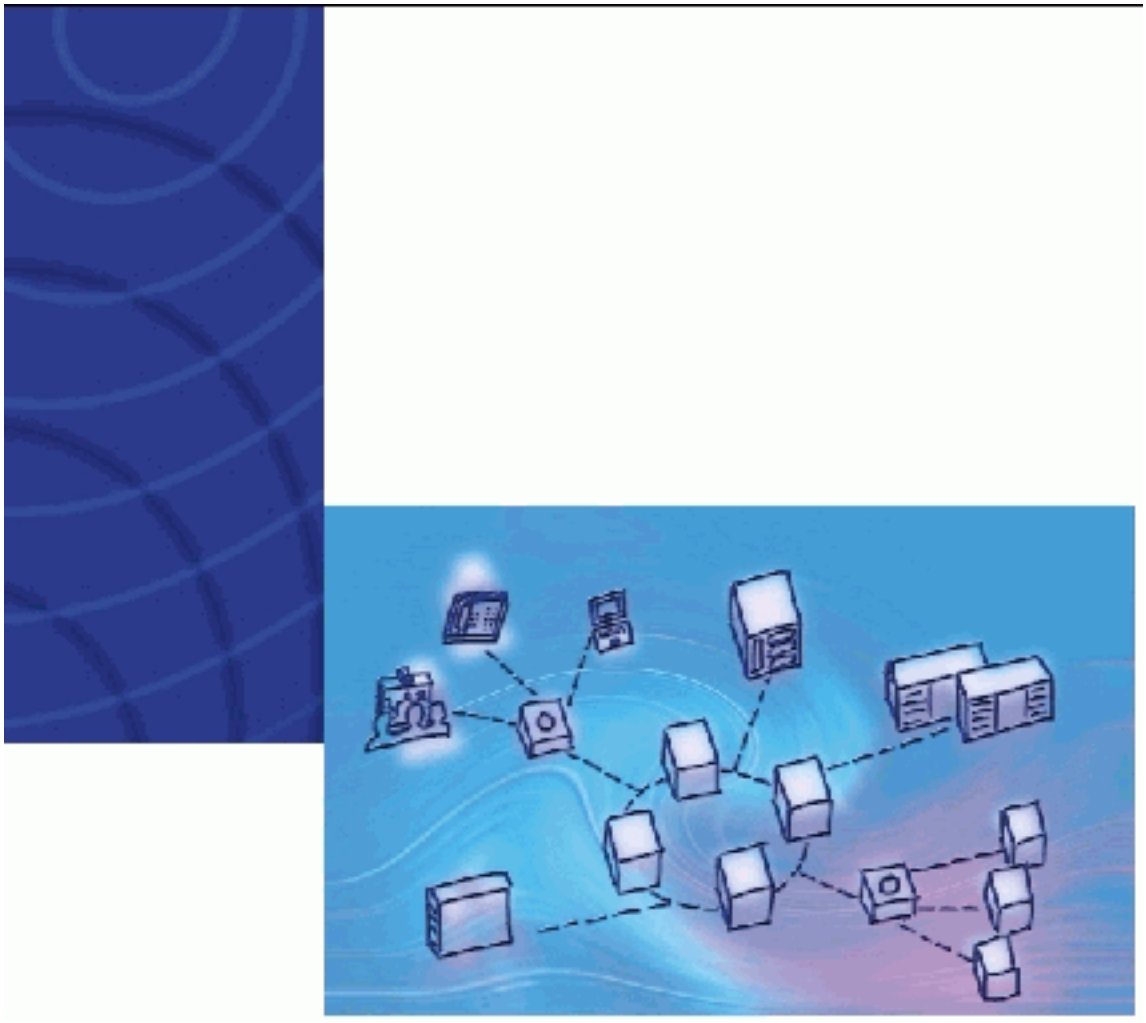


TCP / IP

Avancé et Pratique

swisscom fixnet

TCP / IP

Avancé et Pratique

Un cours pour le personnel technique de Swisscom.

Auteur : Eric Baltensperger
Christian Bersier
Hans Peter Bucher
Patrick Gaillet
Florian Gindrat
Bruno von Gunten
Gilles Landry

Correcteurs : Auteurs
Streisguth Bernard

Méthodique : Eric Barmaz

Classification :

Edition : Août 2002

Version : 2.1.0

Bibliographie

Livres et articles

[1] Lexikon der Datenkommunikation
Autor : Klaus Lipinski
Verlag : DATACOM, (ISBN-Nr. 3-8266-4055-1)

[2] Teleinformatik
Autor : Laurenz Altwegg, Antoine Delley, Patrick Gaillet, Rolf Herheuser, Michel Rast, Bruno Studer, Bruno Wenk
Verlag : Ingenieurschule Freiburg, (ISBN-Nr. 2-940156-13-1)

[4] Lokale Netze
Autor : Franz-Joachim Kauffels
Verlag : DATACOM, (ISBN-Nr. 3-89238-069-4)

[5] Technik der Netze
Autor : Gerd Siegmund
Verlag : Hüthig, (ISBN-Nr. 3-7785-2637-5)

[6] Computer-Netzwerke
Autor : Andrew S. Tanenbaum
Verlag : Wolfram's, (ISBN-Nr. 3-925328-79-3)

[7] Personalcomputer und lokale Netzwerke
Autor : Franz-Joachim Kauffels
Verlag : Markt&Technik, (ISBN-Nr. 3-87791-324-5)

[8] TCP/IP-Grundlagen
Autor : Gerhard Lienemann
Verlag : Heise, (ISBN-Nr. 3-88229-070-6)

[9] TCP/IP-Praxis
Autor : Gerhard Lienemann
Verlag:Heise, (ISBN-Nr. 3-88229-071-4)

[10] IPv6-das neue Internet- Protokoll
Autor : Hans Peter Dittler
Verlag : dpunkt.verlag, (ISBN 3-932588-18-5)

[11] MCSE TCP/IP
Autor : Drew Heywood, Rob Scrimger
Verlag : AMS, (ISBN-Nr. 3-8272-2022-X)

[12] MPLS Technology and Application
Autor : Bruce Davie, Yakov Rekhter
Verlag : Morgan Kaufmann Publishers (ISBN-Nr. 1-55860-656-4)

[13] Le routage dans l'Internet
Auteur : Christian Huitema
Editeur : Exrolles (ISBN-Nr 2-212-08902-3)

Normes et standards

http://www.itu.int
http://www.iso.ch
http://www.ieee.org
http://www.ietf.org
http://www.iana.org
http://www.icann.org

Liens Internet

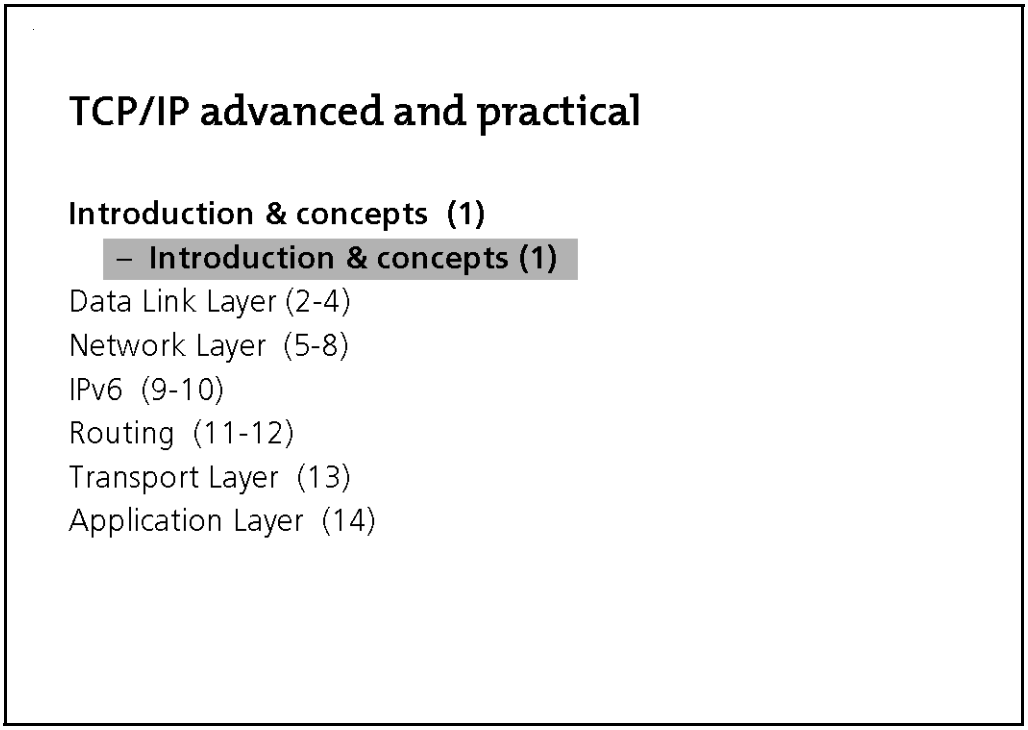
http://www.xdsl.com
http://www.adsl.com
http://www.3com.com
http://www.ripe.net
http://www.switch.ch
http://www.wireless-ethernet.org

Newsgroups

swisscom.fx.nwt.course.tcp-ip

Table des matières

1 Introduction et concepts



Slide 1.1
Introduction et concepts

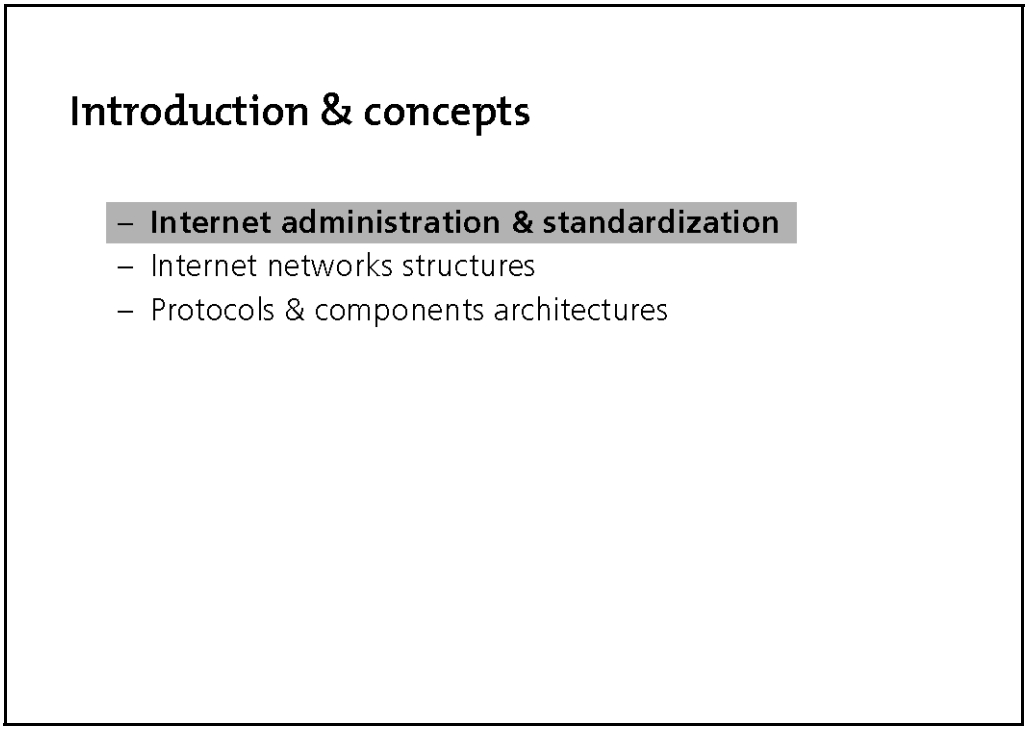
Ce chapitre traite des acteurs présents dans l'Internet, de l'historique de ce réseau, ainsi que des technologies qui y sont utilisées.

Objectifs

A l'issue de ce chapitre, les participants sont capables de se situer dans un environnement Internet, de nommer les différents supports de transmission physique, les couches des modèles de référence OSI et ARPA, ainsi que d'expliquer leur différences.

Ils peuvent également reconnaître les différents éléments présents dans un réseau informatique et indiquer dans quelle couche ils travaillent.

1.1 Administration et standardisation



Slide 1.2
Administration et standardisation

1.1.1 Historique

- **1957 :** Creation of ARPA (Advanced Research Projects Agency)
- **1969 :** Launch of ARPANET project; development of RFCs
- **1973 :** Important protocols are created, Telnet and FTP
- **1974 :** Birth of the concept of «internetwork», TCP
- **1978 :** TCP-IP has reached its actual form
- **1982 :** Migration of Arpanet to TCP/IP. E-mail protocol
- **1983 :** Separation of Arpanet & Milnet (dedicated to military applications). Creation of DNS

Slide 1.3
Historique

L'histoire d'Internet

L'histoire d'Internet a commencé il y a environ 30 ans. Un bref rappel de cette histoire aidera à comprendre le contexte dans lequel Internet s'inscrit.

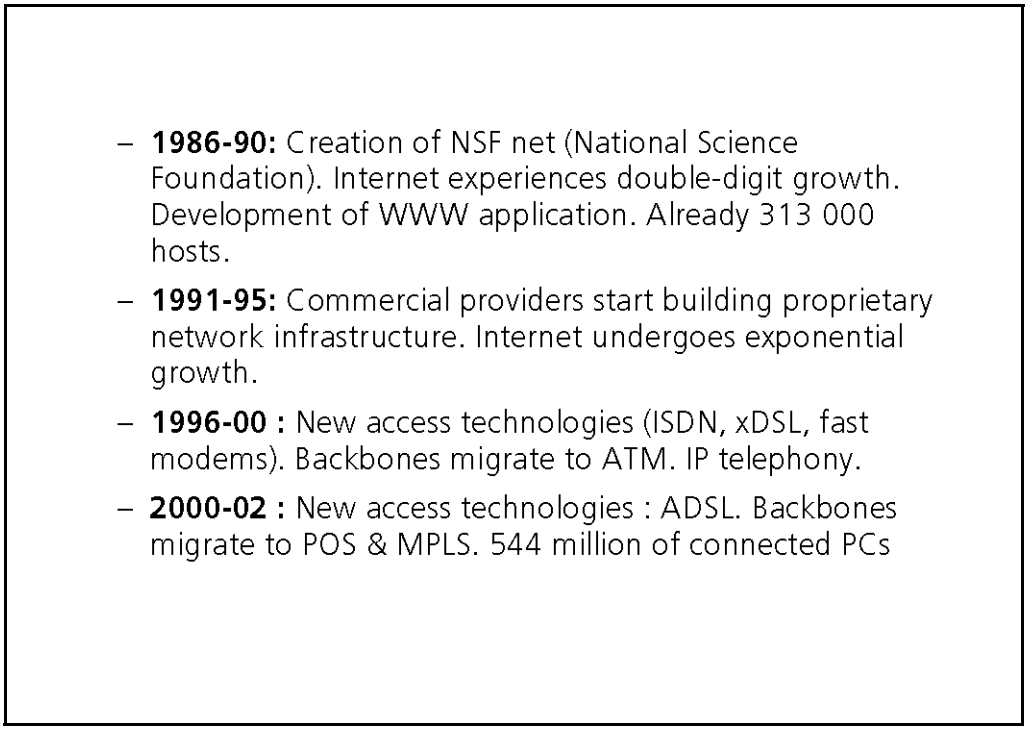
ARPA

Internet a été conçu durant la guerre froide entre l'Est et l'Ouest. La fondation de l'ARPA est une conséquence directe du souhait de l'armée américaine de préserver son avance technique et militaire par rapport à ce qu'était à l'époque l'URSS. Dès le départ, les grands instituts de recherche américains (universités, etc.) ont été également associés.

Recherche et section militaire

En 1983, Internet a été divisé en une section axée sur la recherche et une section militaire.

1.1.2 Développement et croissance



Slide 1.4
Développement et croissance

Le débit des principaux canaux de transmission a été sans cesse augmenté, passant de 56 kbit/s à l'origine à 1,5 Mbit/s au début des années 90, puis à 45 Mbit/s et, depuis 1993, à 622 Mbit/s (STM4), 2,5 Gbit/s (STM16) et 10 Gbit/s (STM64).

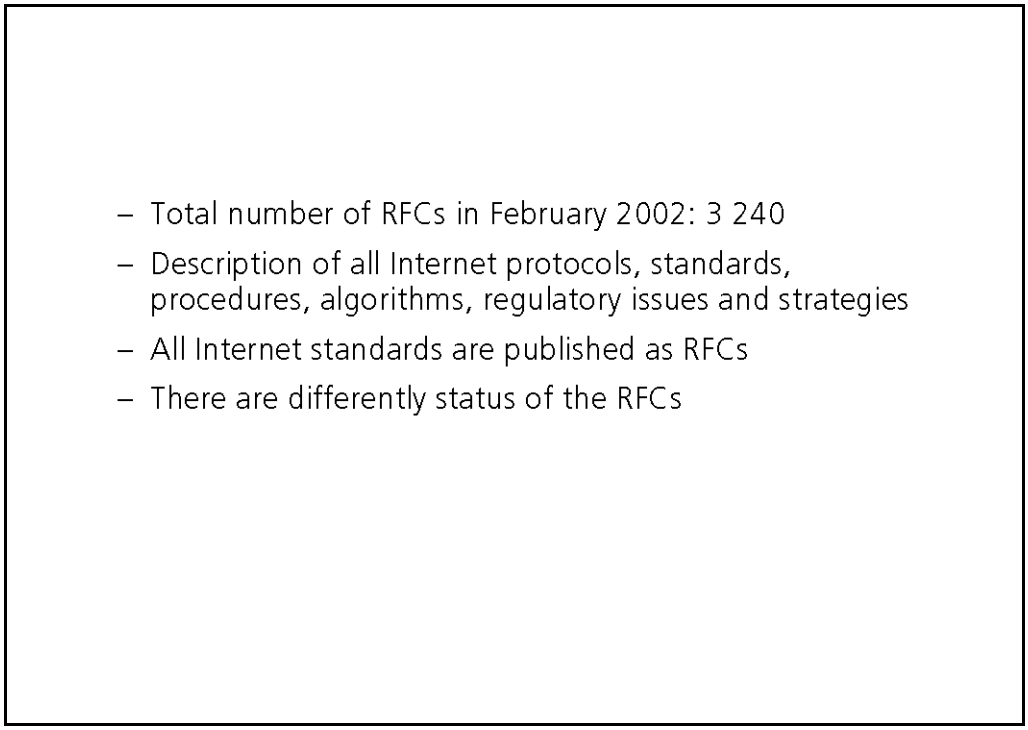
STM4, STM16, STM64

Une estimation, donnée par www.nua.com, porte à 544,2 millions le nombre d'utilisateurs reliés à Internet en février 2002.

544.2 millions d'utilisateurs

Cette évolution est encore loin d'être arrivée à son terme, si l'on songe que des systèmes expérimentaux DWDM (Dense Wave Division Multiplexing) de 10 Tbit/s (Téra) et plus fonctionnent actuellement.

1.1.3 Normes Internet



Slide 1.5
Normes Internet

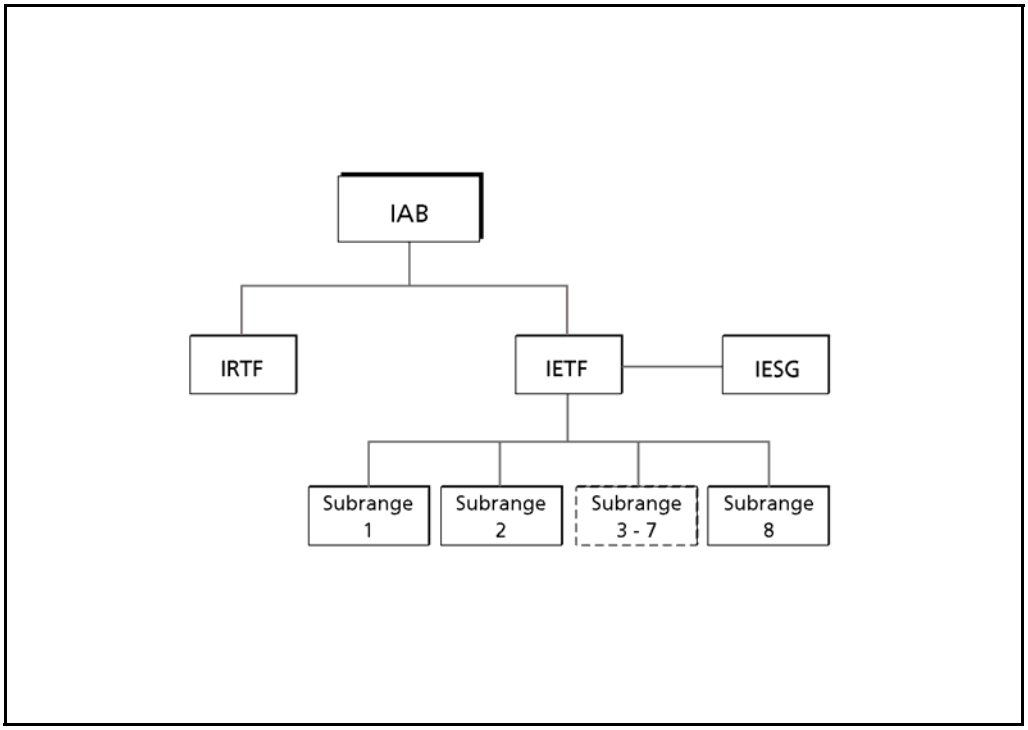
3240 RFC

Les normes Internet proprement dites sont constituées par les "Request For Comments" (appels à commentaires) d'une série comportant désormais plus de 3 240 documents. Les RFC décrivent tous les protocoles Internet, ainsi que les normes, procédés, algorithmes, règles et stratégies de la technique de communication et de réseau. Les normes qui ont été formulées sous forme de RFC se sont généralement assez rapidement imposées.

Statut du RFC

Toutes les normes Internet sont publiées sous forme de RFC, mais la plupart des RFC ne sont pas des normes. Chaque proposition (par exemple un protocole ou la modification d'un protocole) n'est pas devenue une norme par la suite. Certaines propositions restent au stade "expérimental" ou de "proposition" et ne parviennent jamais au statut de protocole "standard".

1.1.4 Instances



Slide 1.6
Instances

IAB, IRTF, IETF, IESG

La plus haute instance coordonnant l'évolution de la gamme des protocoles TCP/IP et le développement d'Internet est l'IAB (Internet Activities Board). En dessous de l'IAB se trouvent l'IRTF (Internet Research Task Force) et l'IETF (Internet Engineering Task Force). Alors que l'IRTF, de taille relativement réduite, se consacre à des tâches de recherche fondamentale sur la gamme des protocoles TCP/IP, l'IETF travaille à résoudre les problèmes se posant à court ou moyen terme. L'IETF est lui-même divisé en huit secteurs coordonnés par un comité commun, l'IESG (Internet Engineering Steering Group).

Les objectifs des différents groupes de travail sont définis lors de réunions organisées à intervalles réguliers, puis publiés sur Internet.

1.1.5 RFC : Etat et statut

State	Importance
Initial	Submitted protocol suggestion
Proposed standard	Submitted protocol suggestion, as standard suggested
Draft standard	Proposed protocol which has been reviewed and on the basis of which at least two independent implementation run
Standard	An official standard of the TCP/IP protocol family
Experimental	Protocol for experimental purposes only
Informational	RFC for information only
Historic	Protocol that is no longer in use

Status	Importance
Required	All Internet nodes must support the protocol
Recommended	All Internet nodes should support the protocol
Elective	Internet nodes can use this protocol
Limited use	Protocol not intended for general use
Not recommended	Protocol not recommended

Slide 1.7
RFC : Etat et status

RFC sont gratuits

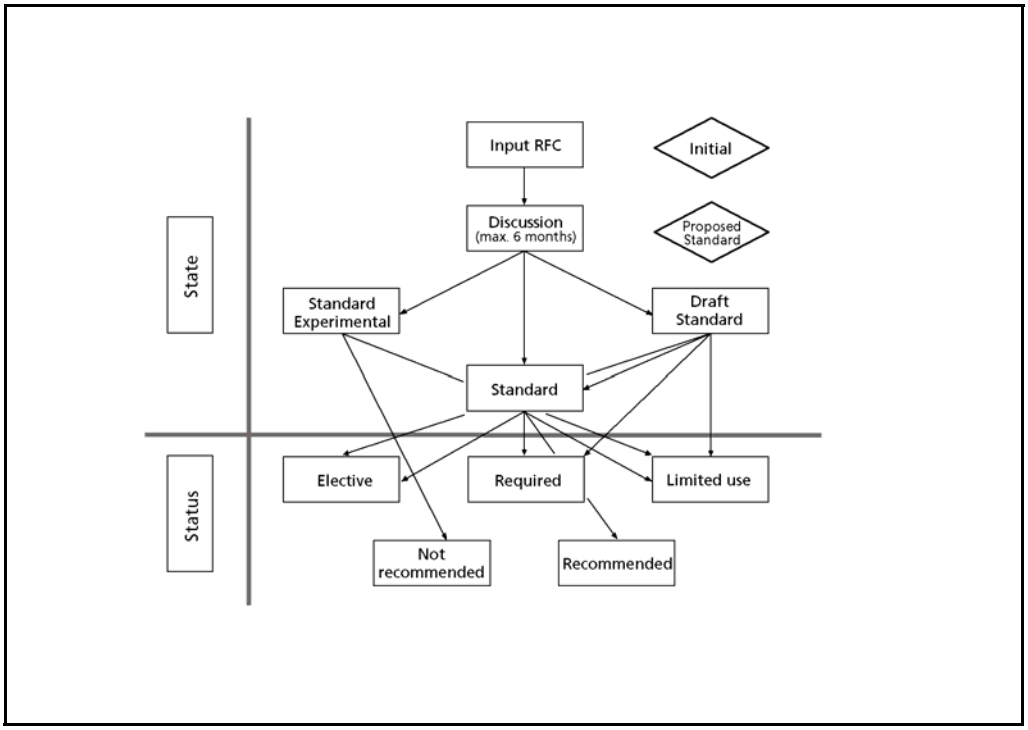
Les différents RFC sont publiés et sont librement accessibles à travers Internet. Chaque RFC est doté d'un état (state) et/ou statut (status).

RFC, base de donnée

Les RFC sont numérotés par ordre chronologique. Si un RFC est modifié, il reçoit un nouveau numéro. Tous les trois mois est publié un index permettant de retrouver la version actuelle d'un RFC.

Un RFC n'est au départ qu'une recommandation et n'est adopté qu'après avoir été discuté. La conversion d'un tel document en matériel et logiciels est autorisée par sa publication sur Internet. Les décisions des différents groupes de l'IAB sont par exemple publiées sous formes de "Request For Comments".

1.1.6 RFC : Normalisation



Slide 1.8
RFC : Normalisation

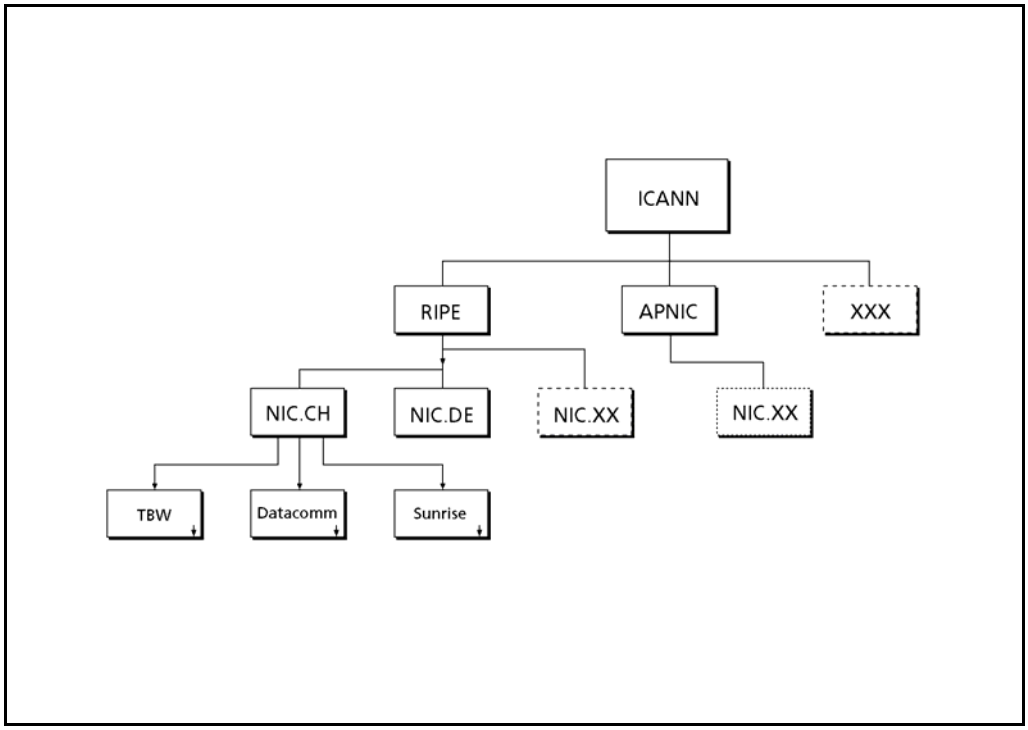
RFC

Les responsables du réseau ne se rencontrant plus personnellement en Californie du Sud pour délibérer sur un nouveau RFC, on utilise ce que l'on appelle des projets (drafts). Les projets sont en quelque sorte des documents de travail de l'IETF, fondé en 1986, où des groupes de travail lui sont rattachés.

RFC 1111

Ils sont publiés sur Internet pour une durée maximum de six mois, pendant laquelle ils sont discutés, avant d'être éventuellement publiés en tant que RFC de l'IETF ou de groupe de gestion de l'IESG. Le RFC 1111 (Request for Comments on Request for Comments) définit la structure des RFC et leur normalisation.

1.1.7 Administration d'Internet



Slide 1.9
Administration d'Internet

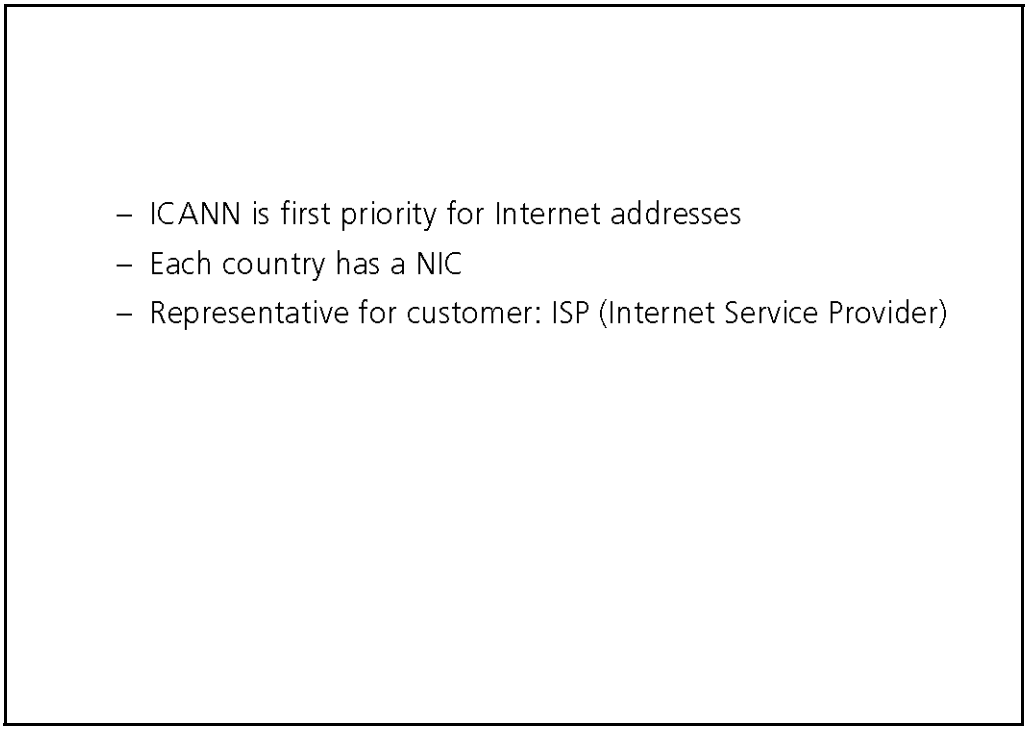
FNC

Lorsque l'armée s'est retirée au début des années 80, il a été décidé de confier l'administration au FNC (Federal Network Council).

RIPE, APNIC

L'ICANN (Internet Corporation for Assigned Names and Numbers) est probablement l'instance la plus importante d'Internet. L'ICANN est une institution privée à but non lucratif, chargée de la gestion des adresses IP et des noms de domaine. Il forme ainsi le sommet de la hiérarchie, le niveau immédiatement inférieur étant formé par exemple des contrôleurs IP qui lui sont subordonnés : RIPE (Réseaux IP Européens) et APNIC (Asian-Pacific Network Information Center).

1.1.8 Enregistrement des adresses



Slide 1.10
Enregistrement des adresses

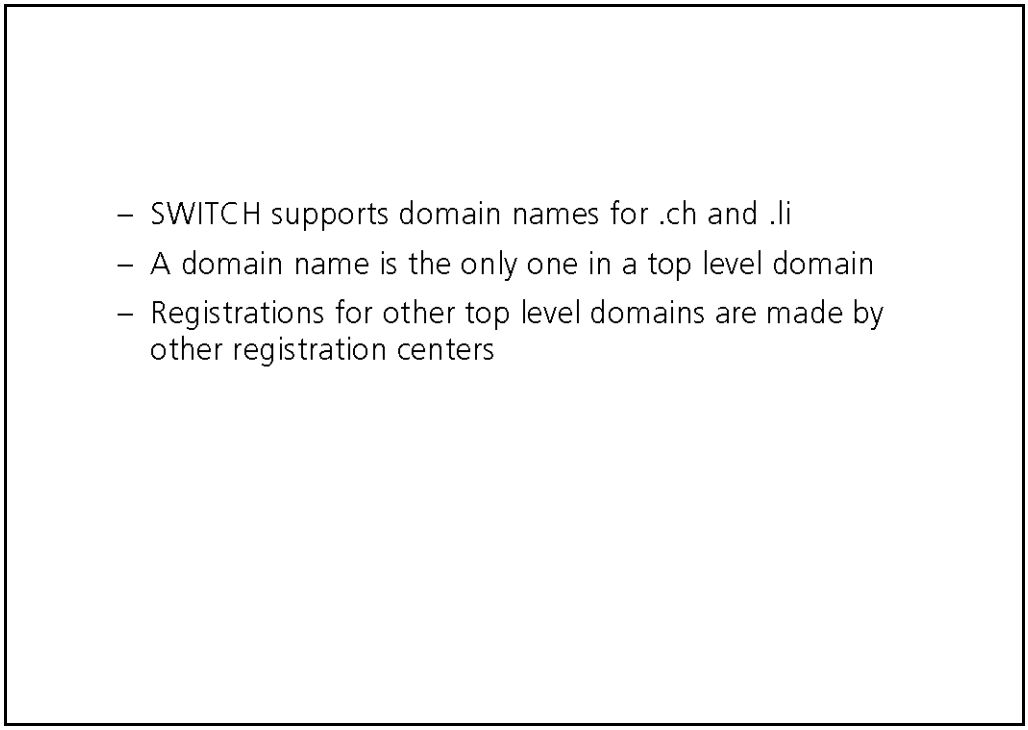
IANA, ICANN

De nombreux "critiques du système" redoutaient apparemment surtout le monopole de l'IANA (Internet Assigned Numbers Authority) dans le domaine de l'attribution de domaines IP et de domaines de premier niveau. Ils voulaient mettre en place de nouveaux domaines de premier niveau indépendamment de l'IANA. C'est pour cela qu'a été fondée l'organisation de droit privé ICANN.

national NIC

Les trois institutions ICANN (IANA), RIPE et APNIC gèrent et attribuent les plages d'adresses IP nécessaires aux NIC (Network Information Center) nationaux. Tout en bas de la hiérarchie se trouvent les fournisseurs d'accès, ou plutôt leurs clients, dont les ordinateurs peuvent être identifiés à l'aide de l'adresse IP.

1.1.9 Administration des noms de domaine



Slide 1.11
Administration des noms de domaine

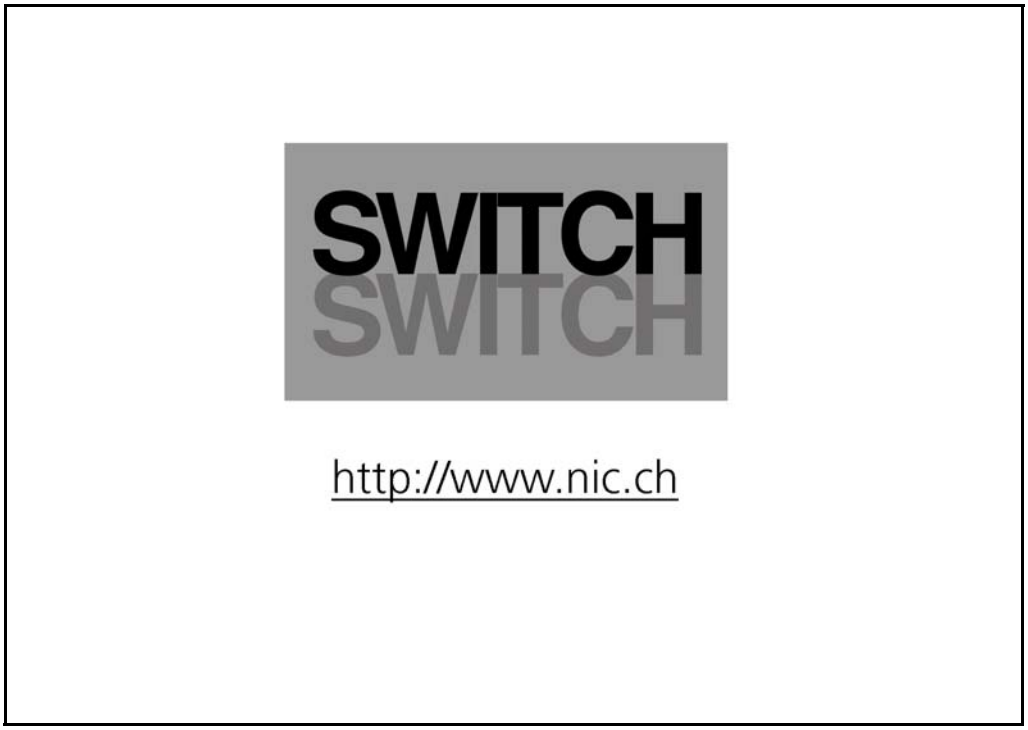
SWITCH exploite le centre d'enregistrement des ccTLD (Country Code Top Level Domains) ".ch" et ".li". Diverses autres instances sont chargées des autres noms de domaine de premier niveau.

La responsabilité de l'enregistrement et de l'administration des noms de domaine à l'intérieur du ccTLD ".ch" a été déléguée en 1987 par l'IANA à SWITCH. La délégation de responsabilité pour le ccTLD ".li" date de 1993.

Nom de domaine

Un nom de domaine doit être univoque. Un nom de domaine terminé par ".ch" ou ".li" doit comporter 3 lettres ou chiffres au moins, 24 au plus et doit commencer par une lettre ou un chiffre. Le seul caractère spécial autorisé est le trait d'union (-) Ce dernier ne doit toutefois pas figurer au début ou à la fin du mot ou de la séquence de chiffres. Les lettres accentuées, telles que é, â, ä, ö, etc. ne sont pas autorisées.

