

TCP/IP

➡ La technologie IP
(Origines, Structure, Composants,
Standards, Adressage, DNS, ARP,
RARP, ICMP, Transport...)

➡ IPv6
(Apports, Adressage,
Classes de Service, Transition...)



➡ Les Nouveaux Services
(Nouvelles Infrastructures,
Nouveaux Protocoles...)

Généralités

➡ TCP/IP suite de protocoles pour l'interconnexion et le Support des services applicatifs spécifiquement informatiques

➡ Mise en oeuvre par le DOD (DPA)

➡ Déployée dans Internet

➡ Simplicité des protocoles et pragmatisme

➡ IP = « Best Effort »

➡ Indépendant des constructeurs /
Systèmes d'exploitation



Qui fut à l'origine ?

- ➡ 1969: (D)ARPA du DOD avec 4 noeuds
- ➡ 1972: ARPANET ancêtre d'Internet
Début des spécifications de TCP/IP
- ➡ 1980: Unix inclut TCP/IP
- ➡ 1988: Backbone de la NSFnet
- ➡ 1990: Explosion IP en Europe
- ➡ 1992: EBONE et RENATER



Pourquoi cette croissance ?

- ➡ La croissance d'Internet est due à :
- Taille de la communauté Internet (effet boule de neige);
 - Esprit de coopération et éthique;
 - Richesse des services offerts
(connexion à distance, transfert de fichiers, messagerie, news, recherche documentaire...)
 - Adoption de la suite de protocoles TCP/IP simples à mettre en oeuvre;
 - Disponibilité des logiciels en freeware ou en shareware;
 - Disponibilité gratuite de tous les documents relatifs aux standards utilisés;



Quelle est la structure (1/4)?

➡ Interconnexion à différents niveaux =

Backbones:

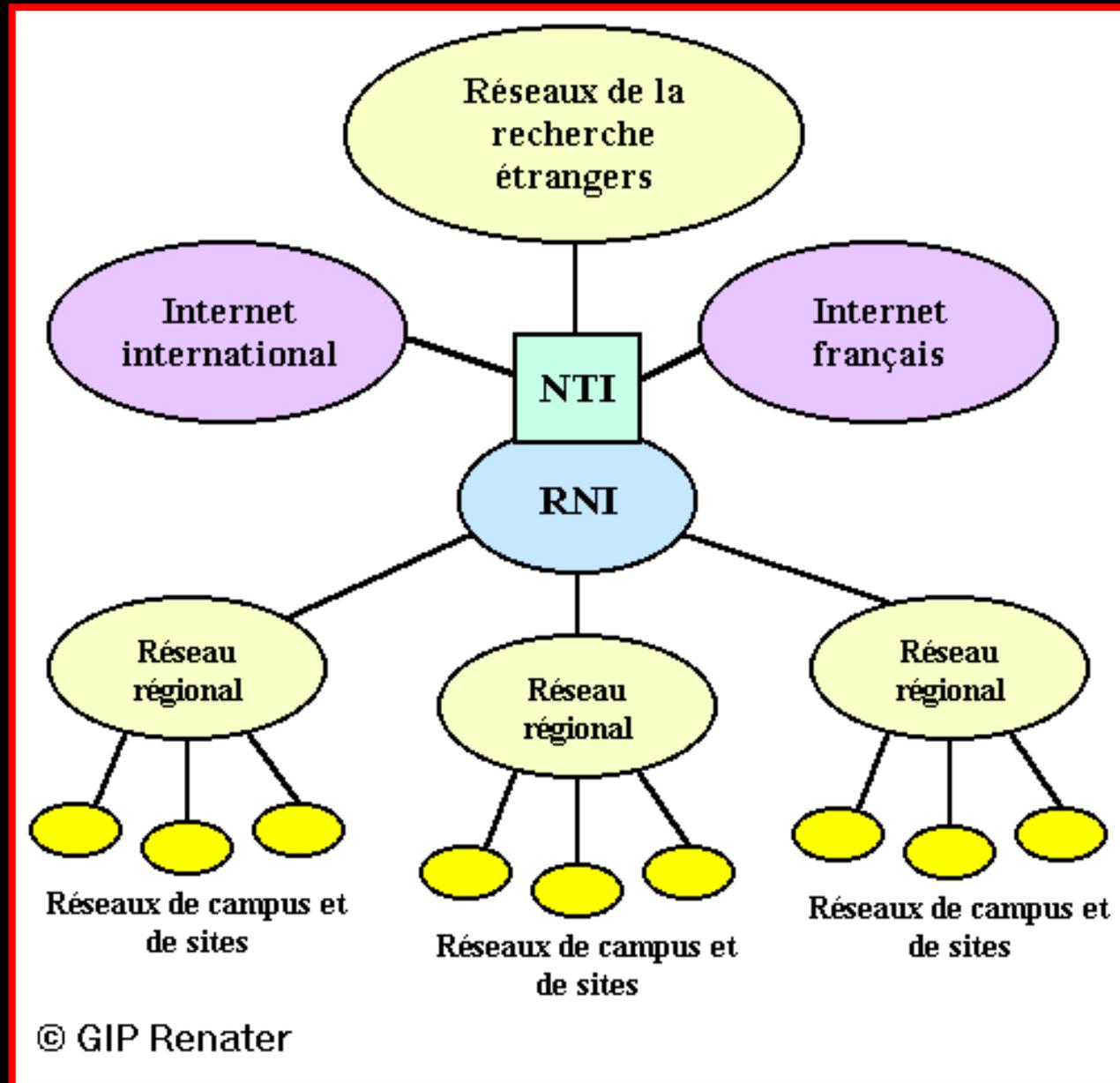
- Réseau local;
- Réseau de campus;
- Réseau régional;
- Réseau national;
- Réseau mondial;

➡ On parle d'Internet lorsqu'il s'agit du réseau mondial

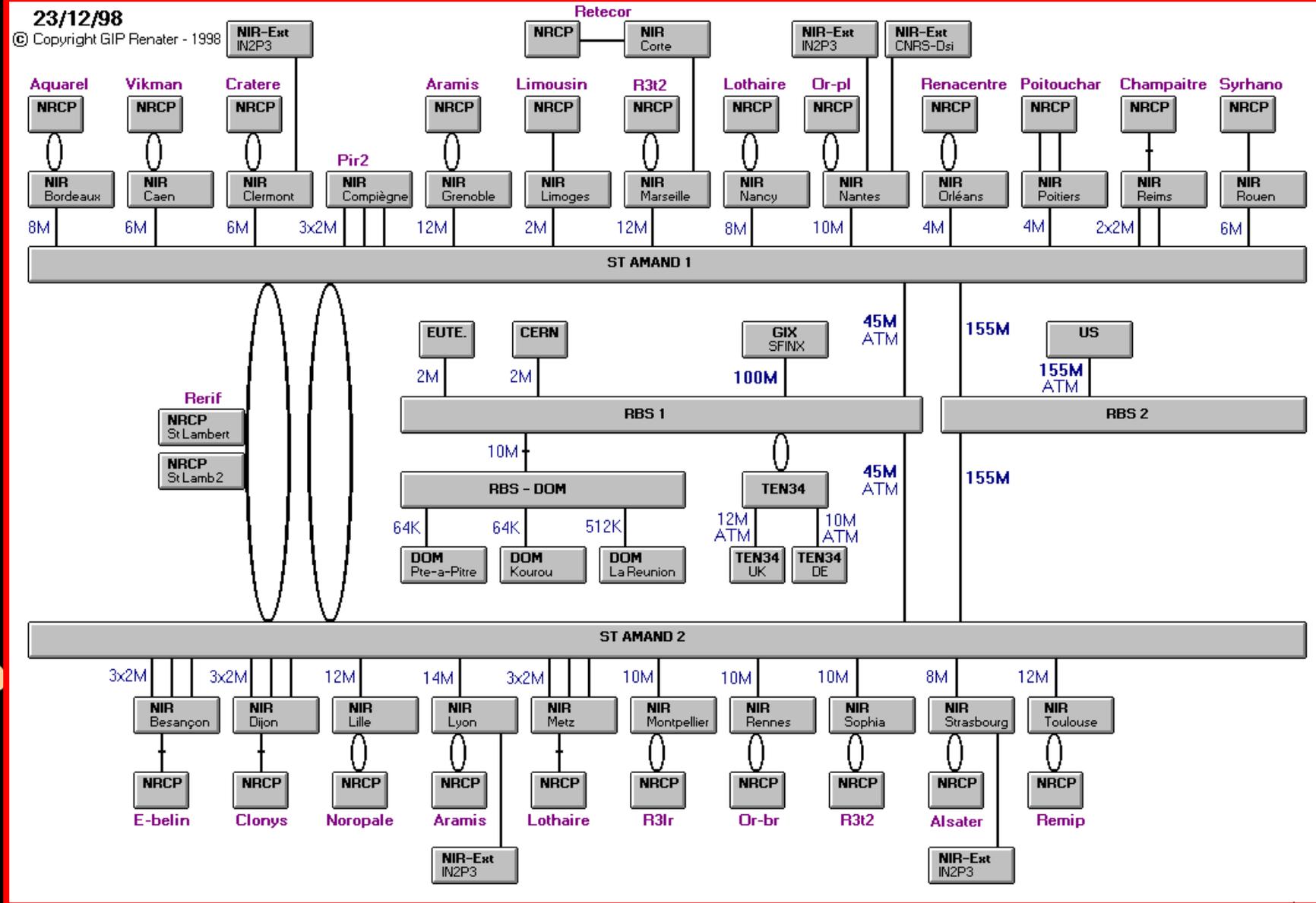
➡ On parle d'Intranet lorsque les services TCP/IP sont utilisés à un niveau limité (local, entreprise ou même régional) ou à un usage spécifique (qui peut être mondial)



Quelle est la structure (2/4)?



