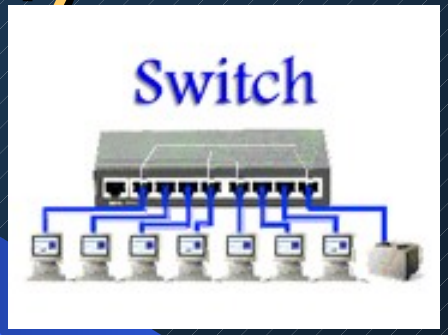
Les équipements (1/4)

- **Hubs ou répéteurs :**
  - 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 (2/4)



- **Switchs ou commutateurs :**
  - 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 équipements (3/4)

- **Switchs (suite) :**
  - Cut through : Après avoir reçu les 6 octets qui permettent de remonter les informations concernant les adresses, le switch commence à renvoyer le paquet vers le segment destinataire sans que la trame ne soit entièrement arrivée dans le switch.
  - Store and forward : Le switch sauvegarde la totalité du paquet dans un buffer, vérifie les erreurs CRC ou autres problèmes, puis l'envoie s'il est valide sinon le rejette. Si le paquet présente des erreurs, il est rejeté.
  - Fragment free : Cette méthode est moins utilisée que les précédentes. Elle fonctionne comme cut through si ce n'est qu'elle stocke les 64 premiers octets du paquet avant de l'envoyer : la plupart des erreurs et des collisions interviennent lors du temps de transmission des 64 premiers octets du paquet.

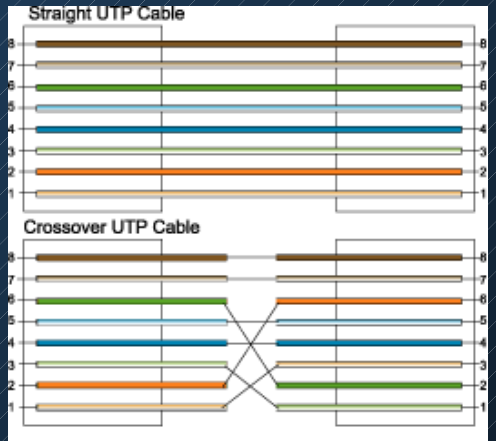
Les équipements (4/4)

Principe du pont transparent en 5 étapes.

- L’apprentissage
- L’inondation
- Le filtrage
- Forwarding
- Vieillissement (aging)

Les fonctionnalités de base

- Vitesse des ports et mode de fonctionnement :
  - Autonégociation et autosense (vitesse) ➔ échanges de trames FLP (Fast Link Pulse).
  - On peut forcer les vitesses et les modes négociables.
- Croisement logiciel du câble RJ45 :
  - (Auto-)MDIX. Même activé, il faut parfois également activer l'autonégociation afin que le MDIX soit effectif.

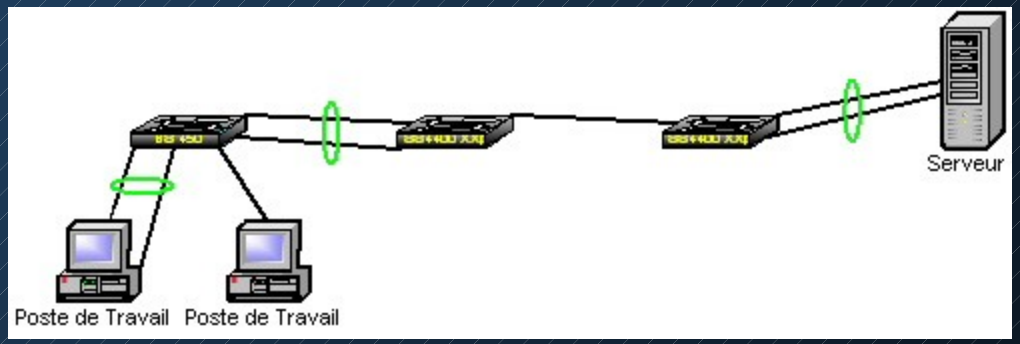


Les fonctionnalités évoluées (1/7)

- Administration et supervision :
  - Accès en telnet, ssh, web, client propriétaire, …
  - Supervision par SNMP (MIB implémentée plus ou moins complète) et RMON.

Les fonctionnalités évoluées (2/7)

- 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.

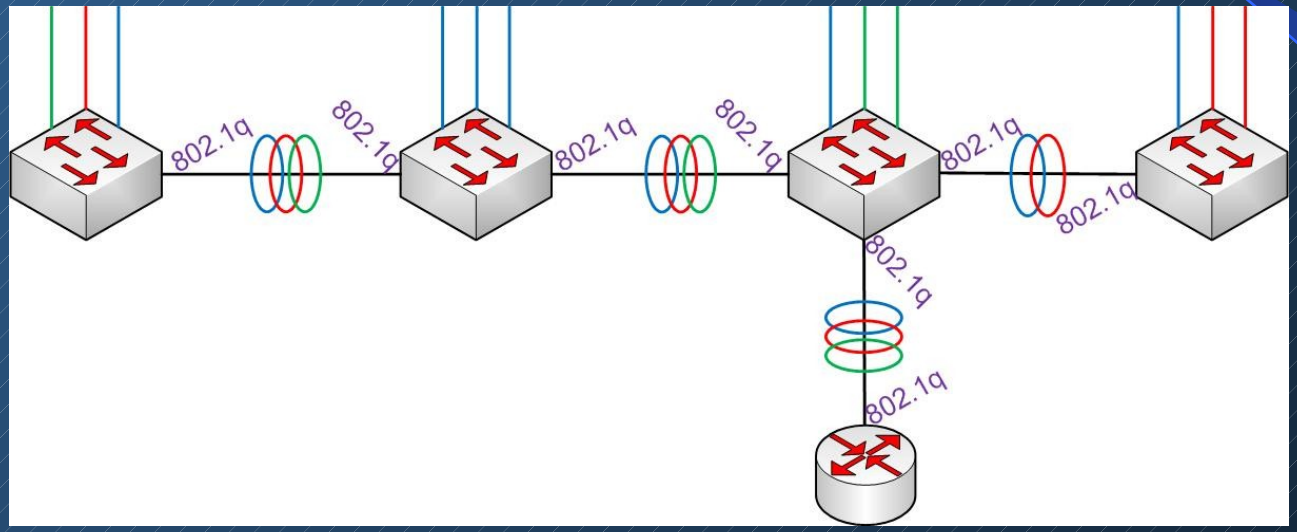


Les fonctionnalités évoluées (3/7)

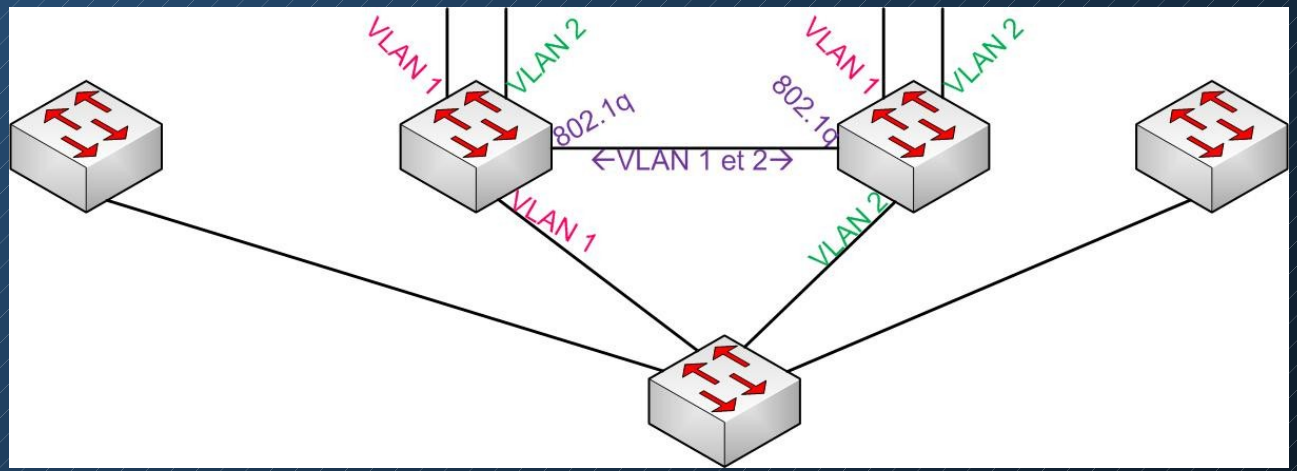
- Virtual Local Area Network (802.1q) : séparer virtuellement des réseaux physiquement identiques :
  - Affectation du VLAN par *port*, ou VLAN de niveau 1 ;
  - Affectation du VLAN par *adresse MAC* ou VLAN de niveau 2 ;
  - Affectation du VLAN par *adresse IP* ou VLAN de niveau 3 ;
  - Séparation de réseaux IP => nécessité de passer par un routeur pour aller d'un VLAN à l'autre ;
  - Tag/marquage sur un port lorsqu'il est nécessaire d'indiquer dans le paquet le VLAN d'appartenance (utile pour l'interconnexion de 2 switchs) ;
  - Les VLANs ingress et egress d'un même port peuvent être différents ;
  - Séparation des domaines de collisions, de broadcasts et de multicasts IP.

Les fonctionnalités évoluées (4/7)

Exemples d'architectures



Utilisation des tags pour transmettre plusieurs VLAN sur un même lien.



Bouclage physique sans tempête de broadcasts.

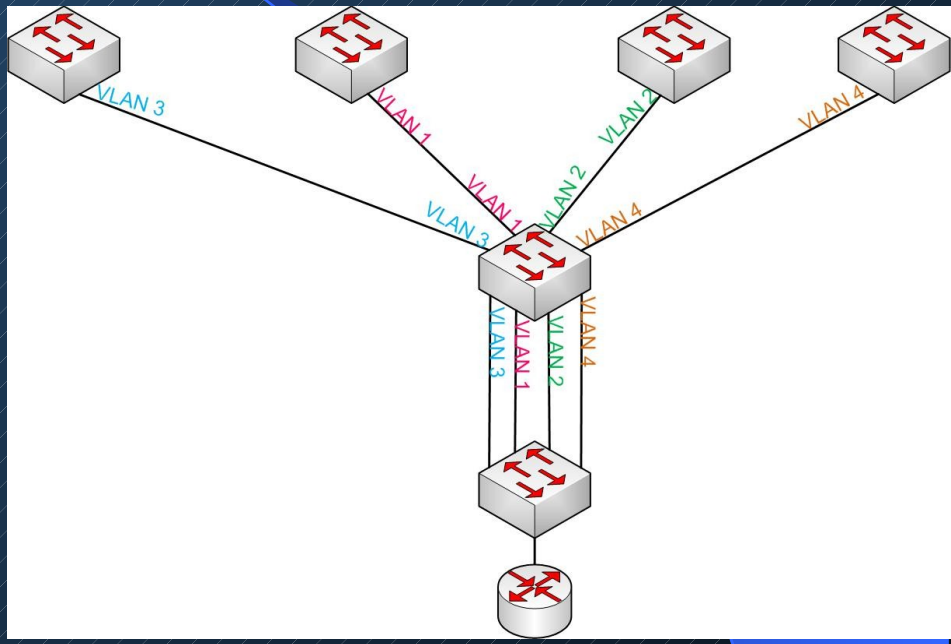
Répartition de charges vers le switch du bas.