1.1.10 SWITCH



Slide 1.12
SWITCH

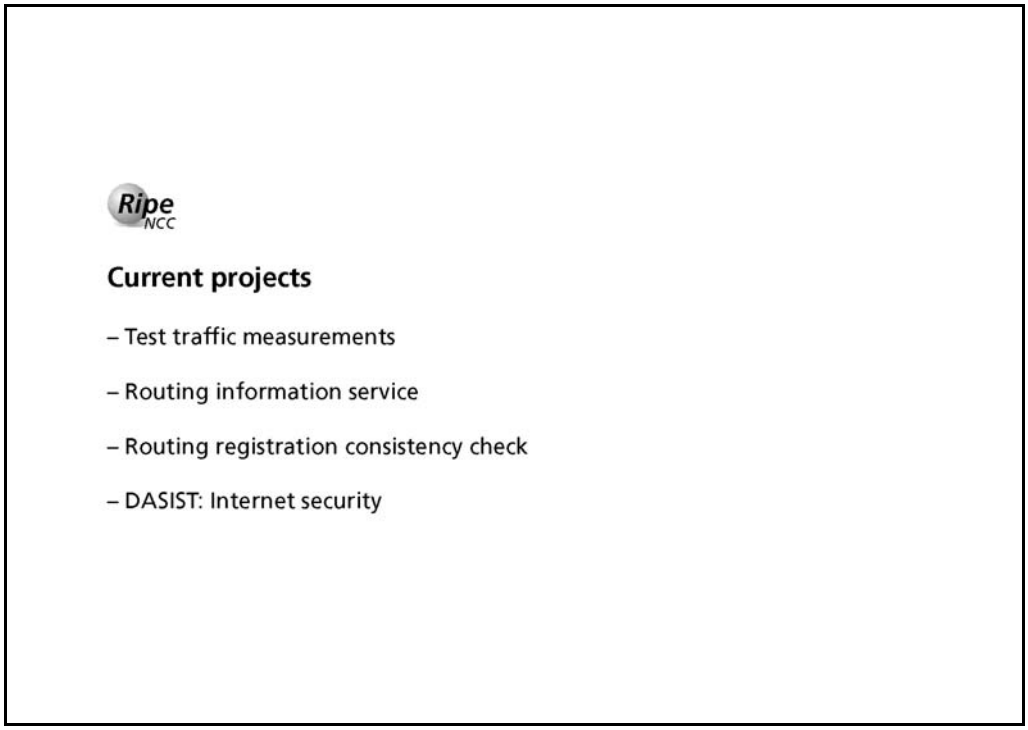
SWITCH

SWITCH (Swiss Academic and Research Network) est une fondation créée en 1987 par la fédération et les huit universités cantonales pour favoriser la diffusion des techniques modernes de transmission.

SWITCH exploite un puissant réseau de recherche pour les universités et l'enseignement supérieur technique. Comme nous l'avons déjà indiqué plus haut, elle est également chargée de la gestion des domaines ".ch" et ".li".

SWITCH Domain Name Registration
Limmatquai 138
CH-8001 Zurich, Suisse
e-mail : helpdesk@nic.ch
Téléphone : 01 268 15 80

1.1.11 RIPE



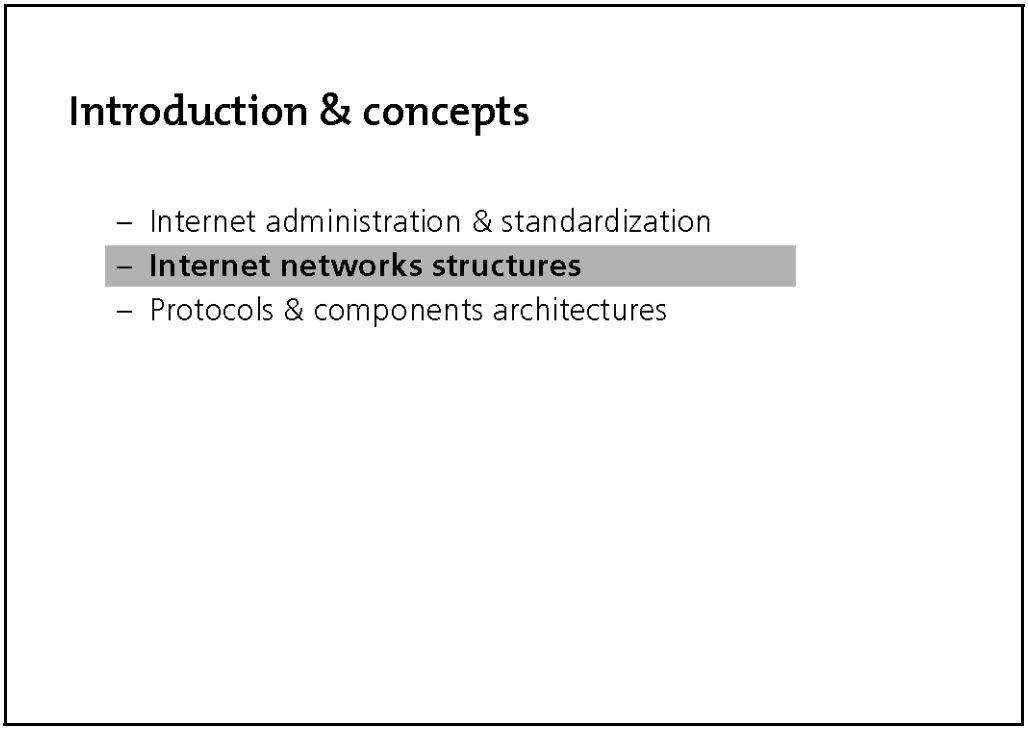
Slide 1.13
RIPE

RIPE, NCC, Nom de domaine

RIPE est une association à but non lucratif visant à développer les réseaux reposant sur TCP/IP en Europe. RIPE a été fondée en 1989 et organise régulièrement des séances afin de coordonner les sujets techniques correspondants. Elle exploite un NCC (Network Coordination Centre) pour traiter les aspects opérationnels, tels que la gestion des noms de domaine européens et des tableaux d'acheminement. RIPE est uniquement compétent pour l'Europe. Tous les documents produits sont publics.

Sont membres de RIPE : BelWue, le CERN, EASInet, EUnet, GARR, HEPnet, NORDUnet, SURFnet, SWITCH, XLINK.

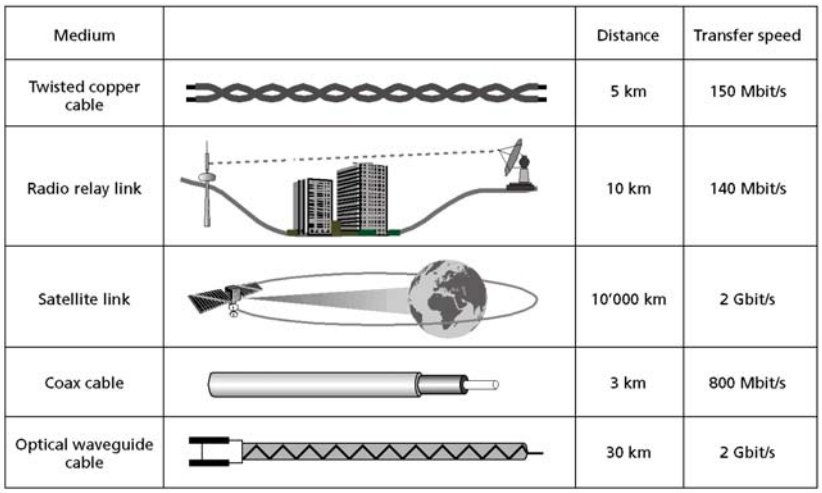
1.2 Structure des réseaux



Slide 1.14
Transmission

Les supports de transmission sont les véritables transporteurs des paquets d'informations. On distingue entre transmission physique et transmission logique.

1.2.1 Transmission physique



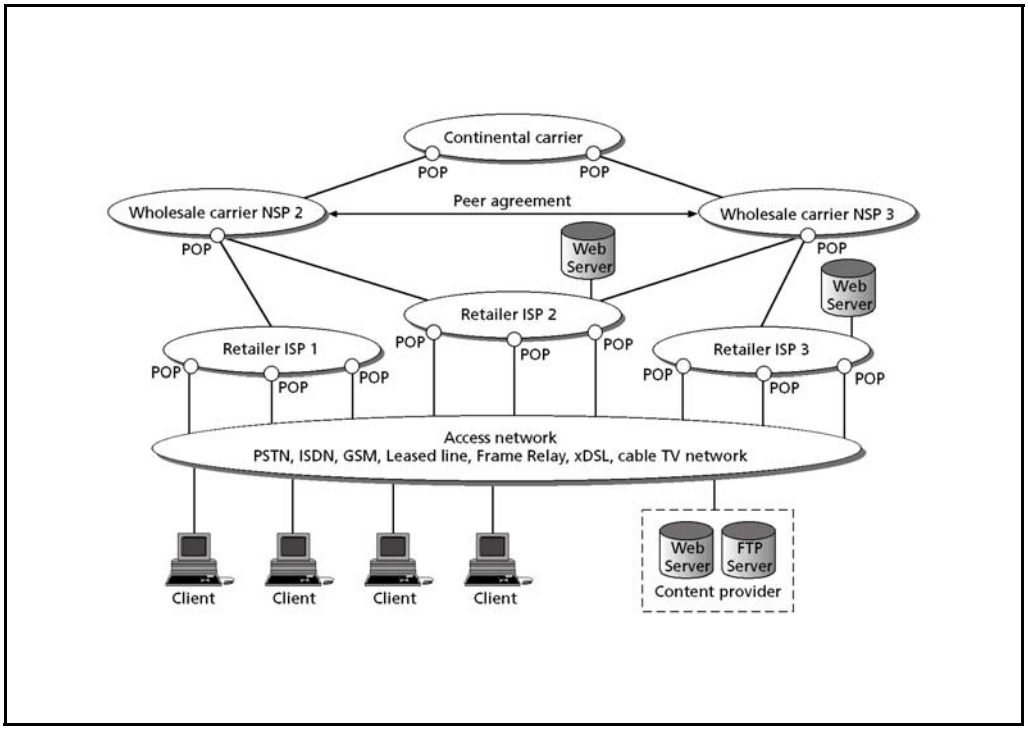
Slide 1.15
Transmission physique

La transmission physique des informations s'effectue à travers des lignes. La ligne désigne ici la liaison concrète entre deux points. Cette liaison peut être constituée par un câble en cuivre, à fibre optique, une liaison radio ou par satellite.

ISP, CATV

Internet se compose essentiellement d'un ensemble de liaisons diverses de cette nature. Dans le domaine des fournisseurs d'accès à Internet (ISP : Internet Service Provider), tels les gros opérateurs nationaux et internationaux ainsi que les plus grandes entreprises (UBS, Nestlé), ces liaisons physiques sont généralement des fibres optiques. Chez les clients particuliers et les PME, la liaison à Internet passe généralement par les câbles téléphoniques ordinaires. Il est également possible de réaliser une liaison à travers la télévision par câble (CATV) ou par satellite.

1.2.2 L'accès au réseau



Slide 1.16
L'accès au réseau

Pour accéder à Internet, vous avez besoin d'un modem, d'une ligne téléphonique, d'un PC avec un logiciel Internet et d'un abonnement auprès d'un fournisseur de services Internet (ISP : Internet Service Provider).

POTS

Les petites entreprises ou les particuliers accédant régulièrement à Internet optent souvent pour des lignes ISDN, ou encore ADSL, qui assurent un accès plus rapide et plus fiable (moins d'erreurs).

ISDN, ADSL

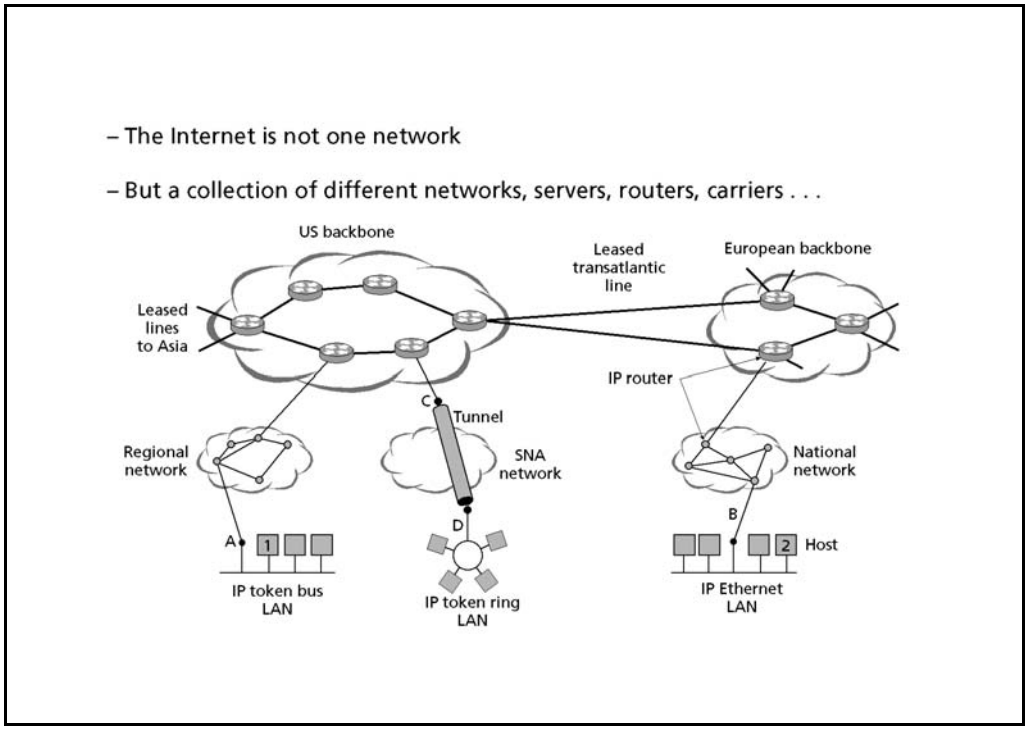
Les entreprises plus importantes utilisent pour cela des lignes louées, qui les relient directement au point de présence (PoP : point of presence) le plus proche de leur fournisseur d'accès.

Leased Line

Lorsque vous appelez une adresse Internet (URL), le logiciel de l'utilisateur (le navigateur) examine d'abord la mémoire cache de son système. Si la page recherchée est déjà mémorisée, elle est chargée dans le navigateur et affichée sur l'écran de l'utilisateur. Dans le cas contraire, le programme transmet la demande de l'utilisateur au prochain ordinateur d'un nœud Internet. Dans les PME et chez les particuliers, c'est généralement l'ordinateur du fournisseur d'accès à Internet (bluewin, AOL, CompuServe, etc.) qui s'en charge. Dans les entreprises, c'est en général un ordinateur spécial, désigné par serveur Proxy qui joue se rôle.

URL, Cache, Serveur proxy

1.2.3 Internet



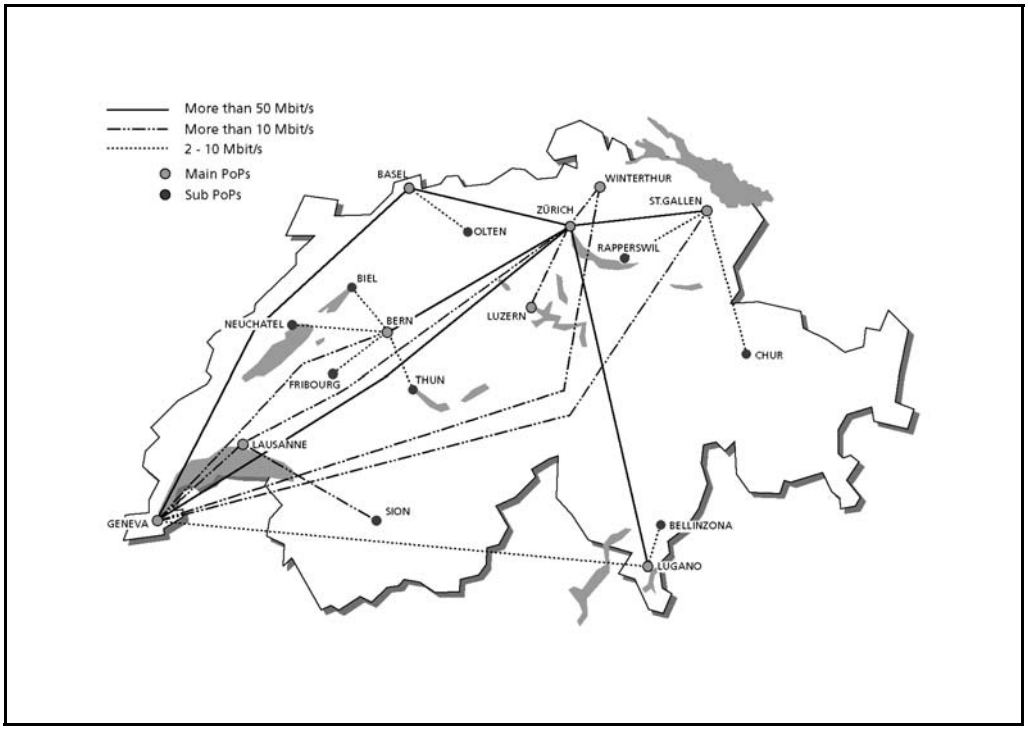
Slide 1.17
Internet

Le terme Internet signifie littéralement "inter-réseau", ce qui décrit très bien ses fonctions et ses tâches.

Une caractéristique essentielle d'Internet est qu'il n'est pas organisé et exploité de manière centralisée par un seul opérateur. Il se compose au contraire de nombreux sous-réseaux, gérés de manière décentralisée, mais tous reliés entre eux.

Les règles d'adressage univoque au niveau mondial, ainsi que les caractéristiques des protocoles TCP/IP doivent être respectées pour assurer la compatibilité de l'ensemble. D'où les avantages liés au caractère international du réseau, mais aussi les inconvénients résultant d'une qualité de réseau très hétérogène (par exemple, sur le plan des performances ou de la sécurité). Les lacunes de l'architecture d'Internet en matière de sécurité doivent être comblées à l'aide de procédés de sécurité tels que le codage, la signature électronique ou les Firewalls.

1.2.4 IP-plus

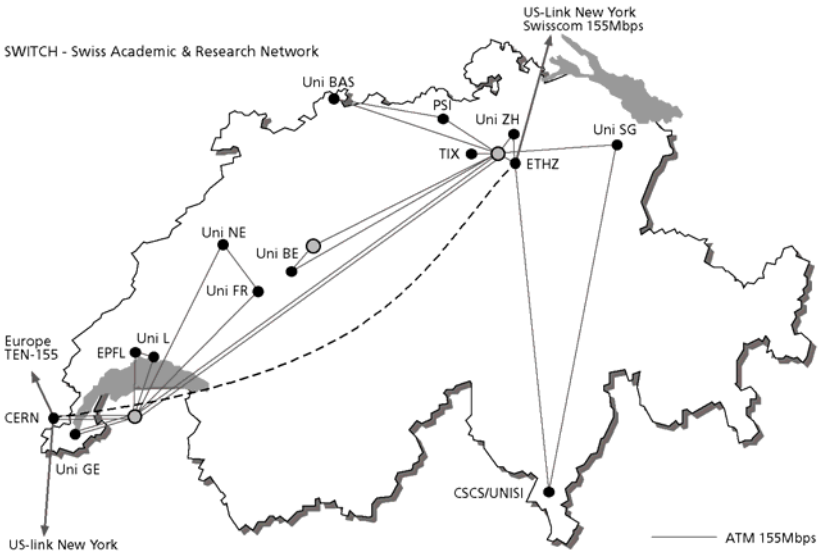


Slide 1.18
IP-plus

IP+ est un des "coeurs" du réseau Internet en Suisse. Si les clients académiques sont connectés au réseau SWITCH, la plupart des clients commerciaux (ISP:Internet Service Provider) le sont à IP+. Ce réseau, propriété de Swisscom, est composé d'une étoile de links principaux à plus de 50 Mbit/s, centrée à Zürich.

Depuis les extrémités de cette étoile, des links secondaires, classés en deux catégories (2-10 Mbit/s et > 10 Mbit/s) partent en direction de "sous-points de présence" (Sub PoP's).

1.2.5 Switch



Slide 1.19
Switch

Réseau ATM, POS

Le nouveau SWITCHlan est un réseau ATM reposant sur l'infrastructure SDH de diAx, autour d'une épine dorsale composée d'une liaison POS (Packet over Sonet) de 2,5 Gbps entre le CERN et l'EPFZ.

STM-1, SDH ring

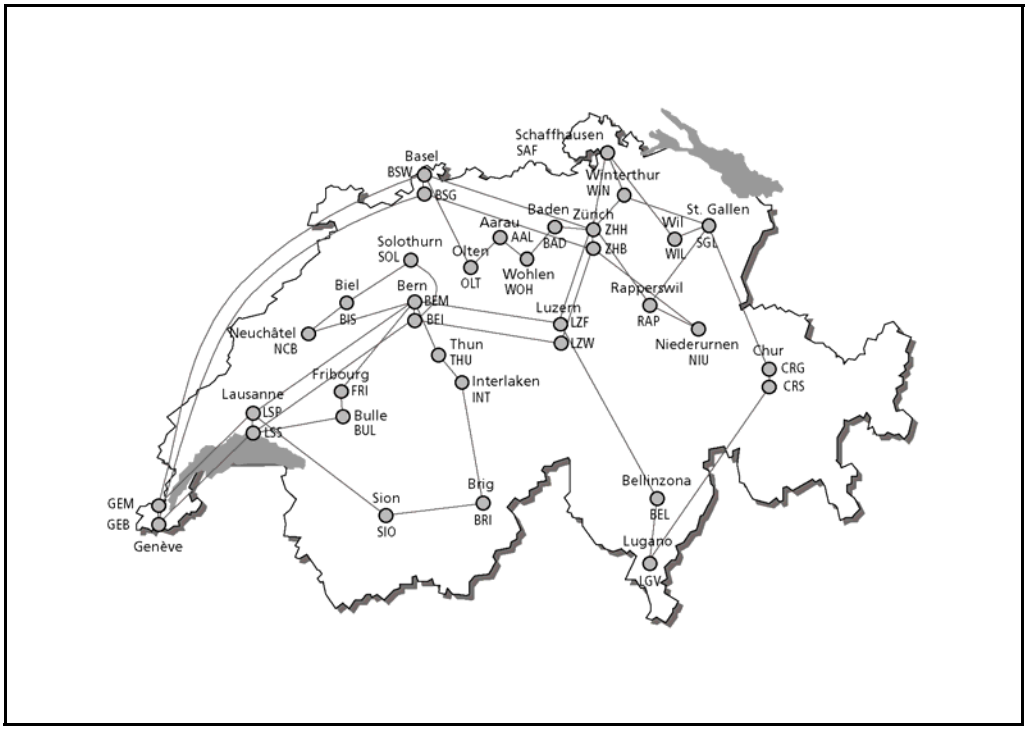
Les liaisons STM-1 sont construites d'après une topologie ATM en double étoiles avec des concentrateurs situés au Lignon (GE) et à Altstetten (ZH). Chaque site est relié au sein du réseau principal ATM par deux liaisons STM-1 qui utilisent physiquement différents chemins sur le circuit SDH.

Les hautes écoles techniques connectées sont reliées à SWITCHlan à travers le réseau de Cablecom Media AG. Les points d'interconnexion entre ces deux réseaux sont situés à l'EPF de Zurich, à l'université de Berne et à Lausanne.

lignes louées

Quelques sites mineurs sont reliés à SWITCHlan par des lignes louées à faible débit.

1.2.6 IPSS



Slide 1.20
IPSS

IPSS

La figure représente la topologie géographique des lignes du réseau IPSS sur lequel repose la plupart des nouveaux services à large bande offert par Swisscom. Le coeur du réseau relie sous la forme d'un double circuit toutes les localités importantes de la Suisse.

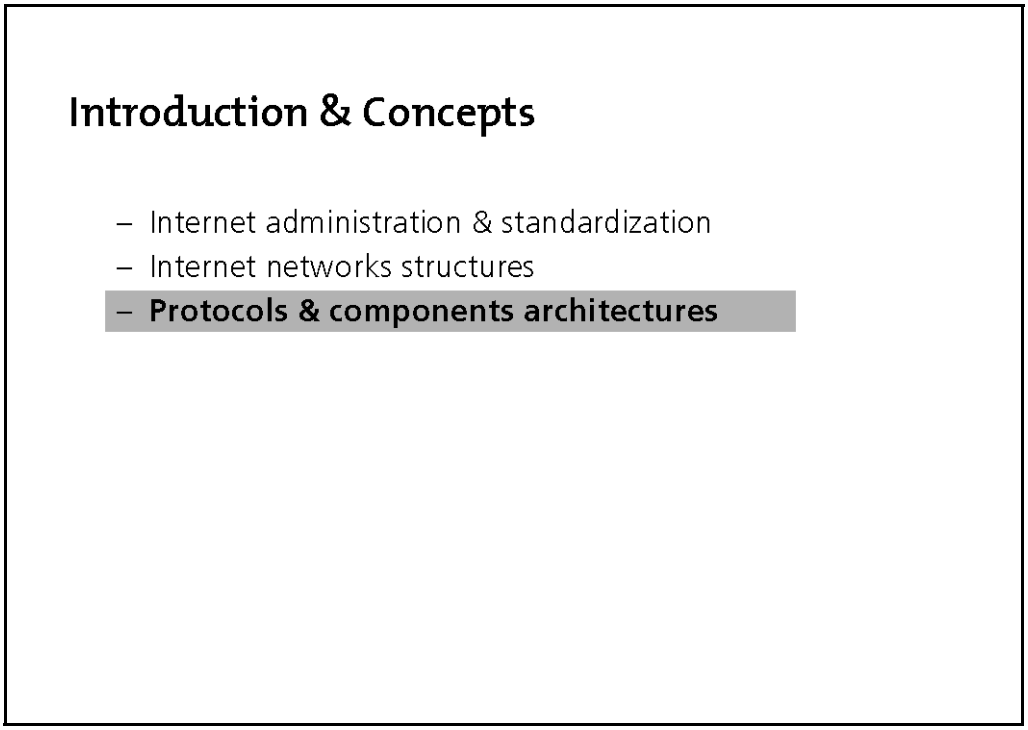
BBCS, LAN-I

Le but est de prendre la première place sur le marché des services destinés à l'utilisateur final et reposant sur IP. IPSS offre des services de base, en quelque sorte des produits brut. Ils permettent la réalisation de services à valeur ajoutée tels que BBCS (interconnection pour l'accès Internet ADSL), LAN-I, etc...

Connectivité "bout-en-bout"

Le réseau IPSS offre le transport des paquets IP avec une fonctionnalité "bout-en-bout", selon le type de connexion recquis. Il met à disposition des qualités de services différenciées, tenant compte des exigences de service du client (SLA).

1.3 Architectures de protocoles et composants



Slide 1.21
Architectures de protocoles et composants

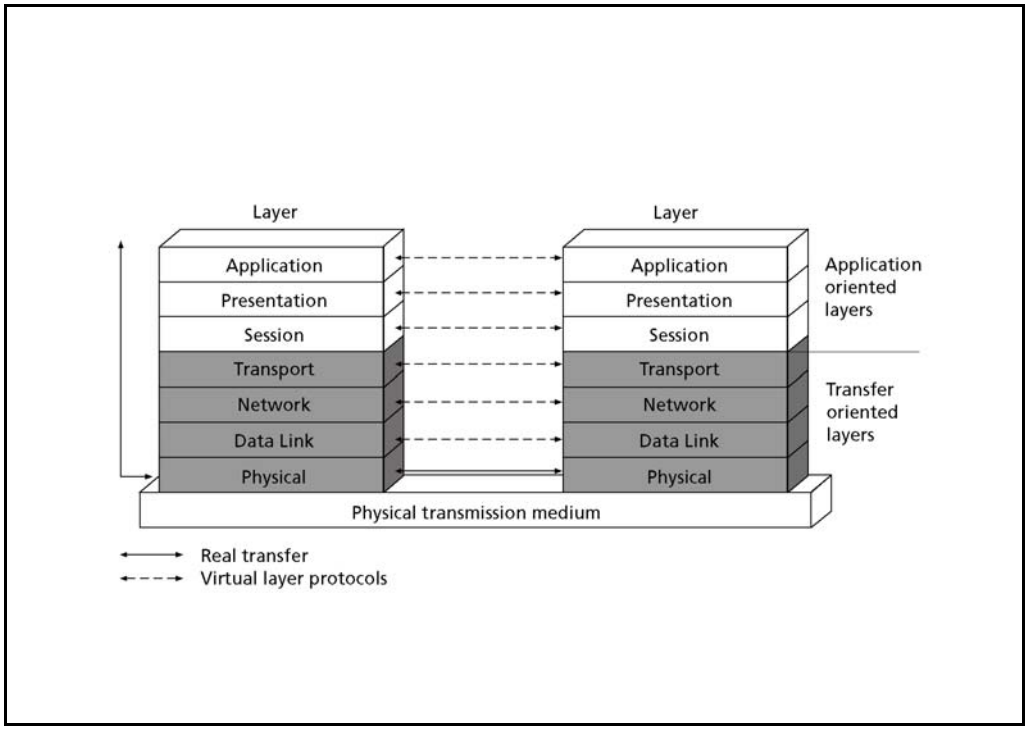
Un protocole est un ensemble de règles ou de formalités pour l'échange de messages entre partenaires, concrètement entre ordinateurs. Les protocoles coordonnent et rendent possible l'échange de messages qui ne pourrait se dérouler efficacement sans eux, surtout lorsque le nombre de participants est important.

La communication entre ordinateurs est très complexe. Toutes les tâches requises ne peuvent donc être traitées efficacement dans le cadre d'un seul protocole.

L'architecture des protocoles nous montre les relations qui s'établissent entre les différents protocoles d'une même famille. Les architectures de protocoles les plus utilisées sont:

- l'architecture ISO/OSI, le véritable modèle de référence;
- l'architecture ARPA.

1.3.1 Architecture OSI



Slide 1.22
Architecture OSI

Model ISO/OSI, les sept couches

Le modèle (officiellement modèle de référence ISO-OSI) sert actuellement de cadre général de description des caractéristiques et fonctions des protocoles. L'empilage des couches repose sur le principe selon lequel chaque couche fournit certains services à la couche placée immédiatement au-dessus d'elle. Le modèle décrit simplement quelles tâches les couches doivent accomplir. Les principes suivants ont abouti au système en sept couches du modèle OSI :

- Une nouvelle couche doit être créée chaque fois qu'un nouveau degré d'abstraction est nécessaire.

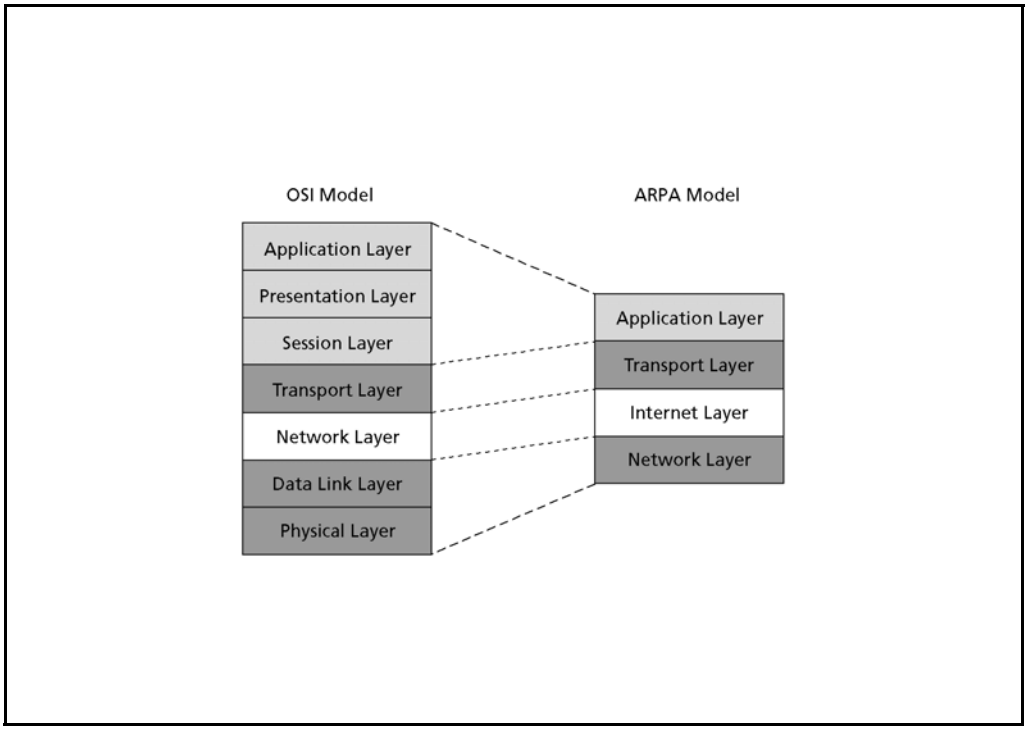
Chaque couche a une fonction

- Chaque couche doit remplir une fonction bien définie.
- Le choix de la fonction a pris en compte la définition de protocoles normalisés au niveau international.
- Les limites entre les différentes couches ont été définies de façon à ce que le flux d'informations à travers les interfaces soit aussi réduit que possible.

Maîtrise des couches

- Le nombre de couches est suffisamment élevé pour éviter la cohabitation de plusieurs fonctions différentes dans une même couche et suffisamment petit pour éviter que l'architecture ne devienne difficile à maîtriser.

1.3.2 Architecture ARPA



Slide 1.23
Architecture ARPA

DoD

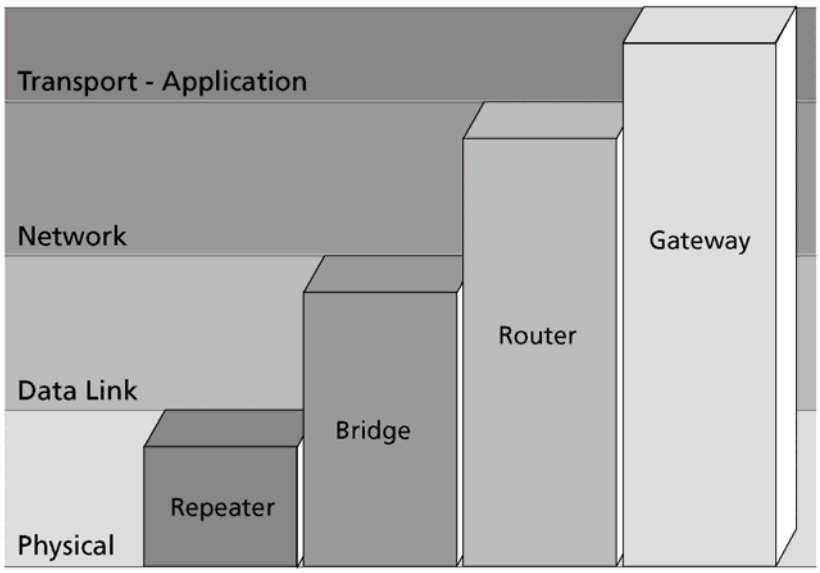
L'architecture ARPA, souvent appelée modèle TCP/IP ou DoD (Departement of Defense), est représentée sous la forme d'une pile de quatre couches.

Le modèle TCP/IP ne fait pas de distinction entre les couches 1 et 2. Dans le modèle OSI, la couche 1 correspond aux caractéristiques de transmission des supports de communication par cuivre, fibre optique et sans fil. La couche 2 délimite le début et la fin des trames et les transmet d'une extrémité à l'autre avec la fiabilité voulue. Un modèle correct devrait comporter ces deux aspects sous forme de couches distinctes. Ce n'est pas le cas du modèle TCP/IP.

D'autre part, le modèle TCP/IP regroupe les trois couches supérieure dans une couche d'application unique.

Aujourd'hui, nous utilisons de préférence les dénominations OSI, avec la différenciation des couches 1 et 2. Dans les faits, nous travaillons donc avec un pseudo modèle à cinq couches, comprenant les couches physique, liaison de données, réseau, transport et application.

1.3.3 Composants standards



Slide 1.24
Composants standards

Répéteur

En couche physique (1), l'équipement présent s'appelle répéteur. Comme son nom l'indique, sa tâche ne consiste qu'à répéter un signal reçu, que celui-ci contienne des erreurs ou non. On l'utilise pour créer des réseaux de diffusion, comme Ethernet, sur une structure cablée en étoile, ou alors comme réémetteur lorsque les distances l'exigent.

Bridge

Le pont, en anglais bridge, sert de liaison entre des segments réseaux de couche 2. Généralement, il peut déjà prendre des décisions d'acheminement local simples et fait de la détection d'erreurs.

Router

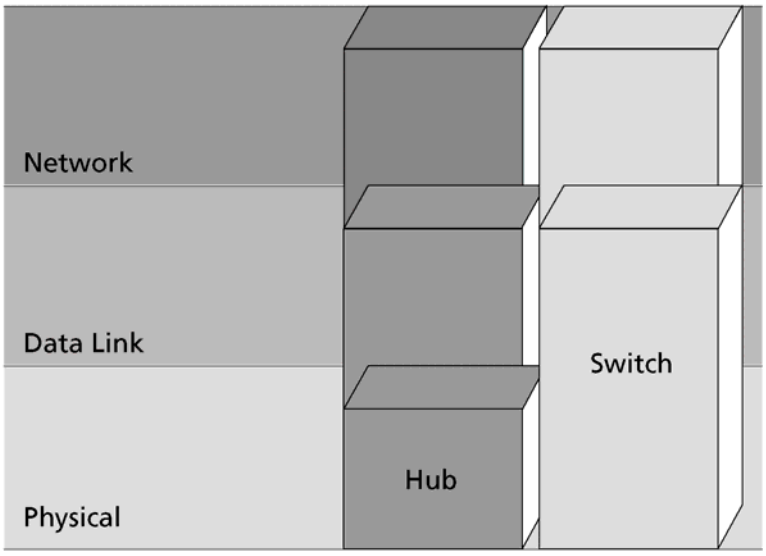
Le routeur est l'élément d'articulation de tous réseau "informatique". C'est lui qui prend des décisions d'acheminement global, sur la base d'informations divulguées par ses voisins. Il travaille en couche réseau sur la base des champs du protocole IP.

Gateway

Appelé passerelle en français, le Gateway est l'équipement qui va travailler dans toutes les couches supérieures, de transport (4) à l'application (7).

Les termes de pont et de passerelle pouvant preter à confusion, dans la pratique les termes anglais de bridge et de gateway sont souvent utilisés.

1.3.4 Hub & Switch



Slide 1.25
Hub & Switch

Il reste à aborder les termes souvent utilisés de hub et de switch.

Hub

Le hub est en fait un distributeur, un point central depuis lequel sont distribuées les informations sur des câbles menant aux utilisateurs. Dans la majorité des cas, le hub est un répéteur, mais il peut arriver qu'il soit un bridge ou un routeur.

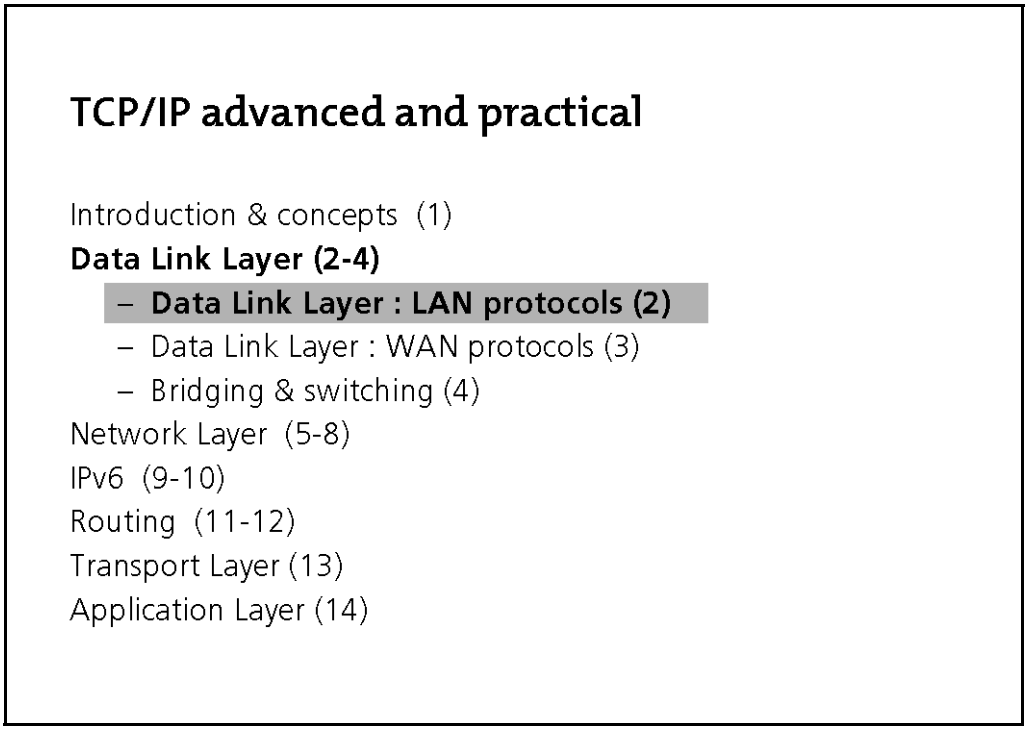
Switch

Le switch est un équipement qui traite une information de manière matérielle (hardware). Il prends des décisions d'acheminement sur la base d'informations simples, comme les adresses Ethernet (MAC), les identificateurs de connexion Frame Relay (DLCI) ou encore des identificateurs de canaux et faisceaux ATM (VPI/VCI). Dans tous ces cas il travaille en couche 2.