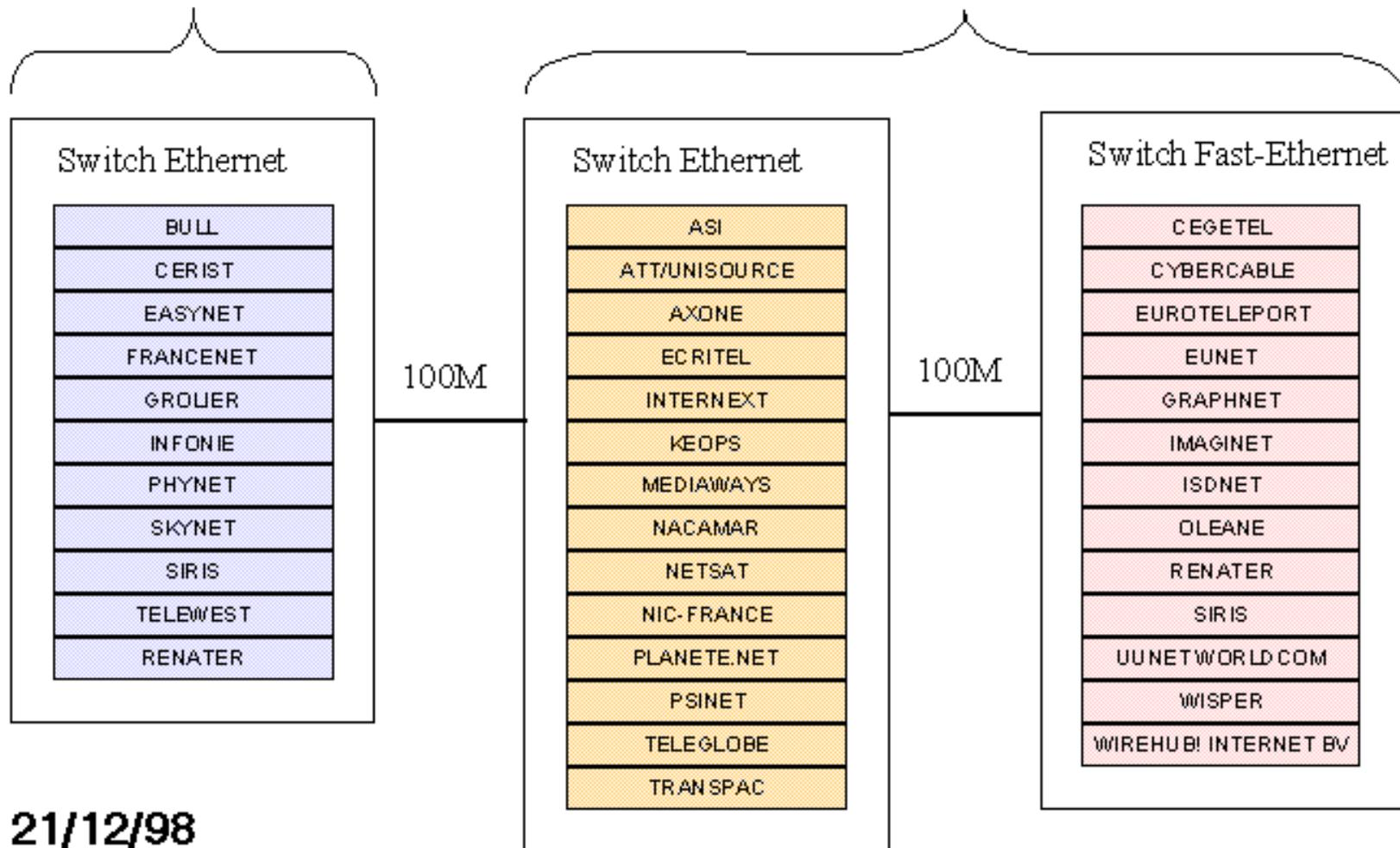
Quelle est la structure (3/4)?



Quelle est la structure (4/4)?

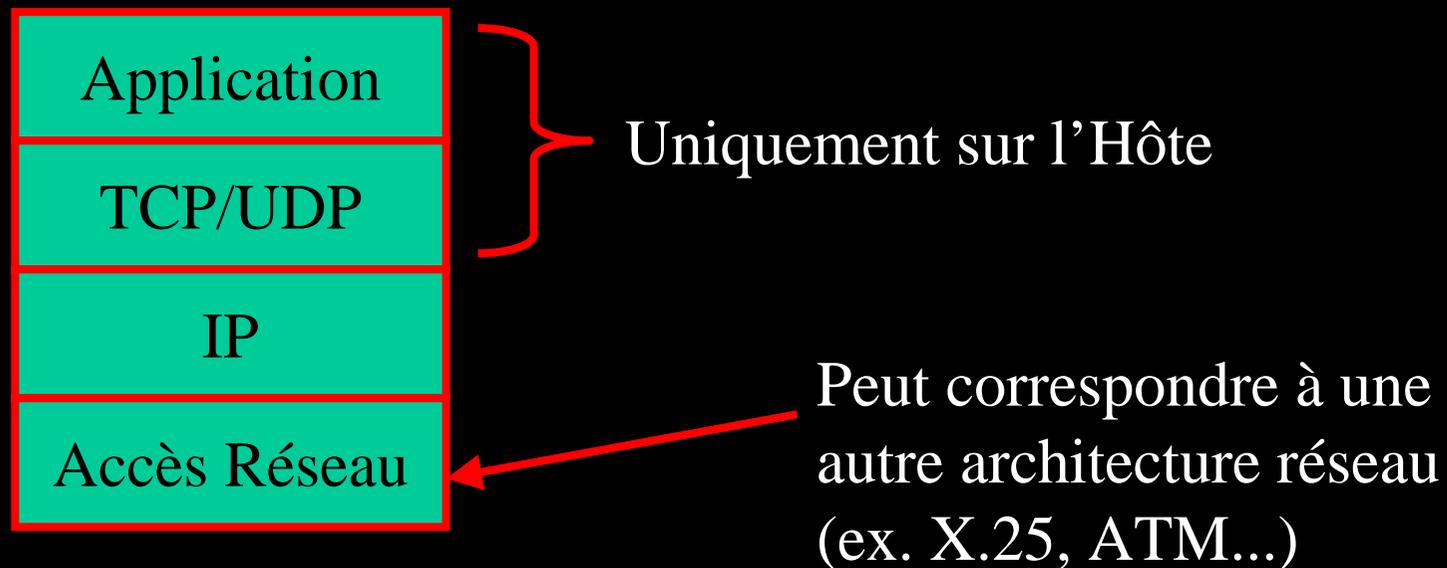
SFINX géré / Managed SFINX

SFINX hébergé / Hosted SFINX



Quels sont les composants ?

- ➡ L 'internet est composé de:
 - Postes de travail;
 - Equipements d 'interconnexion (Routeurs)
 - Réseau physique (liens + hubs + ...)
- ➡ Une architecture de communication:



Quelles sont les applications ?

FTP

NNTP

SMTP

HTTP

POP

Telnet

SNMP

TFTP



Où trouver les standards ?

- ➡ Standards publiés sous forme de documents appelés **RFC** (Request For Comments) (ex. RFC 793 pour TCP)
- ➡ Tous les **RFC** ne sont pas des standards
- ➡ Certains sont pour l'information (**FYI**)
- ➡ Pour obtenir un RFC:
 - `ftp://ftp.inria.fr`



Standardisation

INTERNET SOCIETY
Publication des standards

IAB
Mission de développement

IESG
Développement Technologique

IETF
Définition des standards

IRTF / IRSG
Recherche Technologique

IANA
Adressage et Nommage

Routage
Sécurité
Services
Application
Administration...



Quelles sont les Fonctions d 'IP ?

➡ Transporter des paquets de station à station en passant par des routeurs reliant des réseaux hétérogènes;

➡ Mode sans connexion (Datagramme)

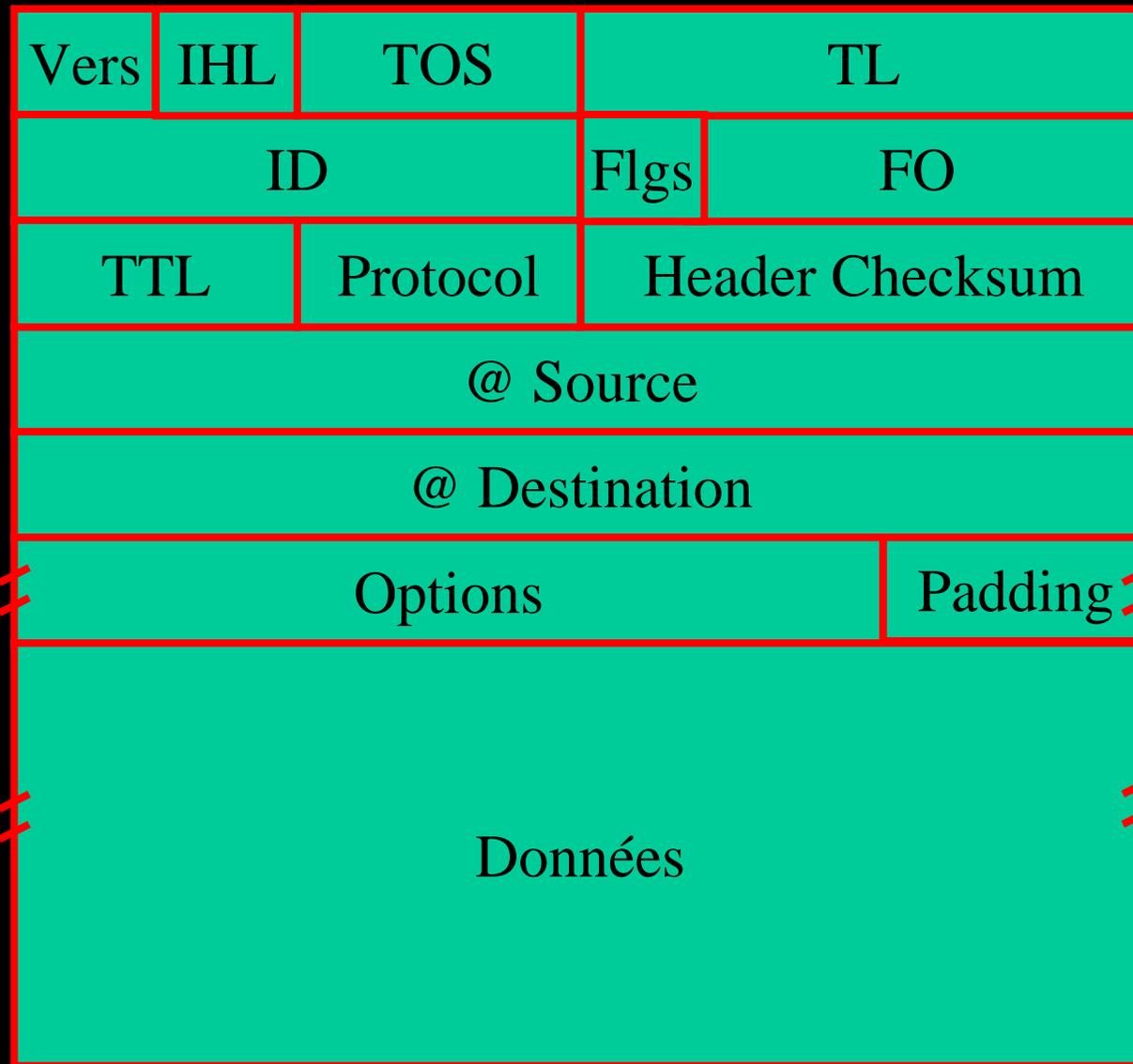
➡ Segmentation

➡ Temps de vie d 'un datagramme pour prévenir les congestions.