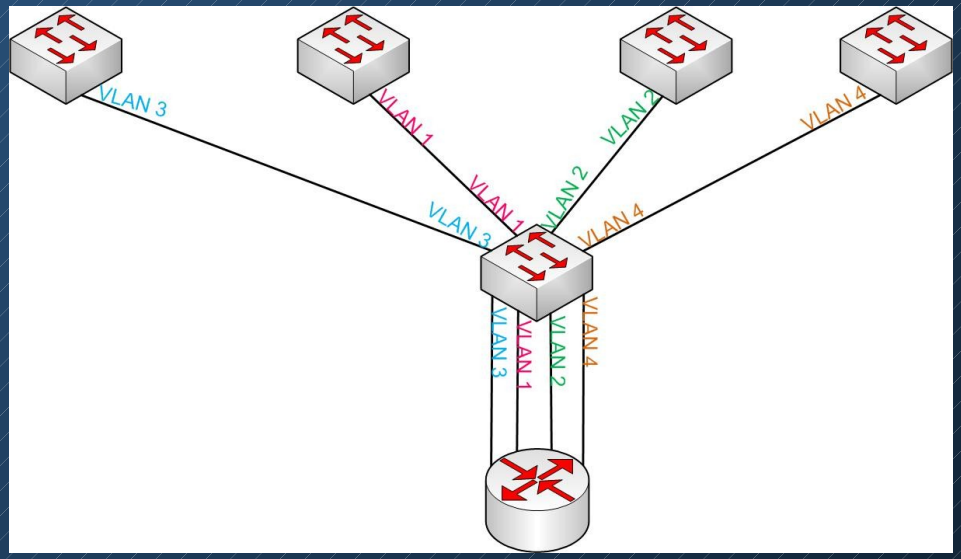
Attention aux multicasts/ broadcasts !

Les fonctionnalités évoluées (5/7)

Exemples d'architectures

Routage inter-VLAN avec une seule interface routeur. Ou 1 plage IP, plusieurs VLAN qui n'ont pas à communiquer entre eux. Attention, si un switch connecte plusieurs VLAN ➔ les multicasts / broadcasts transitent entre les VLANS !



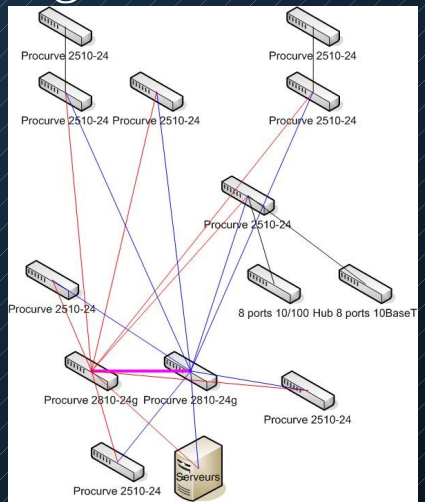


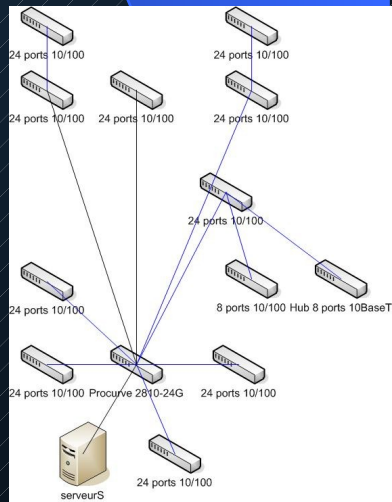
Routage entre des VLAN hermétiques.

Les fonctionnalités évoluées (6/7)

- (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.
- Multiple Spanning Tree Protocol : 802.1s
  - Plusieurs arbres actifs ➔ répartition de charge.
  - Plusieurs VLAN par spanning tree

Si on rajoute à cela la possibilité d'affecter des VLAN différents suivant que le trafic d'un port est sortant ou entrant, nous pouvons alors avoir des configurations très complexes …





Les fonctionnalités évoluées (7/7)

- 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 dans une même file d'attente plusieurs classes de services !) :
  - 0 = Best effort
  - 1 = Background
  - 2 = Réservé (spare)
  - 3 = Excellent effort (business critical)
  - 4 = Application à contrôle de charge (streaming multimédia)
  - 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

- Port Mirroring : recopie de ports (attention toutes les données ne sont pas toujours recopiées !).
- Power over Ethernet : alimentation par le câble réseau des périphériques connectés au switch 15,4 W sur 3, 4, 7, 8 en 802.3af, >30W en 802.3at sur 4 paires.

Le réseau IP

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

L'adressage (1/5)

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

  11000000.10101000.00001010.10000010 = 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.
  - CIDR (*Classless Inter-Domain Routing*).
  - VLSM (*Variable Length Subnetwork Mask*), sorte de CIDR local à l'entreprise.
- Il existe des exceptions : des plages IP réservées et d'autres à ne pas router.

L'adressage (2/5)

$2^7 + 2^6$. $2^7 + 2^5 + 2^3$. $2^3 + 2^1$. $2^7 + 2^2$

11000000.10101000.00001010.10000100 (192.168.10.132/28)

11111111.11111111.11111111.11110000 (255.255.255.240)

Partie réseau Partie machine

- La partie réseau, se sont les bits à 1 du masque sous-réseau.
- La partie machine, se sont les bits à 0 du masque sous-réseau.
- Si cette règle est respectée, les valeurs décimales possibles pour masque sous-réseau sont : 255, 254, 252, 248, 240, 224, 192, 128 et 0

Adresse réseau (1ière adresse) : …… . 10000000 ➔ 192.168.10.128

Adresses machines : …… . 10000001 à …… . 10001110 ➔ 192.168.10.129 à 142

Adresse de broadcast (dernière adresse) : …… . 10001111 ➔ 192.168.10.143

L'adressage (3/5)

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) :

00000000.00000000.00000000.00000000 à 01111111.00000000.00000000.00000000

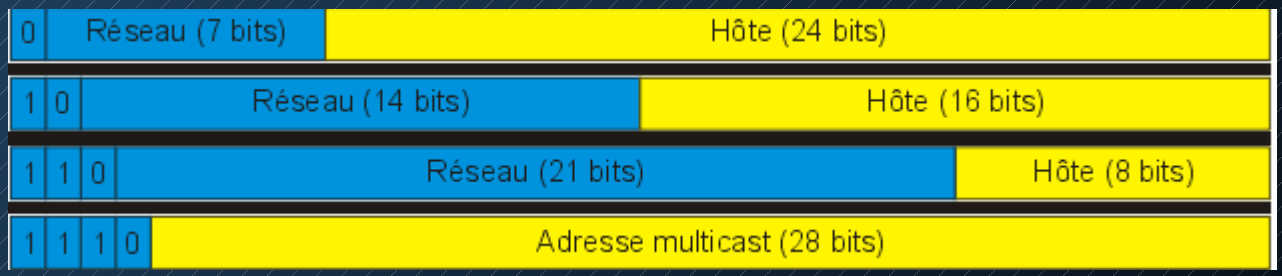
  - Classe B : réseaux 65534 machines max (de 128.0.0.0 à 191.255.255.255) :

10000000.00000000.00000000.00000000 à 10111111. 11111111.00000000.00000000

  - Classe C : réseaux de 254 machines max (de 192.0.0.0 à 223.0.0.0) :

11000000.00000000.00000000.00000000 à 11011111.11111111.11111111.00000000

  - Classe D : adresses multicasts
  - Classe E : réservée à des usages expérimentaux



L'adressage (4/5)

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

→ Plage IP : 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

→ Plage IP : 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

→ Plage IP : 192.168.8.0 → 192.168.11.255

L’adressage (5/5)

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 (1/2)

- Correspondance entre l'adresse MAC (adresse matérielle) 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.

ARP/RARP (2/2)

0 à 7	8 à 15	16 à 23	24 à 31
Hardware type (01 pour eth)		Protocol type (0x0800 pour IP)	
Hardware Address Length (06 pour eth)	Protocol Address Length (04 pour IPv4 et 16 pour IPv6)	Operation (01 pour request, 02 pour reply)	
Sender Hardware Address			
Sender Protocol Address (@IP)			
Target Hardware Address (que des 1 si request)			
Target Protocol Address (@IP)			

DHCP/BOOTP (1/3)

- 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 réseaux plus ou moins complète.

DHCP/BOOTP (2/3)

Demande d'adresse IP réussie

- DHCPDISCOVER (pour localiser les serveurs DHCP disponibles, port 67)
- DHCPOFFER (réponse des serveurs à un paquet DHCPDISCOVER. Contient les premiers paramètres IP. Port 68)
- DHCPREQUEST (requêtes diverses du client pour par exemple accepter l'adresse IP proposée par un serveur et avertir les autres serveurs de l'offre choisie par le client parmi plusieurs, ou encore pour prolonger son bail)
- DHCPACK (réponse du serveur qui contient des paramètres, bail et adresse IP du client)
- DHCPNAK (réponse du serveur pour signaler au client que son bail est échu 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, il a déjà son adresse IP)

DHCP/BOOTP (3/3)

Toute adresse IP délivrée par un serveur DHCP l'est pour un temps donné : c'est le bail. Lorsqu'on arrive à T1, le client demande en unicast le renouvellement du bail. Sans réponse du serveur, arrivé à T2 le bail est échu et le client doit redemander une adresse par diffusion. Si le client n'a toujours pas de nouvelle adresse IP, alors il doit désactiver son adresse et ne peut plus communiquer.

Longueur du bail : Sur un réseau où les machines se branchent/débranchent souvent, il faut donner des bails courts pour éviter d'épuiser inutilement le pool d'adresse IP.

Sur un réseau où les machines restent longtemps connectées, il faut préférer des bails plus longs afin de ne pas surcharger le réseau avec les broadcasts des DHCPDISCOVER/DHCPOFFER/DHCPREQUEST.

Gestion avancée avec DHCP : Il est possible d'affecter une adresse IP libre choisie au hasard ou de configurer dans le serveur des couples @IP/@MAC. Il est également possible d'affecter les adresses IP en fonction du réseau d'origine de la requête, de mettre à jour un DNS.

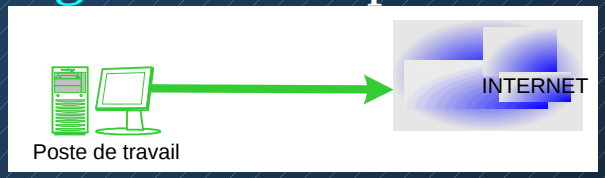
Client et serveur DHCP sur des segments différents : Implémenter un relais DHCP ou un UDP helper sur le routeur du site client.

Paramètres que DHCP peut fournir au client : RFC 2132.

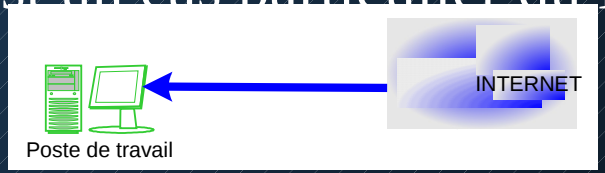
La translation d'adresse (1/3)

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.