On trouve des solutions plus modernes, comme MPLS, qui offrent des possibilités de travail mixte entre les couches 2 et 3. Le choix de l'acheminement est tout d'abord effectué en couche 3. Ensuite, au travers d'algorythmes et de protocoles appropriés, des tables de retransmission (couche 2) sont créées et utilisées par le switch.

En principe, la commutation ne s'effectue qu'en couche 2. Les informations de retransmission en couche 3 sont trop complexes (hiérarchie) et nécessiteraient trop de temps de traitement.

2 Liaison de données : Protocoles LAN



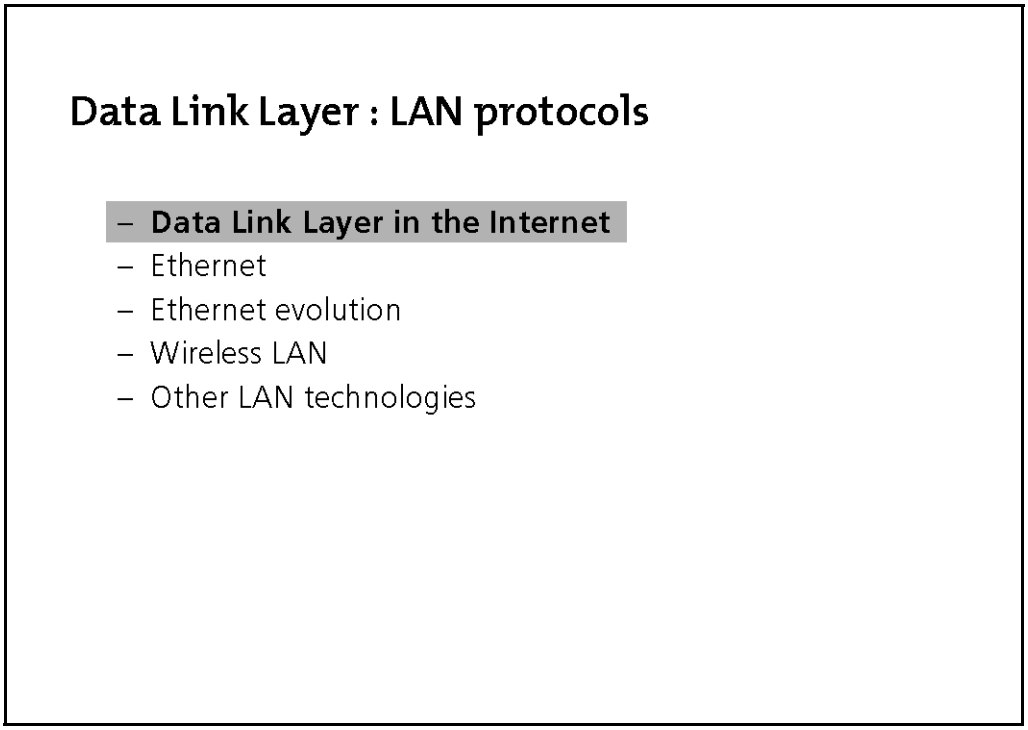
Slide 2.1
Liaison de données : Protocoles LAN

Après un aperçu des fonctions de base de la couche liaison de données, ce chapitre traite particulièrement des protocoles LAN.

Objectifs

A l'issue de ce chapitre, les participants sont capables de différencier les normes Ethernet, de nommer les avantages et inconvénients de la procédure d'accès CSMA/CD. Ils peuvent expliquer le principe du bridging et nommer d'autres technologies LAN.

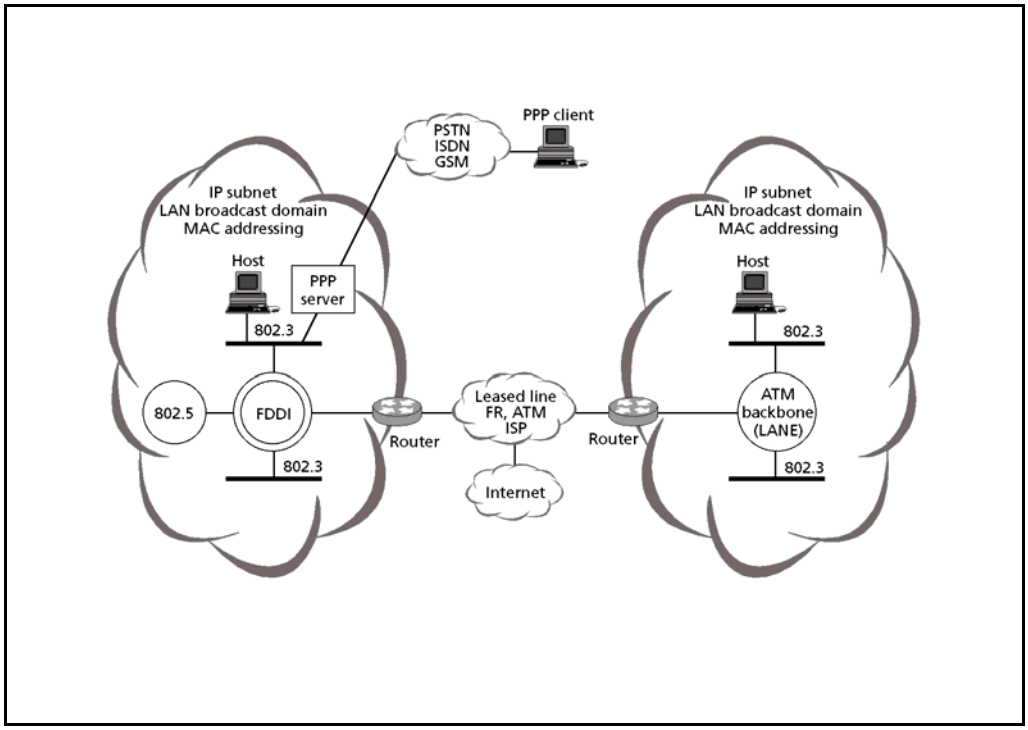
2.1 Couche liaison de donnée dans l'Internet



Slide 2.2
Couche liaison de donnée dans l'Internet

Avant de débuter l'étude des LAN, posons d'abord quelques bases sur les rôles de cette couche liaison de données dans l'Internet, d'une manière générale.

2.1.1 Aperçu

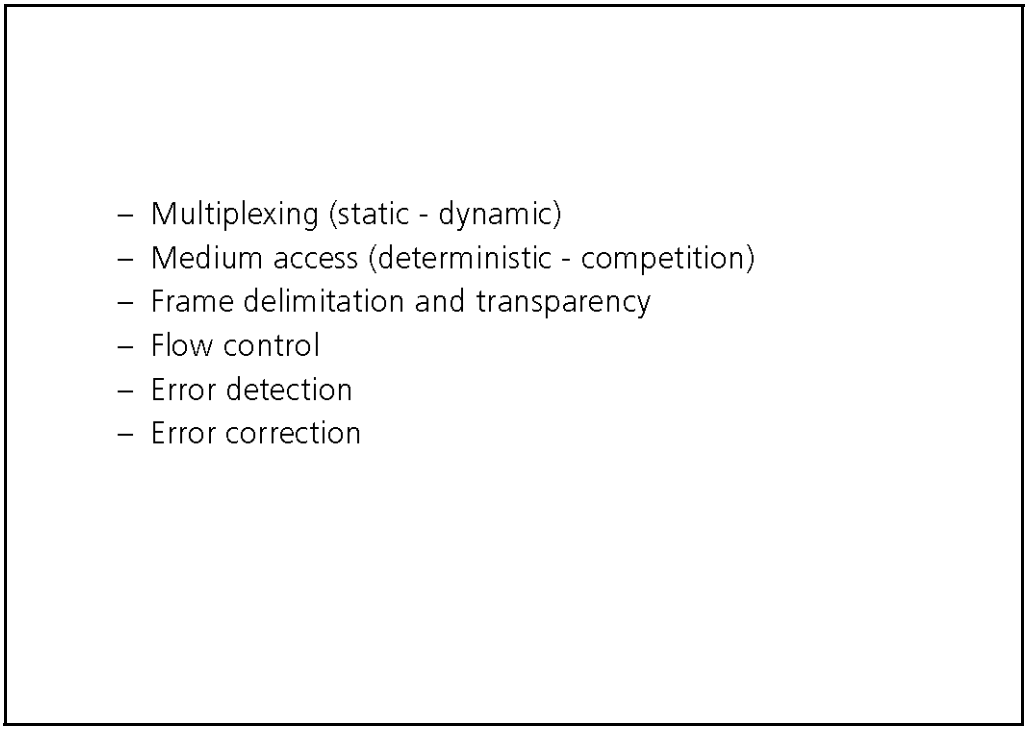


Slide 2.3
Aperçu

IP fonctionne sur un large éventail de technologies de réseau. Pour les distances courtes, (à l'échelle d'un bâtiment ou d'un campus) les technologies LAN sont largement répandues (Ethernet, fast Ethernet, Gigabit Ethernet, Token Ring, …). La plupart des liaisons longue distance (WAN) sont réalisées sur des lignes point à point (circuits loués) ou sur des réseaux à commutation de paquet (Frame Relay, ATM). Les liaisons point à point sont utilisées dans deux situations:

- Connection d'un réseau d'entreprise au monde extérieur (à L'internet) ou à un autre réseau d'entreprise au travers de liaisons qui sont généralement permanentes,
- Connection d'utilisateurs individuels ou de petits groupes vers un réseau IP au travers de réseaux commutés ou résidentiels (ISDN, GSM, CATV).

2.1.2 Fonctions de base

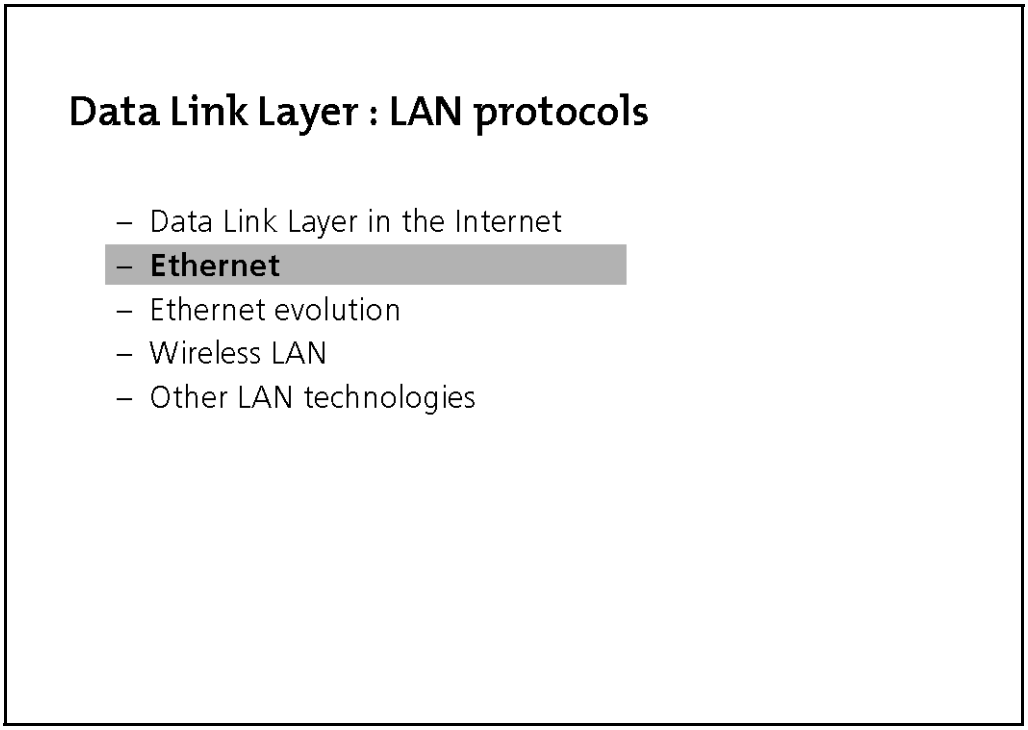


Slide 2.4
Fonction de base

Couche 2, Frame

La couche liaison de données (OSI layer 2, data link layer) prend en charge les problèmes de qualité des lignes. Elle met en œuvre différents mécanismes (détection d'erreur, partage du médium, délimitation d'unités de données) pour livrer aux couches supérieures un service fiable de transmission de bloc de données. Ces blocs sont généralement appelés des trames (Frame).

2.2 Ethernet



Slide 2.5
Ethernet

Dans ce paragraphe le terme "Ethernet" est utilisé indifféremment pour désigner deux technologies normalisées similaires : "Ethernet v2" et "IEEE 802.3". On précisera "Ethernet v2" et "IEEE 802.3" lorsque des différences existent entre les deux standards.

2.2.1 Caractéristiques d'Ethernet

- Bus topology
- Use CSMA/CD access procedure
- Use MAC (Media Access Control) addresses
- 70s: research project from Xerox
- 80s: published as specification
- Two standards exist today
- Ethernet V2 (from DIX: Digital, Intel and Xerox)
- IEEE 802.3 (from IEEE)

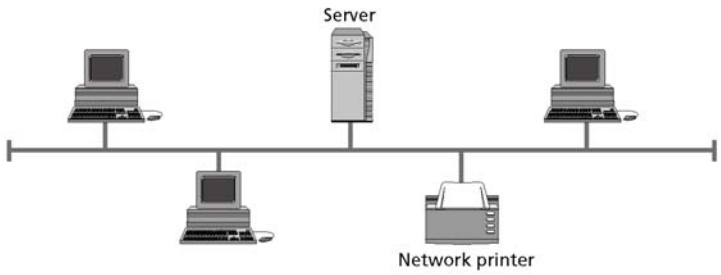
Slide 2.6
Caractéristiques d'Ethernet

Ethernet, IEEE 802.3, Ethernet v2

Ethernet a tout d'abord été, dans les années 70, un projet de recherche de Xerox. Ces recherches ont débouché sur le standard Ethernet v1, suivi par la version 2. En s'inspirant de ces travaux, l'IEEE (Institute of Electric and Electronic Engineering) a proposé le standard 802.3.

Aujourd'hui les 2 normes existent et peuvent cohabiter sur le même support physique.

2.2.2 Topologie en bus



- Shared media, all nodes connected to the same "wire"
- Each node can communicate directly with other nodes
- Uses MAC addresses (Media Access Control)
- "Made for" broadcasting

Slide 2.7
Topologie en bus

Topologie en bus

Ethernet utilise une topologie en bus. Toutes les stations sont connectées sur le même médium physique.

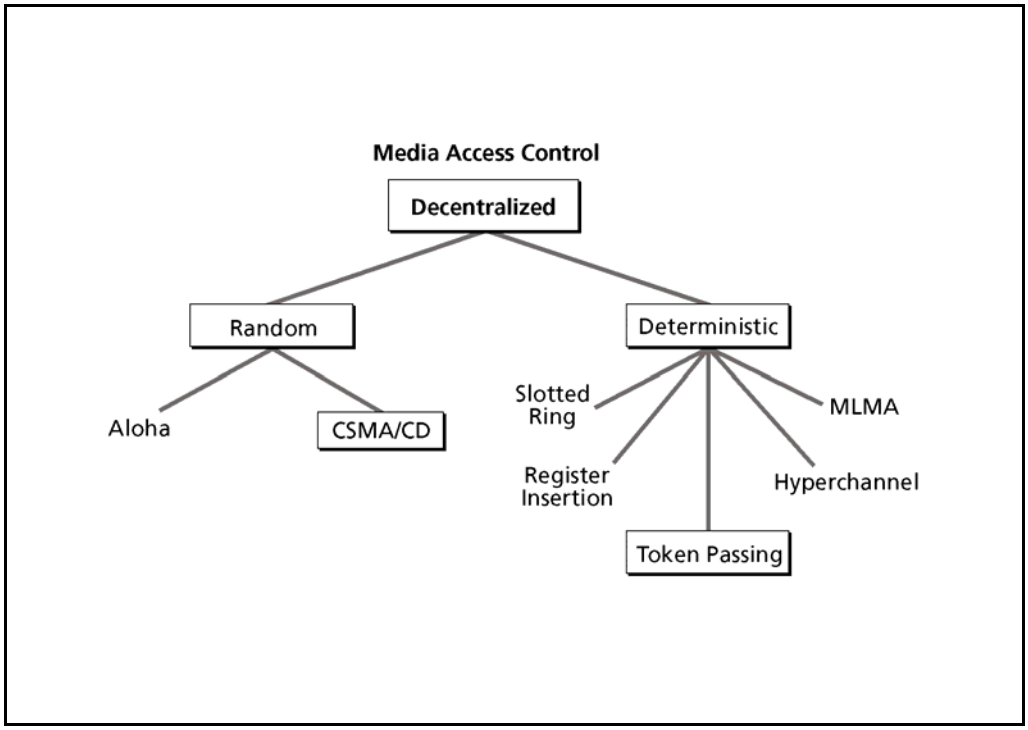
Adresse MAC

Chaque station peut directement communiquer avec les autres en utilisant le domaine d'adressage MAC.

Broadcasting

Cette topologie de réseau a l'avantage de permettre la diffusion (Broadcasting) de manière naturelle. Chaque trame émise dans le réseau est reçue simultanément par toutes les stations.

2.2.3 Procédure d'accès au réseau



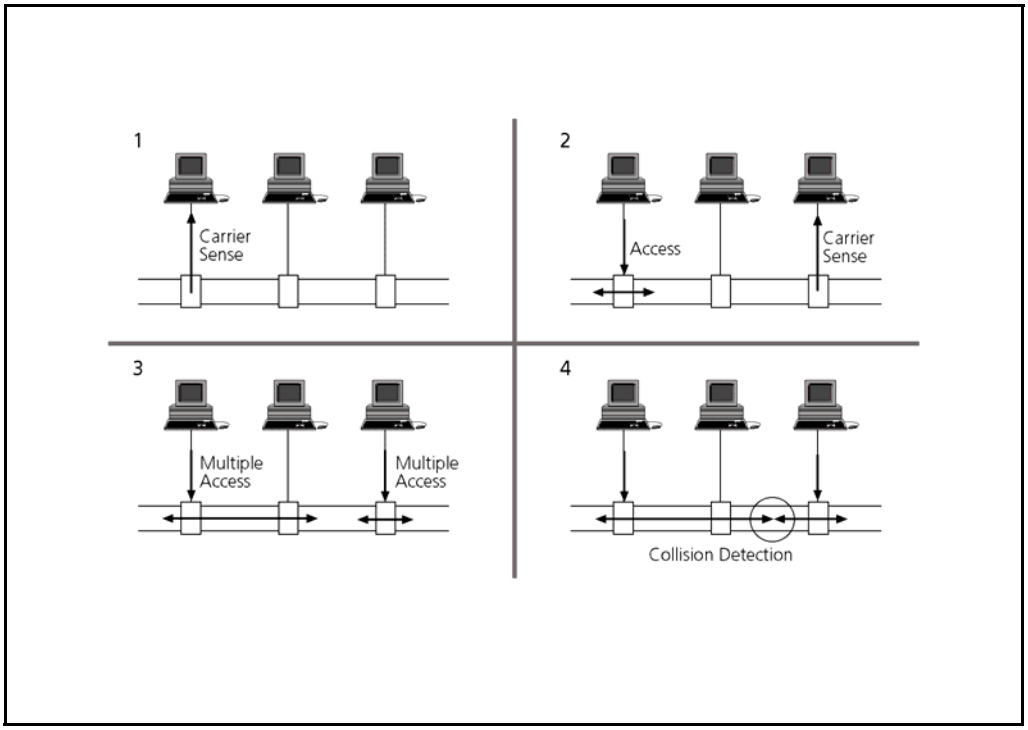
Slide 2.8
Procédure d'accès au réseau

Procédure CSMA/CD

On distingue différentes procédures d'accès au réseau. Nous allons considérer les procédures décentralisées dans lesquelles toutes les stations disposent des mêmes privilèges pour accéder au médium. Aucune station n'a de fonction particulière de gestion de l'ensemble du réseau. On distingue 2 groupes de procédures décentralisées:

- déterministes: une station ne pourra émettre que lorsque son tour arrive, en accord avec les autres stations. Token Passing, la procédure d'accès du Token-Ring (technologie LAN développée par IBM), se situe dans cette catégorie.
- non-déterministes: chaque station peut prendre la parole à n'importe quel instant, pour autant que le réseau soit libre. Ethernet utilise l'une d'elle, CSMA/CD.

2.2.4 Procédure CSMA/CD



Slide 2.9
Procédure CSMA/CD

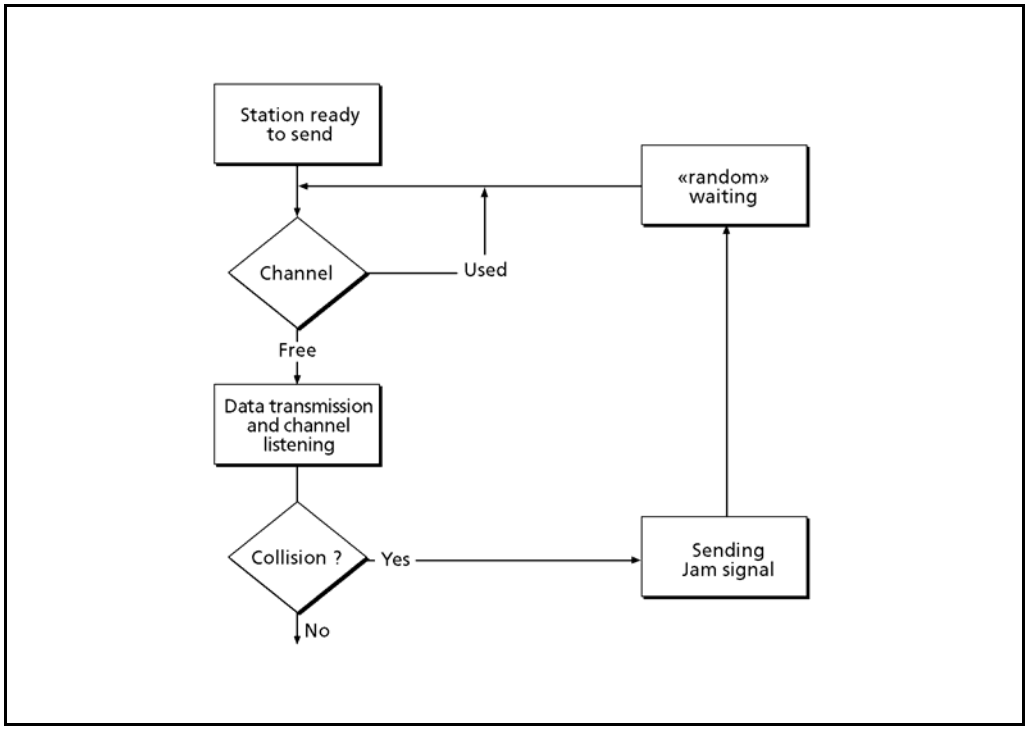
CSMA/CD

CSMA/CD signifie "détection de porteuse à accès multiples avec détection de collision". Une station qui souhaite émettre une trame va déterminer si le canal est libre et, le cas échéant, commencer son émission.

Collision

Une collision peut survenir lorsque, en raison des temps de propagation, une station ne détecte pas que le médium est déjà occupé. Cette collision doit être détectée et suivie d'une procédure de résolution de conflit. Une nouvelle tentative d'émission sera effectuée après une attente d'une durée aléatoire.

2.2.5 Algorithme CSMA/CD



Slide 2.10
Algorithme CSMA/CD

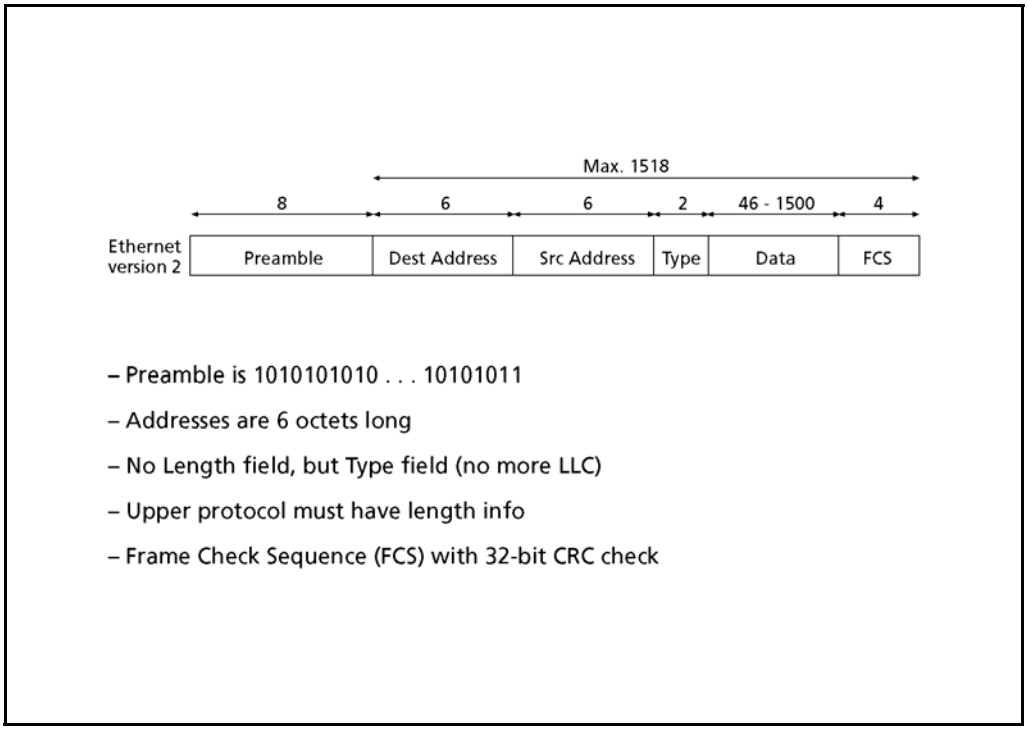
Jam Signal

La station n'émet que si le canal de transmission est libre. En cas de collision, les stations impliquées dans le conflit envoient un signal de brouillage (Jam Signal) sur la ligne. Ceci permet de garantir la détection de la collision par toutes les stations.

L'attente d'une durée aléatoire garantit que les stations impliquées dans une collision ne recommencent pas à émettre simultanément et n'engendrent ainsi une nouvelle collision.

Si des collisions successives devaient se produirent, le support sera considéré comme indisponible après la 16ème collision.

2.2.6 Format de trame Ethernet v2



Slide 2.11
Format de trame Ethernet v2

Ethernet v2

Une trame Ethernet v2 commence par un préambule . Il s'agit d'un signal composé de 1 et de 0 successifs, servant à synchroniser les systèmes. Le dernier bit du 8ème et dernier octet indique le début de la trame par l'envoi d'un "1" au lieu d'un "0".

On trouve ensuite les deux champs d'adresses, destination et source, d'une longueur de 6 octets chacun.

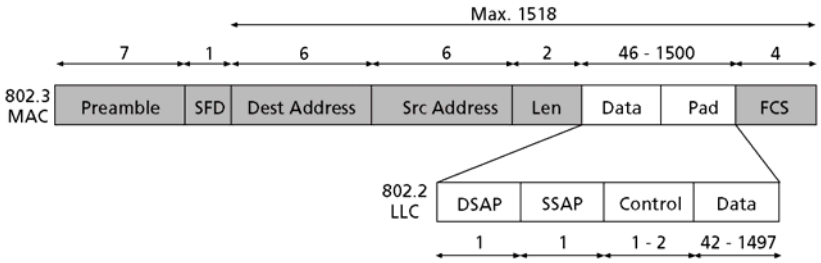
Ethertype

Les 2 octets suivants sont interprétés comme un champ "type" indiquant le protocole encapsulé. Dans ce champ aussi nommé "Ethertype", on trouvera 0x800 pour IP et 0x806 pour ARP.

Aucune indication de longueur n'étant fournie, le protocole encapsulé devra contenir cette information.

La trame se termine par une séquence de contrôle (FCS), un CRC calculé sur 32 bits.

2.2.7 Format de trame IEEE 802.3 MAC



– Preamble is 7x10101010, SFD is 10101011

– Len = Length of data (without padding)

– Frame Check Sequence (FCS) with 32-bit CRC check

Slide 2.12
Format de trame IEEE 802.3 MAC

Start Frame Delimiter

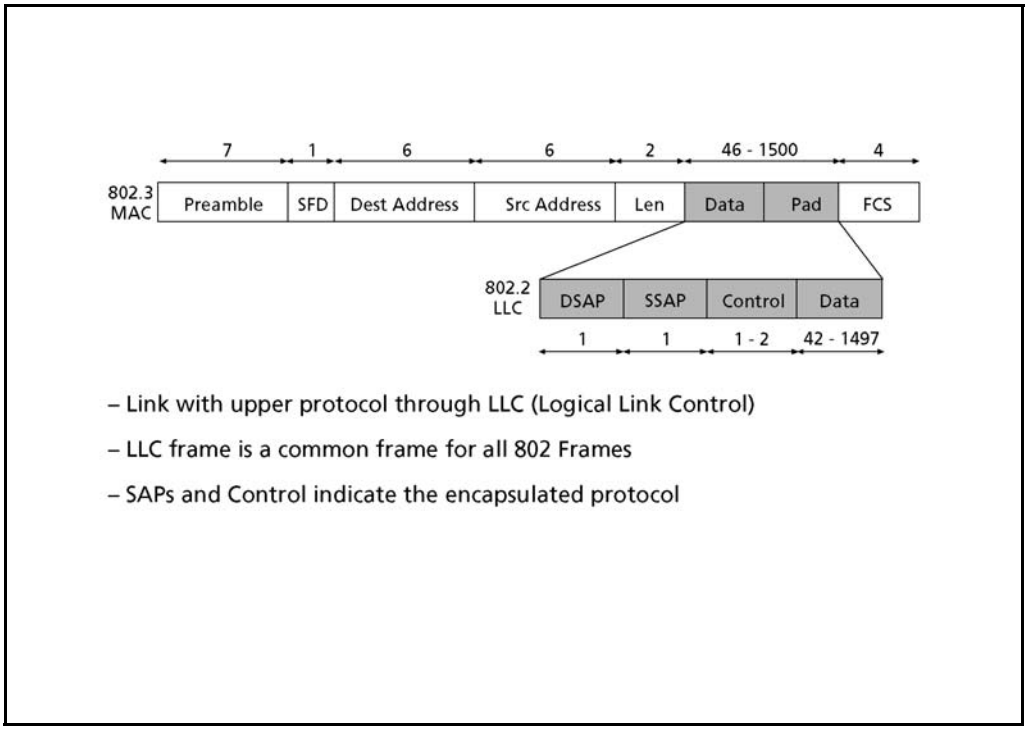
Une trame IEEE 802.3 commence par un préambule et un indicateur de début de trame. Il s'agit d'un signal composé de 1 et de 0 successifs, servant à synchroniser les systèmes. Les derniers bits du SFD (Start Frame Delimiter) indiquent le début de la trame par l'envoi de deux "1" successifs.

C'est une définition différente de la manière de démarrer une trame, mais elle est parfaitement identique à celle utilisée par Ethernet v2.

IEEE 802.3 MAC

La trame débute par les adresses MAC de destination, puis de source, chacune de 6 octets. Le champ longueur (Length) indique le nombre d'octets de données utiles sans le padding (Pad). Pour des raisons liées à la méthode d'accès, les trames Ethernet ne peuvent pas être plus courtes que 64 octets. Lorsque le nombre d'octet de données n'est pas suffisant (< 46 octets) des données de remplissage (Padding) sont introduites. La trame se termine par un FCS (Frame Check Sequence), identique à celui de la trame Ethernet v2.

2.2.8 Format de trame IEEE 802.2 LLC



Slide 2.13
Format de trame IEEE 802.2 LLC

La normalisation des LAN selon IEEE sépare cette couche liaison de donnée en deux sous-couches. La première, étudiée à la page précédente, s'occupe du lien "vers le bas" et est propre à chaque type de LAN.

La deuxième sous-couche, appelée LLC (Logical link Control), s'occupe du lien "vers le haut". Elle est commune à toutes les technologies LAN standardisées par l'IEEE et porte le nom de 802.2.

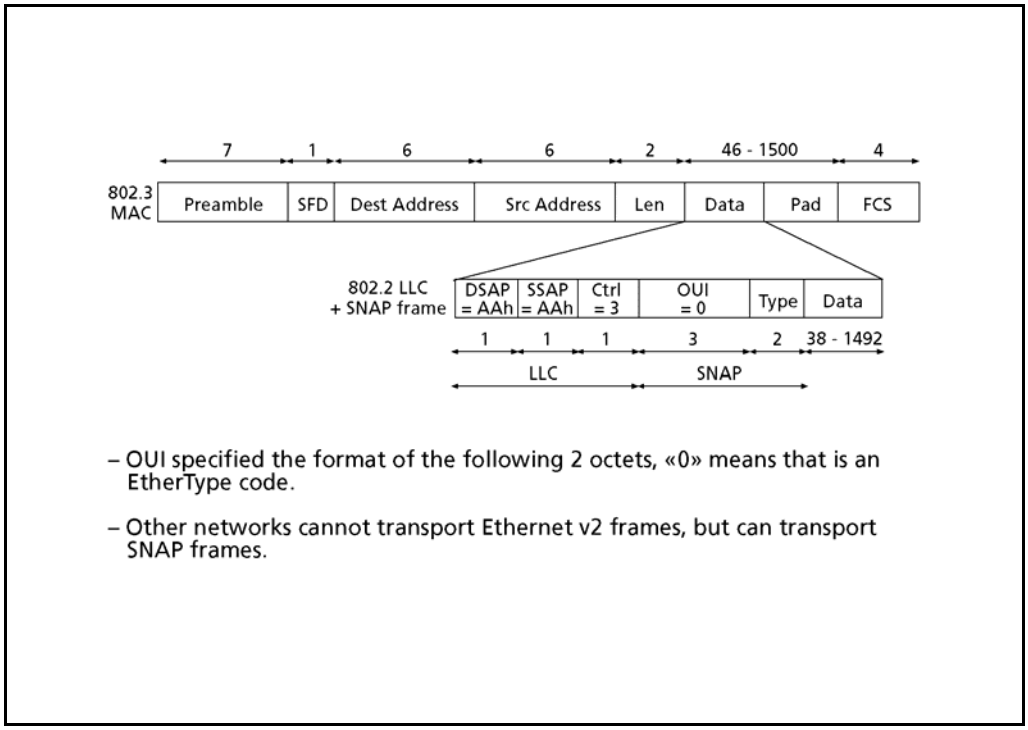
LLC

Cette séparation devait permettre de simplifier le bridging entre les différentes technologies de LAN.

Les trois champs qu'elle comporte indiquent le type du protocole encapsulé. Les deux SAP (DSAP : Destination service access point, SSAP : Source service access point) permettent de différencier le service qui a fourni les données présentes dans la trame et le service qui doit les receuillir. Le champ de contrôle donne des informations sur le type de la trame. La plupart du temps, il s'agira d'une trame d'information non numérotée (0x3).

Dans le cas particulier des paquets IP, on utilise généralement une extension de cet en-tête, l'en-tête SNAP.

2.2.9 Format de trame SNAP



Slide 2.14
Format de trame SNAP

SNAP

La caractéristique principale d'une trame LLC/SNAP (Logical Link Control / Sub-Network Access Point) réside dans le fait qu'elle transporte le champ " Type ", largement répandu de la trame Ethernet v2 et permet de transporter cette information sur d'autre technologie de réseau (Token ring, FDDI, ATM-LAN,…).

LLC

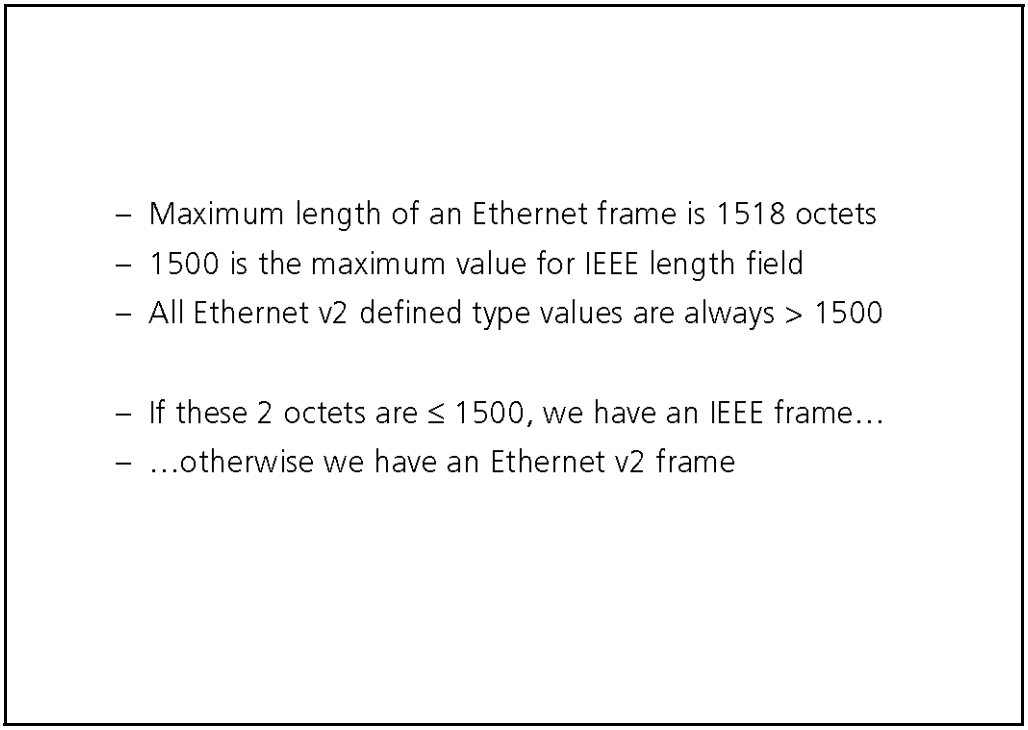
La valeur 0xAA présente dans les identificateurs de point d'accès spécifie que l'en-tête LLC est suivi d'un en-tête SNAP.

OUI

L'entête SNAP contient un identificateur de 3 octets, OUI (Organizationally Unique Identifier), qui indique la manière dont il faut interpréter les deux octets suivants. La valeur 0 indique EtherType.

Le champ suivant sera donc équivalent au champ Type de la trame Ethernet v2. Lorsque le protocole encapsulé est IP, nous trouverons donc la valeur 0x800.

2.2.10 Reconnaissance automatique du format de trame



Slide 2.15
Reconnaissance du format de trame

Les deux formats de trames peuvent cohabiter sur le même réseau. Ces deux formats sont aisément reconnaissables par l'analyse du champ de deux octets qui suit directement les adresses.

IEEE 802.3

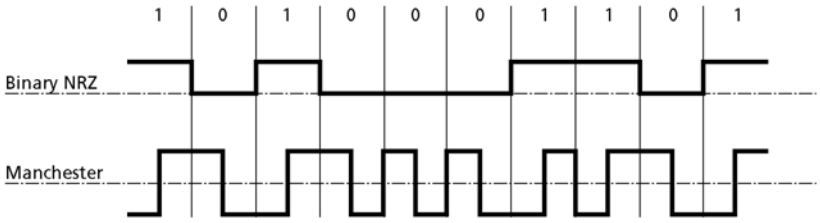
Si sa valeur est inférieure ou égale à 1500, il s'agit d'une trame IEEE 802.3. En effet, dans ce type de trame, ces 2 octets représentent une longueur. Celle-ci étant inférieure ou égale à 1500, nous ne pourrons trouver des valeurs plus élevées.

Ethernet v2

Si cette valeur est supérieure à 1500, il s'agit d'une trame Ethernet v2. Dans ce cas, les fameux 2 octets représentent le type de protocole encapsulé. Les normalisateurs ont fait attention à ce que les valeurs définies dépassent la valeur décimale 1500.

Grâce à cette définition, les deux formats de trames pouront donc être identifiées à la réception.