➡ Encapsule n'importe quel protocole de niveau supérieur; IP=Format d 'encapsulation et non un réel protocole

Datagramme IP (1/2)



Datagramme IP (2/2)

➡ Vers: Version du protocole; actuellement 4 mais 6 pour IPv6

➡ TOS: Type Of Service (Qualité de Service); Non utilisé mais certains constructeurs commencent à le faire.

➡ TL: Temps de vie (TimeLive)

➡ Protocol: Identification du protocole supérieur encapsulé

➡ Options: extensions des possibilités d'IP (Sécurité, timestamp, routing source...)



Comment identifier une machine ?

«Un nom précise ce que nous recherchons,
l'adresse sa localisation,
la route le moyen d'y accéder»

➡ Chaque machine (hôte ou routeur) a une adresse **IP**. Cette adresse correspond à un numéro.

➡ Pour des raisons mnémoniques, elle peut avoir aussi un nom.

➡ Seule l'adresse **IP** permet d'accéder à une machine; c'est pourquoi le nom doit être traduit en une adresse = **DNS**



Quelle est la structure de l '@ (1/3)?

- Unique dans un domaine (l'Internet=monde)
- Configurable par logiciel = adresse logique



En réalité, c'est l'@ du point d'accès d'une machine sur un réseau donc, si un ordinateur change de réseau, il change d'@.



- @ réseau donnée par un organisme officiel (NIC Internet ou IANA), @ machine donnée par l'administrateur local du réseau.

Quelle est la structure de l'@ (2/3)?

➡ @ individuelle, de groupe, de diffusion.

➡ @ sur 32 bits en notation décimale pointée.

Classification pour les @ individuelles:

- Classe A: $0 \leq N1 \leq 127$
- Classe B: $128 \leq N1 \leq 191$
- Classe C: $192 \leq N1 \leq 223$

➡ Classe D pour le Multicast: $239 \leq G1 \leq 254$



A	0	N1	H1	H2	H3
B	10	N1	N2	H1	H2
C	110	N1	N2	N3	H4
D	1110	G1	G2	G3	G4

Quelle est la structure de l '@ (3/3)?

➡ @IP d'un réseau Champ machine=0..0

➡ @IP de diffusion Champ machine = 1..1

➡ @ ne contenant que des 0 utilisé quand la machine ne connaît pas son adresse.

➡ Sous-réseau IP (subnet) = partition d'un réseau, meilleure utilisation du champ machine.



➡ Subnet caractérisé par un masque qui réalise un ET logique avec l '@ machine.

➡ Un routeur interconnecte des sous-réseaux.

Comment fonctionne le DNS ?

➡ Un nom = plusieurs parties séparées par un point.

➡ Nommage hiérarchique par domaine, de la droite à la gauche pour les inclusions. Le champ le plus à droite = catégorie du site ou pays (ex. com, edu, gov, net, fr, uk, jp...)
ex. www-sv.cict.fr



➡ Résolution de la correspondance = fichier local ou distant sur un serveur DNS.

➡ Client/Serveur pour le DNS

Qu 'est-ce que A R P ?

- ➡ Le paquet IP est encapsulé dans une trame LLC ou Ethernet...
- ➡ Prélèvement d 'une trame Ethernet = Filtrage sur l 'adresse physique MA C
- ➡ Obtenir l '@ MA C en ayant l '@ l P = Protocole de résolution d 'adresses A R P
- ➡ Envoyer une requête A R P dans une trame Ethernet de diffusion
- ➡ Réponse de la machine qui reconnaît son @ IP.



Qu 'est-ce que RA RP ?

➡ RA RP (Reverse Address Resolution Protocol) permet de connaître une @ IP en donnant l'@ Ethernet

➡ Utilisé au moment du boot par certaines machine (ex. stations sans disque...)

➡ Serveur RA RP.



➡ RA RP encapsulé dans une trame Ethernet

➡ Une requête RA RP ne peut traverser un routeur

Qu 'est-ce que ICMP ?

- ➡ ICMP (Internet Control Message Protocol)
= gestion simple de réseau
- ➡ Implémenté sur tous les équipements IP
- ➡ Encapsulé dans IP
- ➡ Envoyé lors de problèmes (ex. Network unreachable, Time to Live exceeded...)
- ➡ Utilisé pour vérifier l 'accessibilité d 'une machine: Commande Ping (Echo, Echo Reply)



Transport

➡ Process to Process (EU-EU)

➡ Deux protocoles principaux:

- TCP (Transmission Control Protocol)
Orienté Connexion
- UDP (User Datagram Protocol)
Orienté Sans Connexion

➡ Port : Numéro identifiant le service transport (ex. 21 pour ftpd, 23 pour telnetd...)



➡ Socket = @I P + Numéro de port

Quelles sont les fonctions de TCP ?

- ➡ Contrôle de bout en bout
- ➡ Mode connecté: Etablissement... Libération
- ➡ Contrôle d'erreurs avec retransmission
- ➡ Contrôle de flux avec fenêtrage
- ➡ Contrôle de séquençement
- ➡ Full duplex
- ➡ Segmentation



Limitations d'IP (1/2)

➡ "The internet protocol is specifically limited in scope to provide the functions necessary to deliver a package of bits (an internet datagram) from a source to a destination over an interconnected system of networks. There are no mechanisms to augment end-to-end data reliability, flow control, sequencing, or other services commonly found in host-to-host protocols. The internet protocol can capitalize on the services of its supporting networks to provide various types and qualities of service."
[RFC 791]



Limitations d'IP (2/2)

- ➡ Epuisement des adresses
- ➡ Explosion des tables de routage
- ➡ Absence de type de données
- ➡ Temps de traitement important



Apports d'IPv6 (1/2)

- ➡ Capacités d'adressage plus importants (adresse sur 128 bits au lieu de 32 bits);
- ➡ Hiérarchie d'adressage plus riche et prenant en compte différentes configurations;
- ➡ Autoconfiguration (plug-and-play) possible des adresses;



- ➡ Gestion de la mobilité (I P mobile);
- ➡ Multicast natif

Apports d'IPv6 (2/2)

- ➡ En-tête de base plus simple
- ➡ En-têtes d'extension = +fonctionnalités
- ➡ Mécanismes de sécurité (authentification et confidentialité);
- ➡ Routage par la source possible;
- ➡ Identificateur de flot (flow label);
- ➡ Plan de transition de l'I Pv4 à l'I Pv6;



A dressage IPv6

- ➡ A dressage hiérarchique sur 128 bits
- ➡ @ unicast affecté à un fournisseur d'accès:
 - préfixe (3 bits: 010): identification de l'adressage;
 - registry I D (5 bits): identification de l'autorité régionale dont dépend le fournisseur d'accès;
Actuellement, trois registres ont été définis pour l'Amérique du nord, l'Europe et l'Asie-Pacifique. Chaque autorité affectera les 15 octets restants.
 - provider I D (m bits): id. du fournisseur d'accès;
 - subscriber I D (o bits): id. de l'abonné;
 - subnetwork I D (p bits): id. du sous-réseau;
 - interface I D (128-m-o-p bits): id. de l'interface;



Classes de Service IPv6 (1/2)

- ➡ Dans IPv4 = TOS peu mis en oeuvre
- ➡ Dans IPv6 = Priority et Flow Label
- ➡ Les priorités de 0 à 7 sont affectées aux trafics à débit variable (news, mail, FTP, NFS, telnet, SNMP...) et qu'il est possible de ralentir sans trop nuire à la qualité de service. Les priorités de 8 à 15 sont affectés aux trafics temps réel (audio, vidéo...).



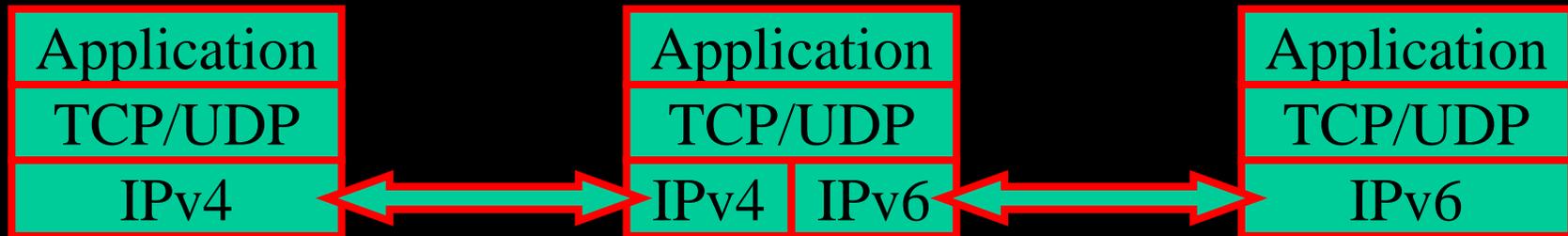
Classes de Service IPv6 (2/2)

➡ La mise en oeuvre d'une identification de flot permet de considérer le flot de données comme appartenant à une même connexion (notion absente d'IP) avec les mêmes contraintes de qualité de service (délai d'acheminement, bande passante...). Il est possible aux routeurs d'effectuer des traitements différenciés.