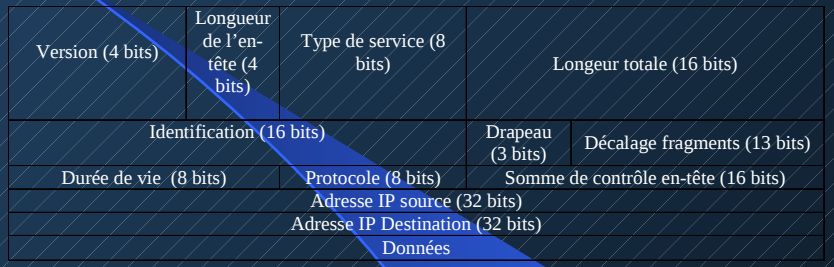


- **Le DNAT (Destination NAT) :**
  - Changer l'adresse IP et/ou le port de la destination.
  - La redirection est un cas particulier du DNAT.



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 des domaines de 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.

Routage sur les PC

Routage sur les équipements réseaux

Routage statique

Routage dynamique

Innondation

Interior Gateway Protocol

(RIP, OSPF, EIGRP)

Exterior Gateway Protocol

(BGP)

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)*

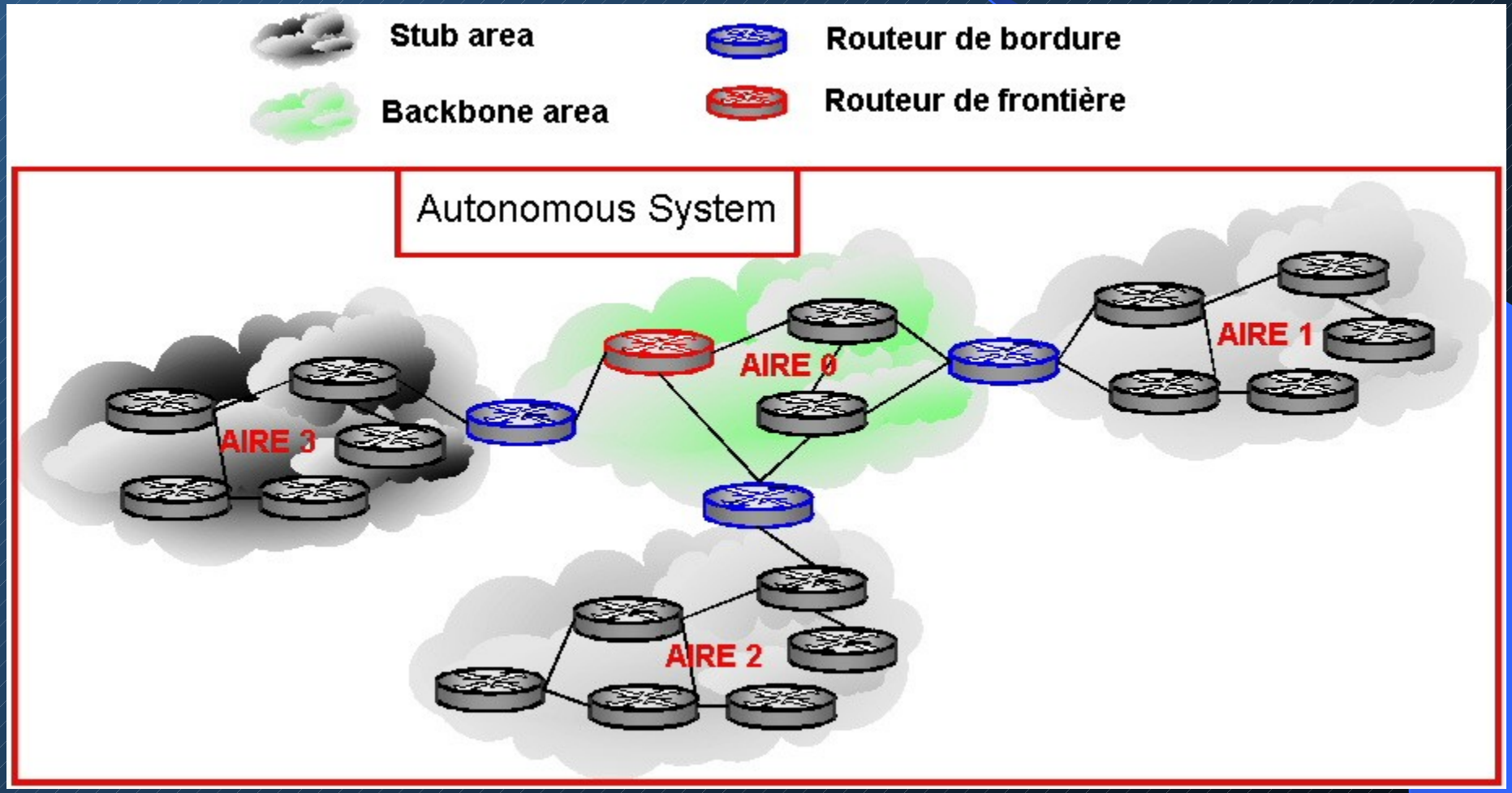
- 15 sauts maximum. Une route de 16 sauts est considérée comme coupée.
- Par défaut, 1 saut = 1 routeur.
- Protocole dépassé, mais encore présent de part sa facilité de mise en œuvre et de compréhension.

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'adresses) et que ces adresses soient 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 reconnu par les organismes de normalisation malgré sa valeur technique. Implémentation existante sous d'autres plateformes (cf. UCARP).

Les protocoles de transport

- TCP
- UDP
- SCTP
- DCCP

TCP (1/11)

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 ports source et destination (0-1023, 1024-49151, 49152-65535) ;
  - Un checksum ;
  - L'émission d'un ACK ;
  - Suivi d'un numéro de séquence des données.
- Protocole en mode connecté.

TCP (2/11)

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 données spéciale dans la zone de données du segment TCP.
- SYN (*synchronisation*) : utilisé lors de l'établissement de la connexion.
- ACK (*acknowledgement*) : accusé de réception.
- RST (*reset*) : réinitialisation ou fin brutale de la connexion.
- FIN (*finalize*) : terminer la connexion.

TCP (3/11)

Adaptation du débit (1/2)

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

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

TCP (4/11)

Adaptation du débit (2/2)

4 algorithmes utilisés dans TCP pour adapter les flux

- Slow-start (démarrage progressif) : découverte de la qualité de la liaison (on envoie 1 puis 2 puis 4 puis … trames, à la taille *mss*, entre 2 ACK. Si pertes ou cwnd >= sstresh, passage à …
- Congestion avoidance (protection contre la congestion) : moins agressif, augmente le débit plus doucement depuis le *slow-start treshold*. Si perte détectée précédemment, sstresh = (fenêtre d'envoi lors de la congestion) /2. Nouveaux algorithmes plus performants pour l'augmentation de débit.
- Fast retransmit (détecter la perte ponctuelle d'un paquet et le renvoyer) : Si le ACK reçu est le 2^{ième} du même type, peut-être qu'une paquet a été perdu. C'est certain, au 4^{ième} ACK identique reçu. Alors : sstresh = cwnd /2. Réémission du paquet perdu. Ensuite, passage à …
- Fast recovery (recalculer la bonne fenêtre de transmission) : cwnd = (sstresh /2) + 3 x taille_seg. Ensuite, pour chaque nouveau ACK dupliqué qui continuerait à arriver : cwnd = cwnd + 1 x taille_seg. Si ACK de toutes les données : cwnd = sstresh, sinon cwnd = cwnd – (Nb segments acquittés) pour ACK partiel.

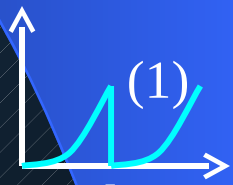
TCP (5/11)

Détection de pertes de paquets

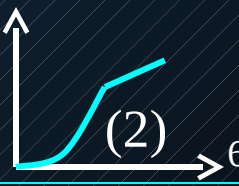
- Alarme RTO (Retransmit Time Out) : timer à l'émission épuisé.
- Duplication des ACK : l'émetteur reçoit les segments n, n+2 et pas le n+1 → il envoie le ACK pour n pour chaque segment reçu en trop.

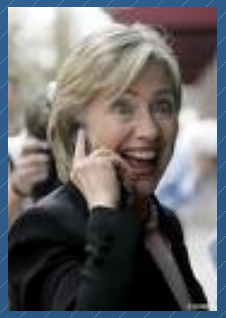
Retransmission

2 mécanismes de détection → 2 types de pertes différents → Comportements de l'émetteur différent.



- Dans le premier cas, c'est peut-être un reroutage ou un changement de topologie entre les 2 extrémités → Qualité de la liaison à redécouvrir (1).
- Dans le second cas, c'est peut-être une congestion (un routeur intermédiaire supprime des paquets) → L'émetteur réduit le débit (2).





TCP (6/11)

Fonctionnement (1/5)

A

B

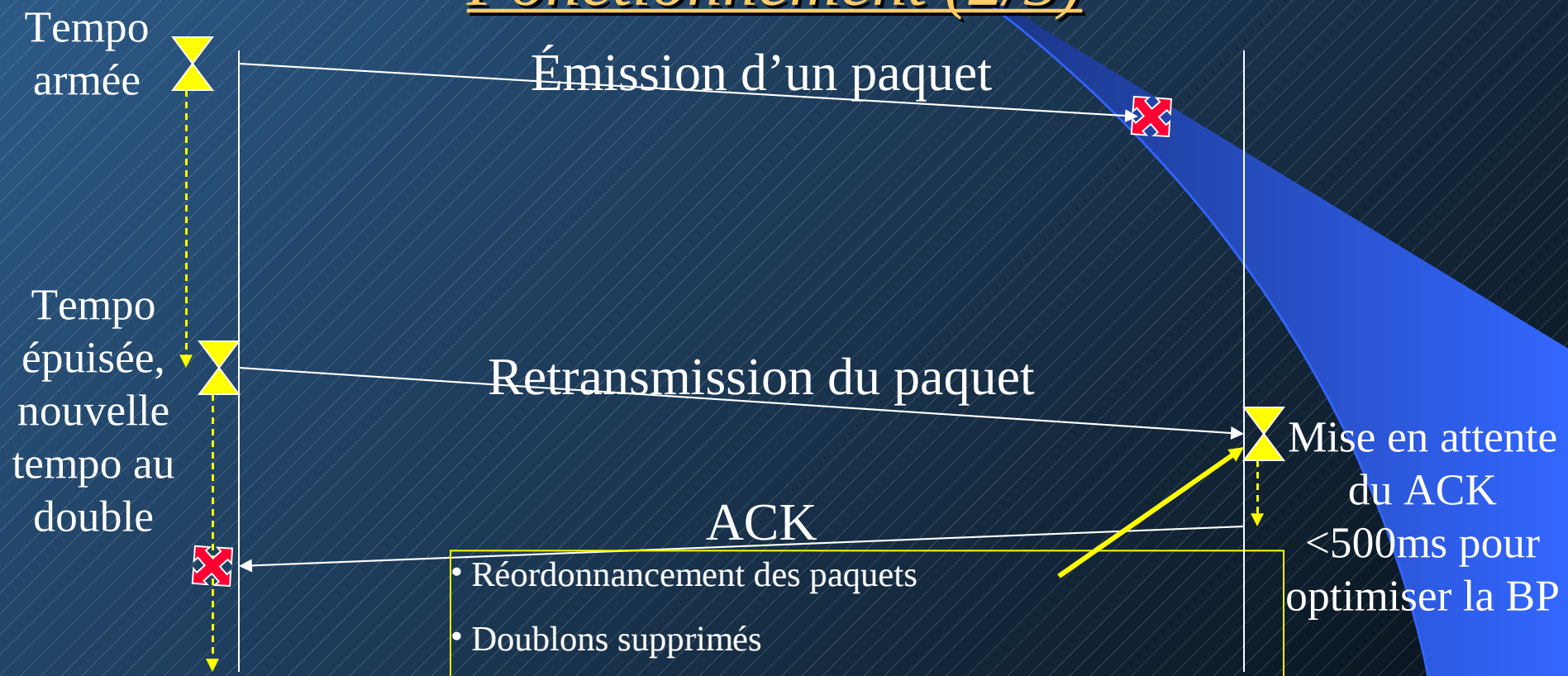
SYN (A→ B)