2.2.11 Code Manchester



– Manchester gives value on edges, in the middle of bit duration.
Positive edge = 1, Negative edge = 0

– Requires double bandwidth as classical binary NRZ . . .

. . . but guarantees synchronization

Slide 2.16
Code Manchester

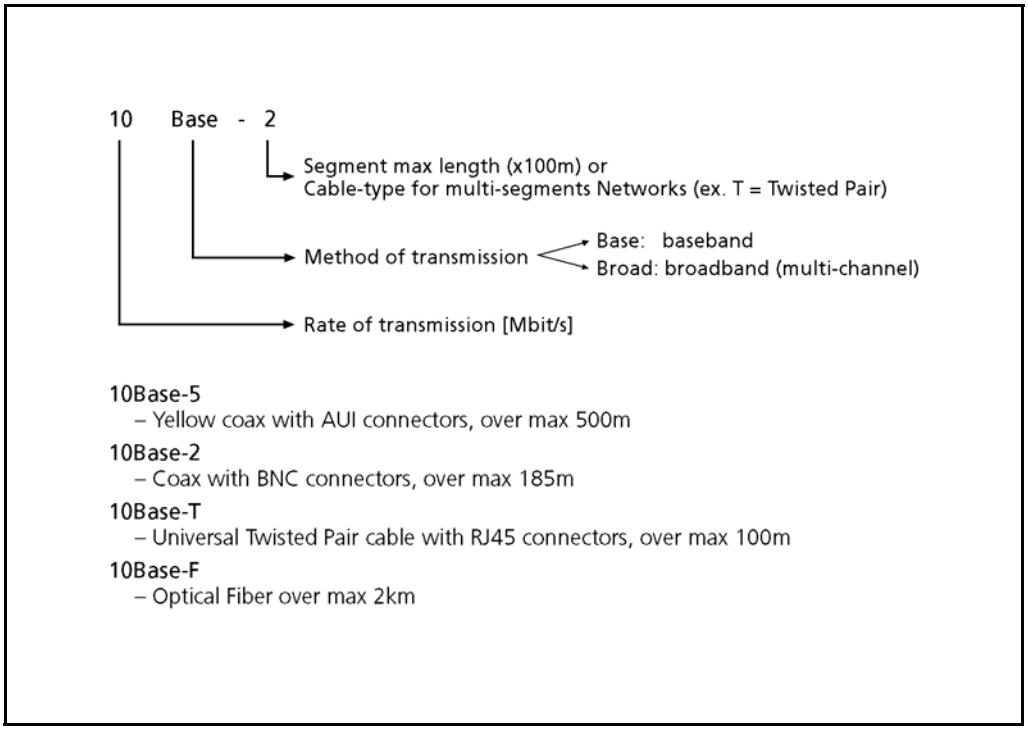
Manchester

Le codage du signal se fait en code Manchester. Ce code donne la valeur non pas avec un état, mais au travers des transitions. Au milieu de la durée de chaque bit intervient une transition. Une montée du signal signifie " 1 ", une chute " 0 ".

NRZ

Ce signal a le désavantage d'utiliser deux fois plus de bande passante que le binaire classique (NRZ : Non-Return to Zero). Cependant, il garantit des transitions dans le signal ce qui permet aux différents systèmes de se synchroniser plus facilement.

2.2.12 Variantes physiques



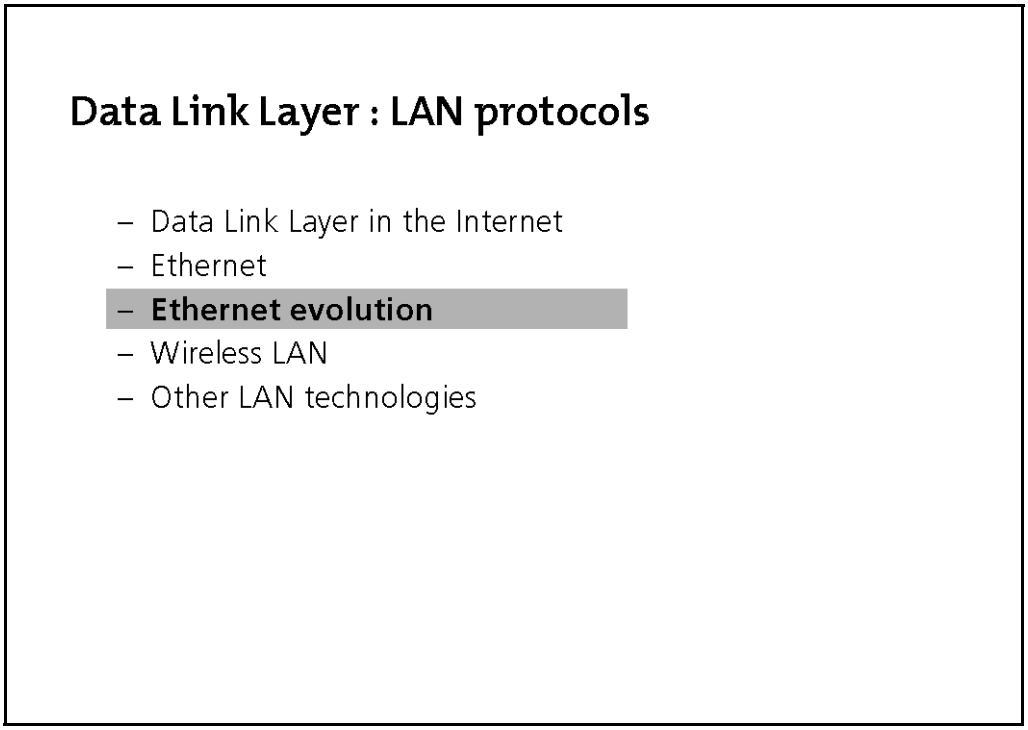
Slide 2.17
Variantes physiques

Les variantes physiques Ethernet sont désignées en commençant par le débit de transmission. Ensuite vient la méthode de transmission utilisée, généralement en bande de base. A la fin, on trouve la longueur max du segment en centaine de mètres, ou le type de support utilisé dans le cas des réseaux multi-segments.

Aujourd'hui la technique 10Base-T est la plus répandue. Elle utilise l'infrastructure moderne du câblage universel des bâtiments. C'est sur cette base que les évolutions à 100 Mbit/s et 1 Gbit/s ont été créées.

La variante sur fibre optique, 10Base-F, permet d'atteindre des distances de l'ordre de 2 km. Elle est surtout utilisée pour son immunité aux perturbations électromagnétiques.

2.3 Evolution de l'Ethernet

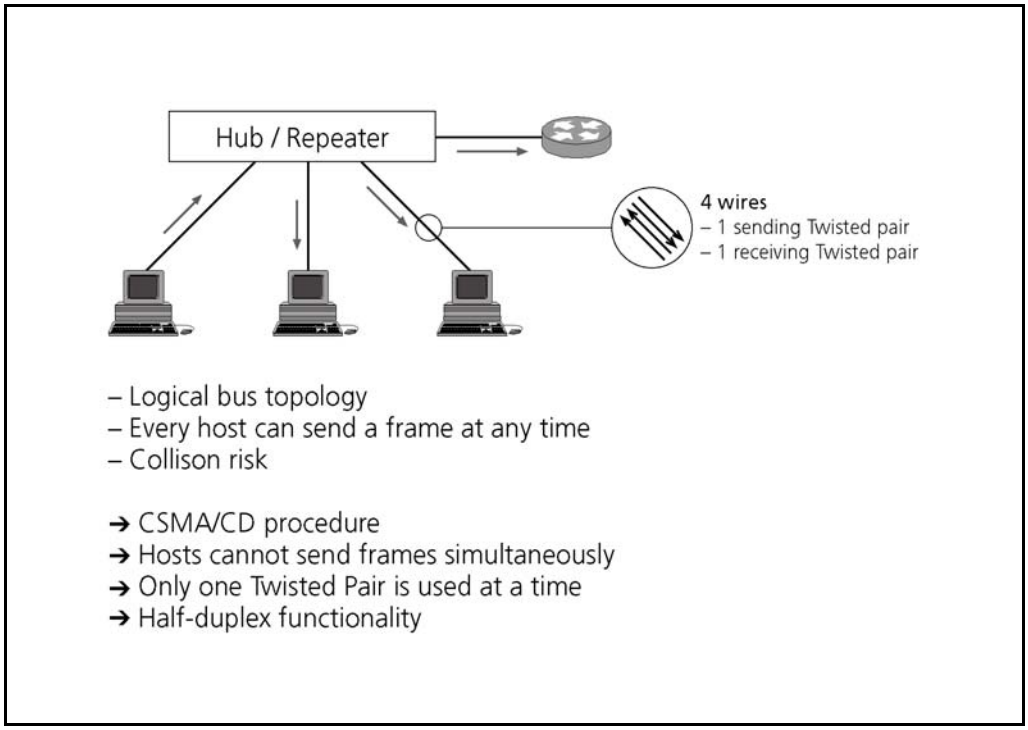


Slide 2.18
Evolution de l'Ethernet

Si dans la connexion du PC au réseau on trouve encore, la plupart du temps, un réseau de type Ethernet standard, le débit de 10 Mbit/s n'est généralement pas suffisant pour l'épine dorsale d'un réseau LAN

Dans cette partie du chapitre, nous allons donc étudier les variantes qui ont succédé à l'Ethernet standard.

2.3.1 Structure classique, half-duplex



Slide 2.19
Half-duplex

Bus topology

Nous l'avons déjà dit, initialement Ethernet est un réseau local utilisant un support physique partagé. Dans le cas des câbles coaxiaux qui courraient de machine en machine, cette fonctionalité "en bus" est facile à imaginer.

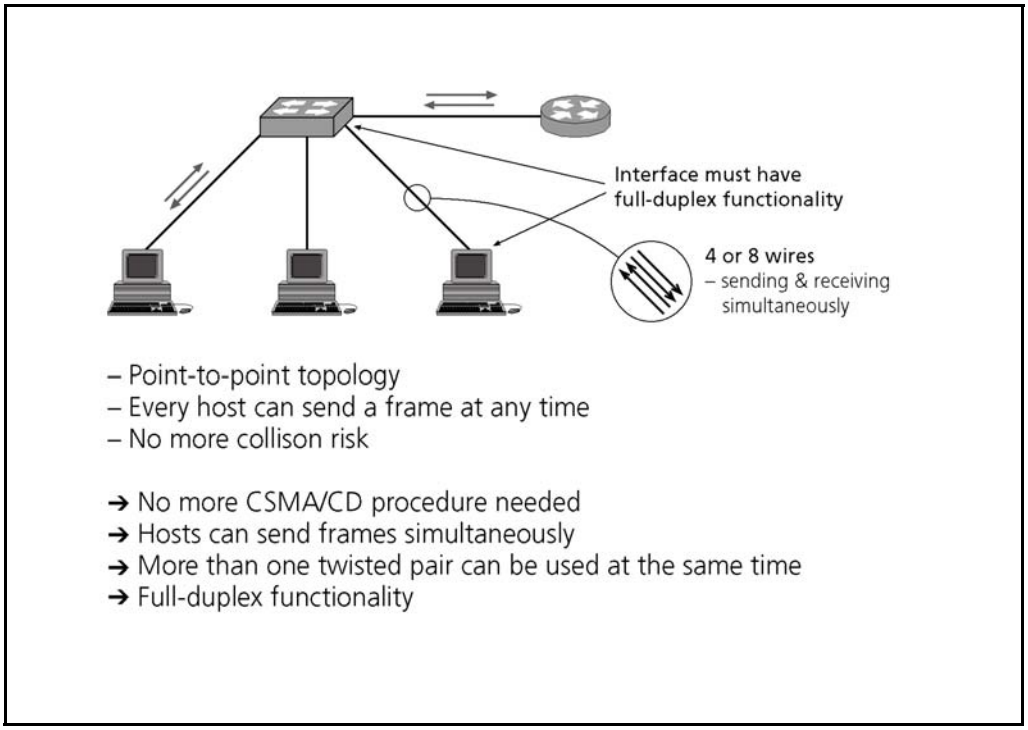
Par la suite, le support physique de ces réseaux Ethernet a évolué, on a utilisé le câblage universel des bâtiments, de plus en plus présent.

La fonctionalité d'Ethernet n'a toutefois pas changé, les machines sont reliées entre elles par un répéteur physique, le hub. Chaque trame émise circule sur tous les câbles de raccordements simultanément. Chaque machine "voit" encore le trafic de toutes les stations. Le support restant partagé, la procédure d'accès CSMA/CD sera conservée.

Half-duplex

Aujourd'hui on appelle ce mode de fonctionnement le mode half-duplex. Dans ce mode de fonctionnement, bien que 2 paires torsadées soient utilisées afin de séparer les sens du trafic, seule une machine pourra émettre. En cas d'échange de données entre deux intervenants, la transmission se fera à tour de rôle dans un sens, puis dans l'autre. On a donc bien un fonctionnement de transmission half-duplex.

2.3.2 Nouvelle structure “switchée“, full-duplex



Slide 2.20
Full-duplex

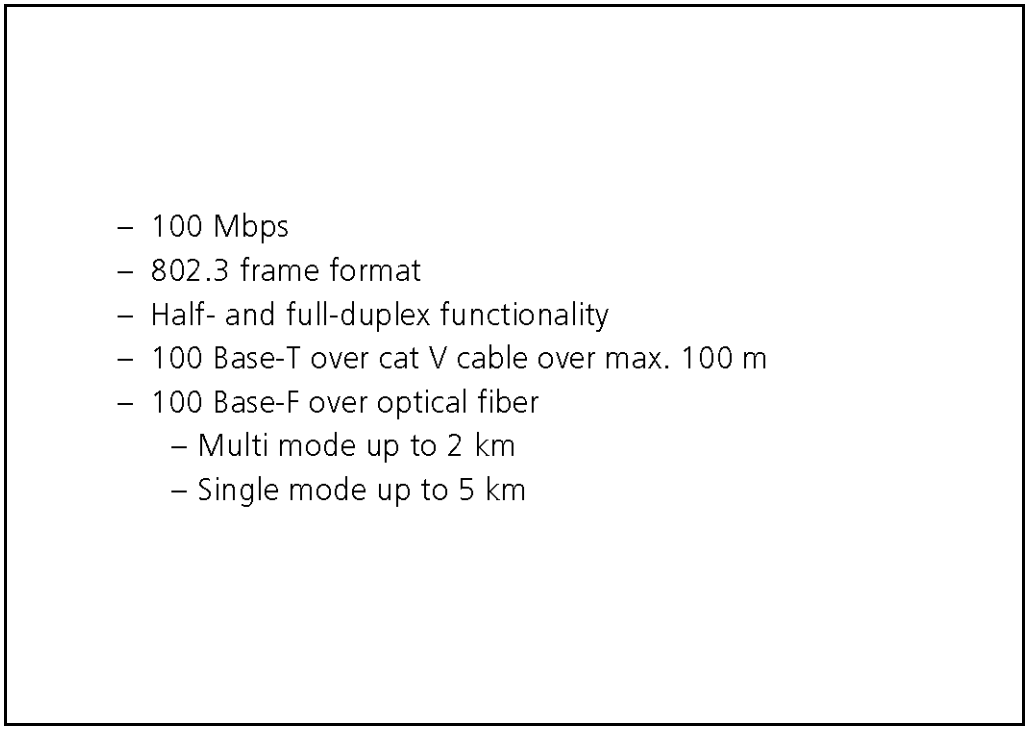
Une évolution du matériel permet aujourd’hui de remplacer le hub par un switch multiport. Cette évolution limite le domaine de collision au seul câble de raccordement. Les deux seuls partenaires de communications possibles n’émettant pas leur trames sur les mêmes conducteurs, la probabilité de collision n’existe plus.

Dans ce cas de figure, pourquoi ne pas se permettre d’utiliser les deux paires de conducteurs afin de transmettre des informations simultanément dans les deux sens ?

Ce mode de fonctionnement, appelé full-duplex, utilise mieux les ressources et permet de se passer de la procédure d’accès complexe qu’est CSMA/CD.

Cette solution offre tout de même un risque. En cas d’échange soutenu de données, on va faire passer, tout sens confondu, deux fois plus d’informations au travers du réseau dans un temps donné. Si l’infrastructure de l’épine dorsale de notre réseau n’offre pas de réserve, on risque de constater un effondrement de certaines liaisons, si ce n’est du réseau entier.

2.3.3 Fast Ethernet



Slide 2.21
Fast Ethernet

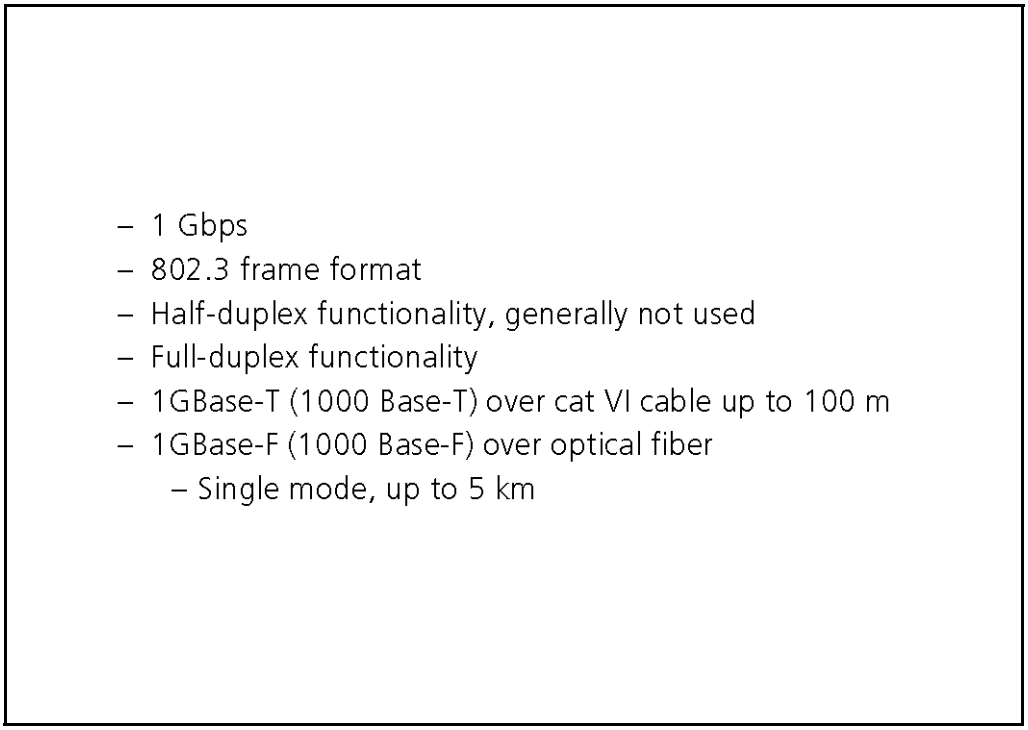
Fast Ethernet est la première évolution de l'Ethernet. Comme son nom l'indique, il s'agit d'une version plus rapide que l'Ethernet standard. Le format de trame 802.3 reste inchangé.

Fast Ethernet offre un débit de 100 Mbit/s, sur 100 m au maximum dans des câbles de catégorie V. En outre, des variantes sur fibres optiques monomodes (2 km) et multimodes (5 km) sont proposées.

Le Fast Ethernet permet le fonctionnement traditionnel en half-duplex, tout comme le fonctionnement plus récent en full-duplex.

Cette technologie, au début surtout utilisée dans les épines dorsales des réseaux locaux, s'installe aussi de plus en plus dans la liaison d'accès, entre les machines et le réseau.

2.3.4 Gigabit Ethernet



Slide 2.22
Gigabit Ethernet

Gigabit Ethernet est une autre évolution de l'Ethernet.

On trouve toujours le format de trame 802.3, propulsé cette fois à 1 Gbit/s.

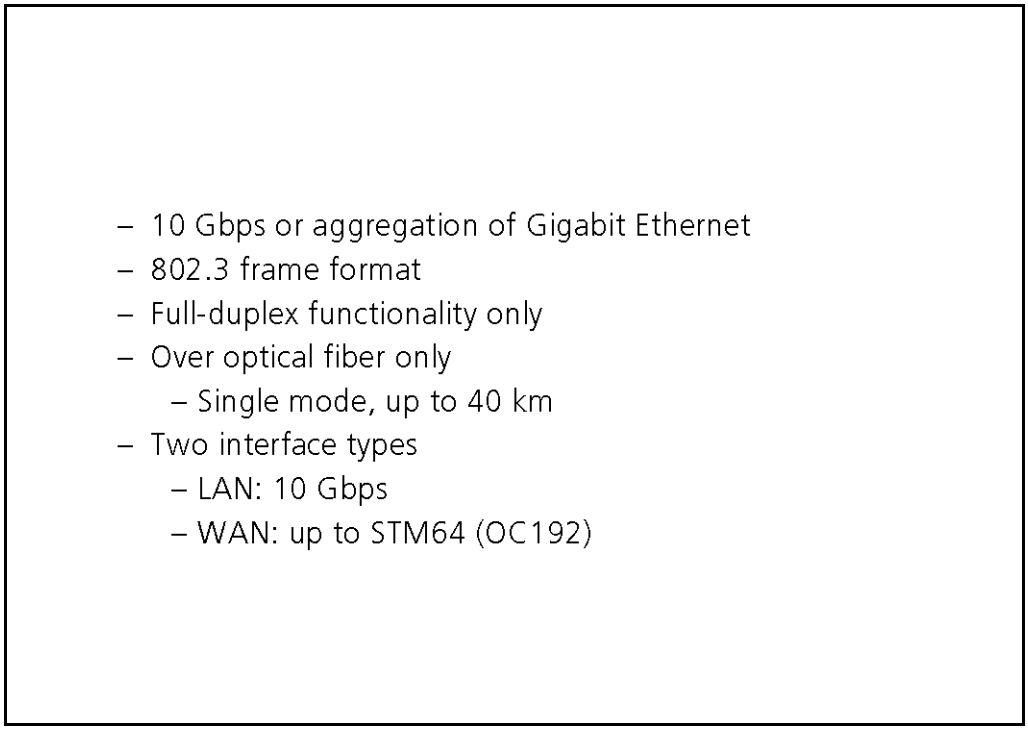
En bonne évolution de l'Ethernet, Gigabit Ethernet pourrait fonctionner sur des câbles à paires torsadées, en half-duplex.

Dans les faits, seule la version full-duplex est mise en oeuvre. Le support de transmission préféré sera la fibre optique monomode (5 km). Toutefois, l'utilisation d'une liaison LAN de 100 m au travers d'un câble universel catégorie VI est possible.

Le Gigabit Ethernet n'est pas proposé sur des fibres multimodes.

On trouve cette technologie dans les épines dorsales des grands réseaux LAN, ainsi que dans les environnements des serveurs. Les équipements de transmission WAN (lignes louées, ...) offrent, de plus en plus souvent, des interfaces Gigabit Ethernet.

2.3.5 10 Gigabit Ethernet, 10GbE



Slide 2.23
10 Gigabit Ethernet

Le 10 Gigabit Ethernet, souvent abbrégé 10Gbe, est une technologie très récente, la normalisation date de mars 2002.

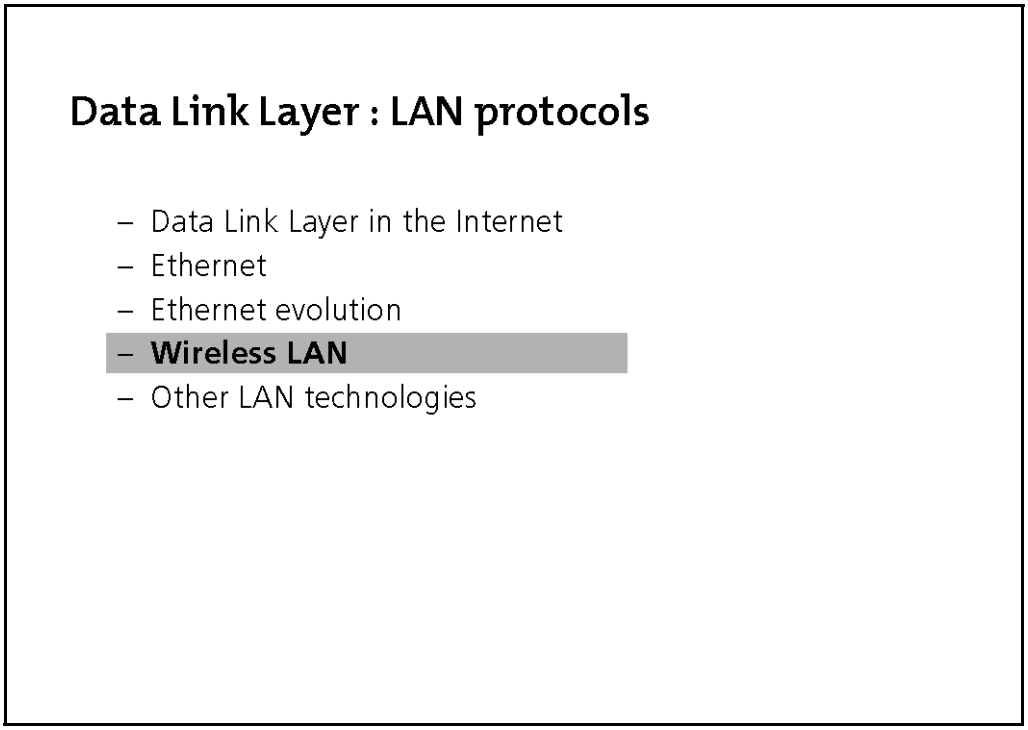
Comme nous pouvons facilement l'imaginer, c'est une évolution de l'Ethernet à 10 Gbit/s. Cependant, en tenant compte des enseignements donnés par les utilisateurs du Gigabit Ethernet, seule la variante full-duplex est normalisée. De plus, pour des raisons des performances limitées des câbles en cuivre, seule une version sur fibre optique monomode est proposée. Celle-ci offre une portée remarquable de 40 km qui se destine aux épines dorsales des réseaux d'entreprises présentes dans plusieurs bâtiments.

On peut utiliser le 10Gbe en mode standard ou l'utiliser pour faire une aggregation de canaux Gigabit Ethernet.

La nouveauté principale est l'interface WAN normalisée, permettant d'introduire directement les données du réseau 10Gbe dans un réseau SDH. Le débit correspondant offrira (presque) 10 Gbit/s, il s'agit du STM64 (Sonet OC192).

La norme du 10Gbe est évolutive et prévoit déjà des possibilités de multiplier les débits. L'avenir semble donc assuré pour cette technologie couvrant aujourd'hui les domaines LAN, MAN et WAN.

2.4 Wireless LAN



Slide 2.24
Wireless LAN

L'évolution des réseaux LAN (Local Area Networks) avance aussi vite que celle des autres technologies.

On entend aujourd'hui par LAN en premier lieu la technologie Ethernet avec la norme 802.3. Cette technologie couvre aujourd'hui les débits de 10 Mbit/s, 100 Mbit/s, 1 Gbit/s et, d'ores et déjà, 10 Gbit/s. Les supports utilisés pour la transmission sont le cuivre et la fibre optique.

WLAN's

C'est ici qu'intervient maintenant la technologie LAN radioélectrique, qui permet, dans un environnement restreint à quelques mètres, de relier les machines sans câble. Un nouveau terme a fait son apparition : le **WLAN.**

2.4.1 IEEE 802.11b

IEEE 802.11b : Transfer rates 1, 2, 5,5 and 11 Mbps
- Works on frequency band 2,4 GHz, up to 3 channels
- Coding: DSSS (Directed Sequence Spread Spectrum)
- Uses CSMA/CD Procedure, with ack!

Land	Permitted Spectrum
US	2,4000 - 2,4835 GHz
Europe	2,4000 - 2,4835 GHz
Japan	2,471 - 2,497 GHz
France	2,4465 - 2,4835 GHz
Spain	2,4465 - 2,4835 GHz
Switzerland	. . .

Slide 2.25
IEEE 802.11b

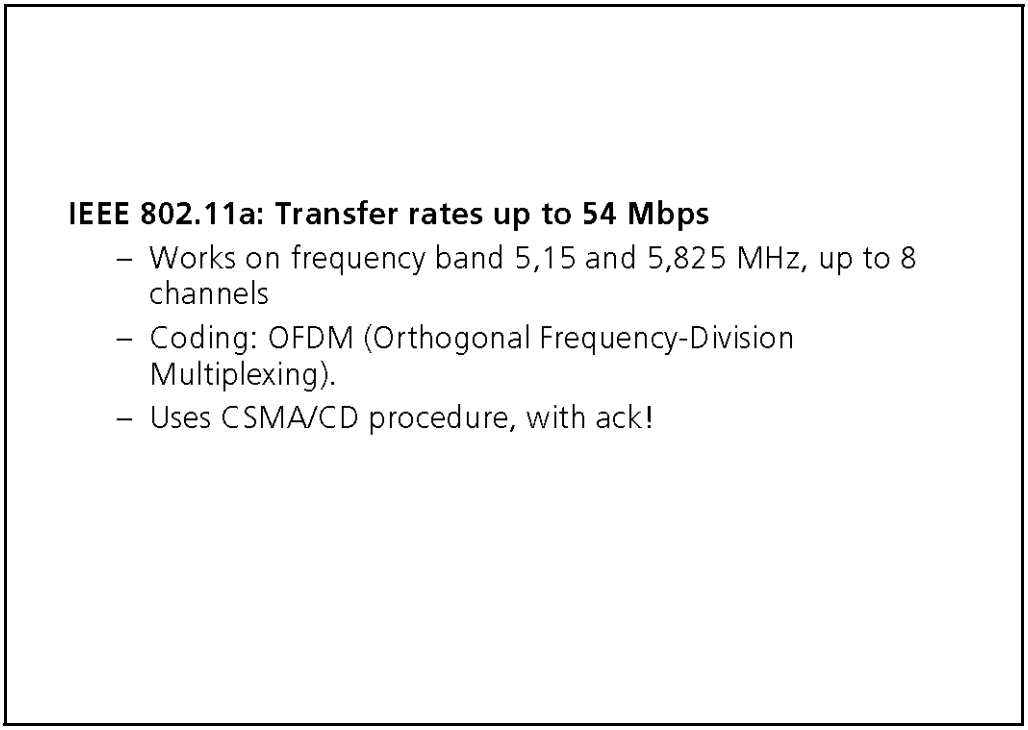
Max 192 stations

On utilise habituellement aujourd'hui la norme 802.11b, qui permet un débit de transfert allant jusqu'à 11 Mbit/s. Le nombre d'utilisateurs dépend des canaux de fréquences utilisés (3 au maximum). Jusqu'à 64 stations par canal ou 192 raccordements au total peuvent être exploités.

Fréquences

Des différences nationales existent en partie pour la définition des fréquences utilisées. Ces dernières se situent dans la bande des 2,4 GHz. Ces fréquences peuvent être utilisées directement, sans licence.

2.4.2 IEEE 802.11a

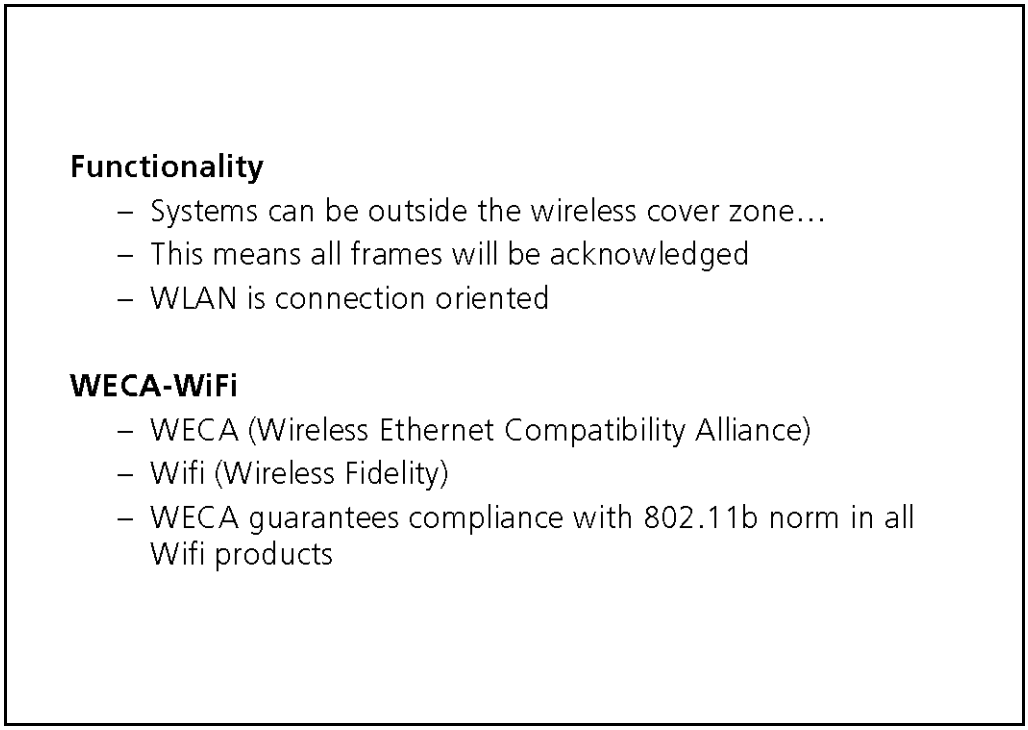


Slide 2.26
IEEE 802.11a

Un nouveau standard se profile pour la technologie WLAN avec la norme 802.11a :

- Les fréquences se situent dans le domaine allant de 5,15 à 5,825 GHz.
- Il existe 8 différents canaux.
- Chaque canal peut transmettre jusqu'à 54 Mbit/s. Cela nous donne une capacité totale maximum de 432 Mbit/s.
- Le nombre de stations possibles s'élève ainsi à 512.
- Un meilleur procédé est utilisé pour la modulation, l'OFDM (Orthogonal Frequency Division Multiplexing). Ce type de modulation est insensible aux perturbations et plus robuste que les précédents.

2.4.3 WLAN : Technique et compatibilité



Slide 2.27
WLAN : Technique et compatibilité

La technique WLAN travaille elle aussi avec le protocole CSMA/CD (Carrier Sense Multiple Access with Collision Detect).

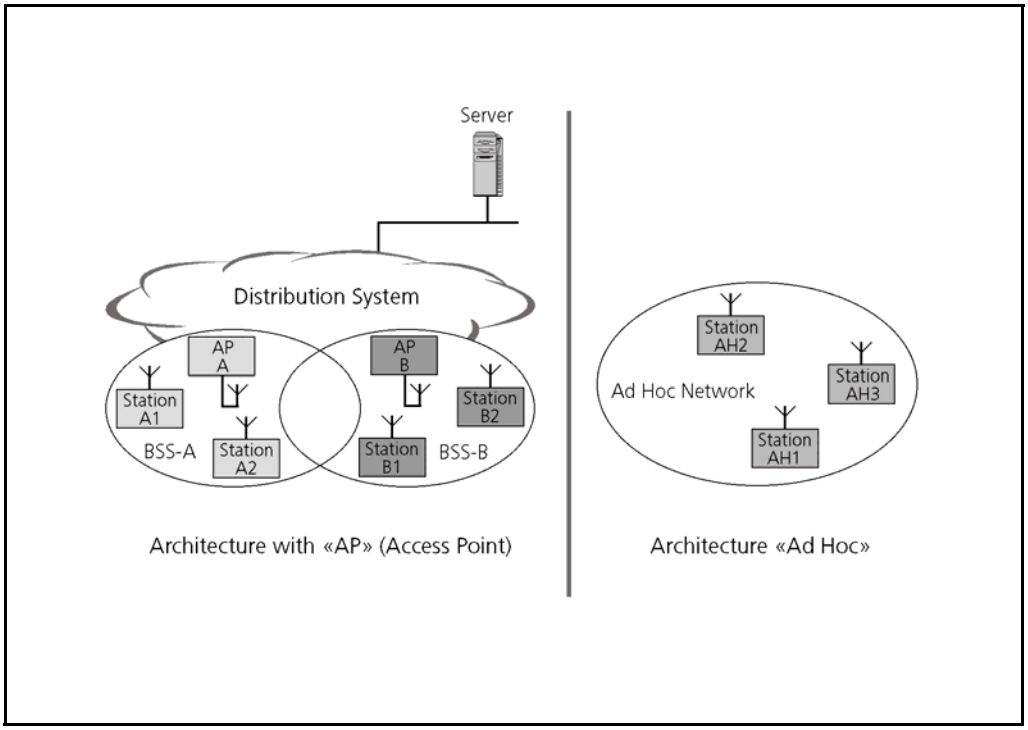
Connection oriented

Des problèmes pouvant survenir avec les stations se trouvant à la limite de la portée du système, un timing plus strict a été mis sur pied, associé à un dispositif de confirmation de réception. Cela signifie que le système 802.11b fonctionne en mode connexion (connection oriented).

WECA, Wifi

Comme les fournisseurs utilisent habituellement, en plus des normes, des extensions privées, une organisation (WECA : Wireless Ethernet Compatibilty Alliance) a été mise sur pied qui octroie un label aux produits respectant la compatibilité avec la norme. Ce label porte le nom de WiFi (Wireless Fidelity).

2.4.4 WLAN : Architecture



Slide 2.28
WLAN : Architecture

Nous distinguons entre deux architectures différentes.

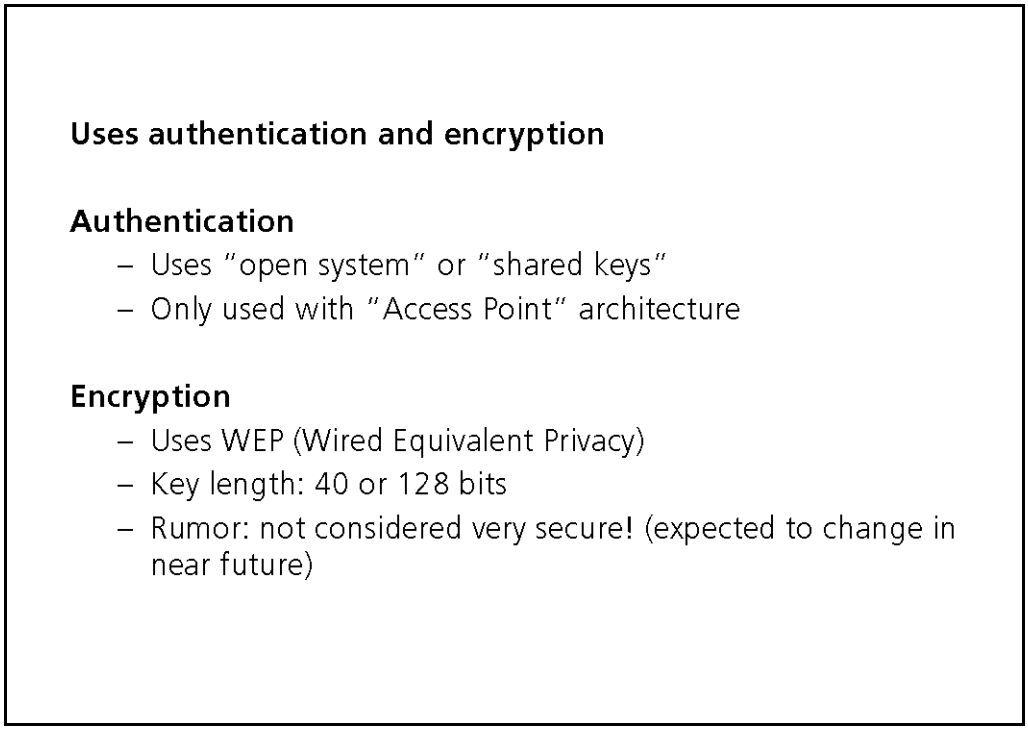
Dans l'architecture ad hoc, les stations sont reliées dans une communication peer-to-peer. Aucune des stations n'a de fonction de coordination (terme spécifique : Independent Basic Service Set, IBSS)

Architecture Ad hoc, IBSS

dans le cas de l'architecture AP, La station AP (Access Point Station) se charge du contrôle du réseau : toutes les communications passent par elle. Cette architecture sert également à réaliser le raccordement au LAN fixe. La station AP est par conséquent installée de manière fixe. Cette architecture est appelée BSS (Basic Service Set). Si la liaison est réalisée vers le LAN local, nous parlons de "mode d'infrastructure"

Architecture AP, BSS

2.4.5 *WLAN* : *Security*



Slide 2.29
WLAN : Security

Pour que le WLAN connaisse une certaine sécurité, la norme 802.11 prévoit les deux mesures bien connues pour empêcher l'accès d'hôtes indésirables

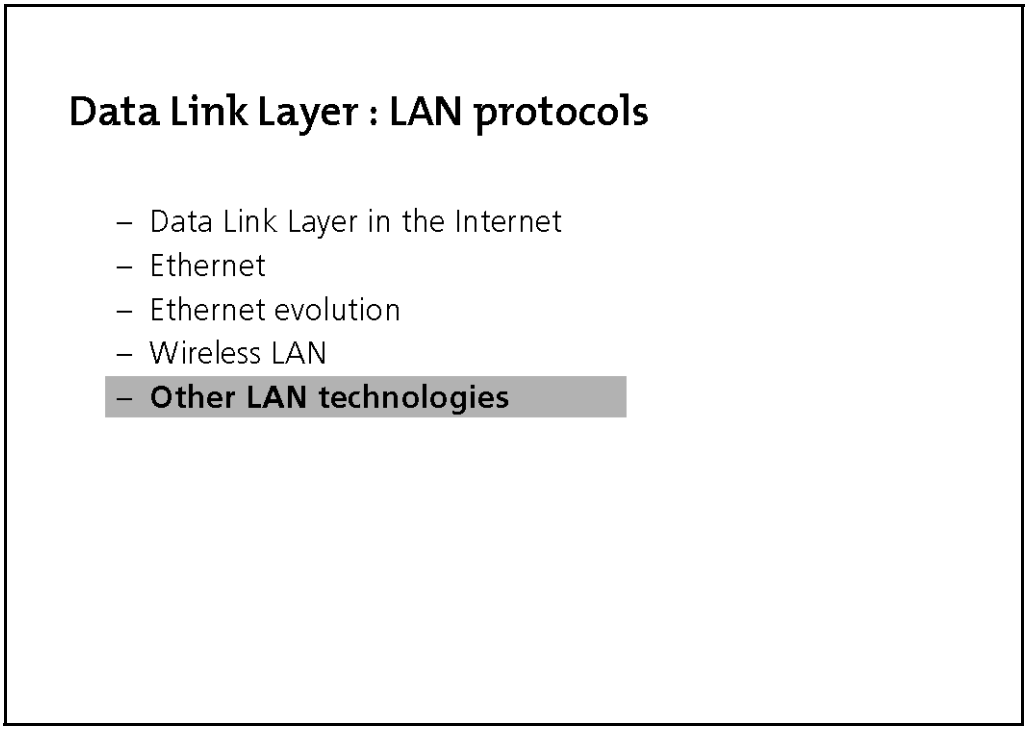
Authentification

Au début, chaque station doit prouver qui elle est. Avec le système "shared key", seules les stations disposant d'une clé secrète peuvent être authentifiées et participer au réseau. Avec le "Open System", chaque station peut demander une authentification, mais peut aussi s'en passer.