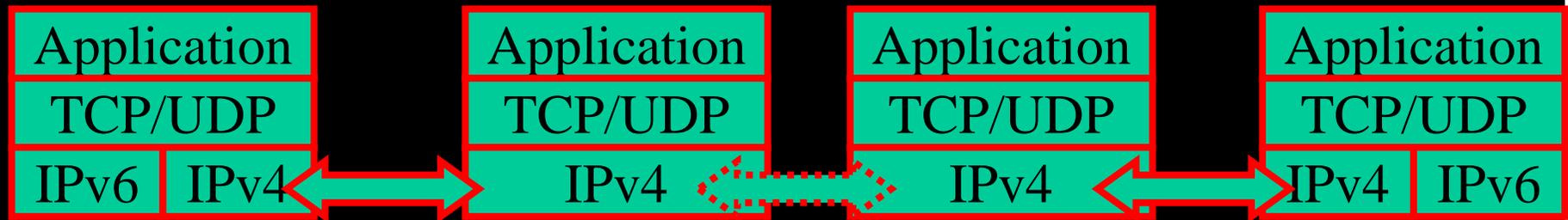


➡ Un flot = id. flot + @ + priorité. Ainsi, deux flots ayant la même étiquette arrivant à un routeur mais provenant de 2 ordinateurs différents seront différenciés.

Transition IPv4 à IPv6



Double pile IP



Infrastructure IPv4 = Tunnel

Hôte ou Routeur



Evolution de l'Internet

- Croissance explosive
- Accès Rapide (SDN, ADSL, Câble, satellite...)
- Nouveaux Terminaux
- Nouveaux Services = Nouvelles Contraintes
- Qualité de Service
- Sécurité
- Commerce électronique
- Téléphonie sur IP



Internet et le temps réel

- Défi majeur pour IP = QOS Temps Réel
- Problème incontournable = Réseau hétérogène non maîtrisé par un seul opérateur ou un seul constructeur
- Nouveaux services =
 - Nouvelle Infrastructure
 - Nouveaux protocoles
 - Nouvelles Applications
- IP temps réel \neq Internet temps réel
- Internet = Réseaux Multiservices + Routage



Nouvelle Infrastructure

- ➡ Pour absorber plus de communications =
Plus de Bande Passante et plus de liens
- ➡ Pour traverser plus vite le réseau=
Nouveaux Routeurs



Nouveaux Supports (1/3)

- ▶ Internet par Fibre Optique
 - L'américain Global TeleSystems (GTS) gère un réseau en fibres optiques nommé Hermès, reliant déjà douze pays et vingt villes en Europe.
 - MCI -WorldCom;
 - Viatel Inc avec le réseau Circé
 - " European Backbone Network " (EBN) de France Telecom et Deutsche Telecom.



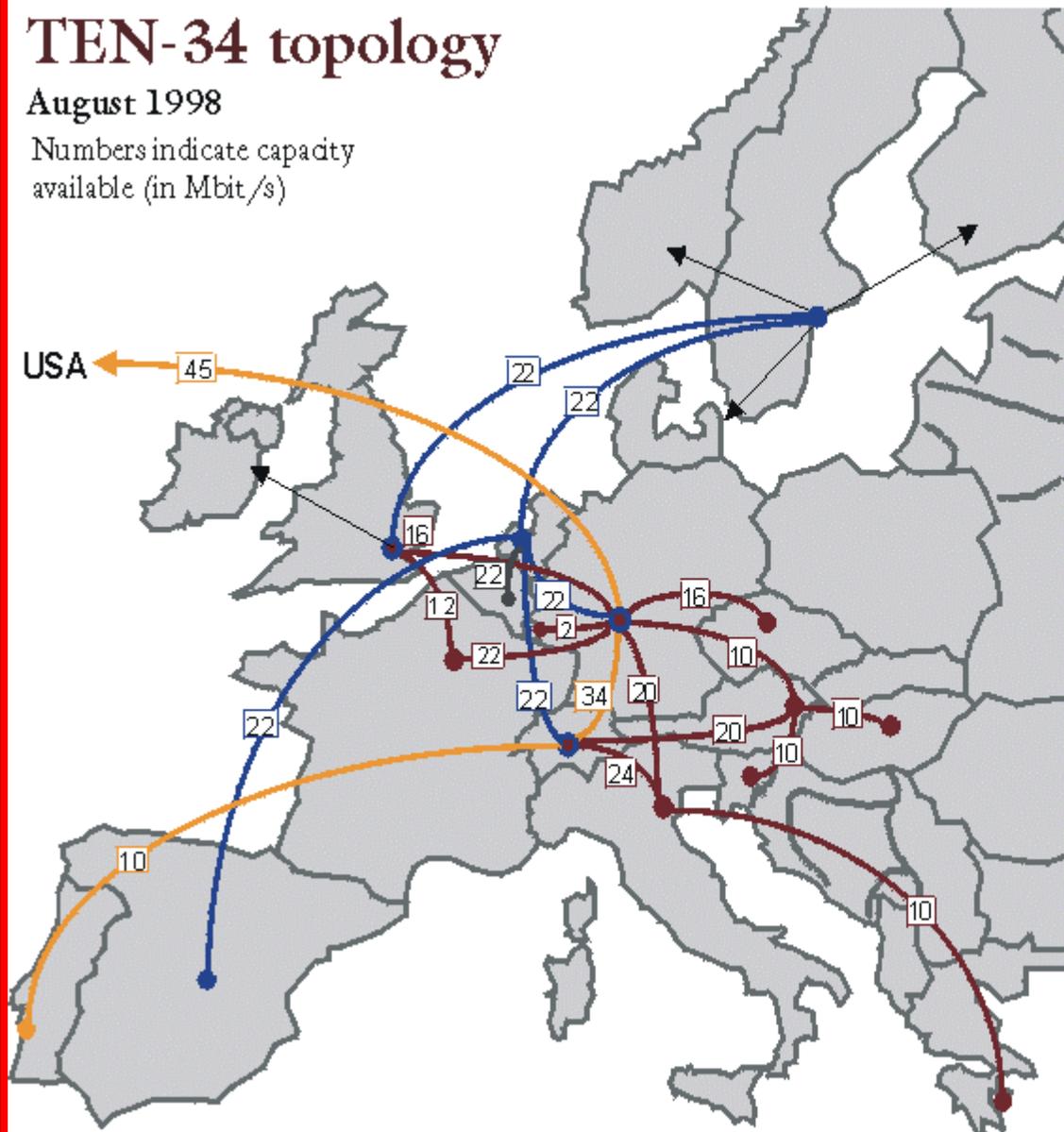
- ▶ TEN34, TEN155...

Nouveaux Supports (2/3)

TEN-34 topology

August 1998

Numbers indicate capacity available (in Mbit/s)



- IP subnetwork
- ATM VP subnetwork
- Interconnection point
- Leased line



TCP/IP (38/66)

© André Aoun-1999

Nouveaux Supports (3/3)

III➔ I ntranet mondiaux et Européens mis en oeuvre par certains constructeurs pour offrir de nouveaux services.

L 'américain RSL COM déploie un réseau dans 24 pays pour offrir des services spécifiques tel que la Voix sur I P

III➔ I nternet par Satellite



Nouveaux Routeurs (1/7)

- Augmentation du Débit
Ethernet 100 Mbps/ Gbps;
Commutation **Ethernet**;
Vlans;
Classical IP;
ELAN...
- Gestion de QOS
Identification de flux;
Gestion des priorités;
Coopération avec technologies support...



Nouveaux Routeurs (2/7)

➤ GigaRouteur:

- Matrice de commutation plus puissante (ex. 4 Gbps) - Matrice physique
- Plusieurs processeurs pour exécuter les différentes tâches;
- Processeurs spécialisés;
- Accès rapide aux tables de routage

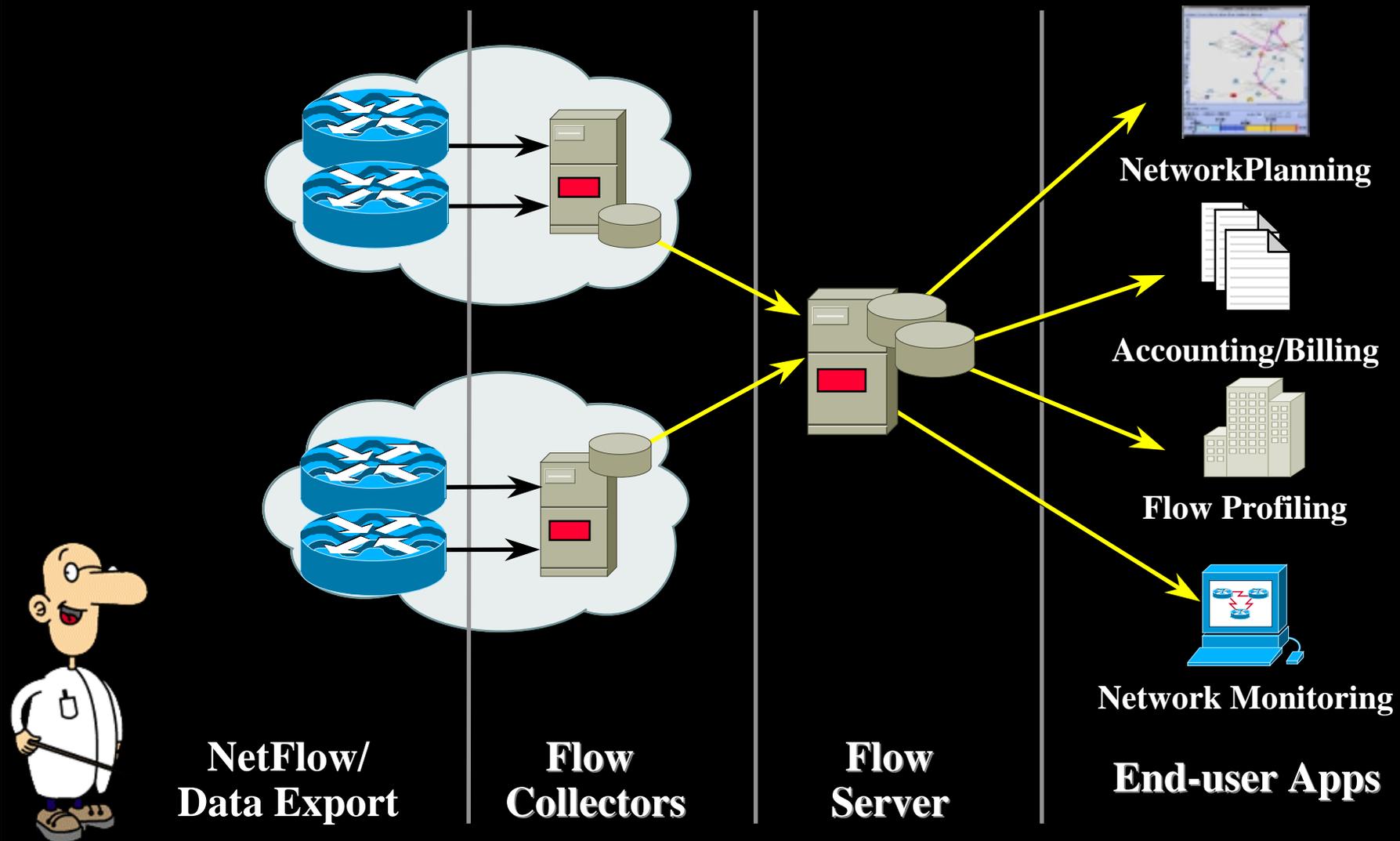
➤ Routeur Commutateur:

- Mémoire partagée jouant le rôle de matrice de commutation;
- Traitement des trames par des circuits en pipeline;



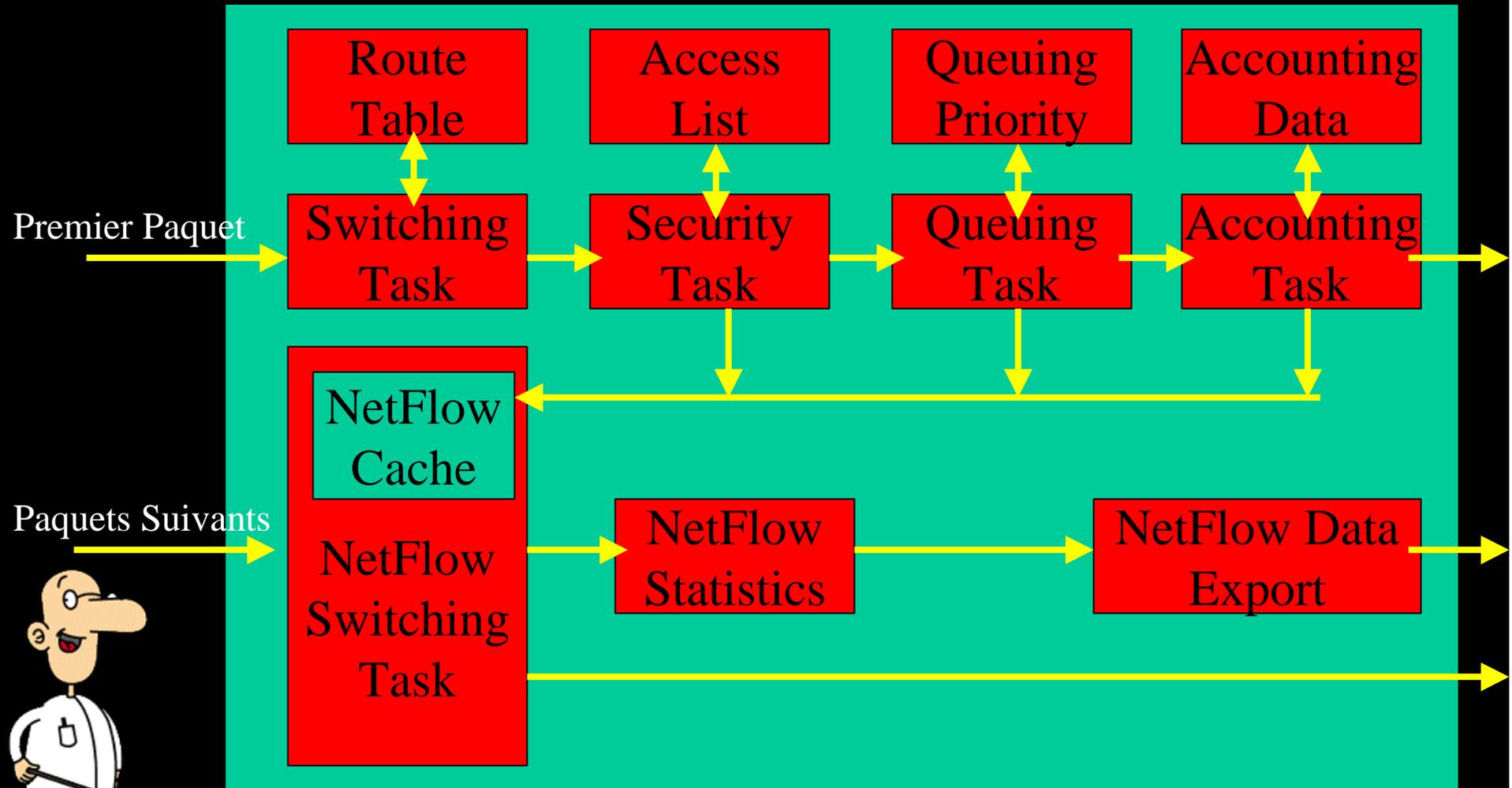
Nouveaux Routeurs (3/7)

NetFlow de CISCO



Nouveaux Routeurs (4/7)

NetFlow Switching de CISCO



Nouveaux Routeurs (5/7)

➤ NetFlow Switching de CISCO

- Détection de flot (@I P , n° port);
- Création d 'un cache associé au flot;
- Paquets suivants selon cache;

➤ NetFlow Lan Switching de CISCO

- Le premier paquet est routé, les suivants sont commutés;



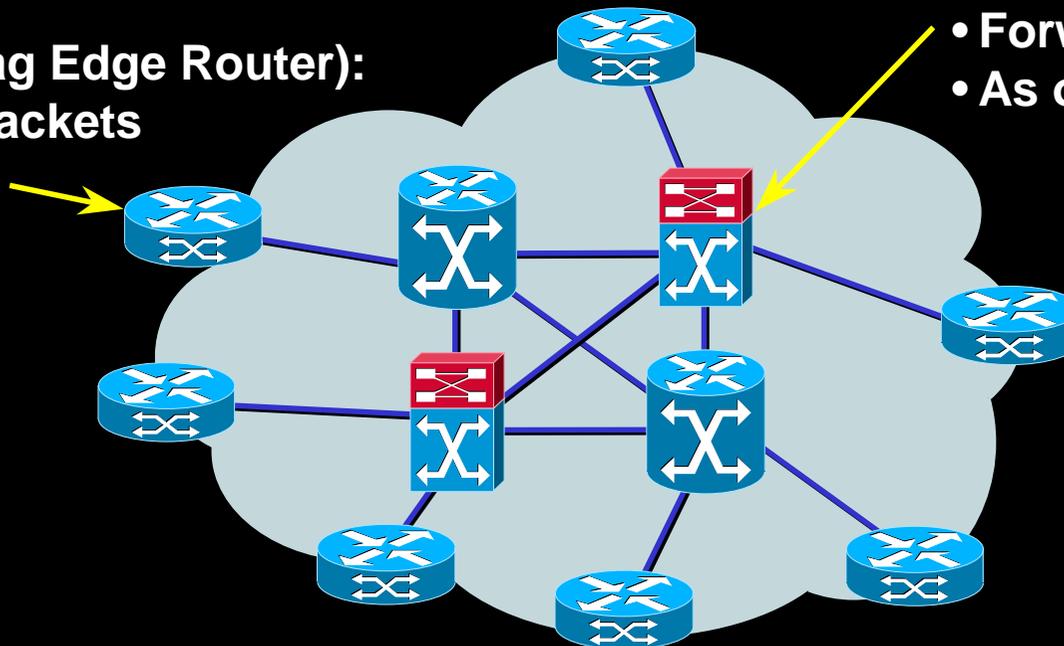
Nouveaux Routeurs (6/7)

➡ Tag Switching de CISCO

- Tag (étiquette) à chaque paquet;
- Associer un tag à chaque route dans les Tag Edge routeurs et dans les Tag Switches;

At Edge (Tag Edge Router):

- Classify packets
- Tag them



In Core (Tag Switch):

- Forward using tags
- As opposed to IP addr



Nouveaux Routeurs (7/7)

➡ IP Switching d 'I psilon

- Association d 'un comutateur A T M et d 'un routeur I P;
- Trafic « flot » commuté;
- Trafic « courte durée » routé;
- Performance dépend du nombre de paquets nécessaires pour détecter un flot;
- Différents flots = QOS adaptatifs;



Gestion des files d 'attente

➡ Custom Queuing: Une portion de mémoire tampon est allouée à chaque flot de données en fonction des @, type de protocole ou nature de l 'application

➡ Priority Queuing: Placement dans la file d 'attente selon une liste prioritaire définie comme précédemment

➡ Weighted Fair Queuing: Les petites séquences sont privilégiées par rapport aux grosses rafales.



Contrôleurs de Flux

- ➡ Contrôleur de flux juste en amont du routeur
- ➡ Le gestionnaire définit des classes de trafics (@I P, n° de port, URL, fichiers vidéo...) et leur alloue une Bande Passante minimale et maximale.
- ➡ Le contrôleur de flux agit sur les différents flux pour assurer la QOS demandée.
- ➡ Compression des données



Nouveaux Protocoles (1/2)

▣▣▣▣ IP n 'a pas d 'informations permettant d 'assurer le séquençement = Pb avec flux continu et synchronisation multimedia

▣▣▣▣ TCP a des Mécanismes de contrôle de flux et de congestion (« slow start ») incompatibles avec les contraintes temps réel

▣▣▣▣ UDP plus performant bien que moins fiable utilisé pour véhiculer les données temps réel

▣▣▣▣ Favoriser la continuité d 'un flux plutôt que la fiabilité



Nouveaux Protocoles (2/2)

➡ Flux Continu = Horodatage des paquets

➡ Gestion de congestion = Feedback de l'état du réseau à l'émetteur

➡ Feedback = Adaptation de l'application (ex. compression plus forte ou fréquence de rafraîchissement vidéo plus faible) au prix d'une qualité moindre.