SYN (B → A) + ACK (A → B)

ACK (B → A)

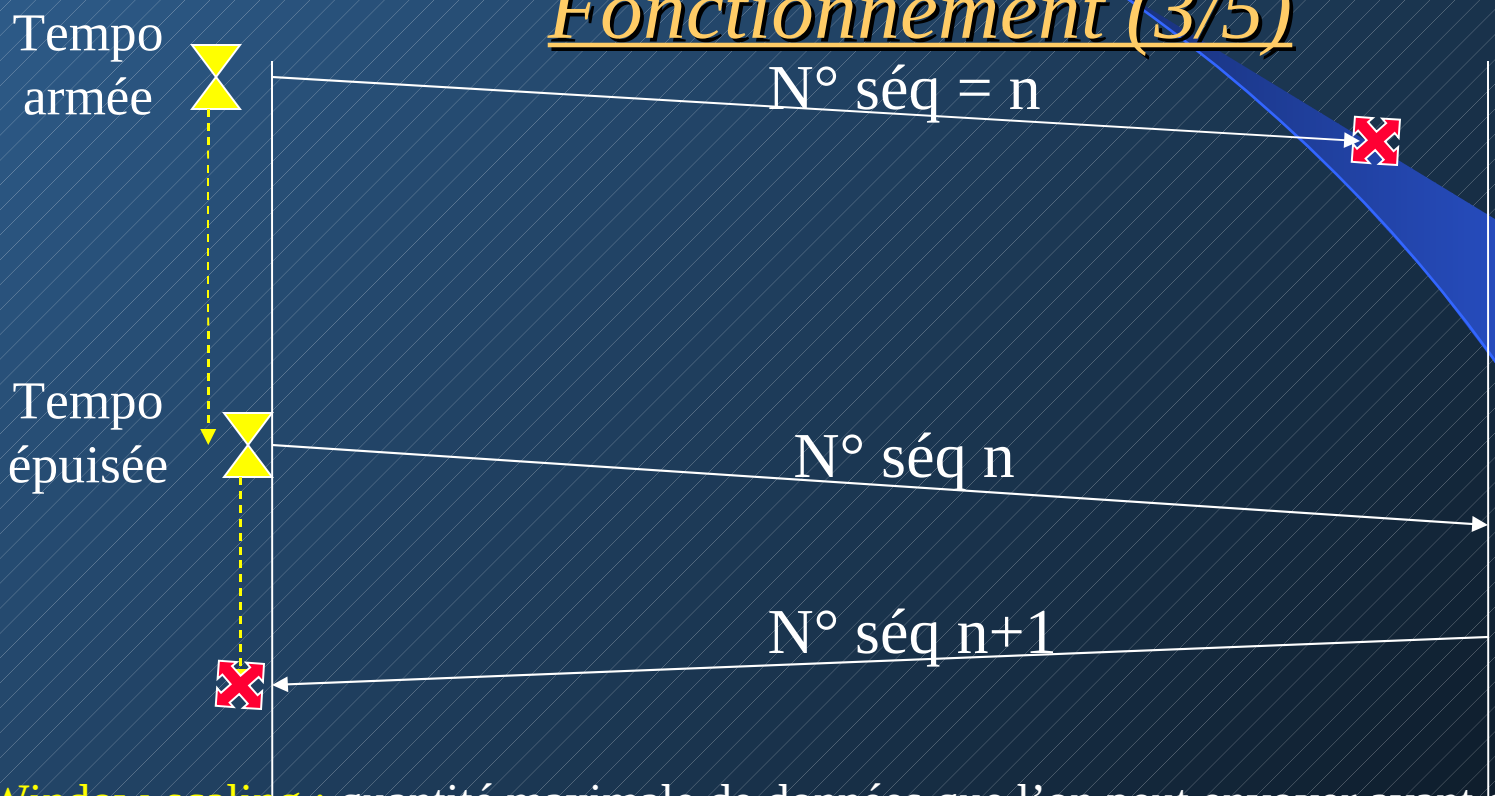
TCP (7/11)

Fonctionnement (2/5)



TCP (8/11)

Fonctionnement (3/5)



Window-scaling : quantité maximale de données que l'on peut envoyer avant de recevoir un ACK

Slow-start streshold : limite de passage du mode slow-start à congestion avoidance

TCP (9/11)

Fonctionnement (4/5)

Fast retransmit activé car doublon du ACK n. Pb de retard ou perte de n+1 ?

4ième ACK n, donc n+1 est bien perdu, n+2 à n+4 reçus. cwnd = (sstresh /2) + (3 x taille_segment)

Fast recovery : cwnd = cwnd + (1 x taille_segment).

TCP (10/11)

Fonctionnement (5/5)

A

B

A et B peuvent transmettre des données

FIN (A → B)

ACK (A → B)

Transfert de données possible ssi c'est à l'initiative de B

FIN (B → A)

ACK (B → A)

Clôture dans les 2 sens

Clôture d'une connexion

TCP (11/11)

L'histoire de TCP

1988 TCP Tahoe = slow start + congestion avoidance + fast retransmit

1990 TCP Reno = Tahoe + Fast recovery

1994 TCP Vegas (rtt basé sur l'acquittement du dernier paquet envoyé)

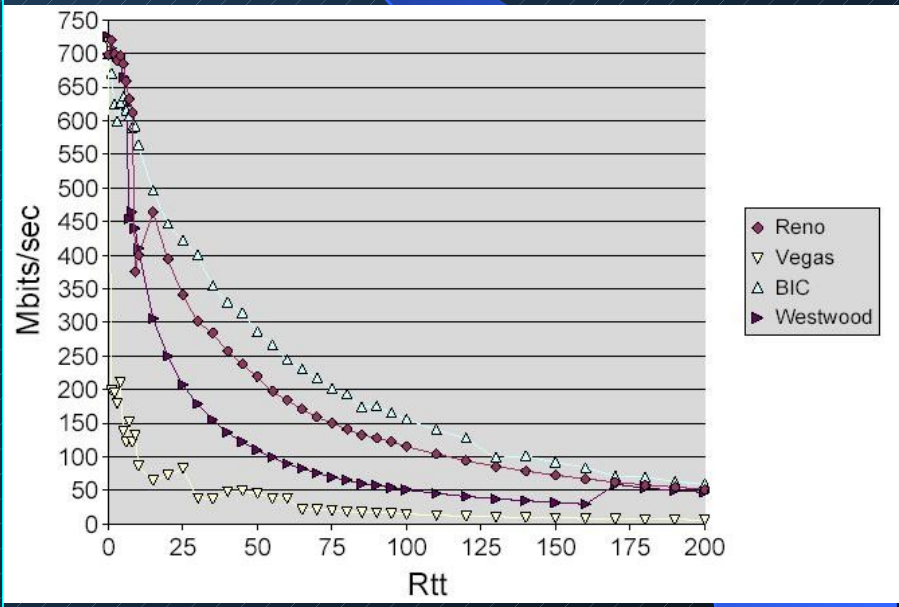
1994 ECN (Explicit Congestion Notification)

1996 SACK (Selective ACKnowledgment)

1999 TCP NewReno = Reno + adaptation aux pertes successives (Fast recovery optmisés, sans SACK)

TCP BIC (Binary Increase Congestion control)

TCP CUBIC (à base d'une fonction cubique)



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

SCTP (1/9)

Similitudes

Stream Control Transmission Protocol, RFC 4960 (septembre 2007). La première RFC (2960) date d'octobre 2000.

Un paquet SCTP invalide est silencieusement détruit.

	UDP	TCP	SCTP
Mode	Non-connecté	Connecté : établissement de la connexion en 3 temps	Connecté : établissement de l'association en 4 temps. Échange de données dès le 3ième message (COOKIE ECHO). Échange de cookie pour la sécurité.
SYN attack	-	Sensible à cette attaque.	Protection par l'utilisation de COOKIE.
Assurance de livraison (fiabilité)	Aucun acquittement des messages, aucune assurance de livraison	Acquittement des messages pour assurer la transmission. L'acquittement sélectif est optionnel dans TCP	Acquittement des chunks pour assurer la transmission. L'acquittement est sélectif : seuls les chunks erronés sont retransmis

SCTP (2/9)

Similitudes

Ordonnancement	Non-garanti.	Garanti.	Au choix. Même non-garantis, les messages arrivant dans le désordre gardent une assurance de livraison.
Adaptatif à la bande-passante	Non.	Oui (contrôle de congestion réseau ou récepteur).	Oui (contrôle de congestion réseau ou récepteur).
Clôture	-	Clôture partielle de la connexion possible (half-closed).	Clôture totale.
Gestion par …	Paquet	Octet	Paquet
Utilisation des ports source et destination	Oui	Oui	Oui
Checksum	16 bits	16 bits	32 bits

SCTP (3/9)

Nouveautés

Une communication entre 2 hôtes est une association entre 2 terminaux d'un réseau.

Un paquet SCTP est constitué d'un en-tête commun et d'un ou plusieurs *chunk* (13 types différents + les *chunks* réservés) contenant des informations de contrôle ou des données. Seuls les *chunks* INIT, INIT ACK et SHUTDOWN COMPLETE ne peuvent être groupés avec d'autres.

On peut agir sur un flux sans impacter les autres flux d'une même connexion.

1 association = plusieurs flux

Une avancée majeure de SCTP est la possibilité de communications multi-cibles (multi-diffusion, multi-homing), où une des extrémités de la (ou les) association est constituée de plusieurs adresses IP.

Plusieurs chemins pour joindre le destinataire.

1 terminal = [@IP1, @IP2, …:port]

(extension : ASCONF) Possibilité de reconfiguration dynamique des adresses ➔ mobilité, clusters.

SCTP (4/9)

Implémentation

En théorie, SCTP est plus performant qu'UDP et TCP.

En pratique, les implémentations actuelles sont moins performantes que celles pour TCP … à fonctionnalités égales.