Cryptage

Le protocole WEP (Wired Equivalent Privacy) utilise des clés de 40 ou de 128 bits pour le cryptage. Il s'agit là toutefois d'un système simple (selon ses développeurs : reasonably strong). Les analyses effectuées par des experts en matière de sécurité ont montré que le code utilisé est relativement simple à casser. On attend ici une amélioration du cryptage à l'avenir (le groupe de travail IEEE 802.11i est en train de définir une extension, qui devrait être publiée en 2002).

2.5 Autres technologies LAN



Slide 2.30
Autre technologies LAN

Dans cette dernière partie relative aux LAN, nous allons citer deux technologies anciennes, qui devraient disparaître à l'avenir.

Ce sont des technologies qui, en parallèle avec les solutions Ethernet, ont grandement aider à démocratiser les réseaux locaux informatiques.

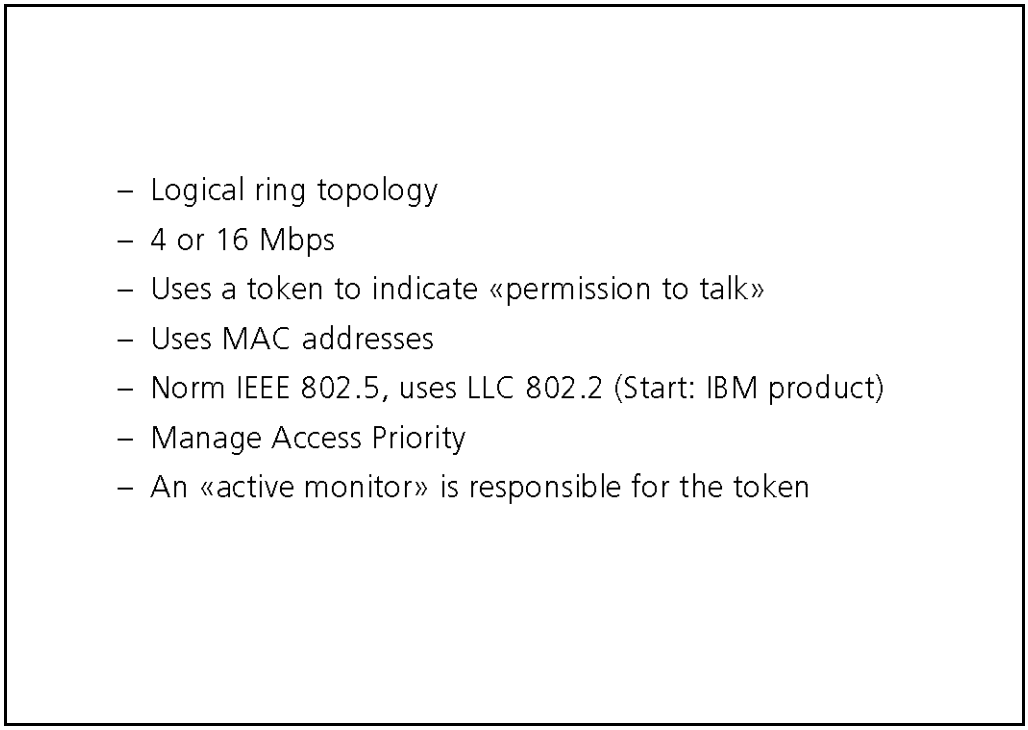
Token Ring

Token Ring est une solution qui a été développée par IBM. De ce fait, toutes les entreprises qui étaient équipées de machines de ce fabricant utilisaient cette technologie de réseau.

FDDI

FDDI, avec un débit de 100 Mbit/s, était 10 fois plus rapide que l'Ethernet. Fort de cet avantage, ajouté à la grande portée du système (100 km), FDDI s'est rapidement construit une place dans les épines dorsales des réseaux locaux (LAN) mais également dans les réseaux des campus et/ou Metropolitains (MAN). Aujourd'hui encore, des solutions MAN sur FDDI sont en fonction.

2.5.1 Token Ring



Slide 2.31
Token Ring

Token Ring

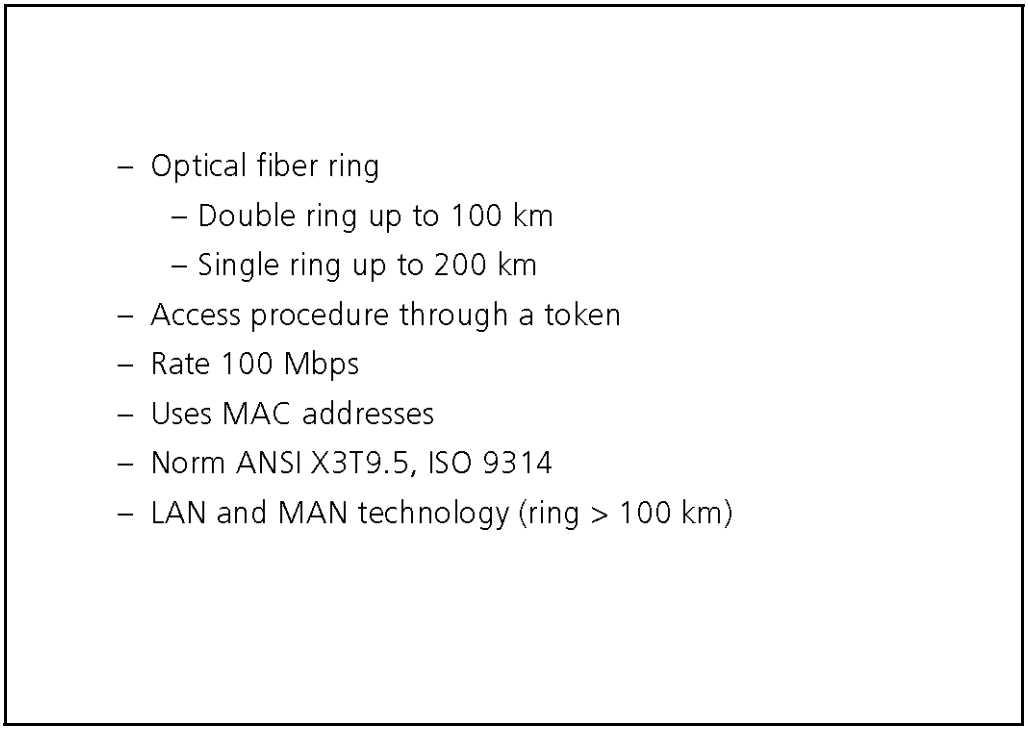
Token Ring est un protocole LAN possédant une structure logique en boucle. Deux vitesses sont disponibles 4 et 16 Mbit/s. Aujourd'hui ces vitesses sont dépassées, aucune version plus rapide ne sera proposée. Il est donc condamné à disparaître.

Sa procédure d'accès utilise un " jeton " (Token) qui, tournant dans la boucle, indique aux stations le moment où elles peuvent prendre la parole. Il s'agit donc d'une procédure d'accès déterministe.

Active Monitor

Token Ring a tout d'abord été développé par IBM, puis normalisé par IEEE (802.5). Il permet de gérer des priorités d'accès (réservation du jeton). Le jeton est en outre surveillé par une station " Active Monitor ". Celle-ci peut détruire les trames qui tournent indéfiniment, les jetons à double et recréer un jeton perdu.

2.5.2 FDDI (Fiber Distributed Data Interface)



Slide 2.32
FDDI (Fiber Distributed Data Interface)

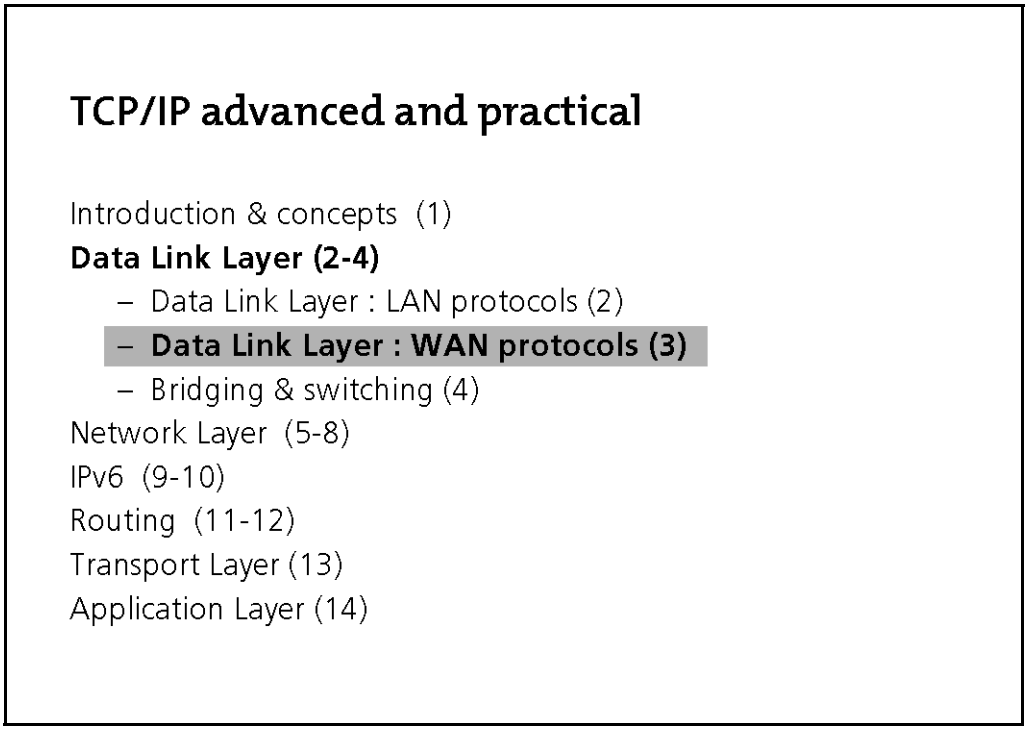
FDDI

FDDI est un réseau LAN ou MAN. A l'instar d'Ethernet, Il utilise l'adressage MAC. Comme Token Ring, il utilise un jeton pour indiquer le droit à la parole aux stations. Il offre un débit de 100 Mbit/s, sur une distance maximum de 100 km.

Il est souvent utilisé pour les épines dorsales (backbones) de réseaux locaux où sa fiabilité a été très appréciée. Il utilise une double boucle en fibres optiques. Dans le cas où la boucle ne serait pas doublée, on double la portée du système (200 km) !

Aujourd'hui concurrencé par Gigabit Ethernet et 10 Gigabit Ethernet, il va certainement disparaître peu à peu du milieu des LAN et des MAN.

3 Liaison de données : Protocoles WAN



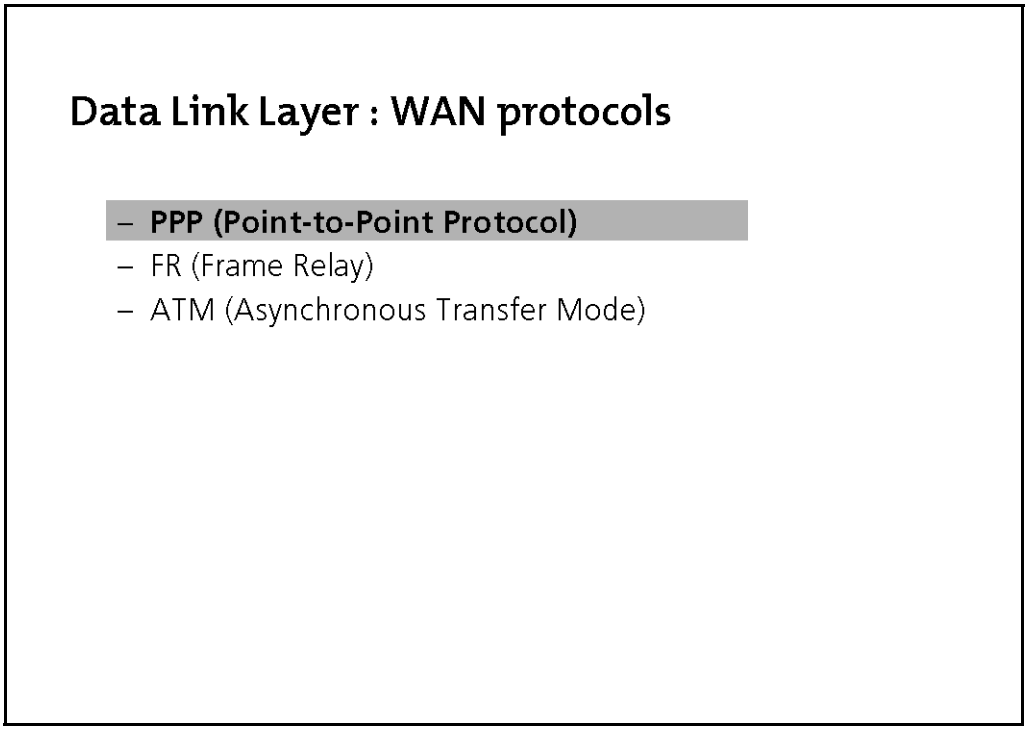
Slide 3.1
Liaison de données : Protocoles WAN

Ce chapitre traite des protocoles de couche 2 spécifiquement utilisés dans les environnements WAN. Après une étude approfondie de PPP, les principes de Frame Relay et ATM sont abordés.

Objectifs

A l'issue de ce chapitre, les participants sont capables de reconnaître les différents composants de PPP, ainsi que de décrire les étapes nécessaires à l'établissement d'une connection. Ils peuvent en outre nommer les principes de fonctionnement de FR et ATM.

3.1 PPP (Point to Point Protocol)



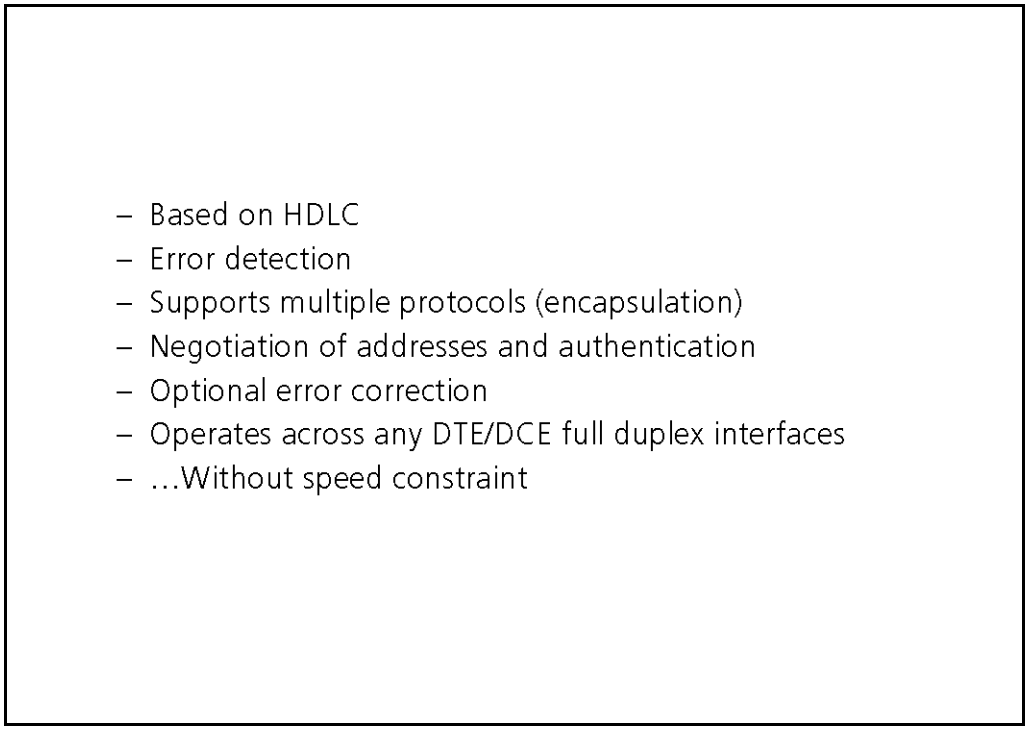
Slide 3.2
PPP (Point to Point Protocol)

PPP, SLIP

Le protocole point à point définit une méthode standard pour transporter des paquets de données sur des liaisons point à point. Il est le successeur de SLIP (Serial Line Internet Protocol) qui proposait une méthode d'encapsulation de paquet IP sur des lignes série asynchrones, orientées caractères.

PPP est décrit dans [RFC 1661] et [RFC 1662] (trame HDLC).

3.1.1 Principes et caractéristiques de PPP



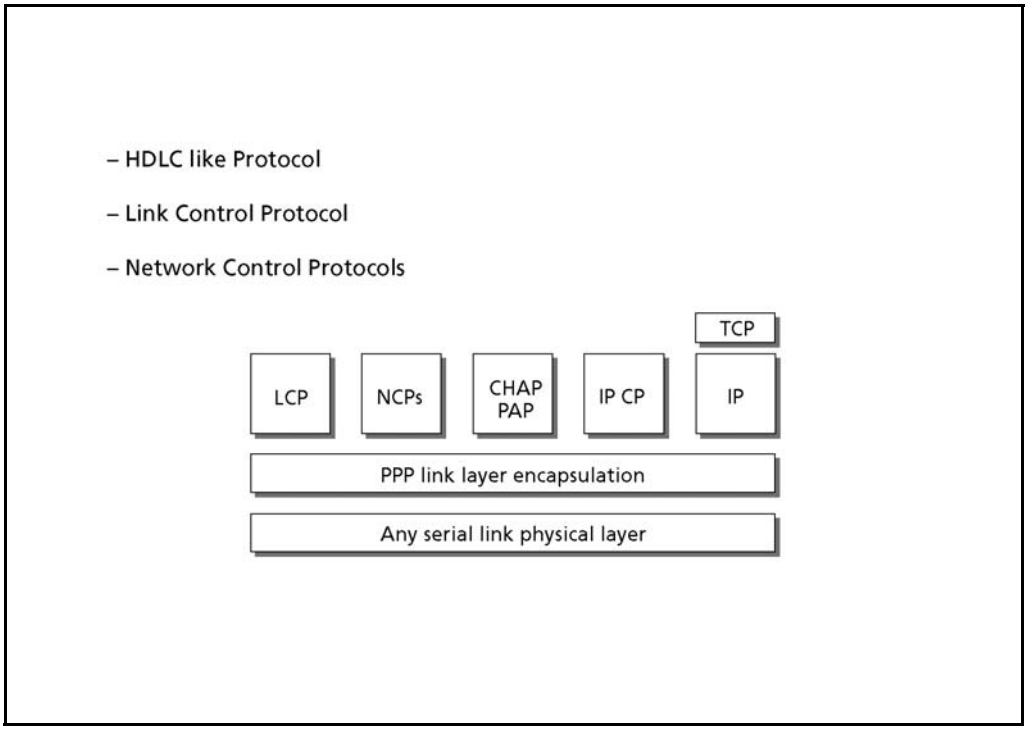
Slide 3.3
Principes et caractéristiques de PPP

HDLC

PPP utilise la structure de trame de type HDLC pour tramer et encapsuler les données des couches supérieures. Il fournit également les mécanismes nécessaires à la négociation des différents aspects opérationnels de la liaison (authentification, adresses, qualité de liaison). Sur une liaison de type asynchrone, PPP peut fonctionner en mode "caractère". Les procédures de délimitation de trame et de transparence sont alors réalisées avec des caractères d'échappement.

Le transfert fiable (optionnel) avec correction d'erreurs est définit dans [RFC 1663]

3.1.2 Composants de PPP

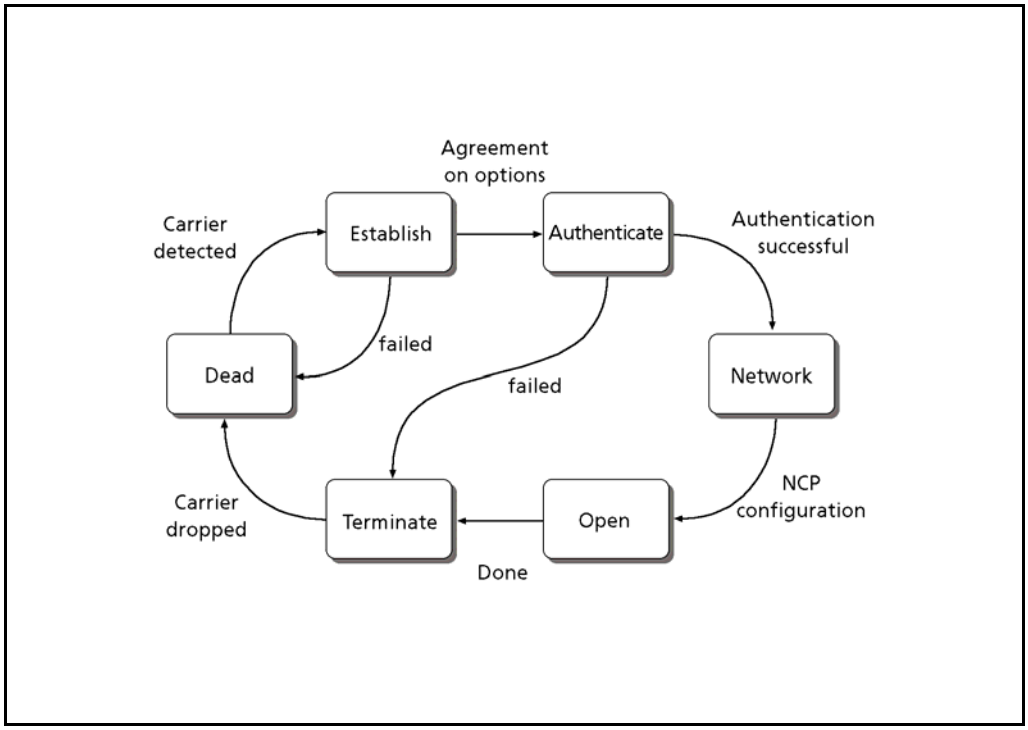


Slide 3.4
Composants de PPP

Les différents éléments fonctionnels de PPP sont:

- Une méthode pour encapsuler et tramer les informations des couches supérieures. Huit octets sont nécessaires pour réaliser cette fonction si la compression d'entête PPP n'est pas activée (réduction à 2 ou 4 octets).
- Un protocole de contrôle de liaison (LCP) qui permet, par exemple de négocier le format d'encapsulation, la méthode d'authentification, la taille des paquets. LCP fournit également les mécanismes pour contrôler l'état de la liaison et pour initialiser et terminer le transfert. LCP
- Différents protocoles d'authentification.
- Une série de protocoles (NCP's), chacun propre à une couche réseau, pour négocier les différents paramètres de fonctionnement de la couche supérieure (adresses, adresse de serveur, …). NCP

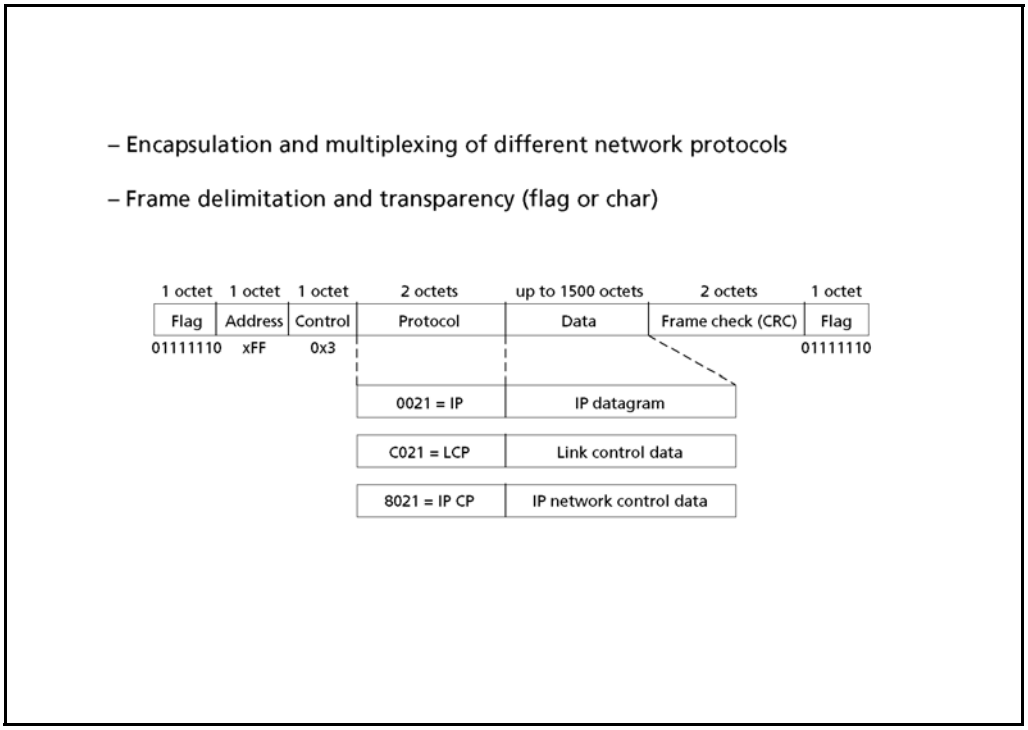
3.1.3 Opérations PPP



Slide 3.5
Opérations PPP

Au début d'une session PPP la ligne est interrompue (Dead). Après que la ligne physique ait été établie (Establish), les négociations d'options (LCP) peuvent démarrer. Si ces négociations sont fructueuses, les deux parties peuvent s'identifier (Authenticate). Dans l'état "Network" le NCP (Network Configuration Protocol) approprié est invoqué pour négocier les paramètres de la couche réseau. Le transfert effectif de données peut débuter dans l'état "Open". Lorsque que le transport de données est terminé (Terminate), la ligne peut être libérée pour passer dans l'état "Dead".

3.1.4 Format de paquet PPP



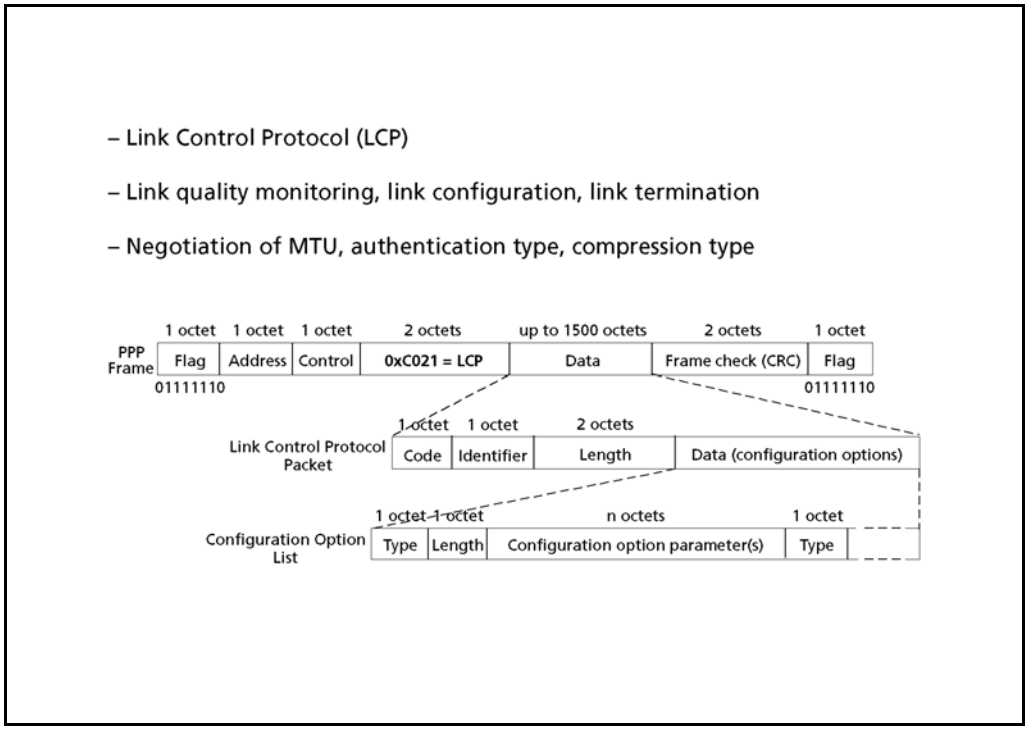
Slide 3.6
Format de paquet PPP

HDLC

Des fanions (flag) sont utilisés pour délimiter la trame. Le champ Address hérité de la structure HDLC, inutile dans le cas d'une liaison point à point, est fixé à 0xFF. Le champ Control est fixé à 0x03. Cette valeur correspond à une trame d'information non-numérotée (UI : Unumbered Information) pour livrer un service sans connexion (LLC type 1). Le champ Protocol contient l'information d'encapsulation qui identifie la nature des données (Data). Ces valeurs sont définies dans une base de données on-line disponible sur le site de l'IANA, selon [RFC 3232].

Protocol Field	Encapsulated protocol
0x0021	Internet Protocol (IP)
0x002D	Van Jacobson compressed TCP/IP
0x8021	IP Control Protocol (IPCP)
0xC021	Link Control Protocol (LCP)
0xC023	Password Authentication Protocol (PAP)
0xC223	Challenge Handshake Authentication Protocol (CHAP)

3.1.5 Négociations LCP



Slide 3.7
Négociations LCP

LCP

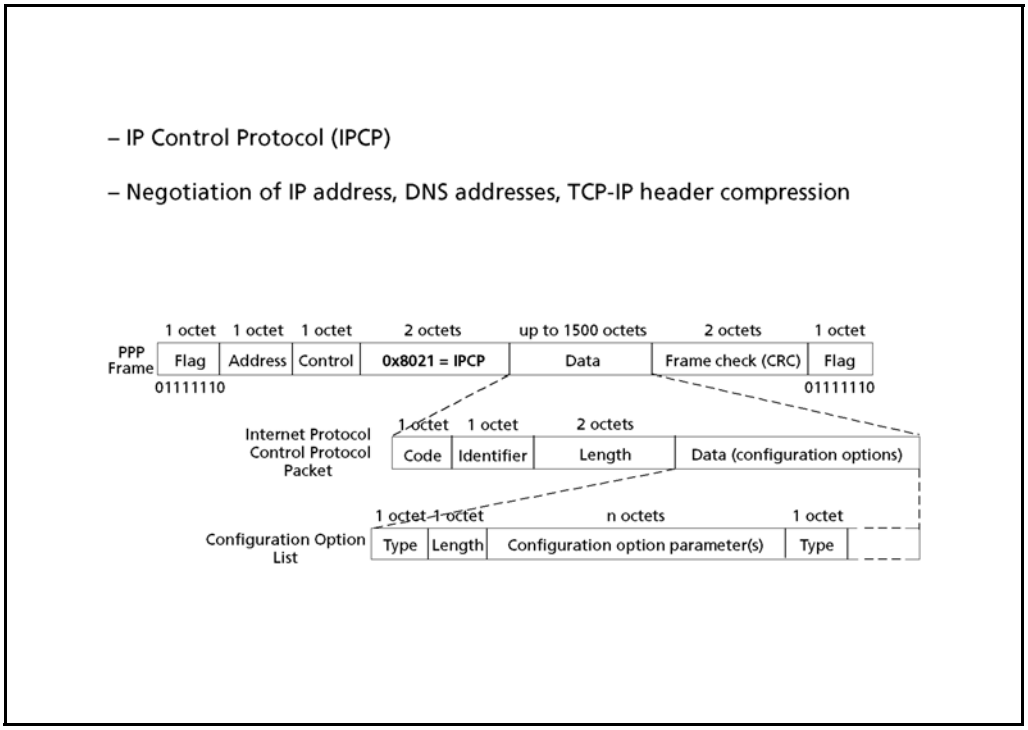
Les paquets LCP (Link Control Protocol) sont encapsulés dans des trames PPP (Protocol = 0xC021). LCP est défini dans [RFC 1548].

Le champ Code identifie le type de paquet LCP. Le champ Identifier est utilisé pour associer les requêtes et les réponses. Le champ Type indique l'option de configuration échangée.

Code Field	Signification
1	Configure-Request
2	Configure-Ack
3	Configure-Nak
4	Configure-Reject
5	Terminate-Request
6	Terminate-Ack
7	Code-Reject
8	Protocol-Reject
9	Echo-Request
10	Echo-Reply
11	Discard-Request

Type Field	Signification
1	Maximum-Receive-Unit
2	Async-Control-Character-Map
3	Authentication-Type
4	Quality-Protocol
5	Magic-Number
6	Link-Quality-Monitoring
7	PPP Protocol-Field-Compression
8	PPP Address-and-Control-Field-Compression
18	End point Disriminator Option

3.1.6 Négociations IP



Slide 3.8
Négociation IP

IPCP

IPCP (IP Control Protocol) est le protocole de contrôle responsable de configurer et d'activer le protocole IP à chaque extrémité de la liaison. IPCP utilise le même mécanisme d'échange de paquets que LCP.

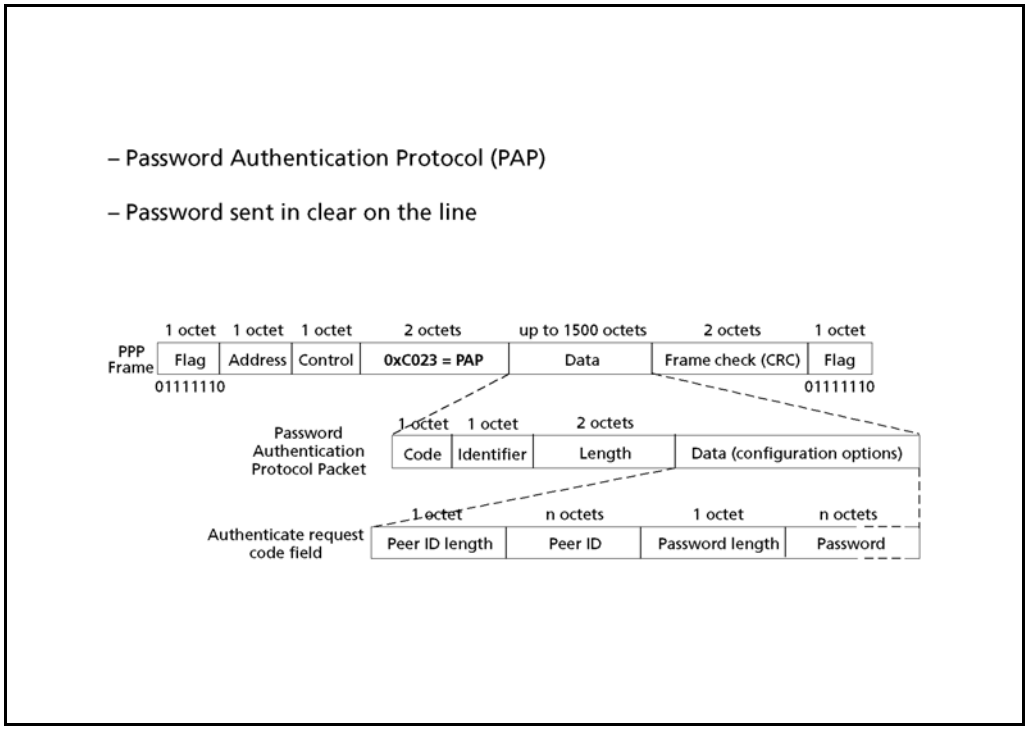
Le champ Code à la même signification que pour LCP. Seul les codes 1 à 7 peuvent être utilisés. Le champ Type indique l'option de configuration IP négociée.

IPCP est défini dans [RFC 1332]. Les options de configuration DNS et NBNS sont décrites dans [RFC 1877] et celles de Mobile IPv4 dans [RFC 2290].

Code Field	Signification
1	Configure-Request
2	Configure-Ack
3	Configure-Nak
4	Configure-Reject
5	Terminate-Request
6	Terminate-Ack
7	Code-Reject

Type Field	Signification
2	IP-Compression protocol
3	IP Address
4	Mobile IPv4
129	Primary DNS Server Address
130	Primary NBNS Server Address
131	Secondary DNS Server Address
132	Secondary NBNS Server Address

3.1.7 Authentification PAP



Slide 3.9
Authentification PAP

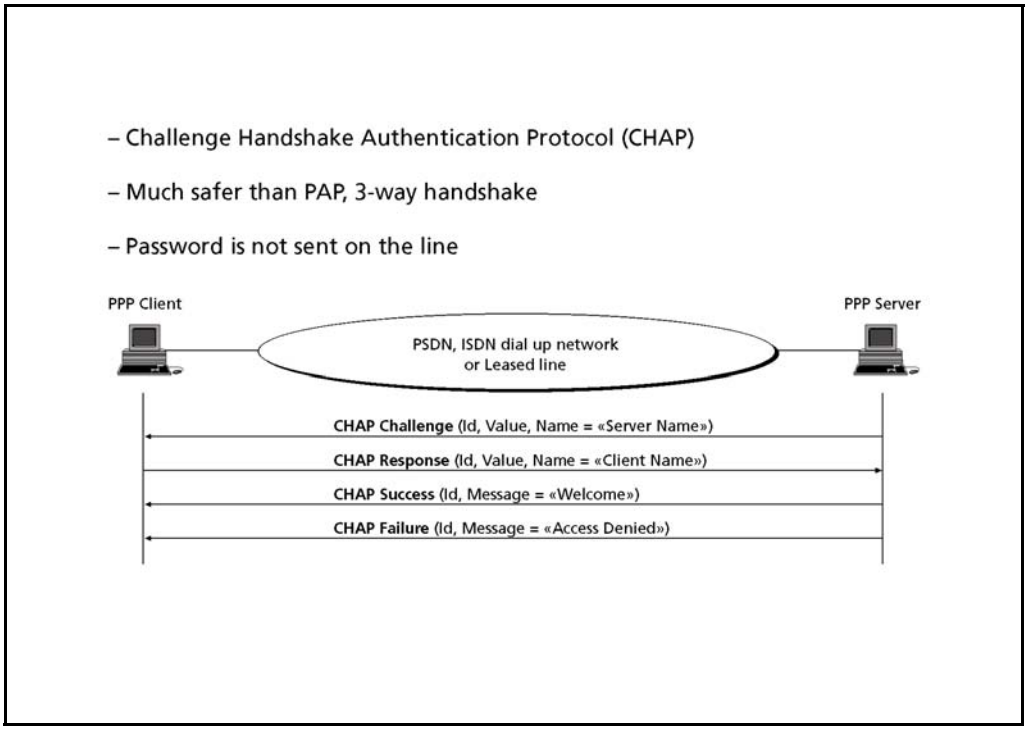
PAP

Lorsque la liaison est établie, PPP propose une phase optionnelle d'authentification. Le protocole PAP (Password Authentication Protocol) fournit une méthode simple qui consiste à envoyer une chaîne de caractères de type "PeerID-Password" de manière répétitive jusqu'à la validation de l'authentification. PAP n'est pas une méthode d'authentification robuste car le mot de passe est envoyé sans chiffrement sur la ligne. Le champ Code identifie le type de paquet PAP.