➡ Deux applications ont servi de base:
- VAT (Visual Audio Tool)
- IVS (I NRI A Videoconferencing System)

RTP et RTCP (1/3)

- ➡ RTP: Real-Time Transport Protocol
 - Reconstitution de la base de temps des flux de données grâce à un numéro de séquence et un horodatage (TimeStamp)
 - Identification de chaque flux
 - Indication du type d'encodage des données

- ➡ RTCP: Real-Time Transport Control Protocol
 - Renvoi à l'émetteur un feedback sur la qualité de la transmission et d'autres informations



RTP et RTCP (2/3)

- Pas de Réserve de ressources
- Pas de Contrôle de congestion
- Pas de fiabilité
- Pas de garantie de temps de latence

- Informations pour le destinataire
- Informations pour l'émetteur (feedback)
- Indépendance vis à vis des couches inférieures
- Chaque flux = Une session RTP (ex. audio et video d'une application multimedia correspondront à deux sessions RTP)



RTP et RTCP (3/3)

- ➡ Utilisation intéressante dans le multicast.
- ➡ Un destinataire dans une conférence multipoint envoie sur le port RTCP un rapport de réception = adaptation de l'émetteur
- ➡ Utilisation de Mixeur pour individualiser la QoS.
- ➡ Utilisation de Translateur (relais RTP) pour traverser les Firewalls qui filtrent les communications multipoints



RTSP

- ➡ RTSP: Real-Time Streaming Protocol
- ➡ Segmentation des données en paquets adaptés à la Bande Passante.
- ➡ Quand le Client a reçu assez de paquets, le logiciel peut jouer un paquet, décompresse le suivant pendant qu'il reçoit un troisième = Technique de bufferisation
- ➡ RTSP est surtout utilisé au dessus de RTP pour bénéficier de ses caractéristiques
- ➡ Contrôle du streaming par le client



RSVP (1/2)

- ➡ Resource ReSerVation Protocol
- ➡ IP reporte l'intelligence sur les extrémités.
- ➡ RTP/RTCP aide l'application à s'adapter au réseau.
- ➡ Pb. Dans le traitement des paquets dans les routeurs = Routage **FIFO**
- ➡ Dans IP, aucun flux n'a priorité sur un autre = l'adapté pour les applications Temps réel



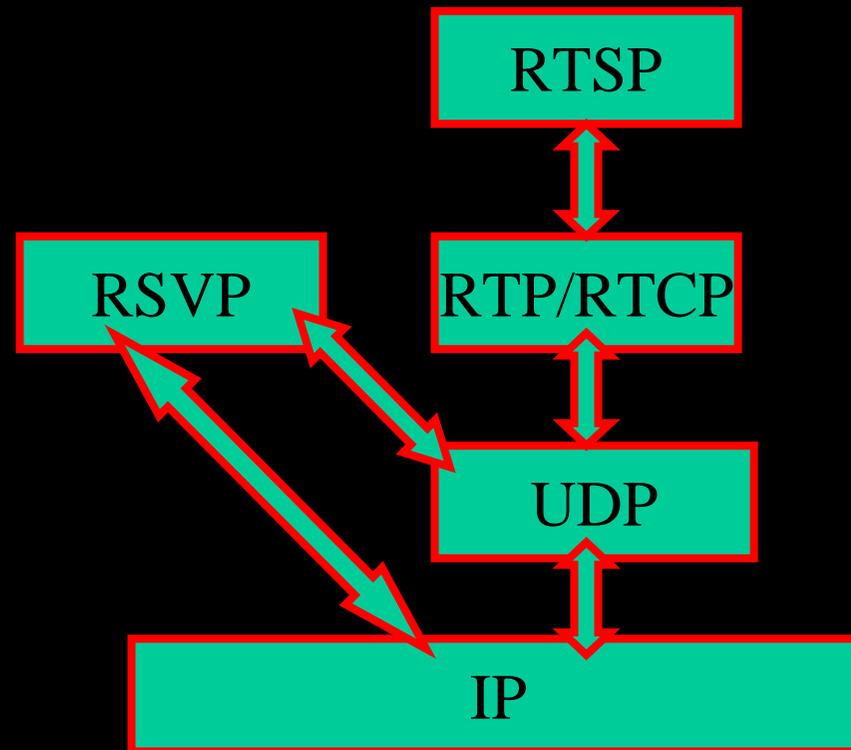
RSVP (2/2)

- ➡ A adapté aux Multicast; l 'Unicast étant un cas particulier;
- ➡ Message RSVP pour demander la réservation des ressources, formulé par le destinataire
- ➡ Le message RSVP parcourt les différents routeurs jusqu 'à l 'émetteur
- ➡ RSVP doit s 'adapter aux protocoles de routage



Architecture pour Temps Réel

Applications Temps Réel



VPN (1/2)

➡ Virtual Private Network basé sur un tunnel (encapsulation) de niveau 3 ou 2

➡ Objectifs :

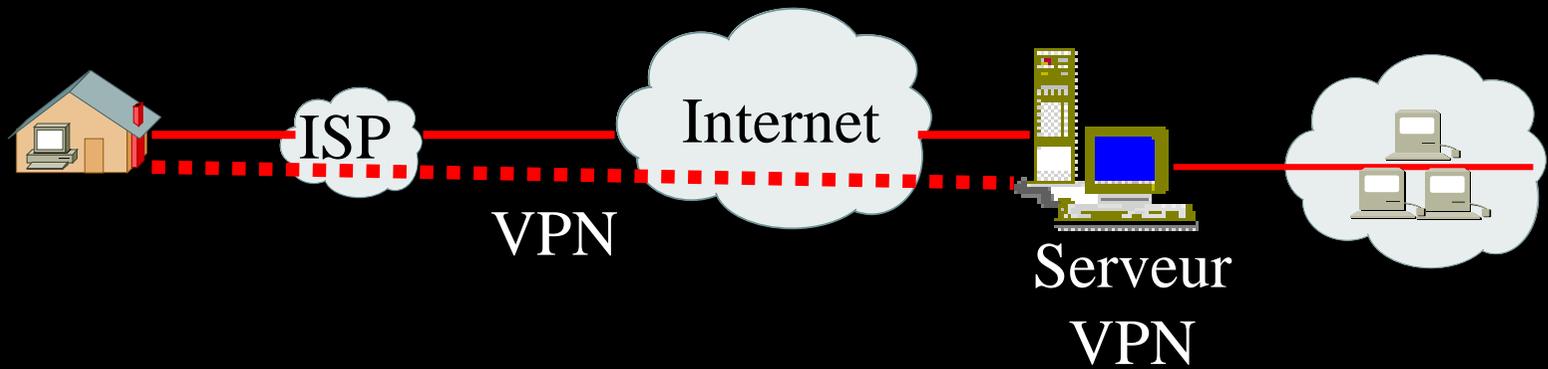
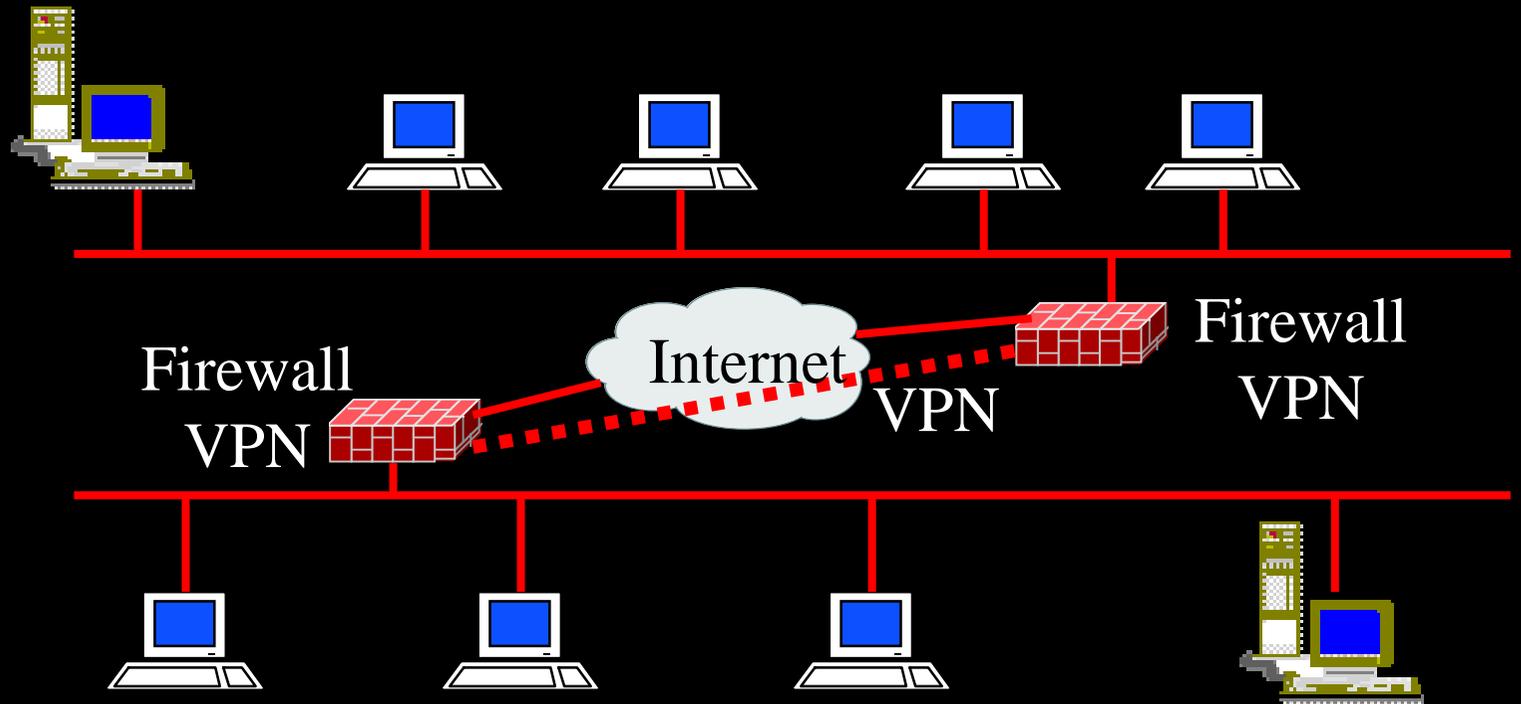
- Economie;
- Sécurité (Authentication, Chiffrement);
- QOS ?