Conversion aisée d'un programme TCP sur SCTP (primitives similaires).

Empreinte réseau supérieure à TCP (20 octets) et UDP (8 octets) : en-tête commun de 12 octets, et *chunks* DATA hors données de 16 octets. Certains *chunks* sont moins volumineux que DATA.

L'agrégation des flux contre-balance cette lourdeur sur des réseaux à haut-débits.

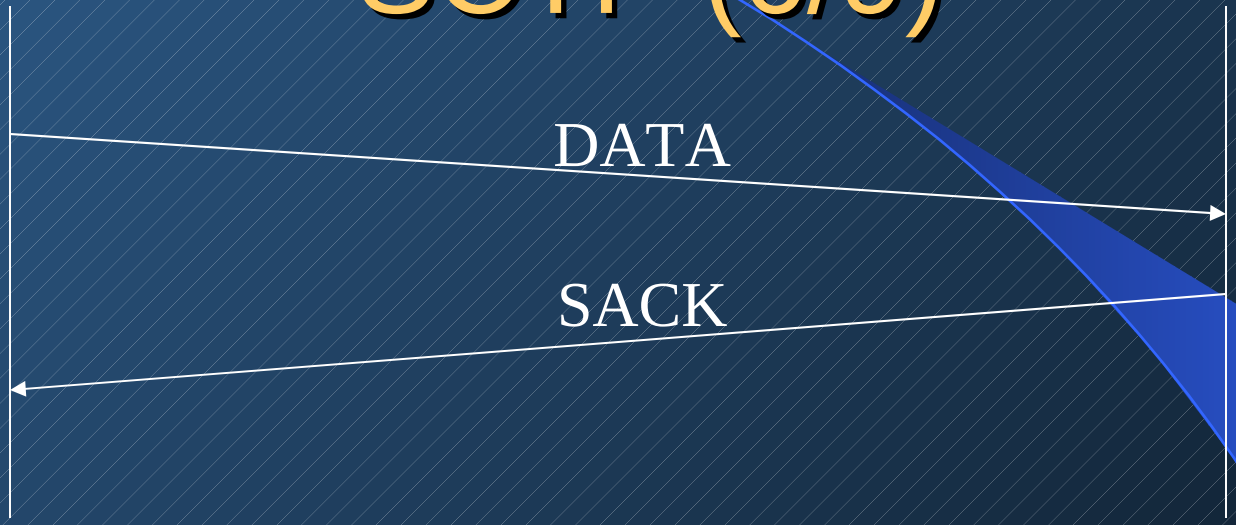
SCTP (5/9)

Cookie envoyé pour la sécurité

Des données peuvent être transmises

Établissement d’une association

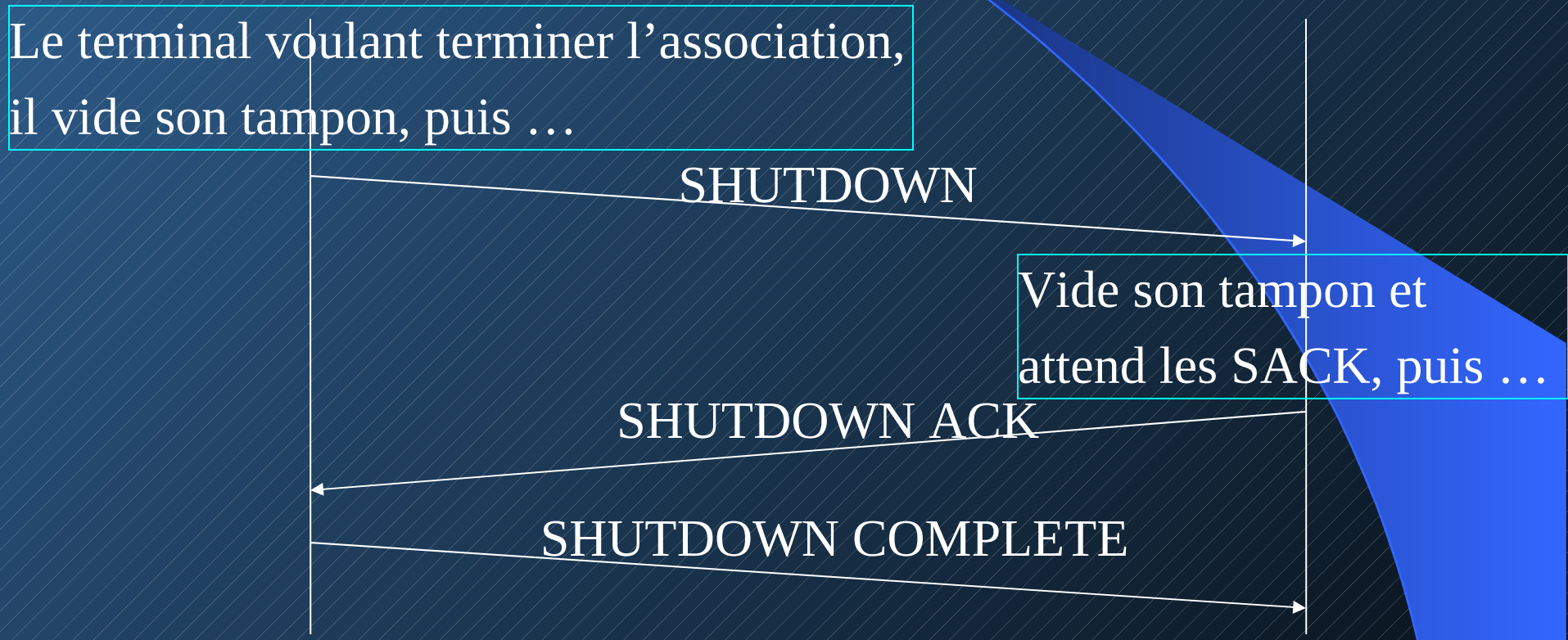
SCTP (6/9)



HEARTBEAT, HEARTBEAT ACK et ERROR sont également des paquets de contrôle fréquemment utilisés.

Plusieurs *chunks* différents (DATA, ACK, HEARTBEAT, ERROR, etc.) peuvent être groupés dans un même paquet. Le schéma ci-dessus représente donc qu'une partie de chaque paquet échangé.

SCTP (7/9)



Clôture normale d'une association

SCTP (8/9)

Clôture brutale d’une association

SCTP (9/9)
Adapte sa bande-passante

Fonctionnalité ECN (chunk ECNE).

Acquittement sélectif : SACK N acquitte tous les morceaux jusqu'à N, champ Gap Ack Blocks pour un acquittement sélectif ensuite.

Limitation de bande-passante par le récepteur

a_rwnd (Advertised receiver window credit) : Le récepteur indique à l'émetteur combien d'octets il est encore prêt à recevoir.

Limitation de bande-passante dans le réseau

cwnd (Congestion window) : nombre d'octets que l'émetteur peut envoyer sans attendre un SACK des premiers.

sstresh (Slow-start threshold) : choix d'un algorithme de résolution de congestion (même algorithmes que TCP) :

- Slow start algorithm
- Fast retransmit
- Fast recovery

DCCP

Datagram Congestion Control Protocol, RFC 4340 (mars 2006).

- Détection des pertes de paquets grâce à un mécanisme d'accusé de réception.
- Transport non fiable : détection des pertes mais aucun mécanisme de récupération (retransmission) n'est mis en œuvre.
- Mode connecté.
- Contrôle de la congestion.

Pour suivre l'évolution de la normalisation : http://www.read.cs.ucla.edu/dccp/

L’administration réseau

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

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 de l’utilisateur.
  - Réactivité et définition de procédures pour minimiser les impacts d’un incident réseau.

Les activités (2/2)

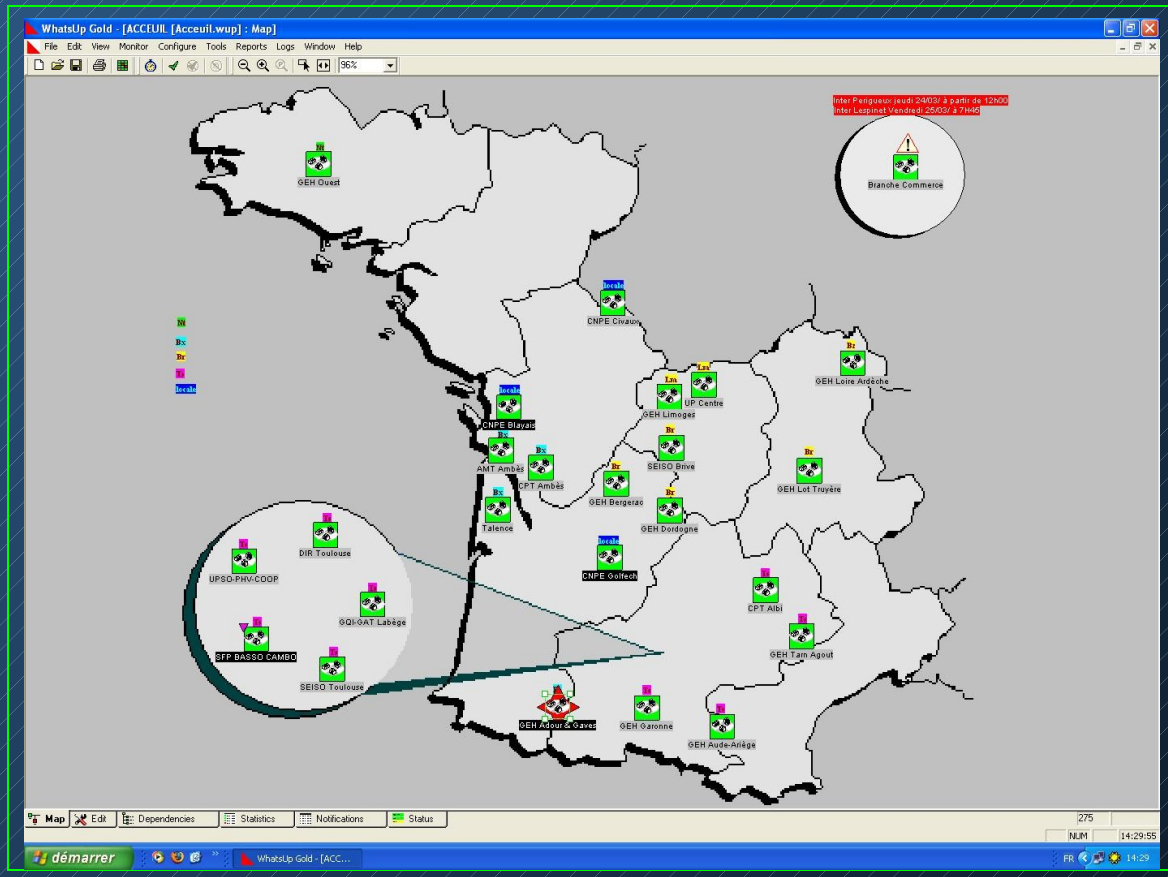
- La gestion du matériel réseau
  - Pour la gestion des stocks de réserve
  - Pour la gestion du matériel en production
  - Pour la gestion des garanties
- La documentation (attention aux extrêmes !)
  - Procédures d’interventions sur incidents
  - Procédures d’interventions programmées
  - Documentations 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, arp -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, ssh , web, client propriétaire, accès par port console, tftp