PAP est défini dans [RFC 1334].

Code Field	Signification
1	Authenticate-Request
2	Authenticate-Ack
3	Authenticate-Nak

3.1.8 Authentification CHAP



Slide 3.10
Authentification CHAP

CHAP

Le protocole CHAP (Challenge-Handshake Authentication Protocol) permet l'authentification d'une station à l'aide d'un mécanisme en trois étapes (Three-way handshake).

Challenge

Après l'établissement le serveur (l'authentifiant) envoie un message "Challenge" au client (l'authentifié). Ce message contient une valeur (Value) générée aléatoirement par le serveur.

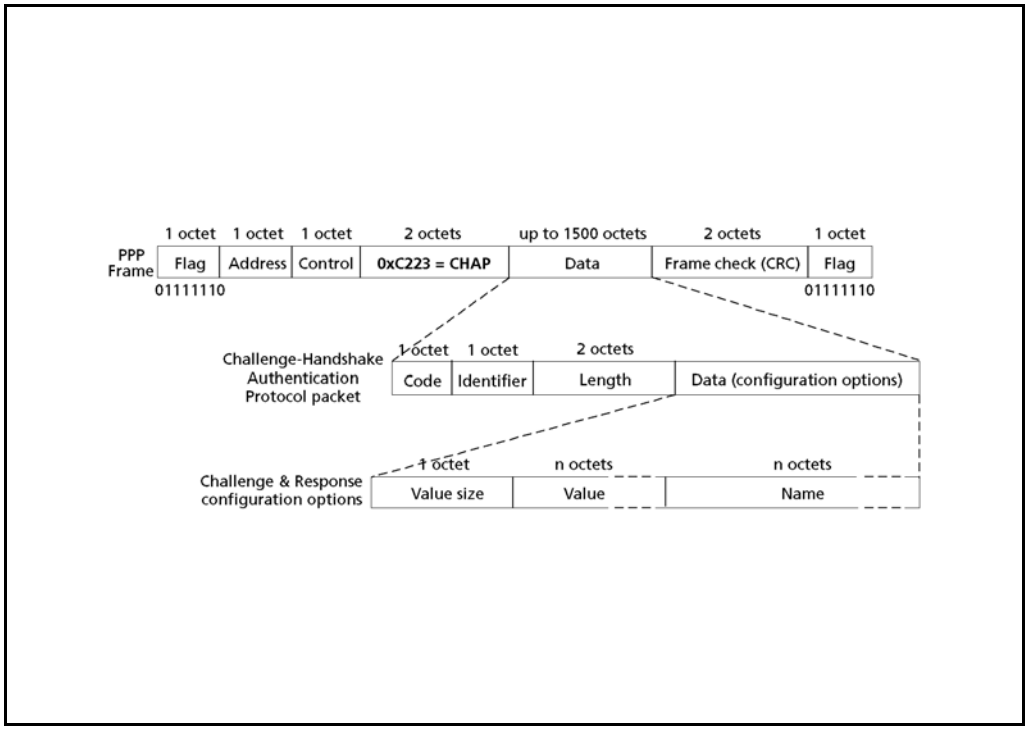
Response

Le client met en œuvre une fonction mathématique (Hash Function) en utilisant comme paramètres la valeur livrée par le serveur et le mot de passe (Secret). Le résultat de ce calcul qui ne permet pas de retrouver les paramètres initiaux est retourné au serveur dans un message "Response".

Success, Failure

Le serveur qui réalise la même procédure peut comparer sont résultat avec celui retourné par le client et, le cas échéant, valider l'authentification avec un message "Success".

3.1.9 Format de paquet CHAP



Slide 3.11
Format de paquet CHAP

Le champ Code identifie le type de paquet CHAP.

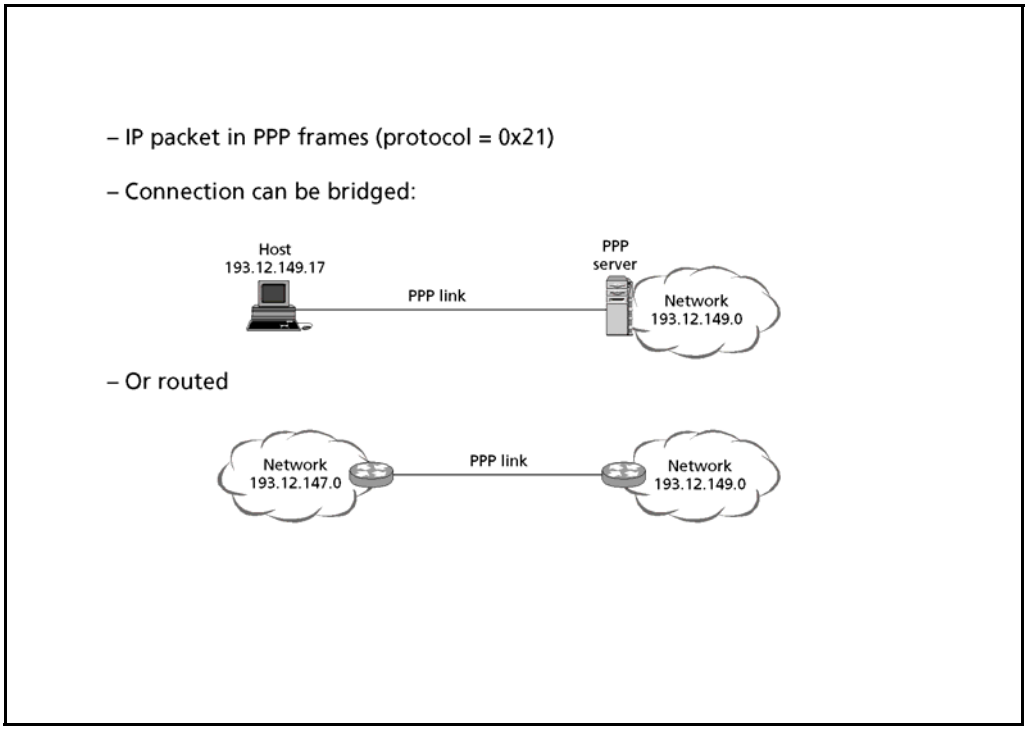
Challenge Value est une valeur de longueur variable, générée par le serveur chaque fois qu'il souhaite authentifier le client.

Le champ Name contient une chaîne de caractères identifiant l'émetteur des paquets "Challenge" ou "Response".

Les messages "Success" et "Failure" contiennent un Message destiné à livrer une information lisible à l'utilisateur.

Code Field	Signification
1	Challenge
2	Response
3	Success
4	Failure

3.1.10 IP sur PPP

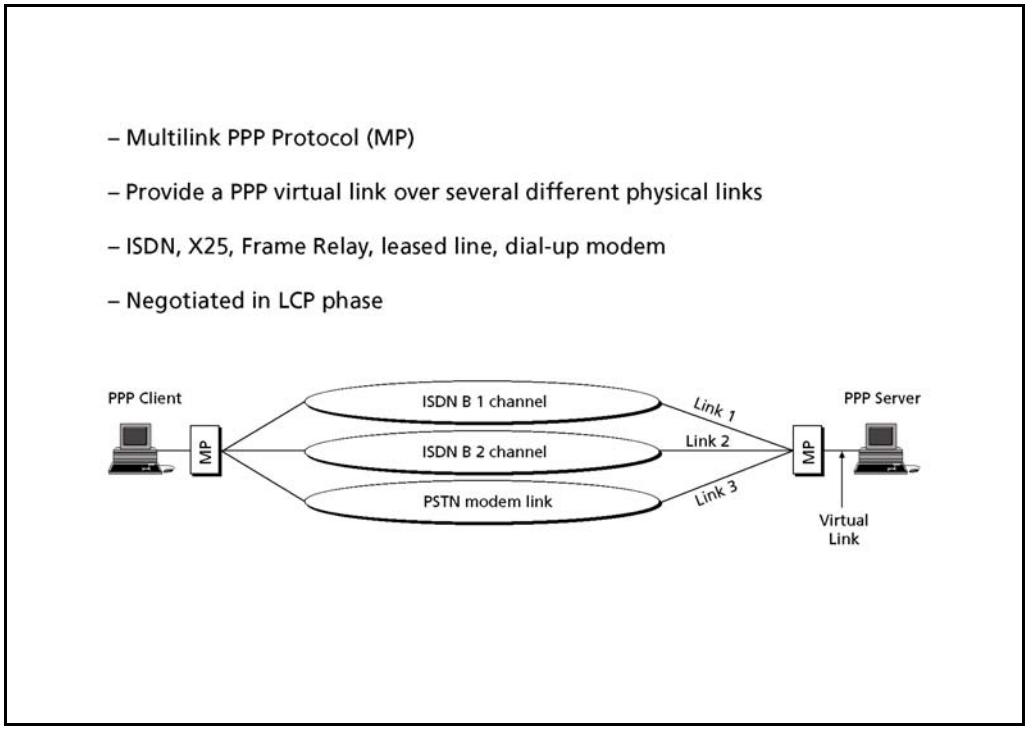


Slide 3.12
IP sur PPP

Une connexion peut être "bridgée". Dans ce cas l'adressage des deux cotés de la liaison fait partie du même sous-réseau IP.

Dans le cas d'une connexion "routée", un routeur se trouve à chaque extrémité de la liaison pour interconnecter deux réseaux appartenant à des espaces d'adressage IP différents.

3.1.11 PPP Multilink



Slide 3.13
PPP Multilink

PPP Multilink

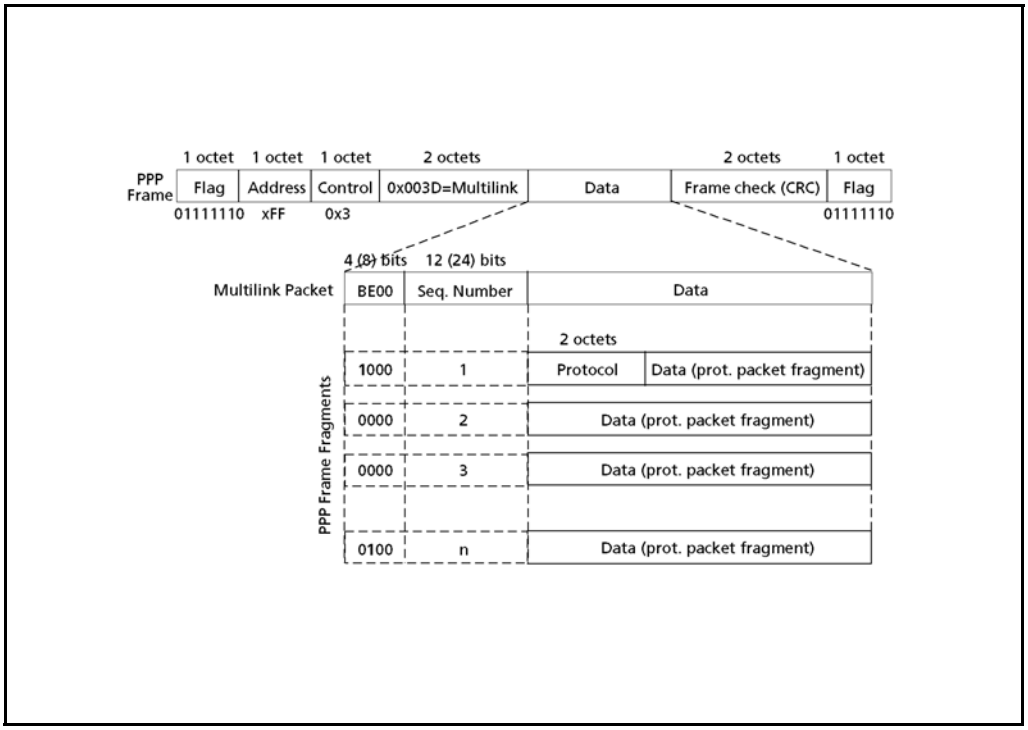
L'objectif de PPP multiliaison est de coordonner différentes liaisons physiques indépendantes entre deux systèmes (channel bundeling) pour obtenir une liaison virtuelle dont la bande passante est approximativement la somme des bandes passantes individuelles. Les liaisons physiques peuvent être de types différents, par exemple, une ligne modem associée à un canal B ISDN.

Channel Bundeling

PPP multilink introduit des options de négociation supplémentaires au protocole LCP (LCP configuration options: Multilink Maximum Recieved Reconstructed Unit, Multilink Short Sequence Number Header Format, End point Discriminator)

PPP multilink est défini dans [RFC 1990]

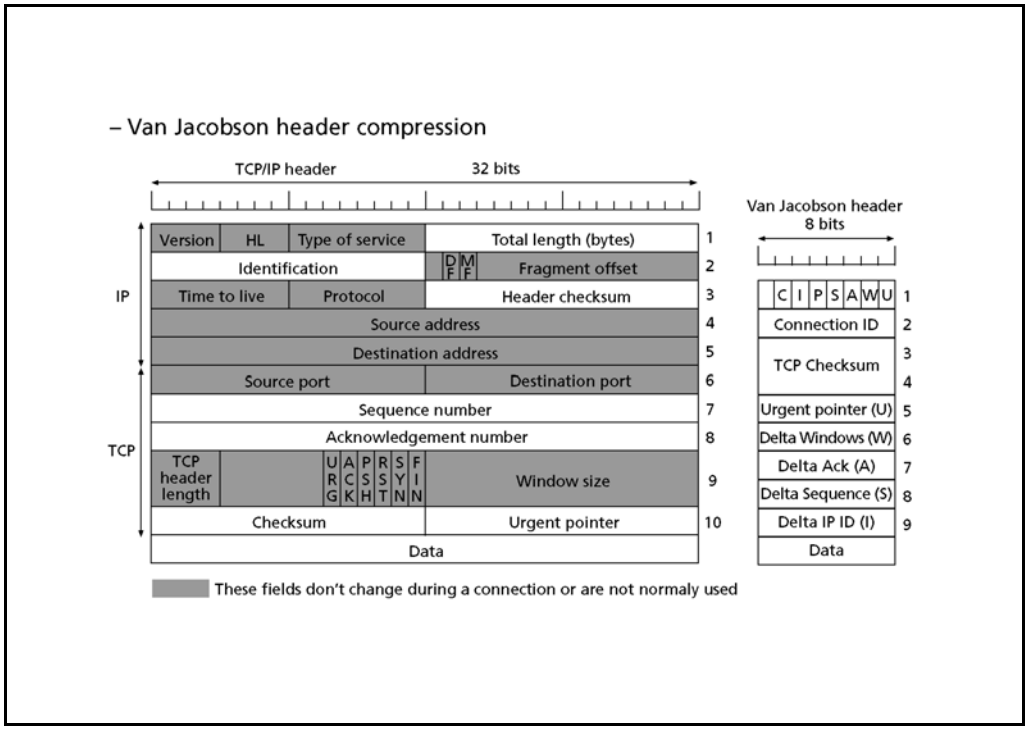
3.1.12 Format de paquet PPP multilink



Slide 3.14
Format de paquet PPP multilink

PPP multilink fournit les mécanismes pour fragmenter, séquencer et réassembler les datagrammes transitant au travers des différentes liaisons. Les paquets sont encapsulés (mais pas tramés) selon les procédures PPP. Ensuite une entête PPP multilink est ajoutée à chaque fragment. Celle-ci contient un numéro de séquence (Seq. Number) de 12 ou 24 bits, destiné à remettre les fragments en séquence du coté réception. Les bits début de fragment (B) et fin de fragment (E) permettent d'identifier le premier et le dernier fragment d'une trame. Ces deux bits peuvent être activés simultanément dans le cas d'un fragment unique.

3.1.13 Compression d'entête TCP/IP



Slide 3.15
Compression d'entête TCP/IP

Van Jacobson

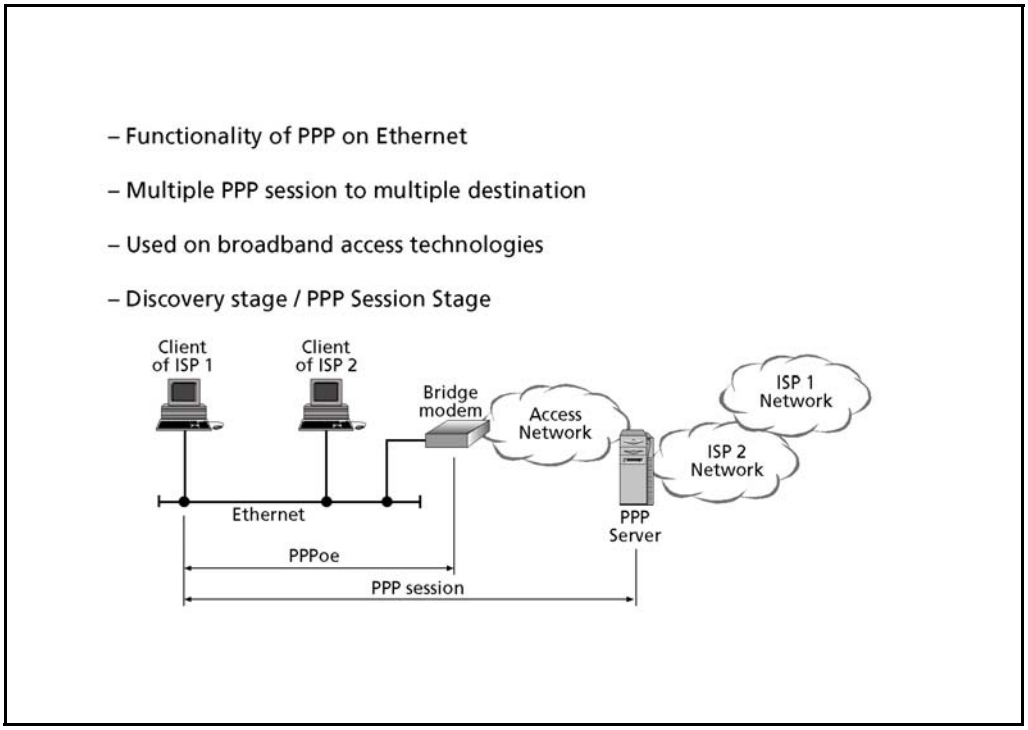
La plupart des informations contenues dans les 40 octets des entêtes TCP et IP ne changent pas durant une connexion ou changent seulement par petits incréments.

Sur les lignes lentes, il peut être avantageux de remplacer ces 40 octets par un entête Van Jacobson dont la taille est comprise entre 3 et 9 octets et qui transporte uniquement des informations de différence par rapport à l'entête précédente.

Le premier octet de cette entête est constitué de fanions (flags) qui indiquent quels champs de l'entête sont transmis. (C : Connection ID, P : TCP push flag). Les champs qui doivent obligatoirement être transmis sont les fanions (1 octet) et une copie du champ de protection TCP (TCP Checksum), (2 octets).

La compression d'entête Van Jacobson est définie dans [RFC 1144]

3.1.14 PPP sur Ethernet



Slide 3.16
PPP sur Ethernet

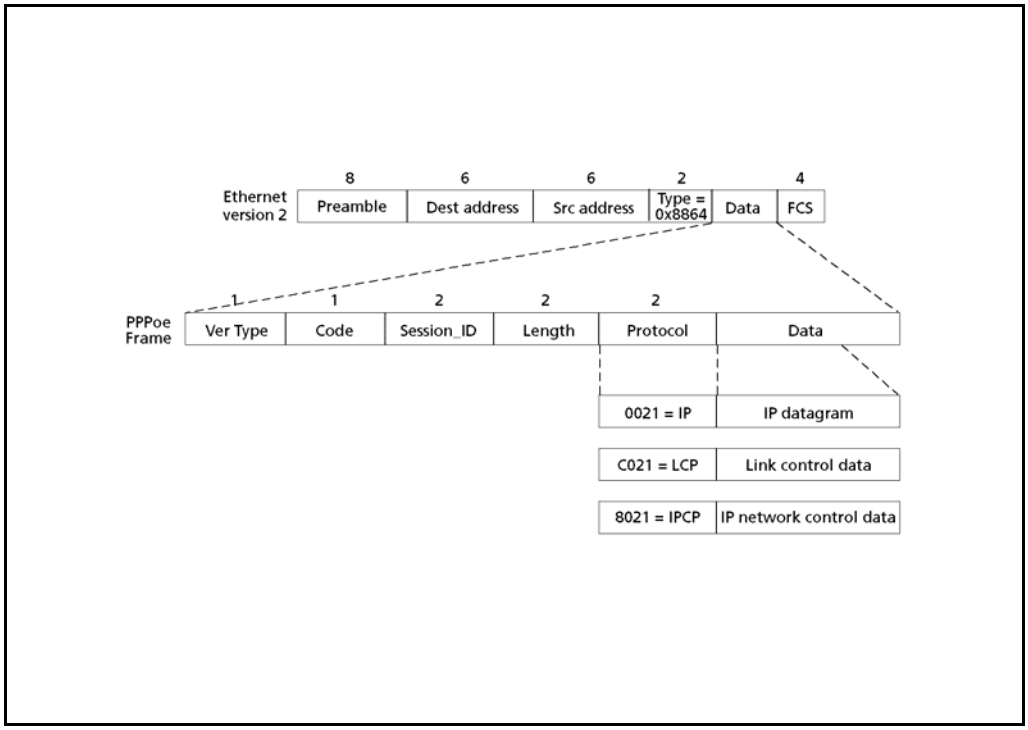
PPPoe

PPPoe (PPP over Ethernet) a été définit pour fournir les fonctionnalités de PPP (Authentification, LCP, NCP, ...) à des utilisateurs raccordés à un segment partagé de type Ethernet. Il est attendu que cette technique soit utilisée sur les technologies de raccordement à haut débit (xDSL) qui généralement livrent à l'utilisateur un raccordement de type LAN "bridgé".

La phase de découverte est constituée de quatre étapes à l'issue desquelles chaque partenaire connaît le numéro de session et l'adresse MAC du partenaire. Durant cette négociation, un type de service (provider ou qualité de service) peut être choisi.

PPPoe est définit dans [RFC2516]

3.1.15 Format de paquet PPP sur Ethernet



Slide 3.17
Format de paquet PPP sur Ethernet

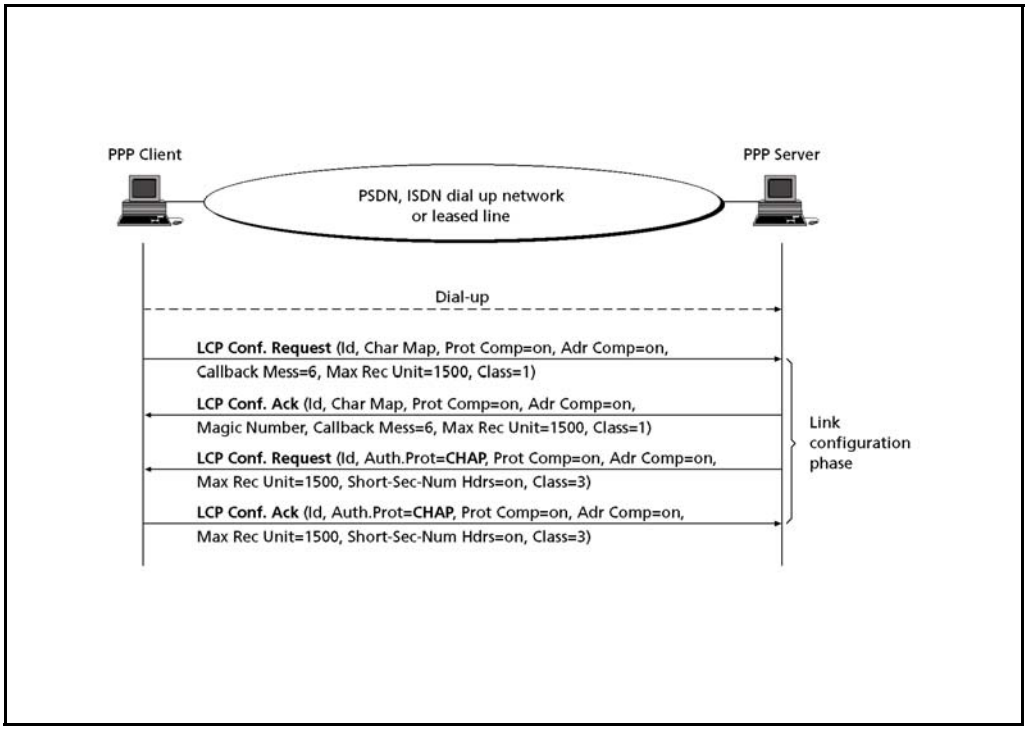
On distingue deux phases distinctes dans le fonctionnement de PPPoe. Tout d'abord une phase de "découverte", pendant laquelle les configurations sont négociées, puis dans une deuxième phase, le fonctionnement actif de la session PPPoe pour la transmission des données. La trame PPPoe est identifiée par la valeur 0x8863 du champ "Ethertype" pendant la phase de découverte, puis par la valeur 0x8864.

Les champs Ver et Type sont tous les deux fixés à 0x1 pour cette version de PPPoe. Le champ Code spécifie le type de message, valable lors des deux phases PPPoe.

Le champ Session_ID associé aux adresses MAC source et destination constitue un identificateur unique de session PPP. La valeur de ce champ est définie dans la phase de découverte.

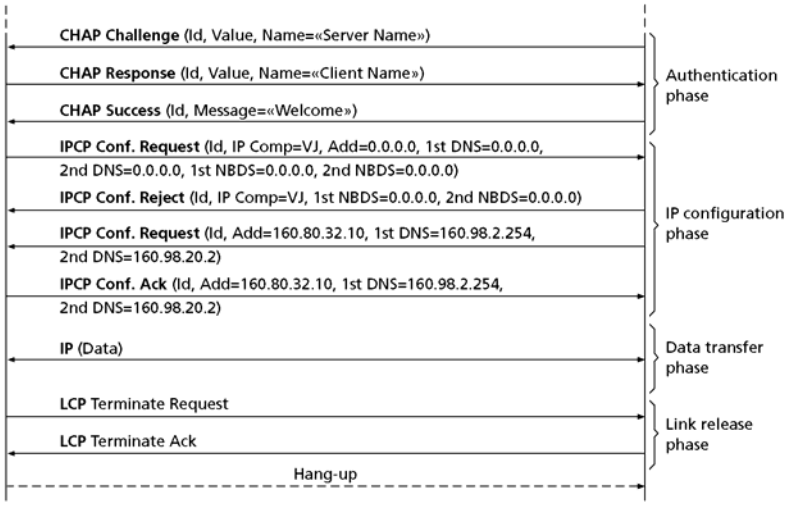
Code Field	Signification
0x00	PPP data
0x09	PADI PPPoe Active Discovery Initiation
0x07	PADO Discovery Offer
0x19	PADR Discovery Request
0xA7	PADT Discovery Terminate
...	

3.1.16 Exemple de session PPP



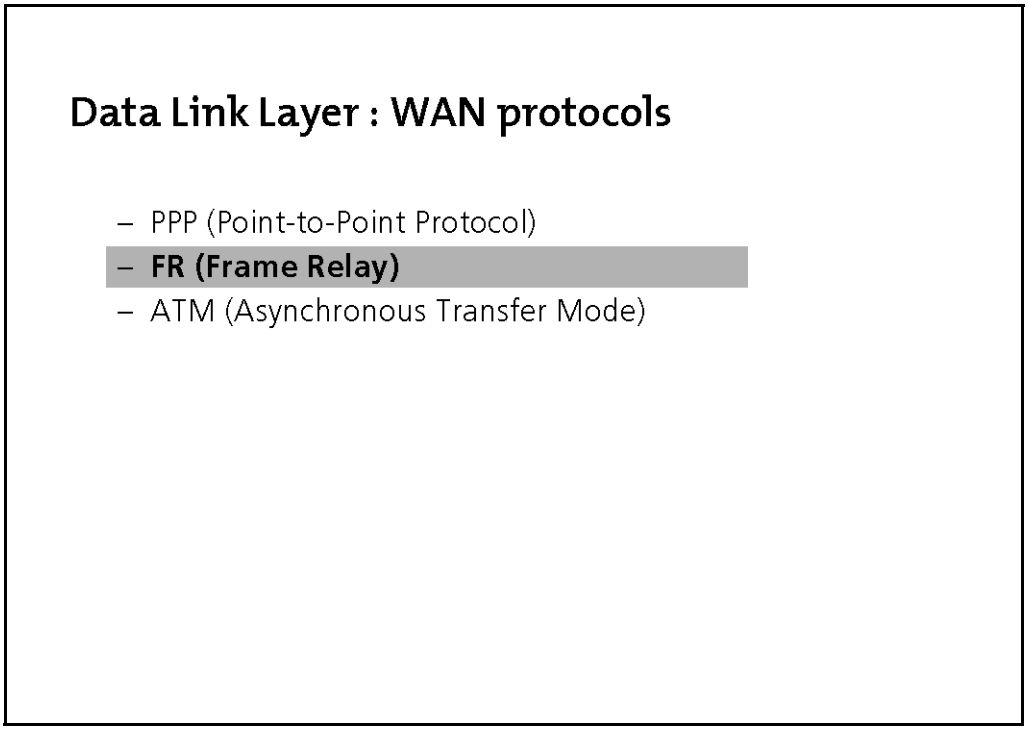
Slide 3.18
Exemple de session PPP

Exemple de session PPP (2)



Slide 3.19
Exemple de session PPP (2)

3.2 Frame Relay



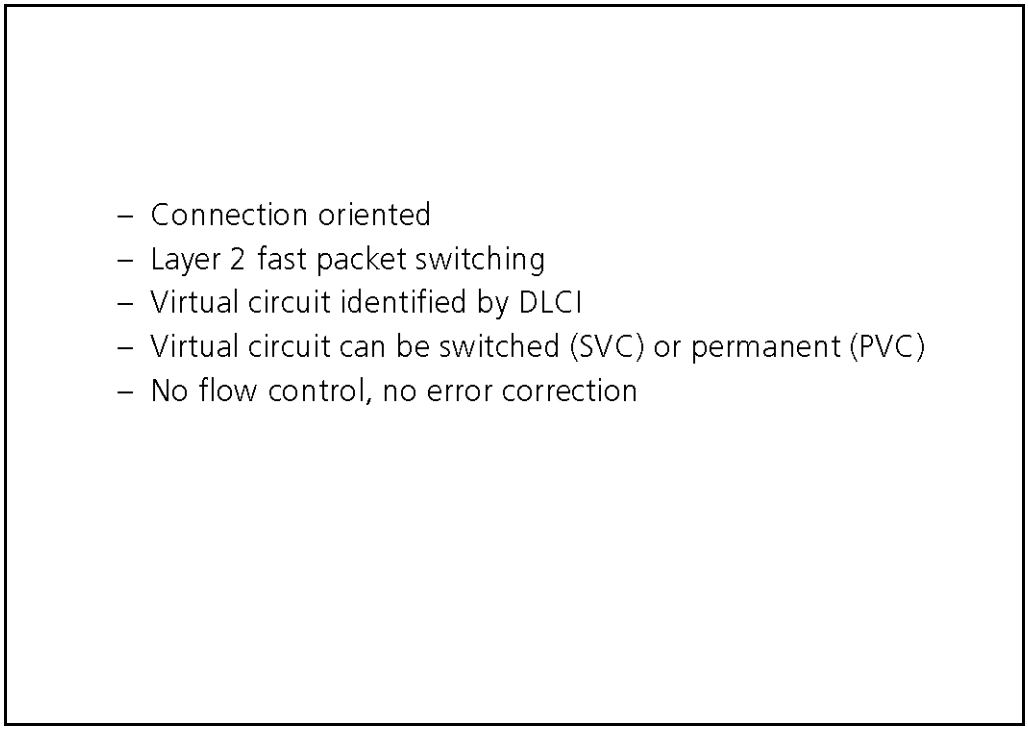
Slide 3.20
Frame Relay

Frame Relay

Frame Relay est une évolution amaigrie de X.25. Son objectif principal est l'amélioration des performances sur des réseaux de bonne qualité (à faible taux d'erreur). X.25 était conçu pour fonctionner sur des réseaux de qualité faible (ligne modem) avec des mécanismes lourds de récupération d'erreurs mis en œuvre au niveau de la couche 2 et de la couche 3. Frame Relay délègue ces fonctions aux systèmes terminaux et réalise la commutation au niveau de la couche 2.

Frame Relay est décrit dans la recommandation UIT [Q.922]

3.2.1 Principes et caractéristiques de Frame Relay



Slide 3.21
Principes et caractéristiques de Frame Relay

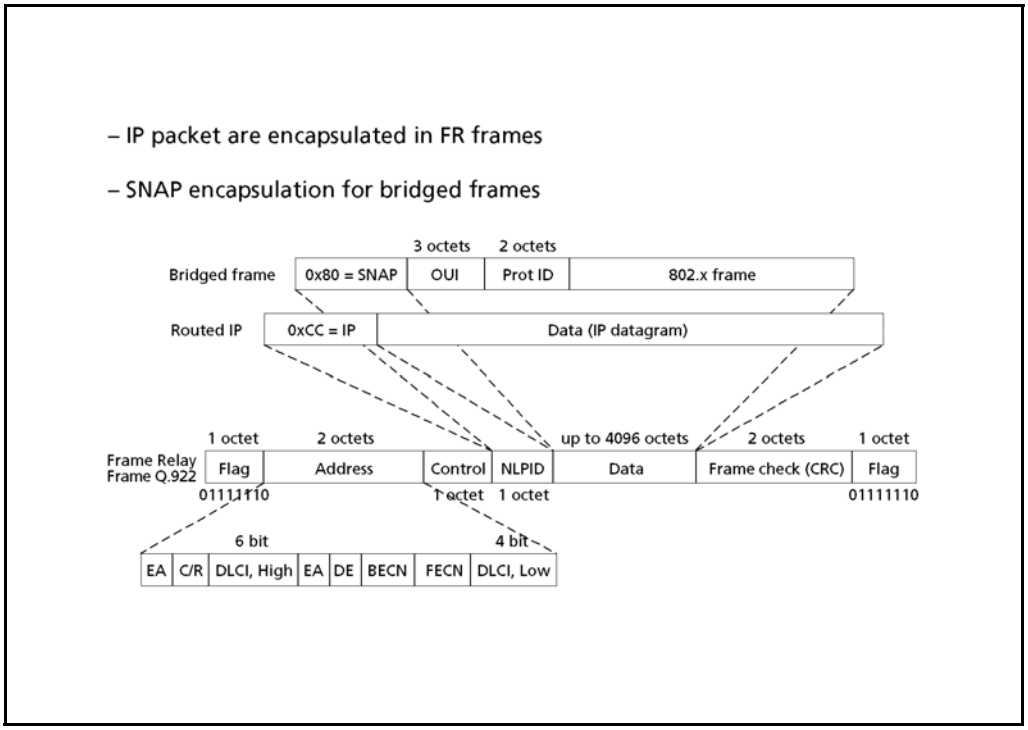
Frame Relay est une technologie de commutation de paquets orientée connexion. Les trames sont transmises de la source vers la destination sur un circuit virtuel pré-établi.

Frame Relay ne fournit ni de contrôle de flux ni de correction d'erreurs. Les trames erronées sont détruites sans notification. D'excellentes performances peuvent être atteintes sur les réseaux de bonne qualité.

PVC, SVC

Les circuits virtuels peuvent être établis de manière permanente (PVC : Permanent Virtual Circuit) ou établis à la demande (SVC : Switched Virtual Circuit) à l'aide d'une signalisation entre usager et réseau.

3.2.2 IP sur Frame Relay



Slide 3.22
IP sur Frame Relay

Le champ Address du paquet FR contient le DLCI (Data Link connection Identifer) qui identifie la connexion virtuelle à laquelle le paquet appartient. Le bit d'extension d'adresse (EA) marque le dernier octet du champ d'adresse. Les trames avec le bit DE (Discard Eligibility) activé sont détruites prioritairement dans les situations de congestion du réseau. Les notifications de congestion explicite (BECN, FECN) sont activées par un nœud congestionné.

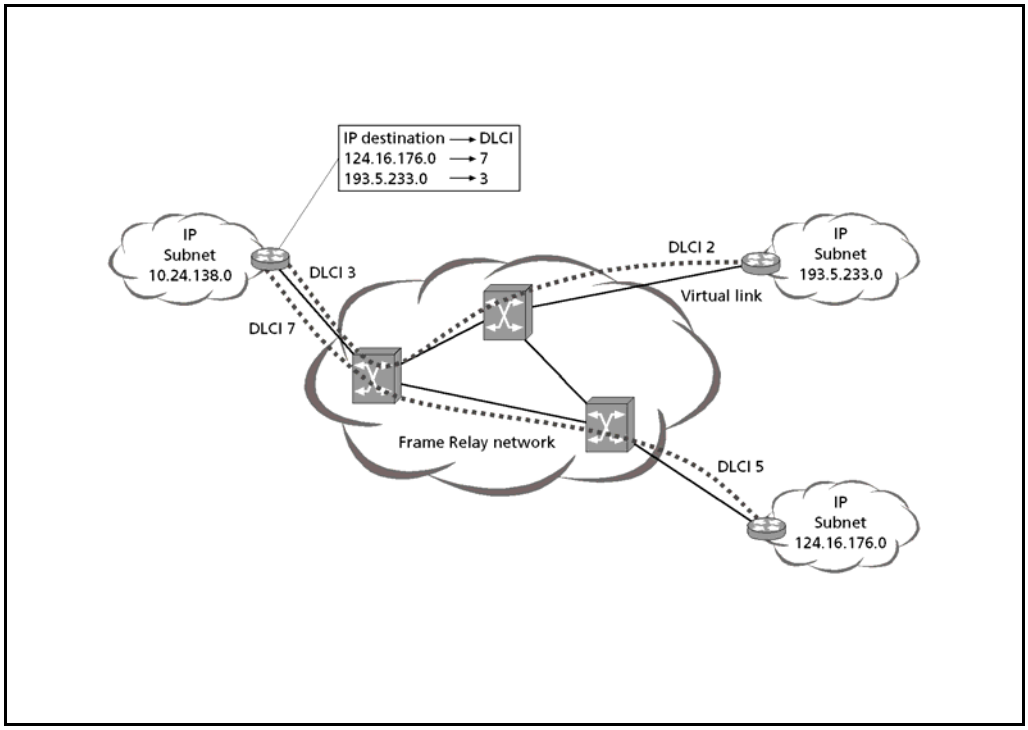
DLCI, EA

Le champ NLPID (Nework Layer Protocol Identifier) sert à identifier le protocole contenu dans la trame FR. Il peut s'agir par exemple de IP (NLPID = 0xCC) ou d'un entête SNAP qui identifie à son tour le protocole encapsulé (par exemple Ethernet)

DE, BECN, FECN, NLPID

Le procédé d'encapsulation de IP sur FR est décrit dans [RFC 1490]

3.2.3 IP sur Frame Relay: exemple

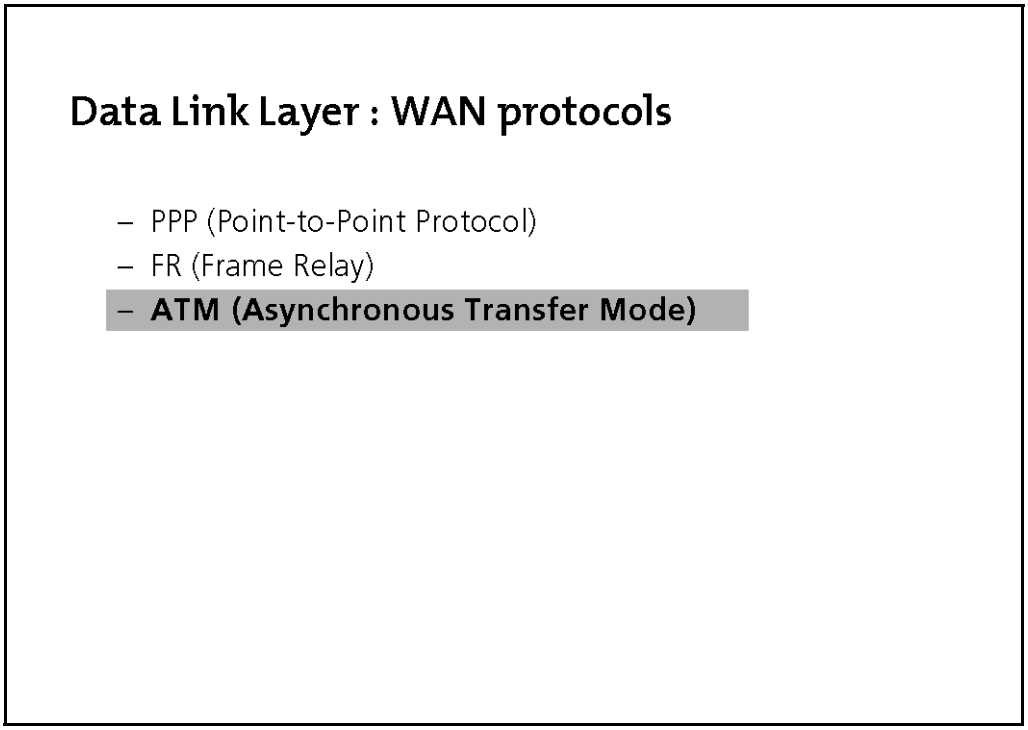


Slide 3.23
IP sur Frame Realy : Exemple

FR forwarding

L'acheminement des paquets Frame Relay est réalisé par l'analyse et la traduction des champs DLCI. Une connexion virtuelle est considérée par les routeurs comme port physique dédié.