➡ Protocoles:

- **PPTP** (Point to Point Tunnelling Protocol) **Microsoft**
- **L2F** (Layer 2 Forwarding) de **CISCO**
- **L2TP** (Layer 2 Tunneling Protocol) **IETF**
- **IPsec** (IP security) **IETF**



VPN (2/2)



Conclusions (1/7)

➡ IP est un protocole qui a eu du succès grâce à sa simplicité

➡ Comment allier IP et QOS ?

- Transformer IP ?
- Transformer l'infrastructure réseau (Liens et routeurs) ?
- Associer IP à d'autres protocoles ?

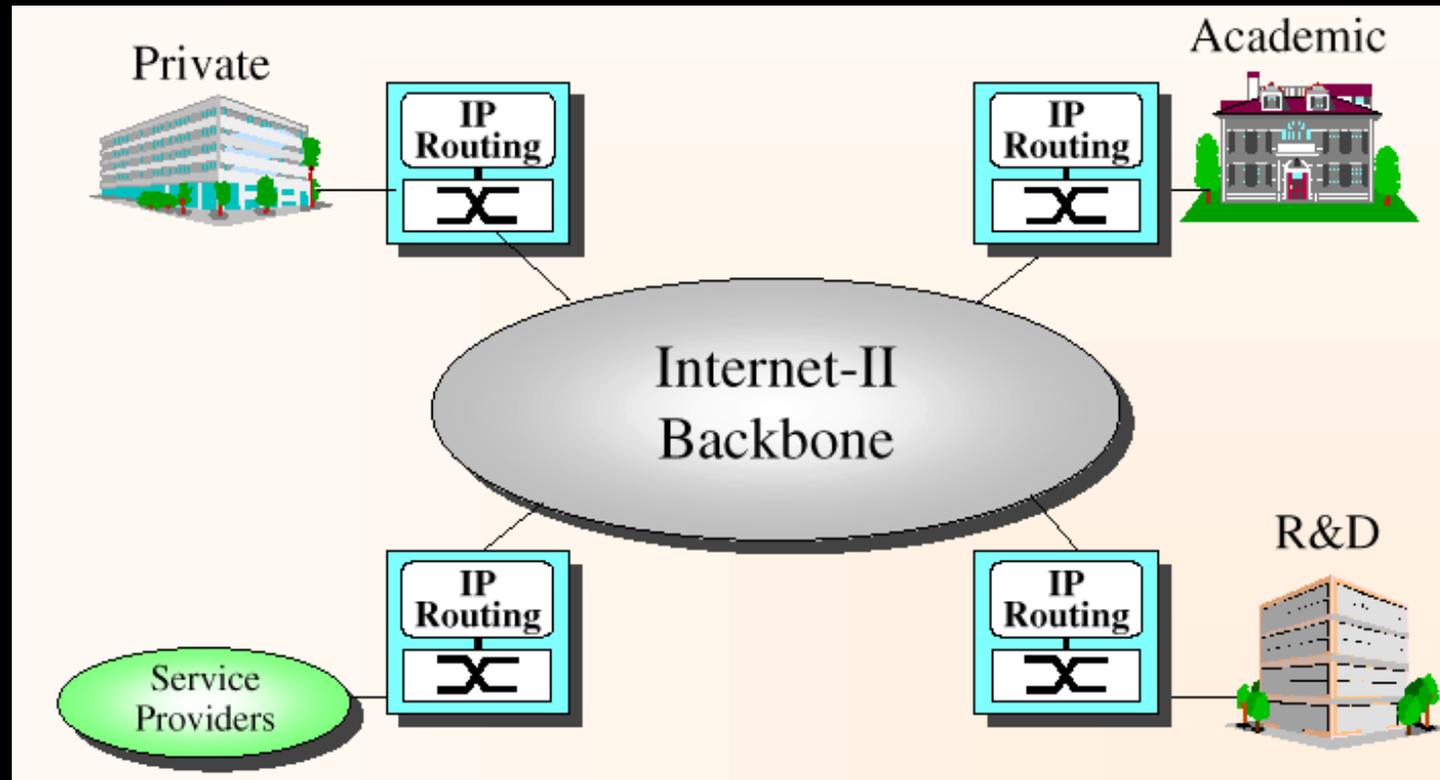


➡ IP multiservices = Facturation différenciée

➡ L'interopérabilité est nécessaire dans l'Internet

Conclusions (2/7)