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

Elle s’appuie essentiellement sur icmp, SNMP et des connexions TCP pour tester les services

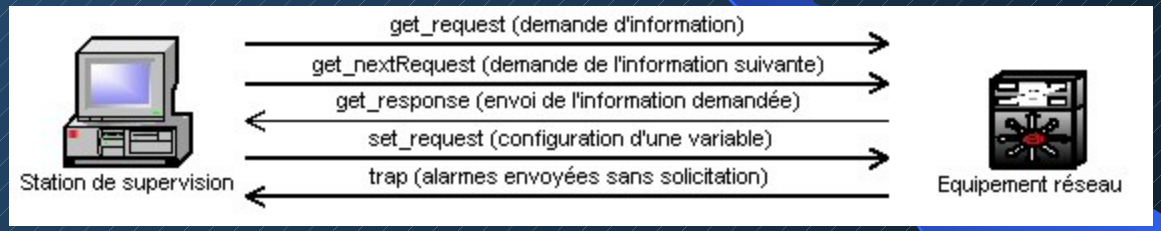


La station de supervision est l’outil principal

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

SNMP (Simple Network Management Protocol)

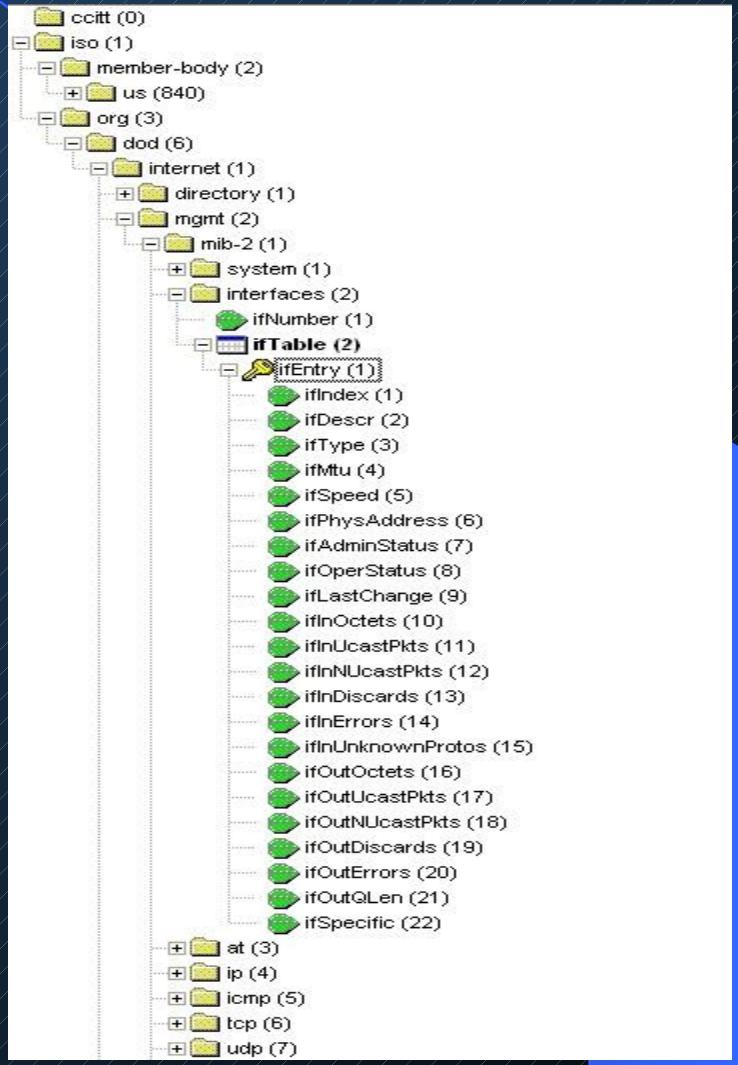
- 5 types de trames :



- 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)

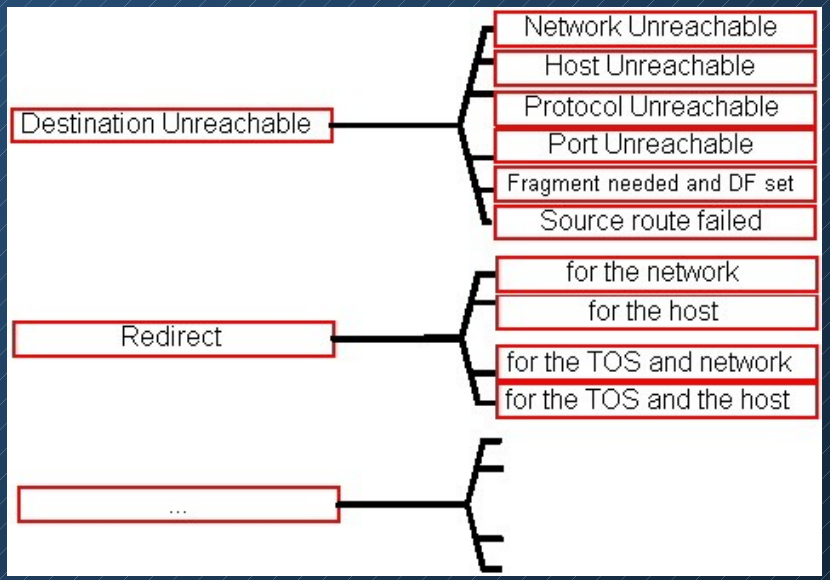
- SNMP s’appuie sur la MIB (Management Information Base) pour se référer à une variable.
- La supervision permet grâce à la consultation de ces variables de :
  - Détecter la panne d’un matériel
  - Détecter les bagottements
  - Tracer les incidents
  - Remonter des alertes



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

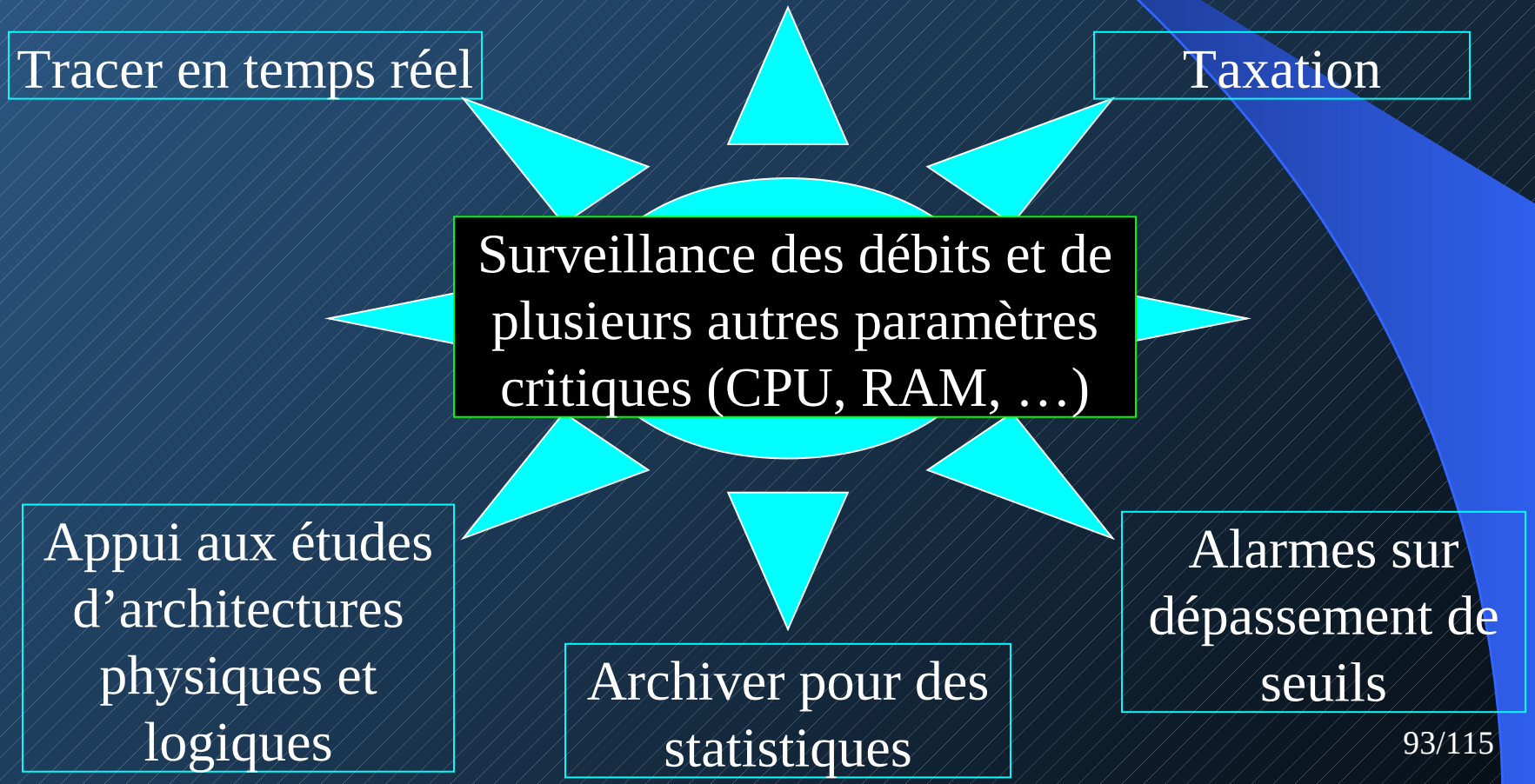
ICMP (Internet Control Message Protocol)

- 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.

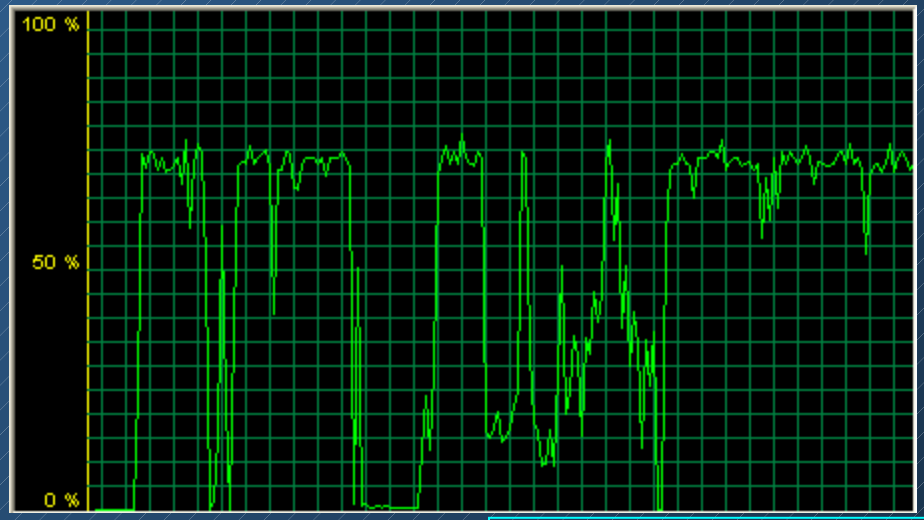


- Le ping (echo_request/echo_reply) est l’aspect le plus connu du protocole, mais il en existe beaucoup d’autres !