3.3 ATM



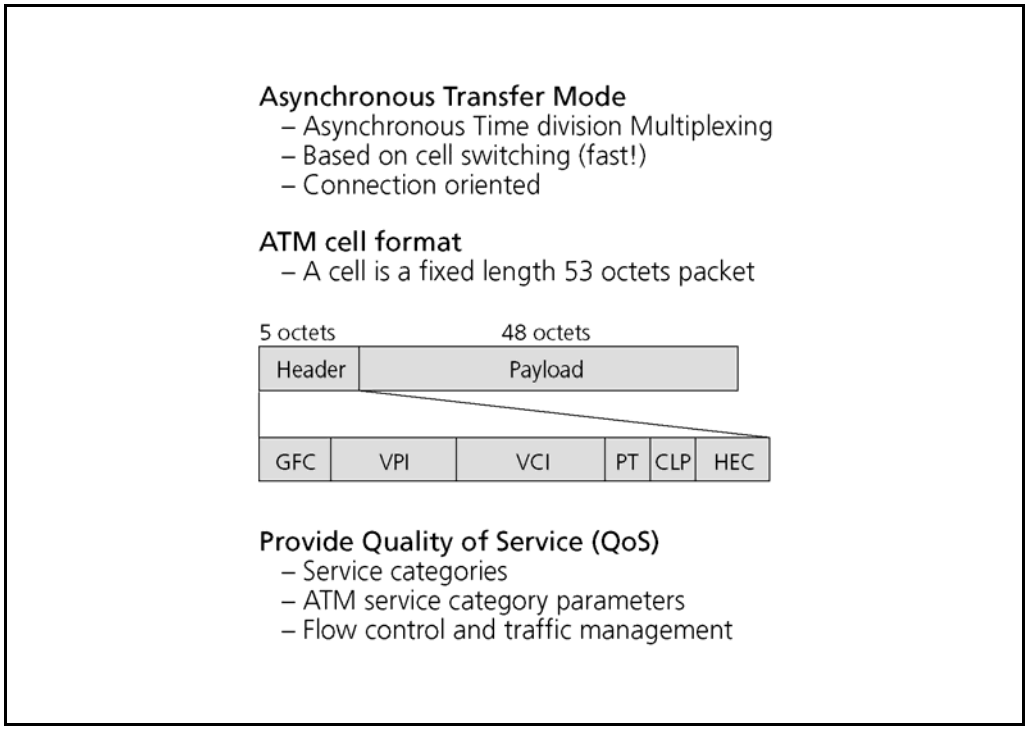
Slide 3.24
ATM

Le mode de transfert asynchrone (ATM) est une technique de commutation et de multiplexage (voire de transmission) qui est une variante de la commutation de paquets. ATM utilise en effet des paquets courts de taille fixe appelés cellules.

La technologie ATM a été développée principalement dans les années 1990. Elle était prévue pour être le mode de transfert d'information du futur réseau universel à large bande RNIS B-ISDN (Broadband ISDN). De ce fait ATM a été conçu pour le support natif de la QoS (Quality of Services) afin d'assurer la convergence des réseaux existants (data, voix et vidéo) vers un réseau B-ISDN. Un réseau B-ISDN intégrant tous les services de télécommunication et utilisant la technologie ATM n'a toutefois jamais vu le jour du fait de l'émergence des réseaux IP.

Actuellement Swisscom utilise la technologie ATM entre les équipements des clients et les routeurs Edge du réseau IPSS. Swisscom propose également une offre de service ATM à ses clients (par ex. Circuit Emulation, Native ATM) grâce à son réseau ATM SWANet. Il est également envisagé d'utiliser la technologie ATM dans les futurs réseaux mobiles de 3e génération UMTS.

3.3.1 Principes et caractéristiques de ATM



Slide 3.25
Principes et caractéristiques de ATM

Les principales caractéristiques du mode de transfert ATM sont :

- une technique de multiplexage temporel asynchrone
- la commutation rapide de cellules
- des services de réseau orienté connexion

Chaque cellule ATM est constituée d'un en-tête de 5 octets et de 48 octets de charge utile (payload). L'acheminement des cellules au travers du réseau s'effectue sur la base de l'analyse de l'en-tête par les commutateurs ATM. L'en-tête contient à cet effet les informations d'identification de la connexion virtuelle à laquelle appartient la cellule.. Cette structure permet une commutation rapide des cellules de façon hardware.

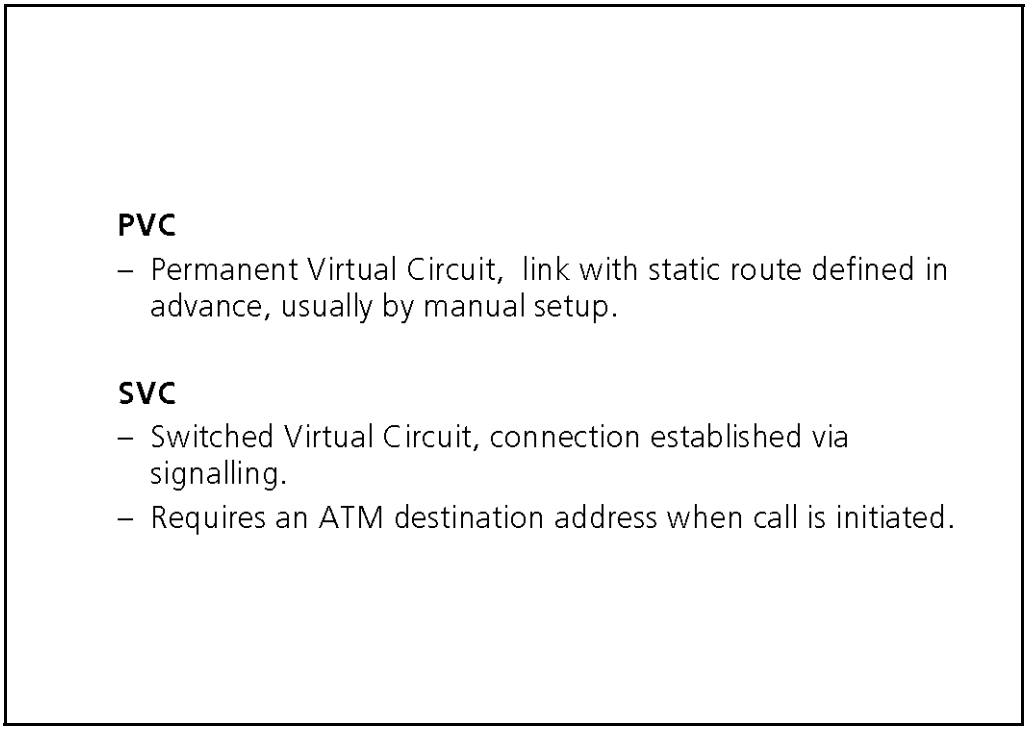
CBR, VBR

Un certain nombre de catégories de services ont été définies, comme par exemple CBR (Constant Bit Rate) ou VBR (Variable Bit Rate).

SCR, CTD

Pour chaque catégorie de services, différents paramètres, comme par exemple SCR (Sustainable Cell Rate) ou CTD (Cell Transfer Delay), permettent de spécifier la qualité de service d'une connexion. L'ensemble de ces paramètres est négocié dans un contrat de trafic. Des mécanismes de contrôle de flux et de gestion de trafic permettent de vérifier pendant la durée de la connexion les paramètres négociés et d'assurer ainsi la qualité de service.

3.3.2 Types de connexions sur ATM



Slide 3.26
Types de connexions sur ATM

L'acheminement des cellules dans les commutateurs ATM s'effectue sur la base de l'analyse des 2 champs VPI (Virtual Path Identifier - identification du faisceau virtuel) et VCI (Virtual Channel Identifier - identification du canal virtuel) de l'en-tête de cellule. Ces 2 champs VPI/VCI identifient la connexion virtuelle ATM à laquelle appartient une cellule. Il existe fondamentalement 2 types de connexion virtuelle ATM :

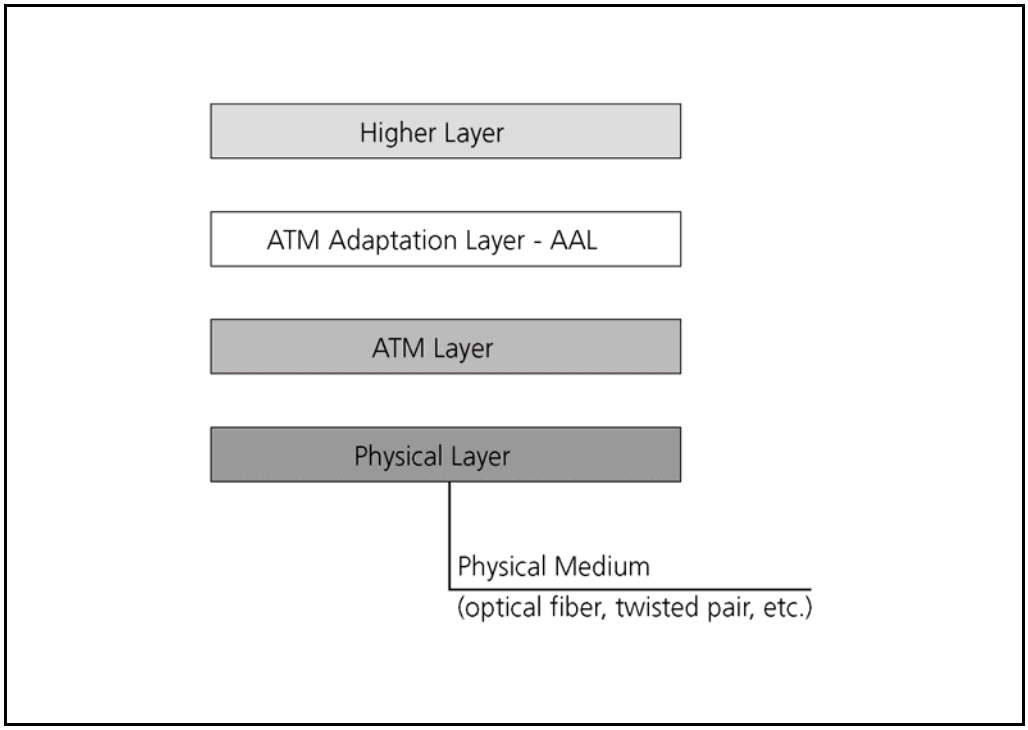
- **PVC** (Permanent Virtual Circuit) : Circuit virtuel permanent — PVC

  Il s'agit d'une connexion avec un acheminement statique, permanent et défini à l'avance. La connexion est configurée en principe de façon manuelle par l'administrateur du réseau dans les commutateurs et l'équipement terminal.

- **SVC (**Switched Virtual Circuit): Circuit virtuel commuté — SVC

  La connexion est établie à l'aide d'une procédure de signalisation. Une adresse de destination ATM est nécessaire.

3.3.3 Modèle de référence ATM (plan d'usager)



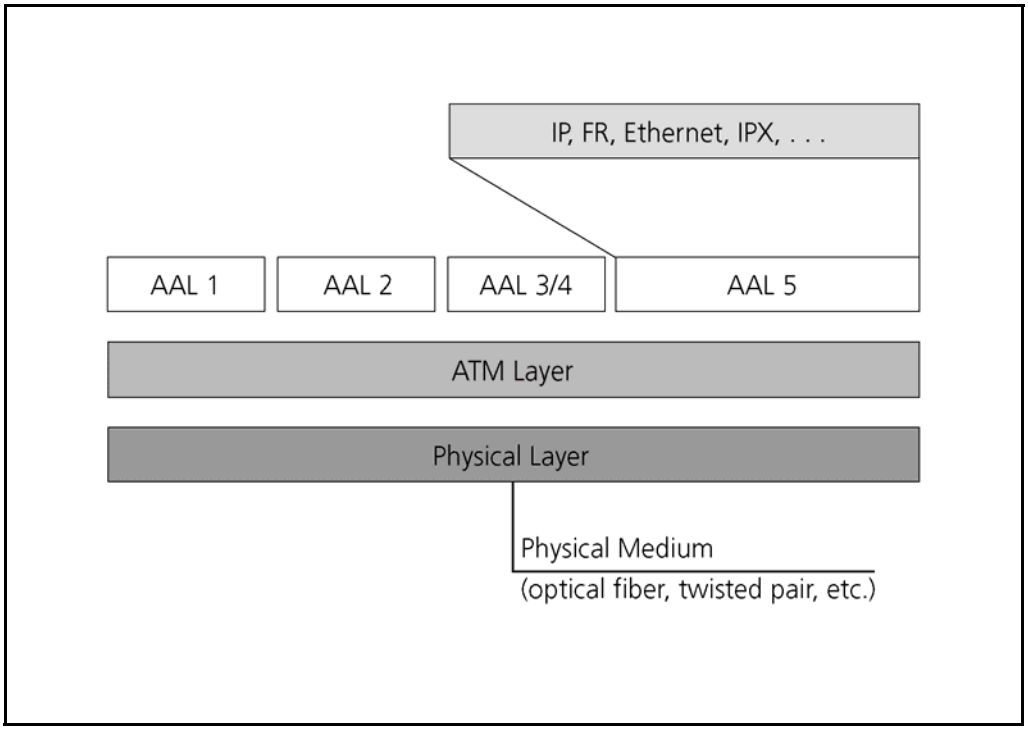
Slide 3.27
Modèle de référence ATM (plan d'usager)

Le plan d'usager du modèle de référence ATM se compose de 4 couches :

- **La couche physique** doit adapter les cellules ATM aux trames de transmission du réseau de transmission choisi (par ex. SDH, ADSL, ATM couche 1).
- **La couche ATM** est responsable de l'acheminement des cellules. Ses principales fonctions sont : le multiplexage / démultiplexage des cellules issues des données d'applications, la création / suppression de l'en-tête de cellule, la translation des identificateurs VPI/VCI de connexion virtuelle.
- **La couche AAL** (ATM Adaptation Layer) adapte les flux d'information à la structure des cellules. La couche AAL réalise des fonctions de bout en bout, c.-à-d. qu'elle n'est pas présente dans les nœuds internes du réseau. Les fonctions de cette couche dépendent des caractéristiques des applications.
- **Les couches supérieures** représentent les fonctions requises par les applications de l'utilisateur (par exemple le protocole IP).

Remarque : le modèle de référence complet comprend, en plus du plan d'usager, un plan de commande (pour la signalisation) et un plan de gestion non traités dans la description et la figure ci-dessus.

3.3.4 AAL : Couche d'adaptation à ATM

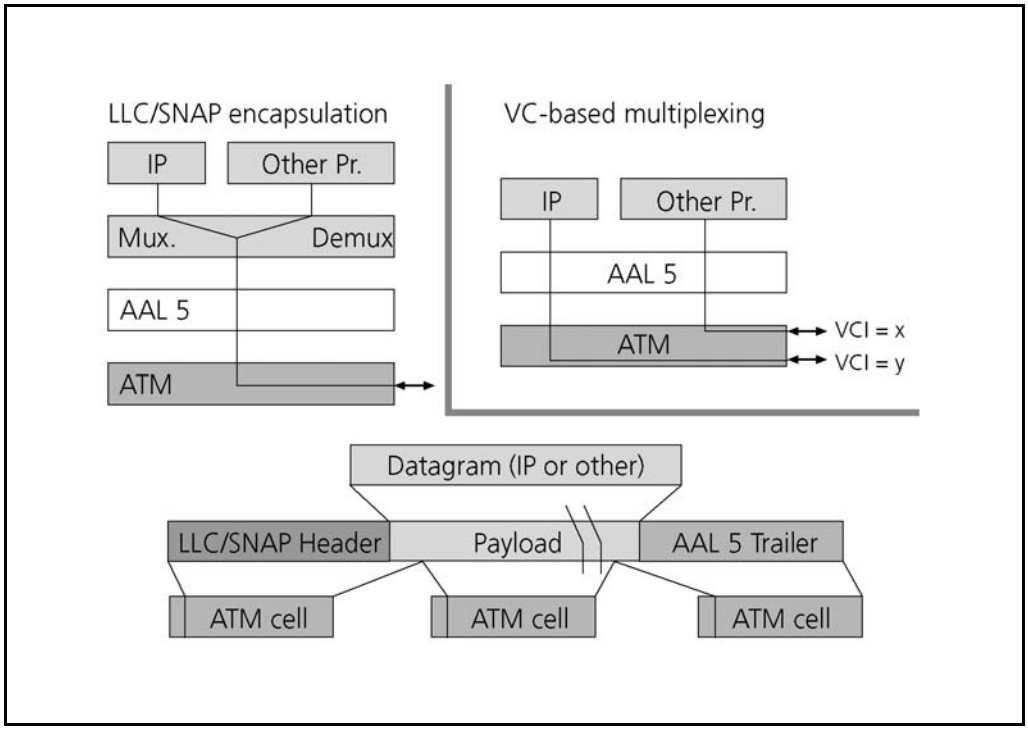


Slide 3.28
AAL : Couche d'adaptation à ATM

Le rôle de la couche AAL est de mettre en œuvre des mécanismes pour adapter les services offerts par la couche ATM aux besoins de l'application transportée. De plus, elle segmente les flux d'information en provenance des applications en unités de données de 48 octets et réassemble les unités de données en flux d'information chez le destinataire. Afin de tenir compte des différentes classes d'applications possibles, 4 différentes AAL ont été définies :

- **AAL 1** est utilisée pour adapter les données d'applications de type voix ou émulation de circuit. AAL 1
- **AAl 2** est utilisée pour adapter les données d'applications de type vidéo ou voix avec compression. AAL 2
- **AAL 3/4** a été prévue pour le transport sécurisé des données. Elle n'est plus beaucoup utilisée. AAL 3/4
- **AAL 5** est l'AAL la plus utilisée. Elle est mise en oeuvre pour le transport de données en général et plus particulièrement de données internet (IP). AAL 5

3.3.5 IP over ATM : Encapsulation

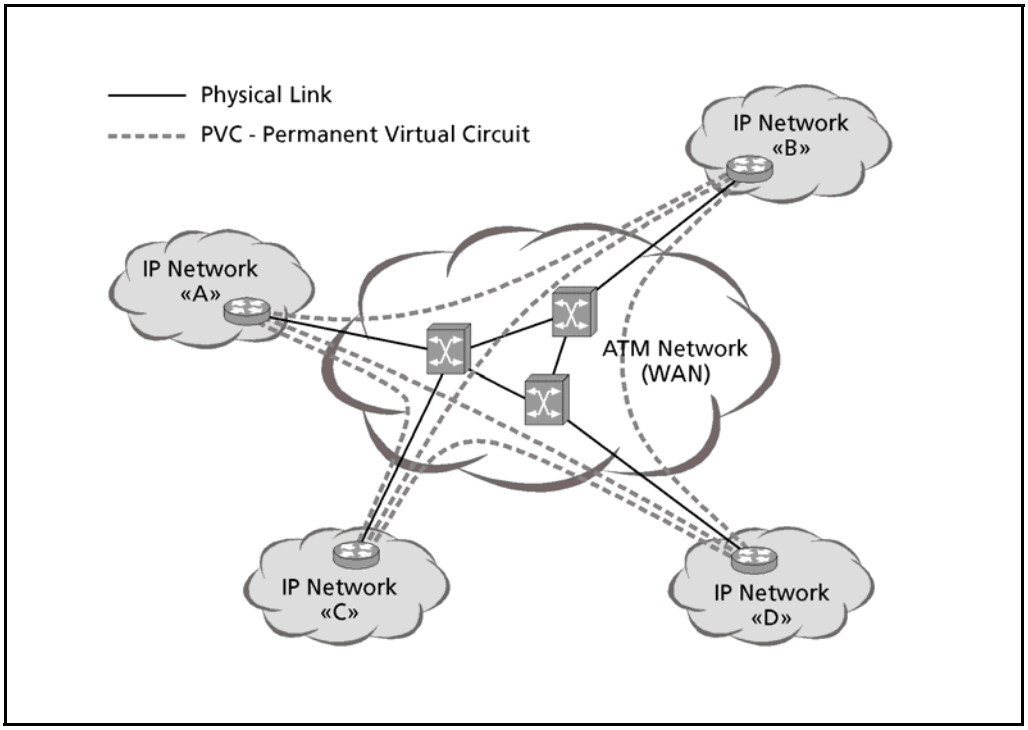


Slide 3.29
IP over ATM : Eencap-sulation

La [RFC 1483] définit 2 méthodes d'encapsulation de datagrammes (unités de données de protocole de couche 3) dans des cellules ATM en utilisant l'AAL 5. La première méthode permet le multiplexage de plusieurs protocoles sur un seul canal virtuel ATM alors que la deuxième part du principe que chaque protocole est transporté sur un canal virtuel ATM séparé.

1. Cette méthode appelée "**LLC encapsulation**" nécessite l'ajout d'un en-tête **LLC/SNAP** (Logical Link Control / SubNetwork Attachment) aux datagrammes pour permettre l'identification du protocole utilisé. Les 8 octets d'en-tête selon le format IEEE LLC/SNAP débutent par 0xAA-AA-03-00-00-00 suivi par 2 octets indiquant le protocole (0x800 pour le protocole IP).
2. Cette méthode appelée "**VC Based Multiplexing**" utilise les connexions ATM pour différencier les protocoles. Par exemple un canal virtuel ATM est utilisé pour transporter les datagrammes IP uniquement et un autre canal virtuel pour les datagrammes IPX. Dans cette méthode, les datagrammes sont passés directement à la couche AAL 5.

3.3.6 IP over ATM : Exemple

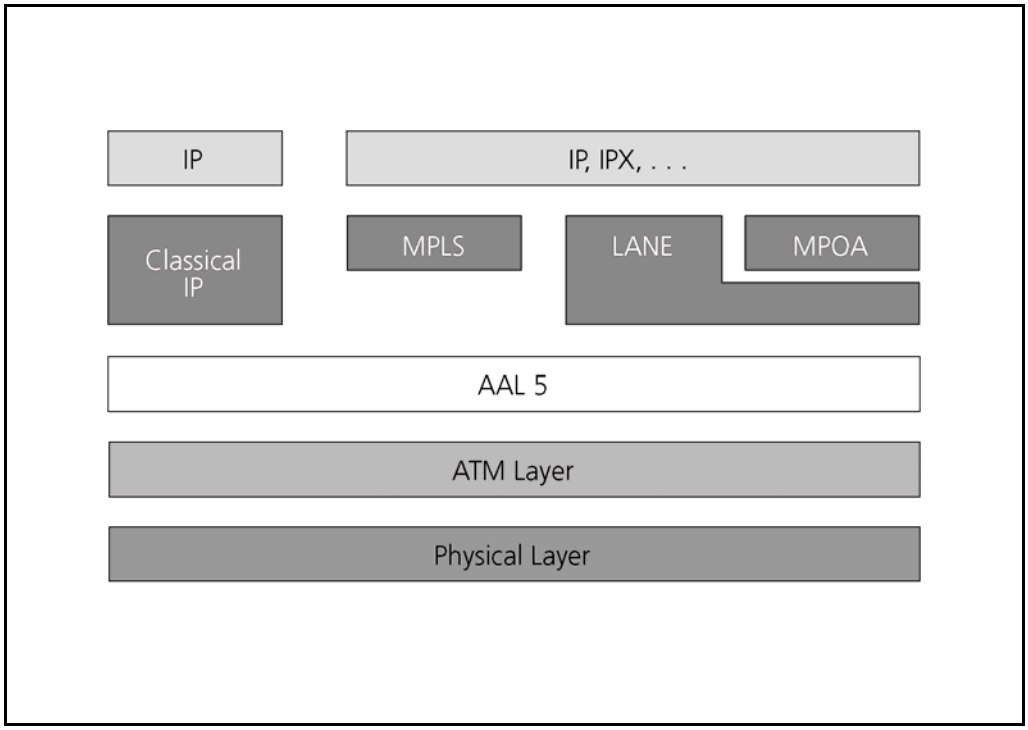


Slide 3.30
IP over ATM : Exemple

La figure ci-dessus montre une façon simple d'interconnecter des réseaux IP entre eux au travers d'un réseau ATM. Les routeurs disposent d'une interface ATM (côté WAN). Un maillage complet de circuits virtuels permanents ATM (PVC : Permanent Virtual Circuit) interconnecte tous les routeurs. Le réseau ATM fournit une connectivité à haut débit alors que les routeurs fournissent l'intelligence pour acheminer les datagrammes IP.

Cette façon d'interconnecter des routeurs présente toutefois un problème de capacité d'extension (scalability). En effet avec un nombre n de routeurs, le nombre de PVCs à gérer est de n(n-1)/2. De même chaque routeur est directement le voisin de n-1 routeurs (les switchs ATM sont invisibles en couche 3).

3.3.7 IP over ATM : Diverses solutions



Slide 3.31
IP over ATM : Solutions

Les principaux problèmes posés par l'intégration des applications et réseaux informatiques existants (c.-à-d. principalement IP) sur un réseau ATM sont dus aux différentes structures d'adressage (IP et ATM) ainsi que des protocoles de routages eux aussi différents. La figure ci-dessus montre les principales solutions proposées par les différents acteurs du marché pour résoudre ces problèmes:

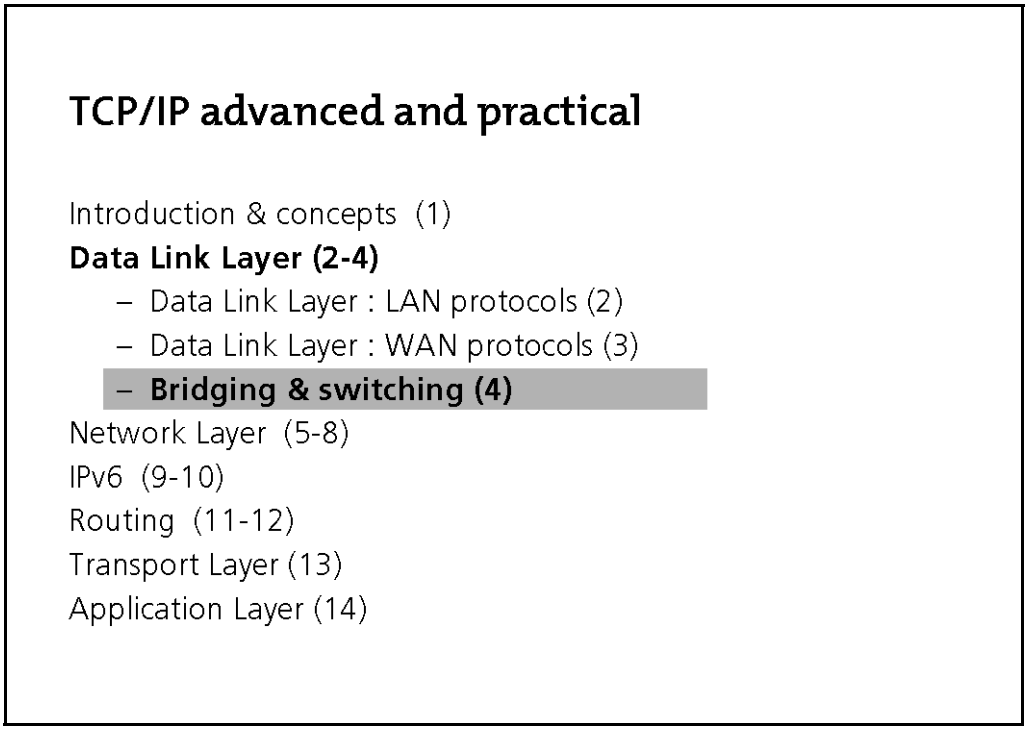
Classical IP : cette solution a été élaborée par l'IETF et est définie dans la [RFC 2225]. Le réseau ATM se comporte comme un ou plusieurs sous-réseau IP (LIS : Logical IP Subnet). La résolution d'adresses IP en adresses ATM est réalisée à l'aide d'un serveur ATMARP (ATM Address Resolution Server) par LIS.

LANE (Lane Emulation) a été spécifiée par l'ATM Forum. LANE permet l'interfonctionnement au niveau 2 de segments LAN classiques au travers d'un réseau ATM. Une résolution des adresses MAC en adresses IP est nécessaire.

MPOA (Multi Protocol Over ATM) a été spécifié par l'ATM Forum. MPOA permet de router des protocoles de couche 3 (par ex. IP) sur un réseau ATM. Dans la pratique MPOA n'a pas été beaucoup mis en oeuvre.

MPLS (Multiprotocol Label Switching) est un nouveau standard de l'IETF. MPLS utilise des références (les labels) pour acheminer les datagrammes de couches supérieures. MPLS peut être mis en œuvre sur un réseau ATM (existant). Dans ce cas les champs VPI et VCI de l'en-tête ATM jouent le rôle de références.

4 Bridging / switching



Slide 4.1
Bridging / switching

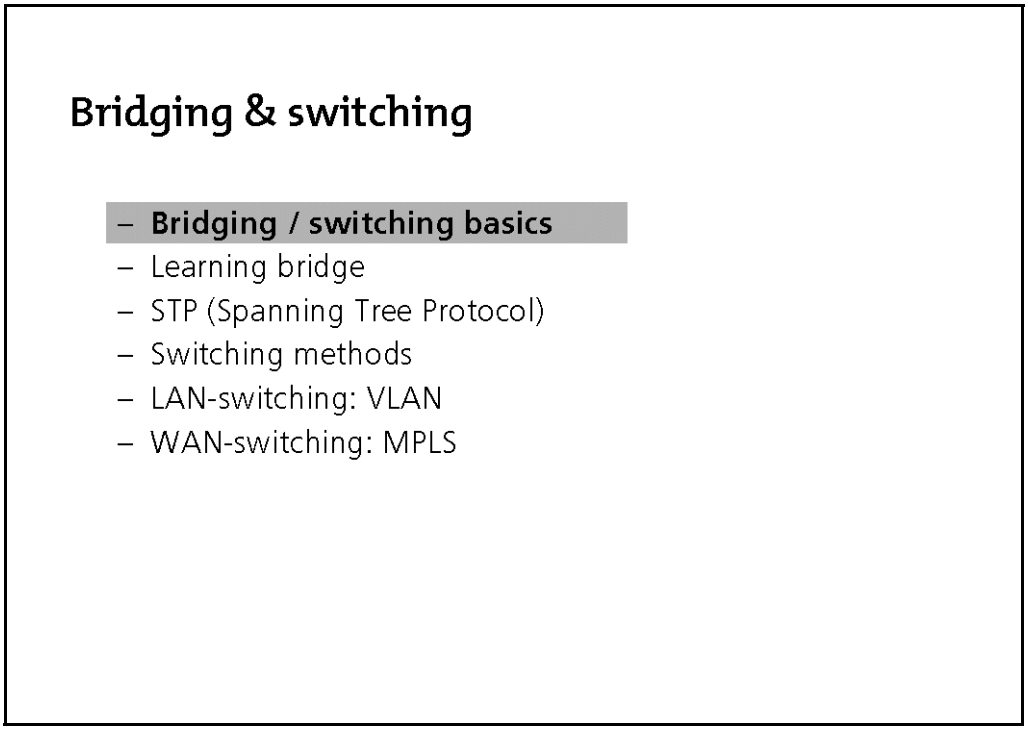
Un réseau LAN bridgé est transparent, il se comporte comme un réseau LAN classique. Aucun changement n'intervient pour les couches supérieures.

Avec l'utilisation de l'auto-apprentissage (Learning Bridge) le bridging est une technique qui demande un minimum de configuration.

Objectifs

A l'issue de ce chapitre, les participants expliquent le fonctionnement du bridging, citent le protocole mis en oeuvre dans un réseau bridgé redondant et reconnaissent ses modes de fonctionnement. En outre, ils peuvent également décrire les principes de fonctionnement des VLANs et de MPLS.

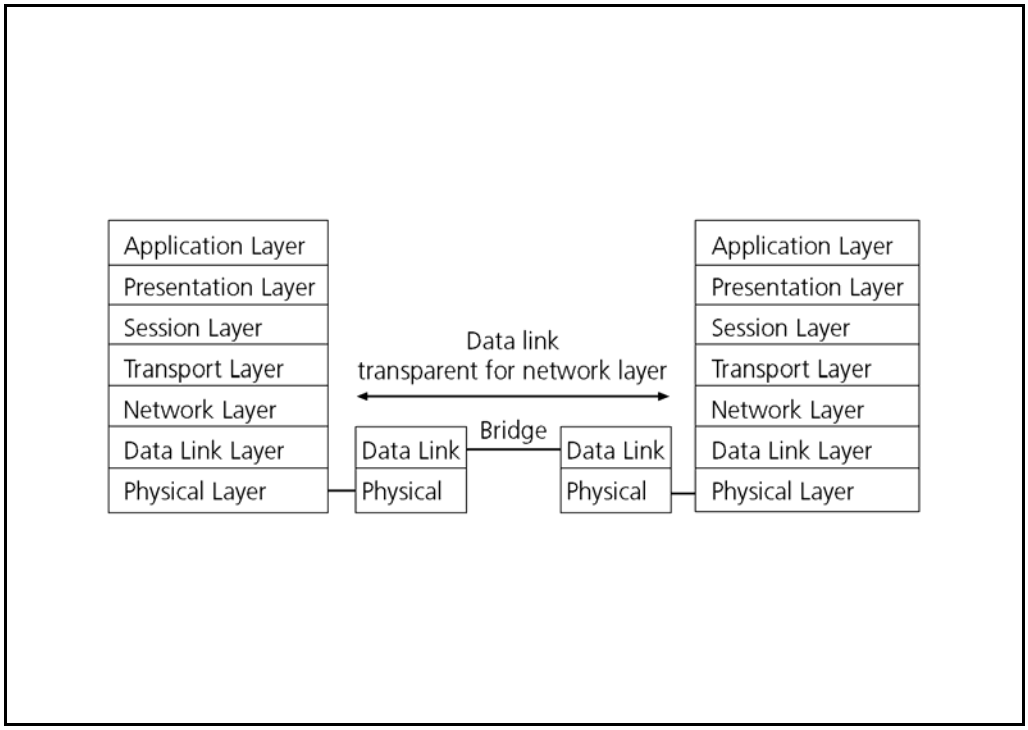
4.1 Notions de base de bridging / switching



Slide 4.2
Notions de base de bridging / switching

Dans cette partie, nous allons aborder la tâche principale d'un bridge ou d'un switch. Cette partie théorique décrit le fonctionnement d'un switch de type Ethernet.

4.1.1 Bridging architecture



Slide 4.3
Bridging architecture

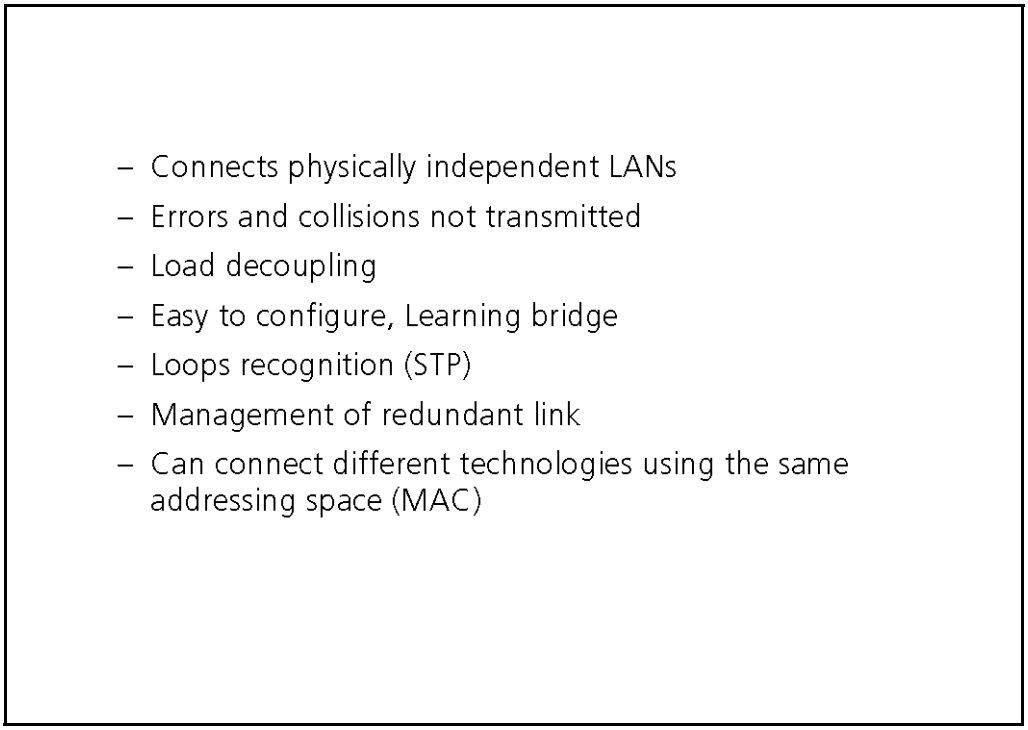
Bridges

Les bridges servent à construire des réseaux locaux performants. Ils s'appuient sur l'adressage MAC pour prendre les décisions d'acheminement des trames. Cela permet un découplement de la charge sur différents segments du LAN.

Adresse MAC

Les bridges peuvent également filtrer des protocoles, des adresses ou des trames trop longues.

4.1.2 Pourquoi utiliser un bridge ?



Slide 4.4
Pourquoi utiliser un bridge?

On utilise des bridges pour lier des LAN's physiquement indépendants. Les erreurs et les collisions ne sont pas transmises.

La fonction d'acheminement des trames permet de découpler la charge sur les différents segments LAN.

découplement de la charge

Associé à une procédure automatique d'apprentissage (Learning Bridge), les bridges sont très simples à configurer. Un mécanisme est prévu pour gérer les boucles. Il s'agit du protocole STP (Spanning Tree Protocol) qui désactive certains ports de façon à interrompre les boucles.

boucles, Spanning Tree

Différentes technologies de méthode d'accès utilisant l'espace d'adressage MAC peuvent être interconnectées.