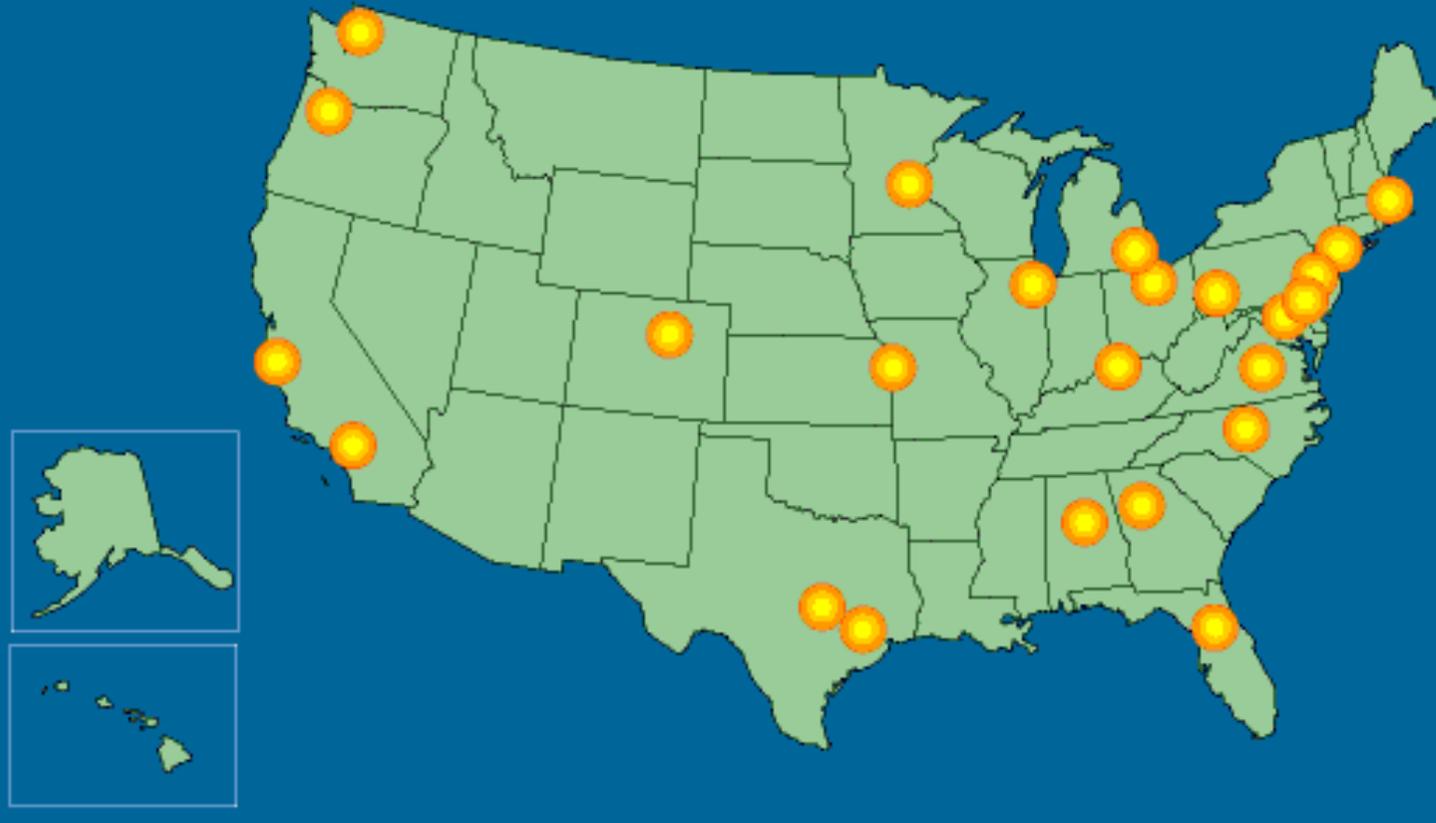
**Next Generation
Internet Initiative**



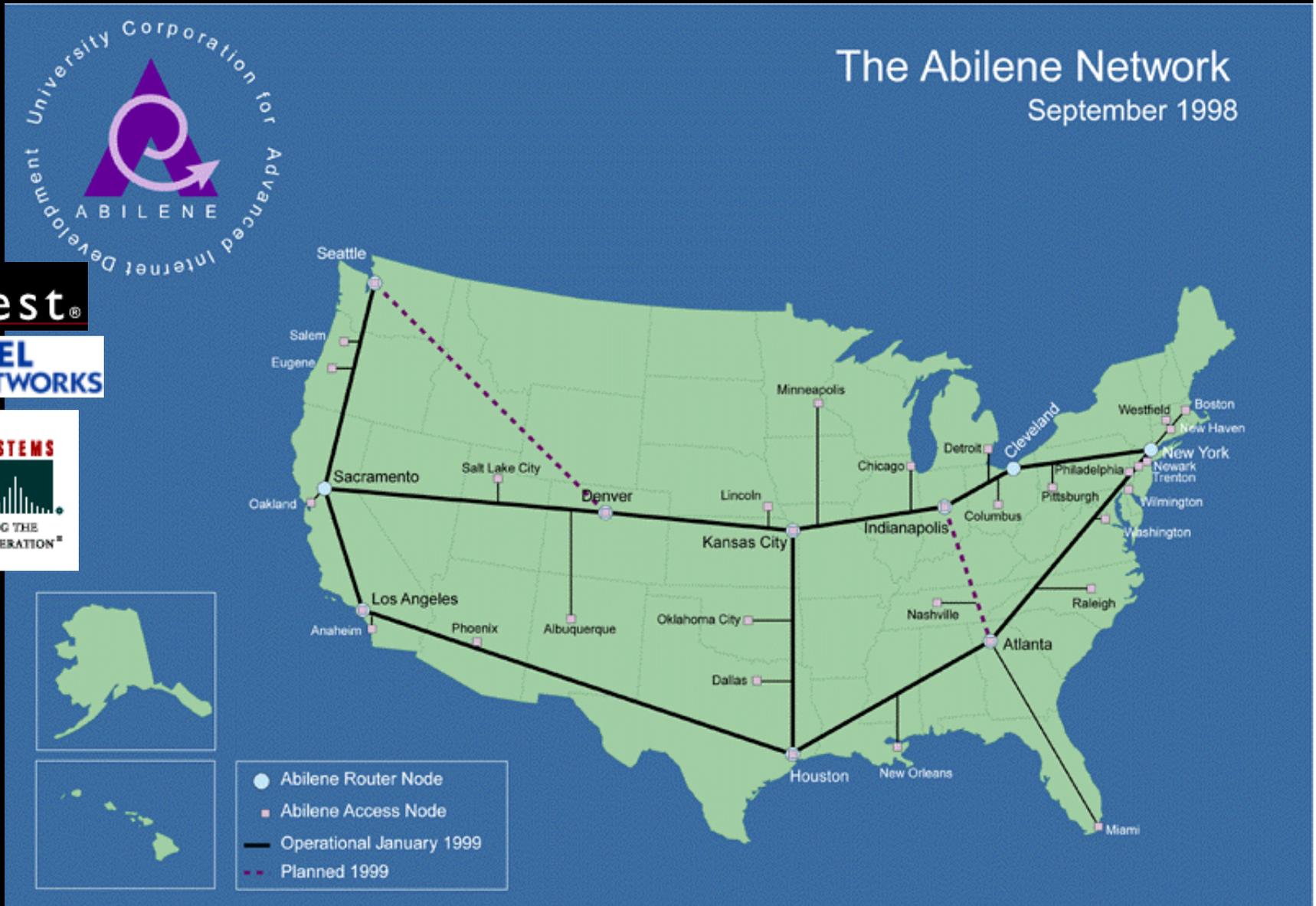
Conclusions (3/7)

Internet2 GigaPoPs

● Denotes GigaPoP Site

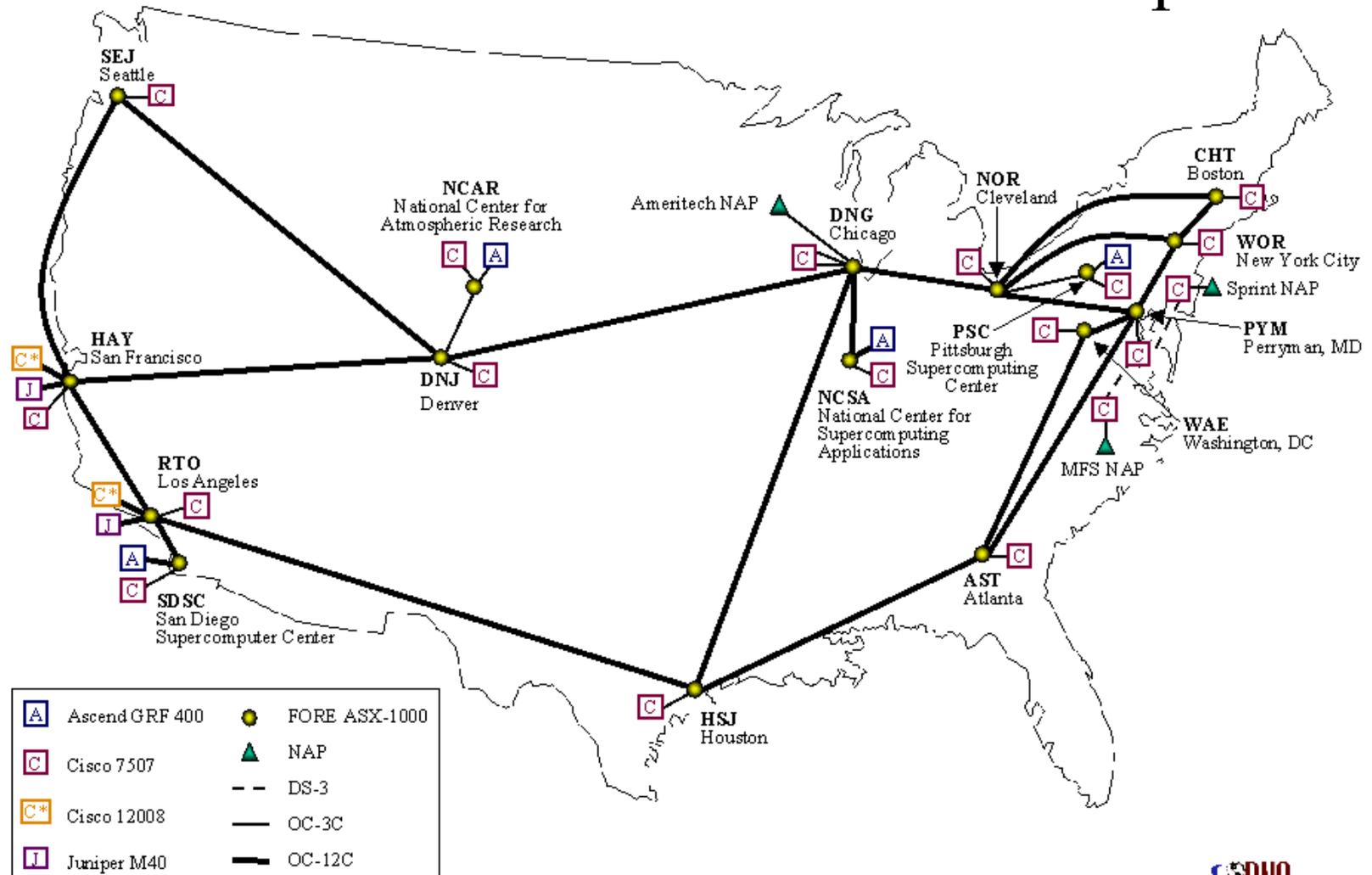


Conclusions (4/7)



Conclusions (5/7)

vBNS Backbone Network Map

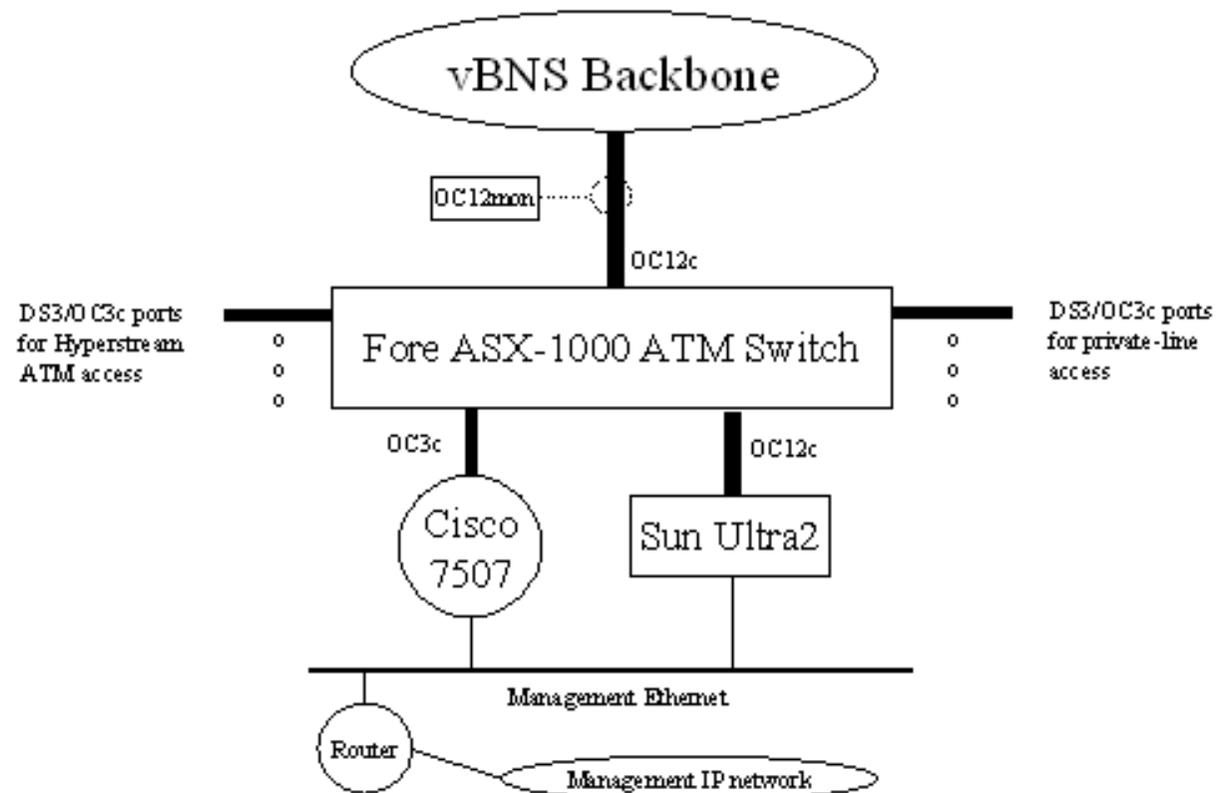


© 1998 MCI Telecommunications Corporation



Conclusions (6/7)

vBNS MCI Terminal POPs



© 1997 MCI Telecommunications Corporation



Conclusions (7/7)

SUPERNET

DARPA's Next Generation Internet Network