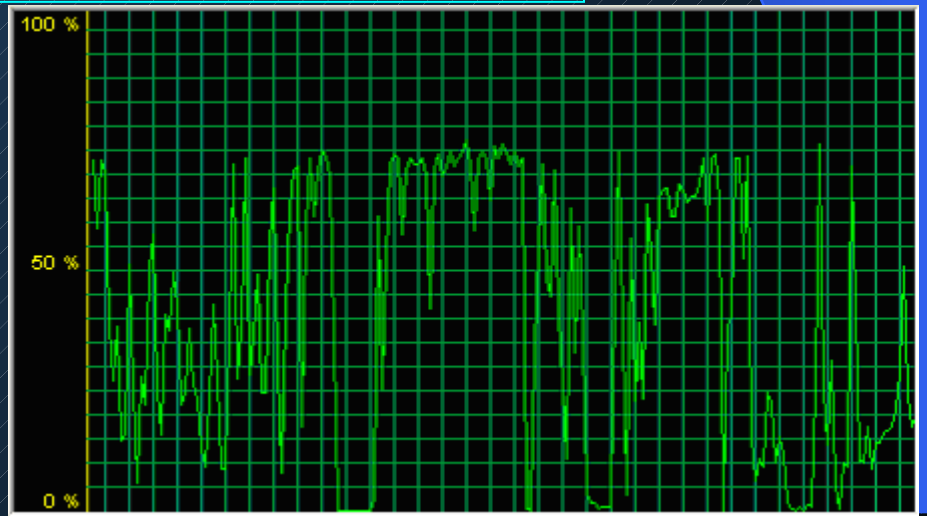
Le monitoring (1/3)



Le monitoring (2/3)

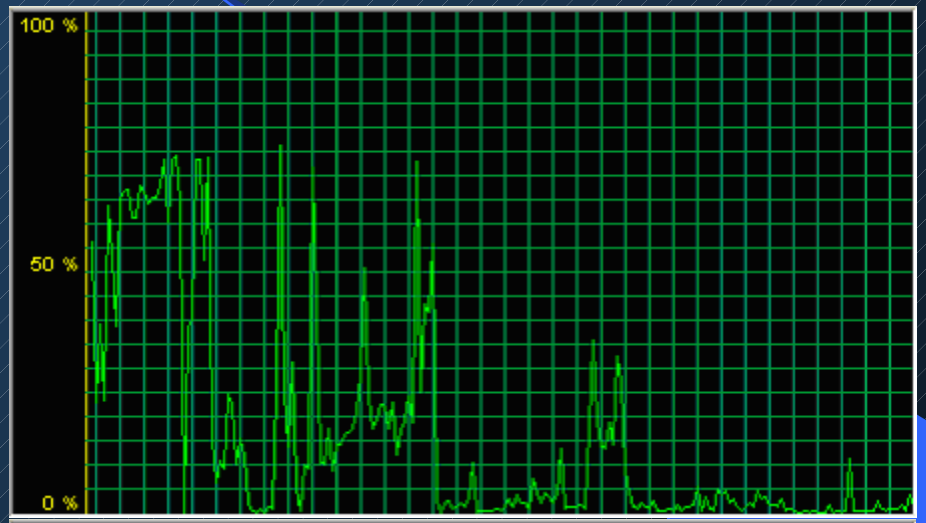


Trafic oscillant ou trafic normal ?

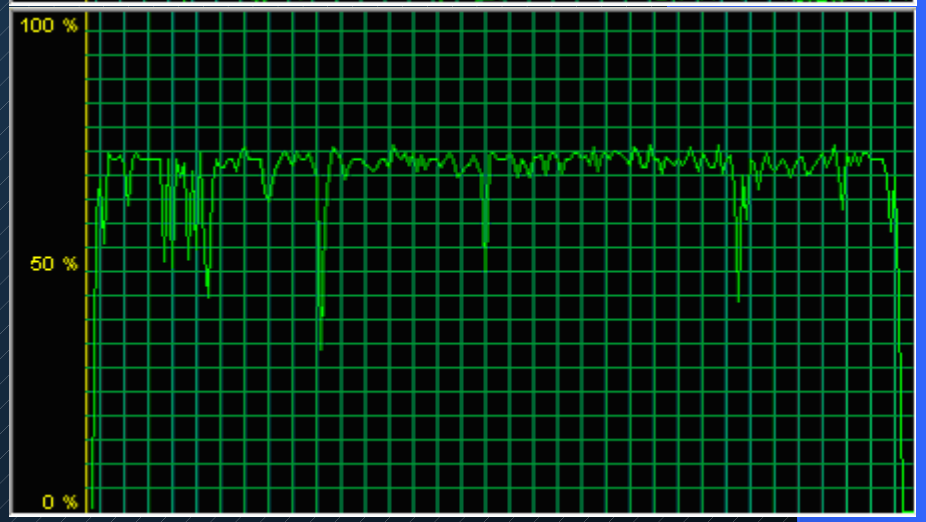


Le monitoring (3/3)

Trafic faible ou transfert de nombreux petits fichiers ?

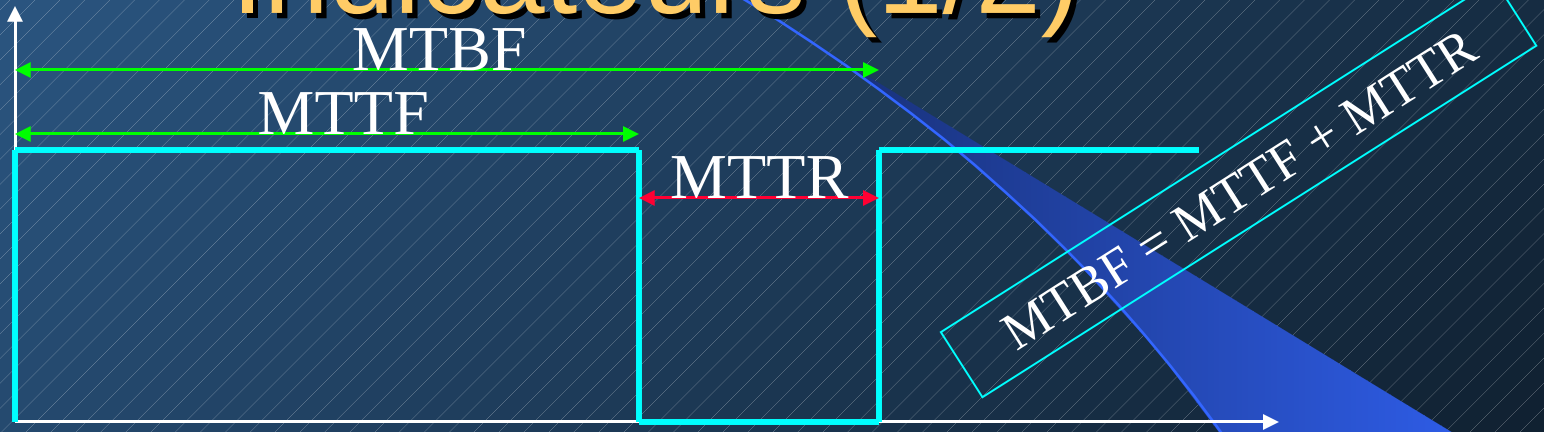


Trafic optimum ou saturation ?



Saturation émetteur, réseau ou récepteur ?

Indicateurs (1/2)



La référence temporelle est le cycle de réparation, ou le cycle d'utilisation.

- MTBF : Mean Time Beetween Failure. C'est l'uptime moyen de l'élément, c-à-d Somme temps OK / nombre de défaillances.

$$\mathbf{MTBF = t_{ok}/Nb_{défaillances}}$$

- MTTR : Mean Time To Repair. C'est le temps moyen nécessaire pour revenir à un fonctionnement normal, c-à-d Somme temps NOK / nombre de défaillances.

$$\mathbf{MTTF = \sum t_{Nok}/Nb_{défaillances}}$$

- MTTF : Mean Time To Failure. Temps avant la panne pour un élément non-réparable.

Indicateurs (2/2)

Disponibilité. Probabilité (entre 0 et 1).

Disponibilité = MTBF / (MTBF + MTTR)

- Taux de défaillance = $Nb_{défaillances}$ / t =~ 1/MTBF
- Maintenabilité = 1/MTTR

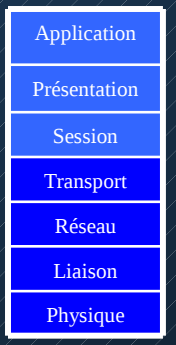
Différencier le système entier (service rendu à l’utilisateur) de ses sous-systèmes qui peuvent être redondés.

Statistiquement, nous avons une première période à risques de pannes puis Théorème de Drenick (cycle de réparation suit l’inverse d’une loi exponentielle).

La sécurité réseau

- Les firewalls
- Les systèmes de détection d'intrusions réseaux (NIDS)
- Les réseaux privés virtuels (VPN)
- Les antivirus
- Le social-engineering
- 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).
  - Ne permet pas de filtrer convenablement le niveau 7 si les flux sont chiffrés

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.
  - Complexité de l'étude de l'emplacement des sondes
  - 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) (1/3)

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 privée** en assurant l'authentification et la non-répudiation des émetteurs/récepteurs, l'intégrité et la confidentialité des données.

Le VPN simule le comportement d'une **liaison dédiée** par l'encapsulation des données (et parfois des en-têtes de routage), avec l'ajout d'un en-tête de routage permettant l'abstraction des réseaux traversés.

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) (2/3)

A EDF

IPSec (Bump In The Stack et pas Bump In The Wire)
SSH (Secure SHell)

Il existe aussi

SSL/TLS
L2TP (sans chiffrement)
PPTP (avec chiffrement)
GRE
…

Les réseaux privés virtuels (VPN) (3/3)

- 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, quelle 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.

Le social-engineering : le pishing

Demande de sa banque/FAI/… d'aller changer en ligne son mot de passe ou de donner son numéro de carte bleu pour régulariser une situation quelconque.

Envoi de correctifs par email.

Sollicitation non-désirée de déverminage en ligne.

Demande d'aide d'une riche jeune demoiselle étrangère.

Pishing essentiellement par email, mais aussi par IM.

Vigilance (email en anglais, interlocuteurs étrangers, sommes d'argent importantes)

Anti-spam/Anti-popup/Antivirus/Anti-spyware

Le social-engineering : le pishing

- Solutions
  - Bloquer les solicitations avec anti-spam et anti-popup.
  - Protéger la machine avec anti-virus et anti-spyware.
  - Restriction d'accès à des sites black-listés.
- Inconvénients
  - Aucune solution technique n'est vraiment efficace. Seule la sensibilisation de l'utilisateur et sa vigilance seront efficaces.

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, …).

SSO : Single Sign On

AAA : Authentication Autorization Accounting

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, jamais de le remplacer.

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)

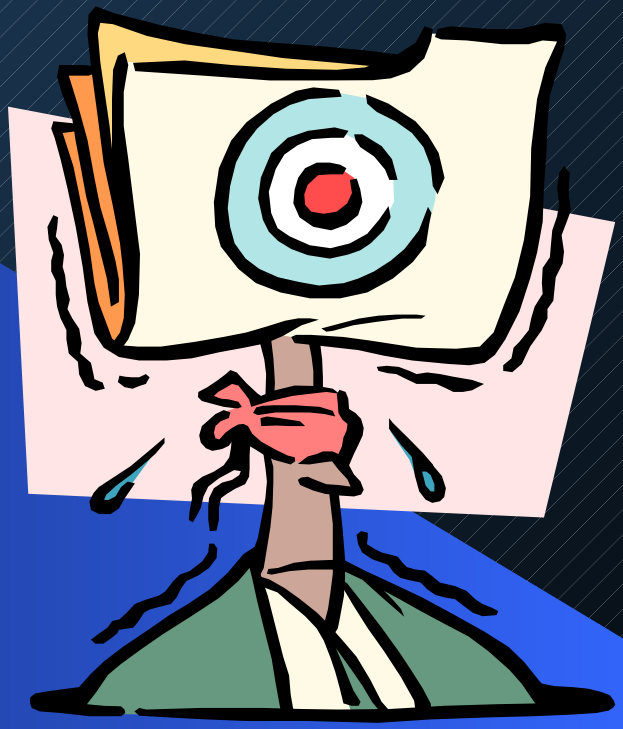
- Avantages.
  - Réactivité face à un problème.
  - Adapter une résolution d'incident au mélange « causes / effets / risques / contraintes ».
  - Vision globale de la problématique.
  - Limiter l'impact d'un incident sur les utilisateurs.
- Inconvénients.
  - Recherche constante des informations.
  - 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

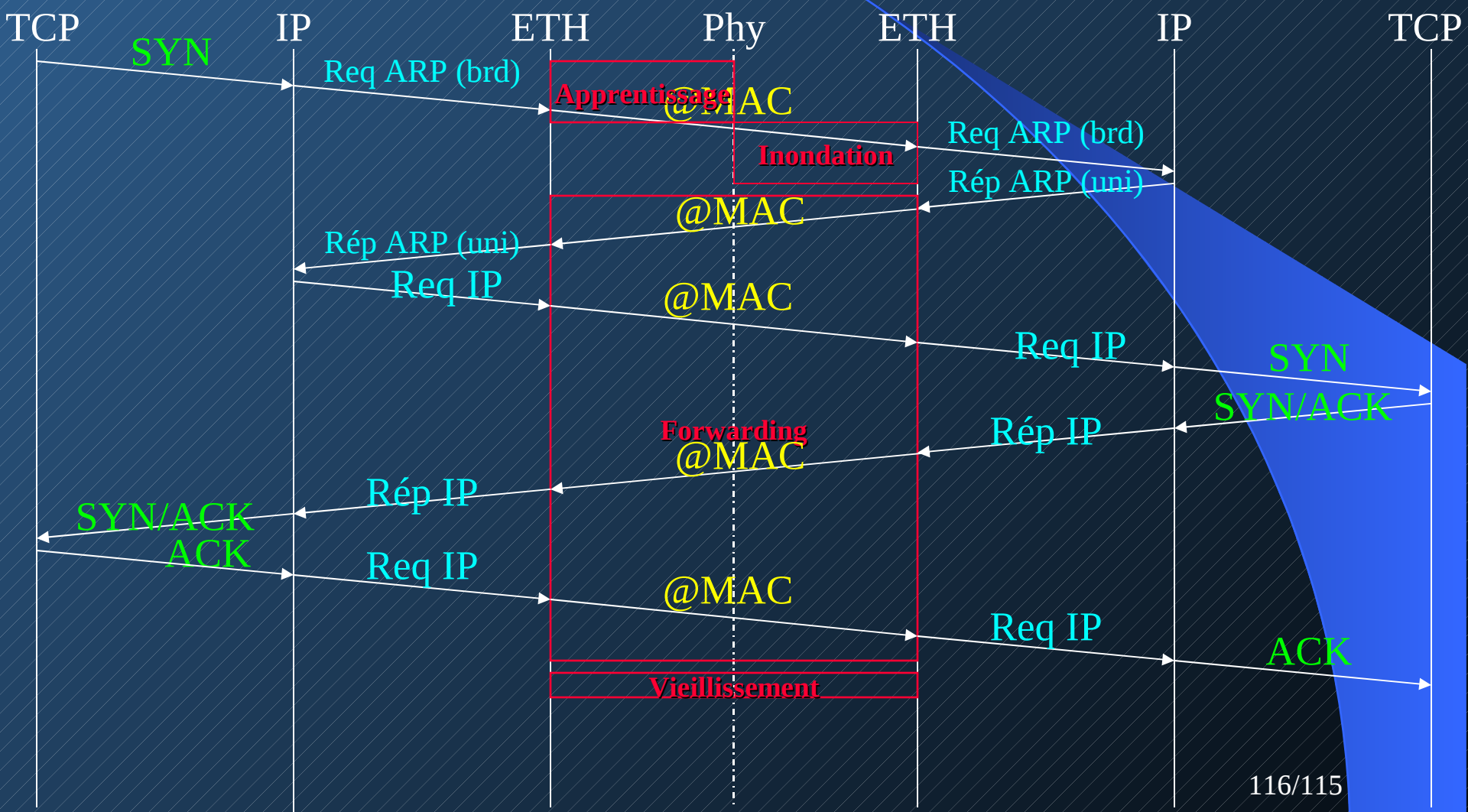
- Euh … qu'est-ce que je pourrai encore rajouter ?
- Évolution niveau 1 : « multiplexage optique ».
- Évolutions niveau 2 : augmentation des débits en WIFI, maturité du WIMAX, 10 Gbps ethernet, ethernet à la conquête du MAN et WAN (802.17 Resilient Packt Ring), CPL, mobilité, déploiement du MPLS et de la QoS.
- Évolution niveau 3 : IPv6, mobilité.
- Évolution niveau 4 : DCCP et SCTP
- Évolutions couches hautes : SIP pour la ToIP et IMS, XMPP pour l'IMS et ToIP, IMAP, multimédia de plus en plus présent.

Questions, remarques (si positives)…

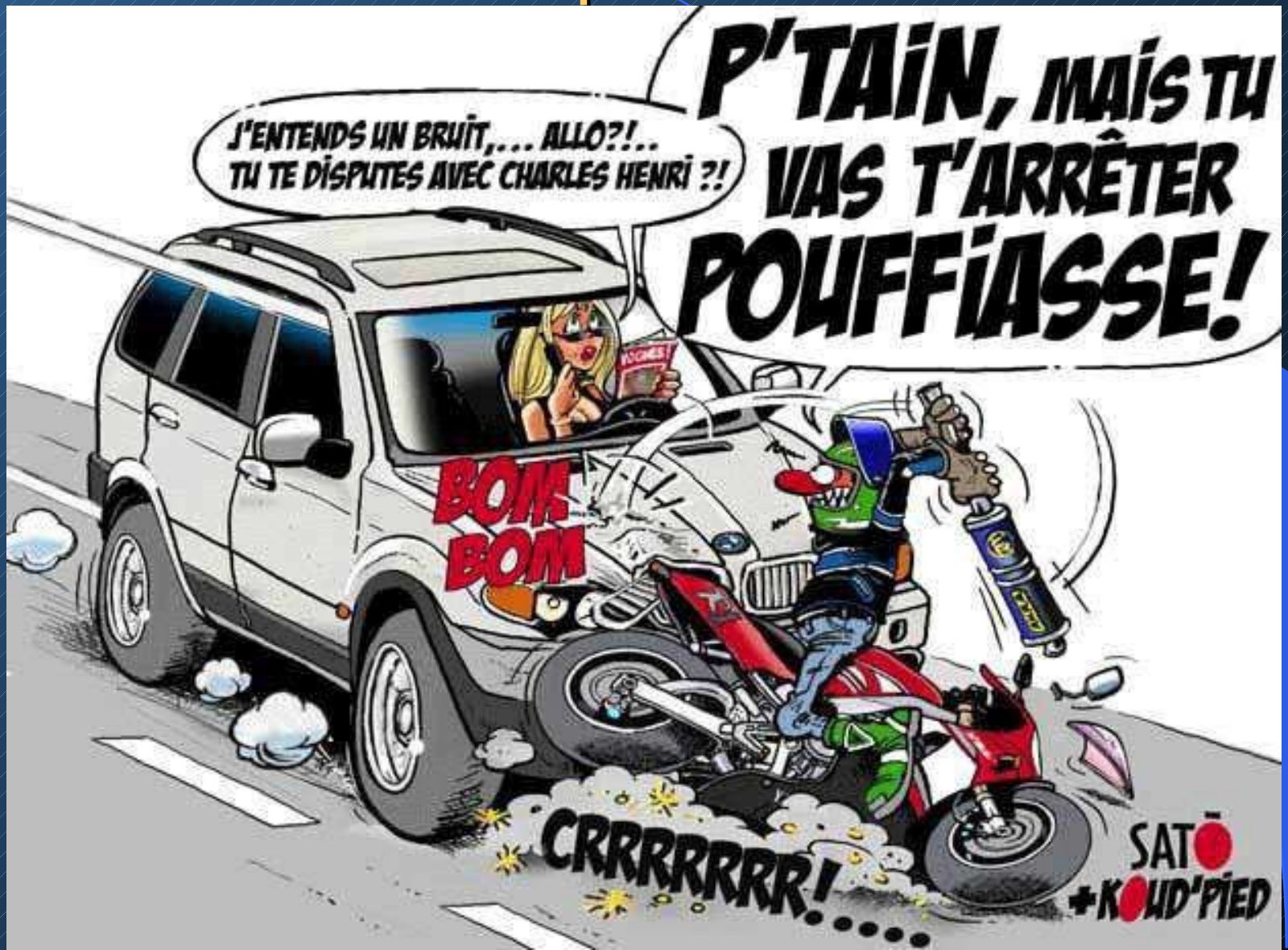
Merci



Etablissement d'une connexion (TCP/IP/ETH/SW)



Attention à ceux qui rentrent en voiture



Resilient Packet Ring

- Disponible sur peu d'équipements et ce sont des équipements haut de gamme (> 10000 euros, prix public), regroupe le meilleur d'ethernet et de SONET.
- Principe : Réseau en anneau FO doublé (au minimum). Les 2 (ou plus) anneaux sont utilisés en sens inverse les uns des autres. En cas de coupure sur un segment d'un anneau, la disponibilité du réseau est préservée en utilisant un autre anneau sur le segment défaillant. Indisponibilité < 50 ms.
- BP négociée par les noeuds à l'aide d'un algo de contrôle d'équité : fairness. 3 classes, A, B, C, A étant la plus haute (bonne BP, et peu de gigue). Peu de gigue pour B, best-effort pour C.
- Chaque noeud sait sur quel anneau envoyer la trame pour arriver le plus vite à destination.
- Trames en transit plus prioritaires que les trames émises par le noeud.
- Protection : mécanisme permettant de garder le réseau disponible après la coupure d'un segment d'un anneau. Il existe le steering (tous les noeuds sont informés qu'ils doivent éviter le segment en panne et envoient en conséquence les trames sur le bon anneau) et le wrapping (le trafic est dirigé vers l'autre anneau par les noeuds adjacents au segment déficient).