4.1.3 Bridging contre switching

Bridging
- Forwarding process based on software algorithm
- Bridge stores incoming frames, than takes the forwarding decision

Switching
- Forwarding decision taken by hardware mechanism
- High-speed forwarding capabilities
- Several switching methods
  - Store and forward
  - Cut-through

Slide 4.5
Bridging contre switching

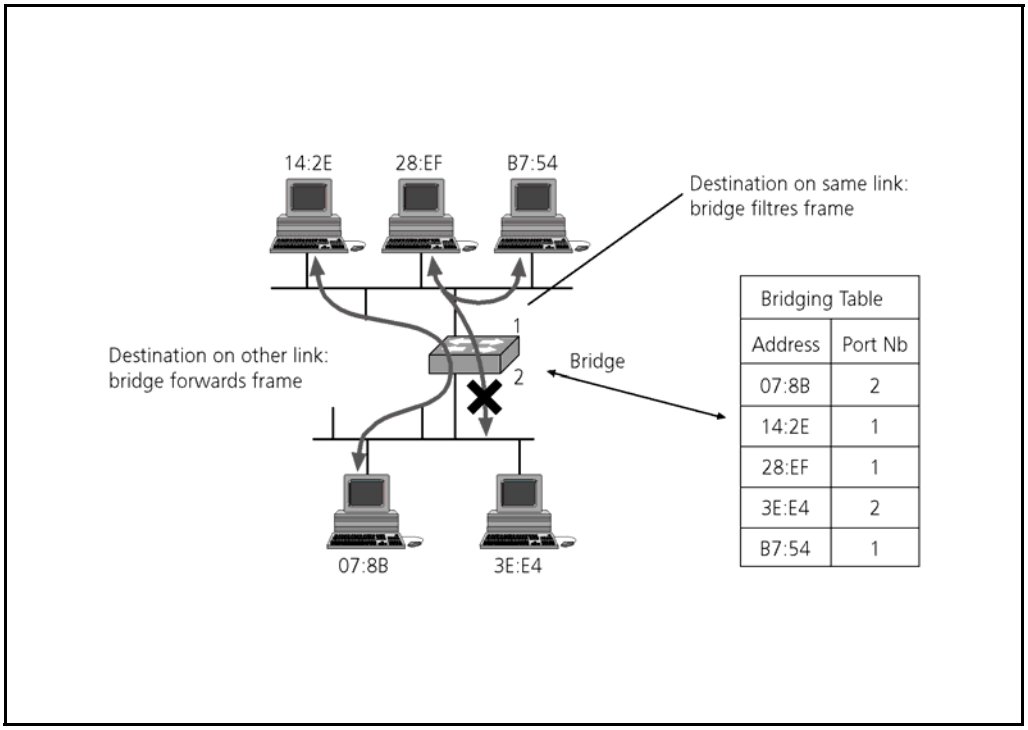
Le bridging et le switching ne sont pas différent sur le principe de fonctionnement. Il s'agit en fait d'une différence de technologie de commutation.

Les bridges traditionnels utilisent un logiciel qui analyse le contenu des trames et prends les décisions d'acheminement. Cette méthode de travail nécessite la mémorisation complète de la trame, son transfert dans la mémoire de travail du bridge, son traitement complet avant de transférer finalement la trame dans les buffers de sortie. Les temps nécessaire à ce traitement crée un délai de retransmission que les réseaux LAN actuels n'osent plus proposer.

Les switches, plus récents, intègrent les capacités de commutation directement dans le silicium. Toutes les manipulations sont faites directement par des Circuits Intégrés. Le délai de traitement est donc beaucoup plus court. Il existe en outre différentes méthodes de switching qui vont encore diminuer ce délai.

Aujourd'hui, tous les LANs "bridgés" sont en fait "switchés". Les procédures et les protocoles ad'hoc sont restés les mêmes, un switch peut donc simplement être considéré comme un bridge multiport récent.

4.1.4 Exemple de bridging

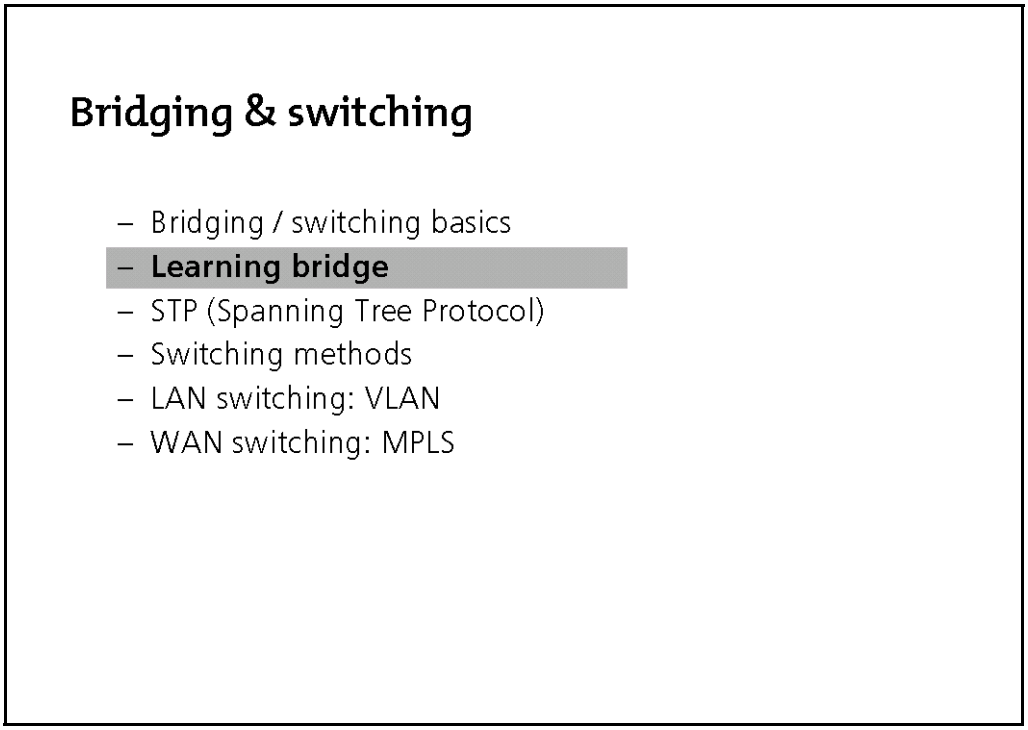


Slide 4.6
Exemple de bridging

La station 14:2E émet une trame à destination de 07:8B. Cette trame est diffusée sur le segment Ethernet supérieur et est reçue simultanément par les 2 autres stations du segment et par le bridge. Si les premières ne sont pas concernées par cette trame, le bridge, lui, constate que l'adresse de destination se trouve sur un autre segment. Il achemine cette trame sur le segment sur lequel se trouve la station de destination.

Une trame émise en direction d'une station faisant partie du même segment arrivera simultanément au bridge et à la destination. Le bridge constatant que la trame est présente sur le segment sur lequel se trouve la destination, ne l'achemine pas sur d'autres segments.

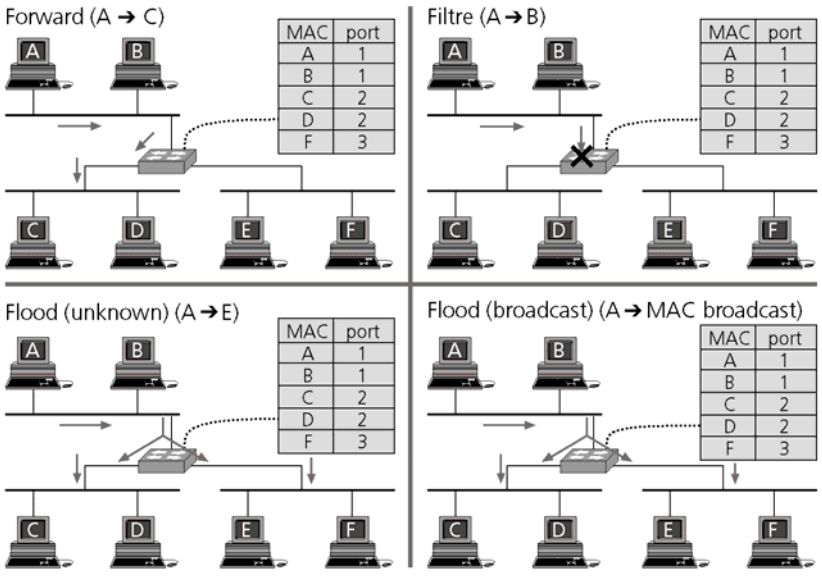
4.2 Learning Bridge



Slide 4.7
Learning Bridge

Cette section va nous permettre d'aborder le fonctionnement du bridge. Toutes les fonctions qui sont décrites s'appliquent aussi aux switchs récents.

4.2.1 Fonctions de base du bridge



Slide 4.8
Fonctions de base du bridge

Un bridge simple connaît trois fonctions basées sur l'étude de sa table de retransmission.

Forwarding

Lorsqu'un bridge reçoit une trame sur un de ses ports, il regarde quelle est son adresse de destination (MAC) et retransmet la trame sur le port de sortie concerné. Le bridge conduit cette trame, on parle de "forwarding".

Filtering

Si le port de sortie est équivalent au port d'entrée, cela implique que la trame a déjà circulé sur le bon segment Ethernet. Le bridge ne doit pas créer un doublon de cette trame en la renvoyant à nouveau. Dans ce cas le bridge filtre la trame.

Cette fonction de "filtering" peut aussi se produire si une trame est spécifiquement interdite sur un segment, par configuration par exemple.

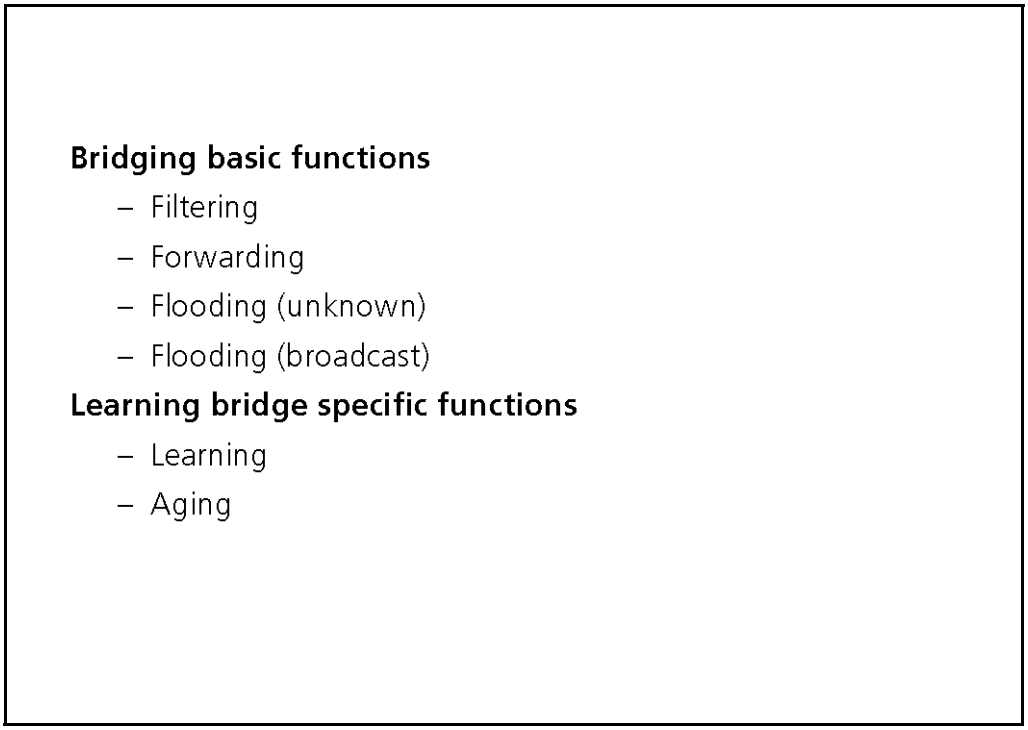
Flooding (unknown)

Dans le cas où le bridge ne connaîtrait pas la destination, il va copier cette trame sur tous les ports de sortie, à l'exception du port sur lequel la trame à été reçue. Le bridge garantit ainsi la connectivité entre des stations dont l'adresse est encore inconnue.

Flooding (broadcast)

Cette fonction de "flooding" sera également utilisée dans les cas des trames de diffusion (broadcast MAC).

4.2.2 Fonctions du Learning Bridge



Slide 4.9
Learning Bridge

Afin d'exécuter correctement les fonctions vue précédemment, le bridge se réfère à une table de retransmission (forwarding table). Cette table peut être configurée manuellement, mais elle nécessite une entrée par machine connectée au réseau.

Learning Bridge

Afin de simplifier la mise en oeuvre du bridge, une fonction d'auto-apprentissage, appelée "Learning Bridge" a été développée.

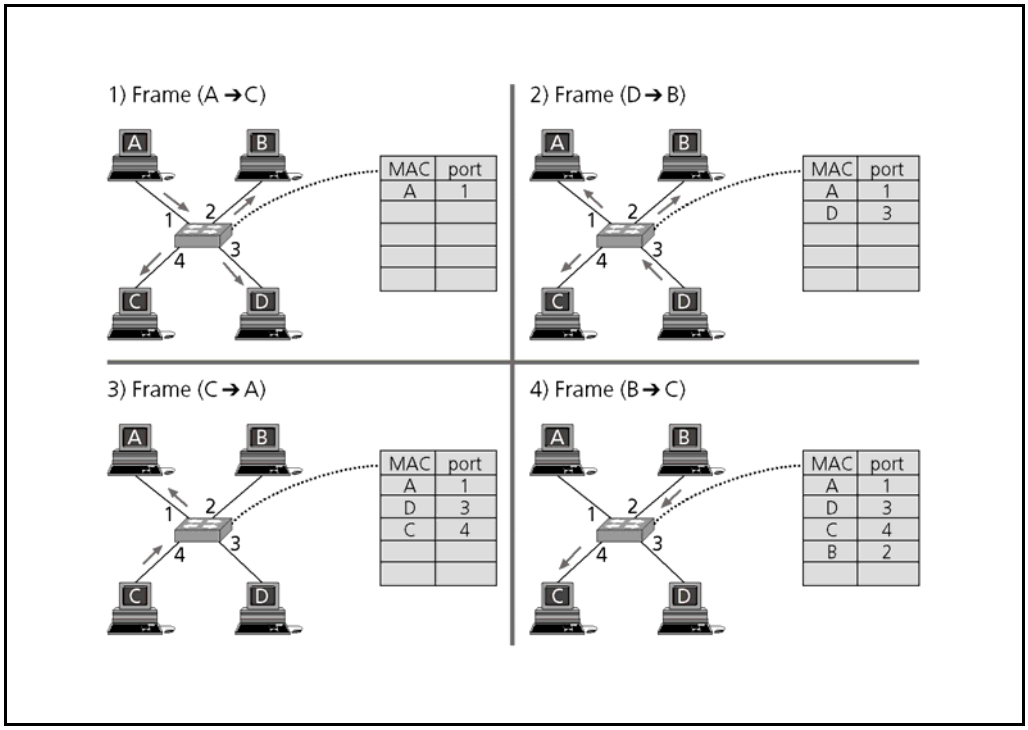
Learning

Chaque machine dans le réseau va copier sa propre adresse MAC dans le champ ad'hoc de l'en-tête de trame Ethernet. Le bridge, lorsqu'il reçoit cette trame, va non seulement lire l'adresse de destination, mais également l'adresse source. Cette adresse sera associée au port sur lequel la trame a été reçue dans la table de retransmission. Il s'agit ici de la fonction d'apprentissage "learning".

Aging

On souhaite toutefois que cette table de retransmission ne contienne que les informations concernant les stations actuellement actives dans le réseau. Cette manière de faire garanti que la mémoire du bridge ne soit pas saturée et, de là, permet au bridge d'offrir des performances maximales. On va donc autoriser le bridge à "oublier" une adresse qui ne génère plus aucun trafic. Il s'agit d'un processus de vielliessement appellé "aging".

4.2.3 Learning Bridge au démarrage



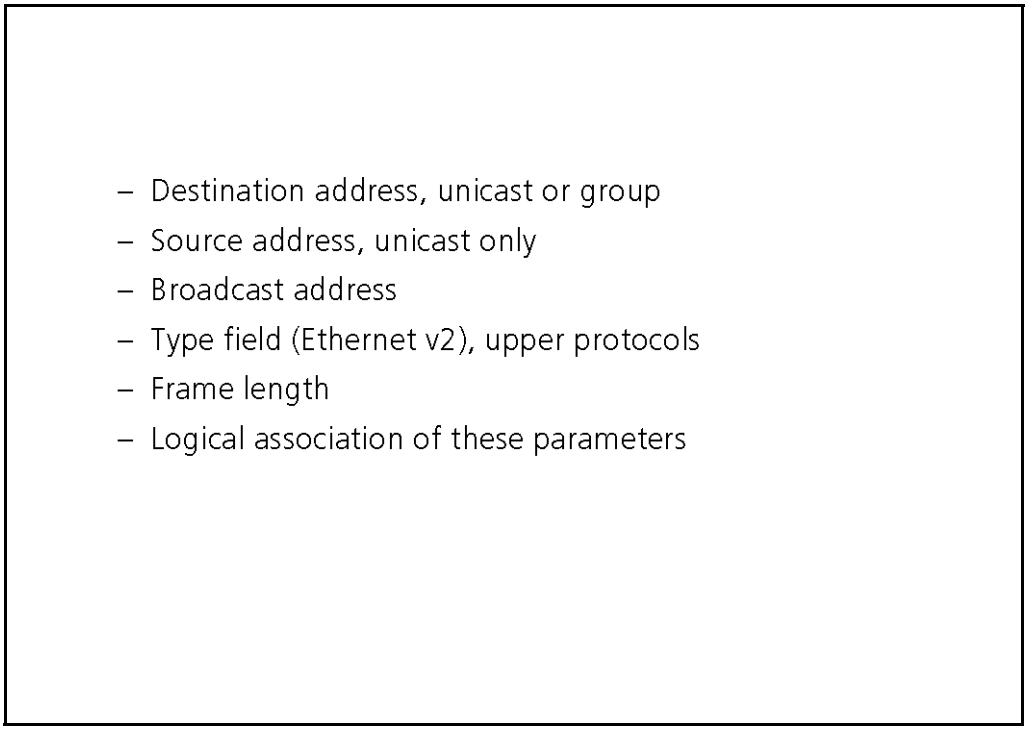
Slide 4.10
Learning bridge au démarrage

Dans cet exemple, on illustre le fonctionnement d'un switch au démarrage. Ses connaissances, nulles au départ, vont progressivement augmenter en fonction du trafic.

Dans un premier temps, ce switch va plutôt faire le travail du répéteur, en diffusant partout les trames. Après quelques échanges de trames, les connaissances acquises vont lui permettre de se mettre à son travail de switching.

Cette phase de démarrage est l'inconvénient assez mineur de cet équipement qui ne nécessite pas de configuration particulière.

4.2.4 Possibilité de filtrage



Slide 4.11
Possibilité de filtrage

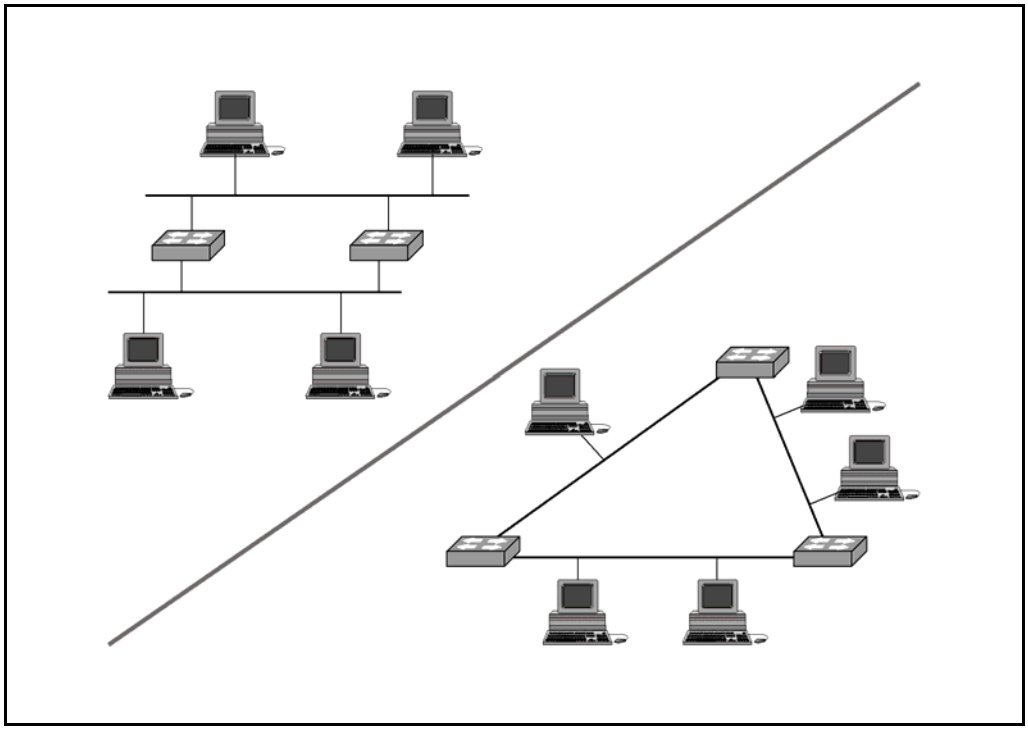
Filtre

Un bridge peut filtrer également des trames selon des critères spécifiques.

- Il peut bloquer toutes les trames en provenance ou à destination d'une adresse particulière.
- Il peut acheminer ou bloquer des adresses de diffusion.
- Il peut empêcher certains protocoles de circuler sur un segment, en analysant le champ Type de la trame Ethernet v2.
- Il peut bloquer des trames trop longues.

On peut aussi imaginer d'autres filtres se reportant aux champs de la trame Ethernet. N'importe quelle association logique des filtres précités est envisageable.

4.2.5 Réseaux redondants bridgés

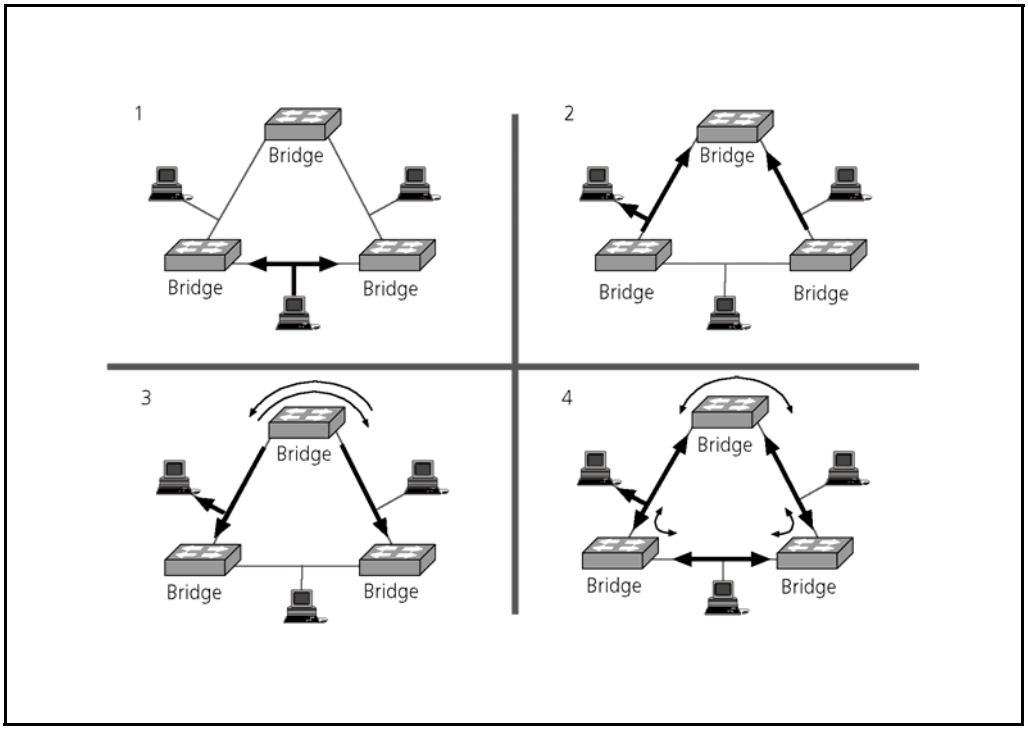


Slide 4.12
Réseaux redondants bridgés

Tout élément d'un réseau, actif ou passif, est une source de panne potentielle. On va donc essayer, en vue d'augmenter la disponibilité du réseau, de créer des structures bridgées redondantes.

Le problème des structures redondantes, c'est qu'elles créent des boucles dans le réseau. Nous allons tout de suite identifier les risques qui y sont liés, ainsi que les solutions pour y remédier.

4.2.6 Comportement des boucles



Slide 4.13
Comportement des boucles

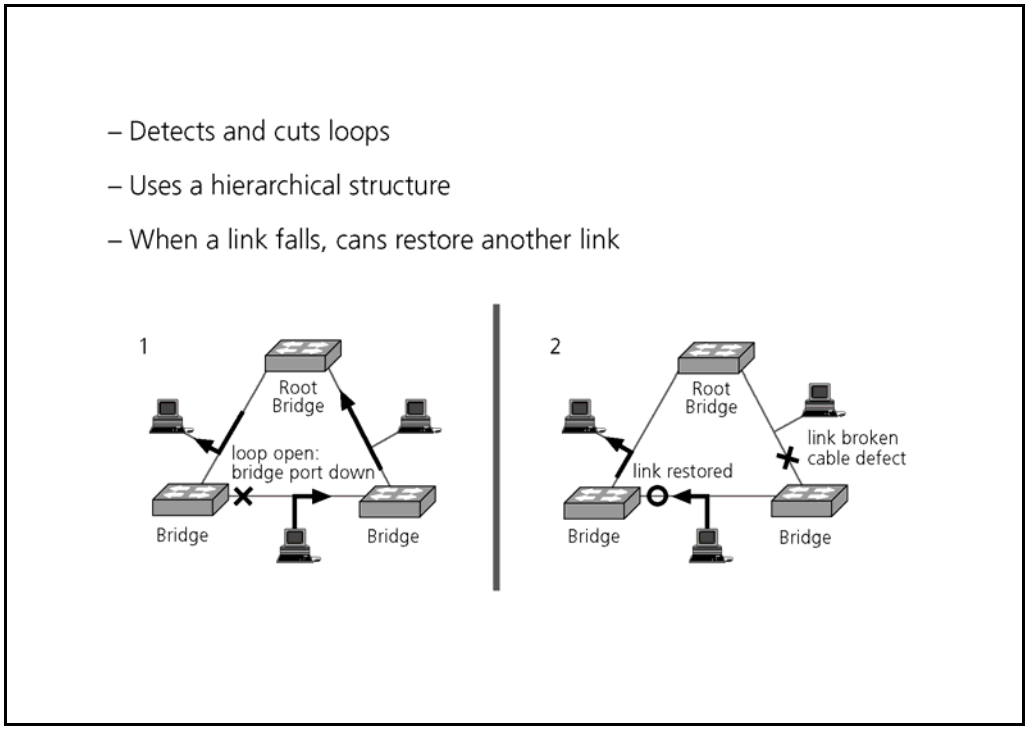
Boucle

Dans un réseau bridgé avec une topologie en boucle, chaque trame émise va être dédoublée et va tourner indéfiniment dans le réseau.

Elle commence par être diffusée sur le 1er segment, où 2 bridges vont la transmettre plus loin (dédoublement). Ensuite, dans notre exemple, les deux trames vont "remonter", chacune sur leur segment en direction du troisième bridge.

Celui-ci va détecter la présence d'une source sur un port, puis de la même source sur l'autre port. Les 2 trames identiques vont circuler indéfiniment dans le réseau en provoquant une charge importante du réseau.

4.2.7 Spanning Tree



Slide 4.14
Spanning Tree

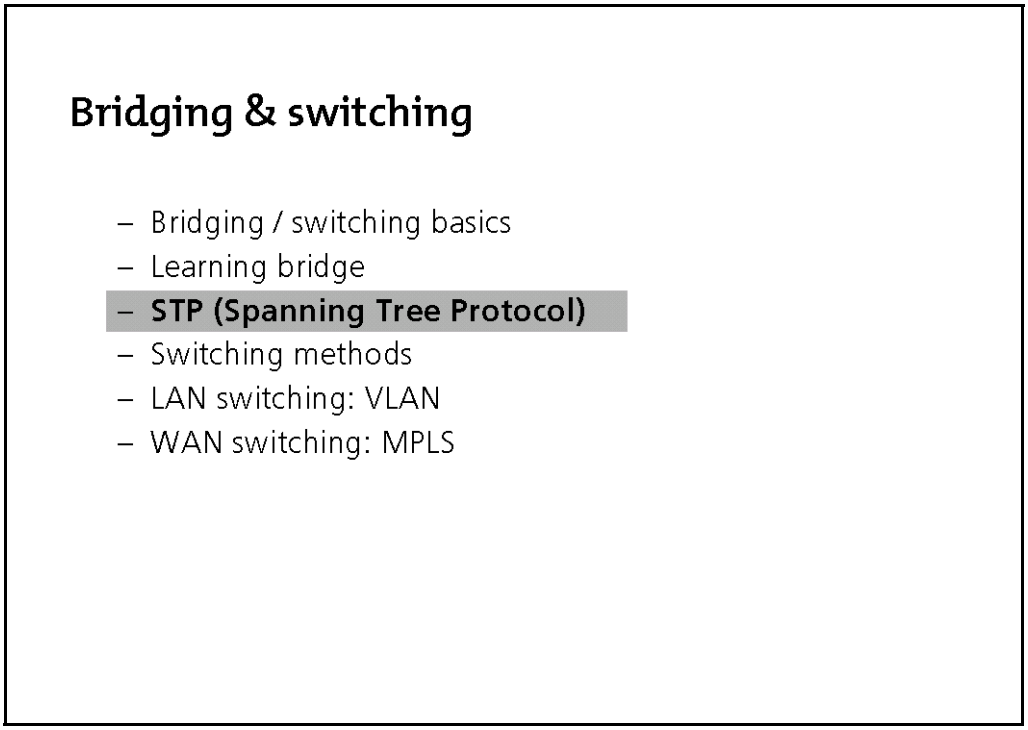
Spanning Tree, Root Bridge

Le Spanning Tree est un protocole qui, associé au Learning Bridge, permet de construire des réseaux bridgé redondants.

Une procédure d'élection d'un "Root Bridge", basée sur l'adresse MAC et sur un paramètre de priorité, est mise en œuvre. Le Root Bridge ne désactive pas de port. Après une série d'échange, chaque bridge a élu un "Root Port" et est conscient de la topologie du réseau. Sur la base d'une décision locale, un des bridges va désactiver un port coupant ainsi la boucle. Le port désactivé n'est jamais le Root Port.

Un trafic Spanning-Tree génère un trafic permanent de surveillance de l'état du réseau. En cas de coupure d'un lien (câble défectueux, par ex.), les bridges rétabliront les liaisons. La partie de la boucle auparavant bloquée par Spanning Tree est utilisée comme de voie de secours.

4.3 STP (Spanning Tree Protocol)

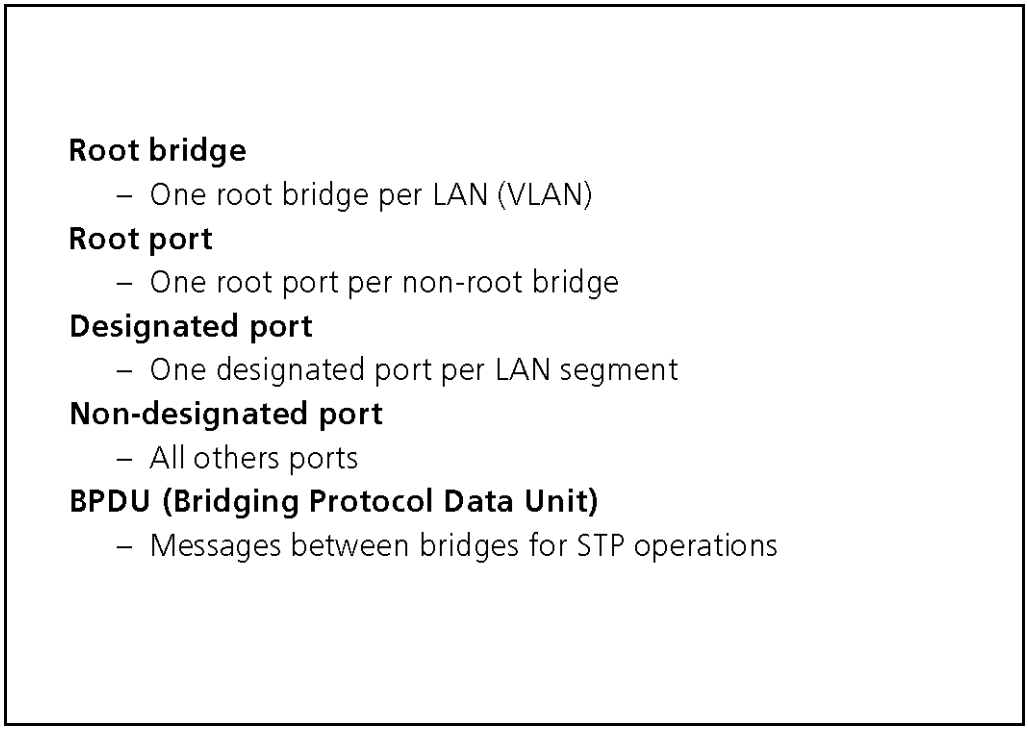


Slide 4.15
STP (Spanning Tree Protocol)

Nous avons vu qu'il suffit de bloquer un port d'un switch pour ouvrir une boucle. Cette section va présenter en détail le protocole qui permet de déterminer quel port sera bloqué et pourquoi.

Nous verrons aussi quels sont les délais de mise en oeuvre de cette solution.

4.3.1 Composants et opérations



Slide 4.16 Composants et Opérations

Avant d'éclaircir la procédure, il convient de placer quelques termes liés à cet environnement du "Spanning Tree".

Root Bridge

Le point central d'un spanning tree est le root bridge. Il s'agit d'un bridge, désigné par l'application de la norme spanning tree, autour duquel toute la structure arborescente (tree = arbre) va être créée (root = racine).

Root port

Chaque bridge standard (non-root bridge) va "mesurer" les coûts des différents chemins le reliant au root bridge. Le port permettant l'accès au chemin le plus avantageux sera élu le root port. Chaque bridge possède un root port, à l'exception du root bridge. Un root port ne sera jamais bloqué.

Designated port

Chaque segment LAN devra posséder un port désigné et un seul. Un root port n'est pas un port désigné. Lorsque plusieurs ports sont connectés sur un segment LAN, c'est le port dont le coût vers le root bridge est le plus avantageux qui sera désigné.

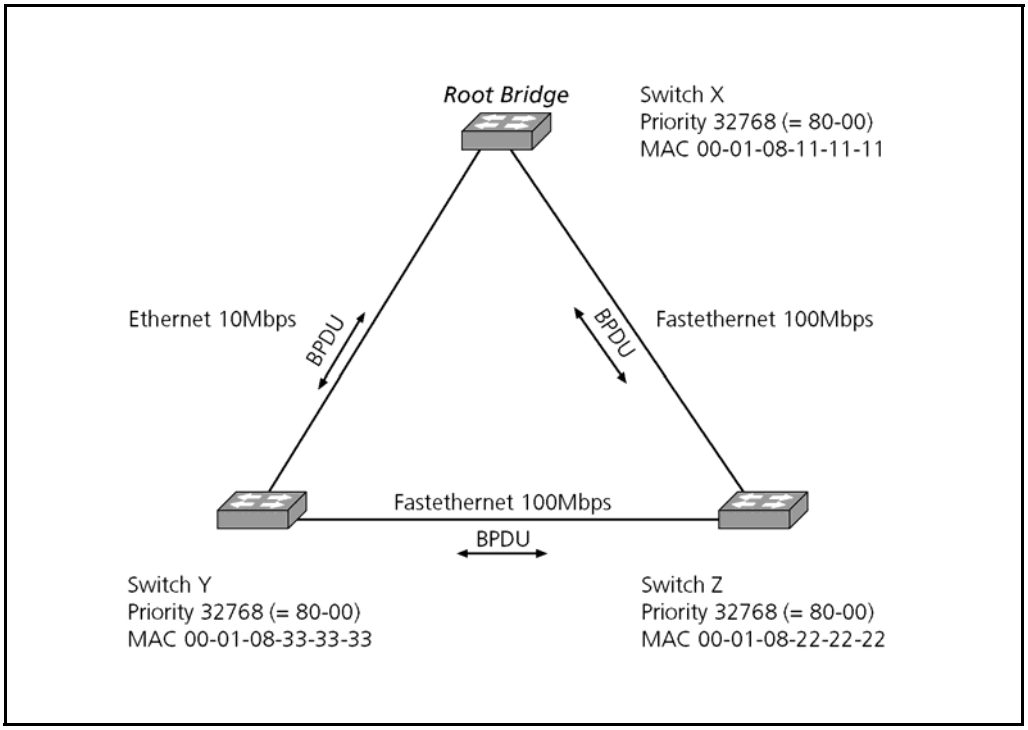
non-designated port

Tous les ports qui ne sont pas élu root port ou designated port sont déclarés non-designated port. En principe c'est les ports bloqués.

BPDU

Une autre notion importante est celle des BPDUs. Une BPDU (Bridge Protocol Data Unit) est en fait le message que s'échangent les bridges. C'est avec ses informations que les bridges procédent aux "élections".

4.3.2 Election du Root Bridge



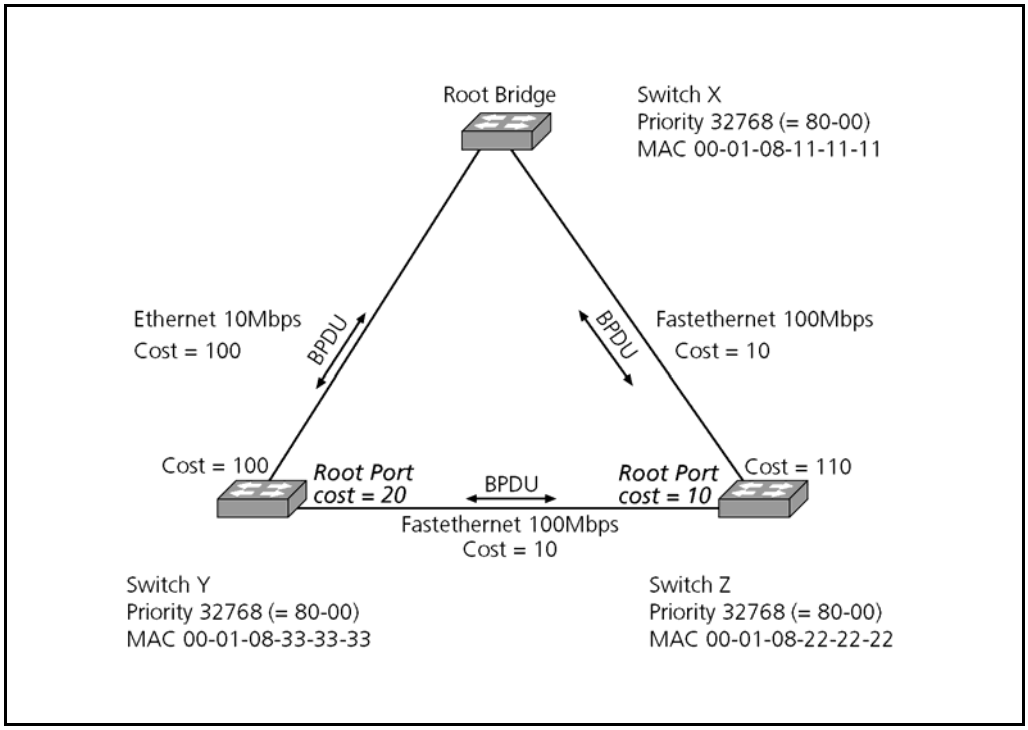
Slide 4.17
Root Bridge

Le root bridge est le bridge qui possède l'identificateur (Bridge ID) le plus petit. Le bridge ID, d'une longueur de 8 octets, est d'abord composé d' un paramètre de priorité codé sur 2 octets. Ce paramètre est généralement fixé à la valeur par défaut 32768 (0x8000). Les 6 octets suivants, sont composés de l'adresse MAC du bridge (généralement l'adresse du premier port du bridge).

Dans notre exemple, les paramètres de priorité ont été laissé à la valeur par défaut, c'est donc uniquement sur leurs adresses MAC que les bridges feront la différence.

Le bridge X sera élu root bridge, il possède l'adresse MAC la plus basse.

4.3.3 Election des Root Ports



Slide 4.18
Root Ports

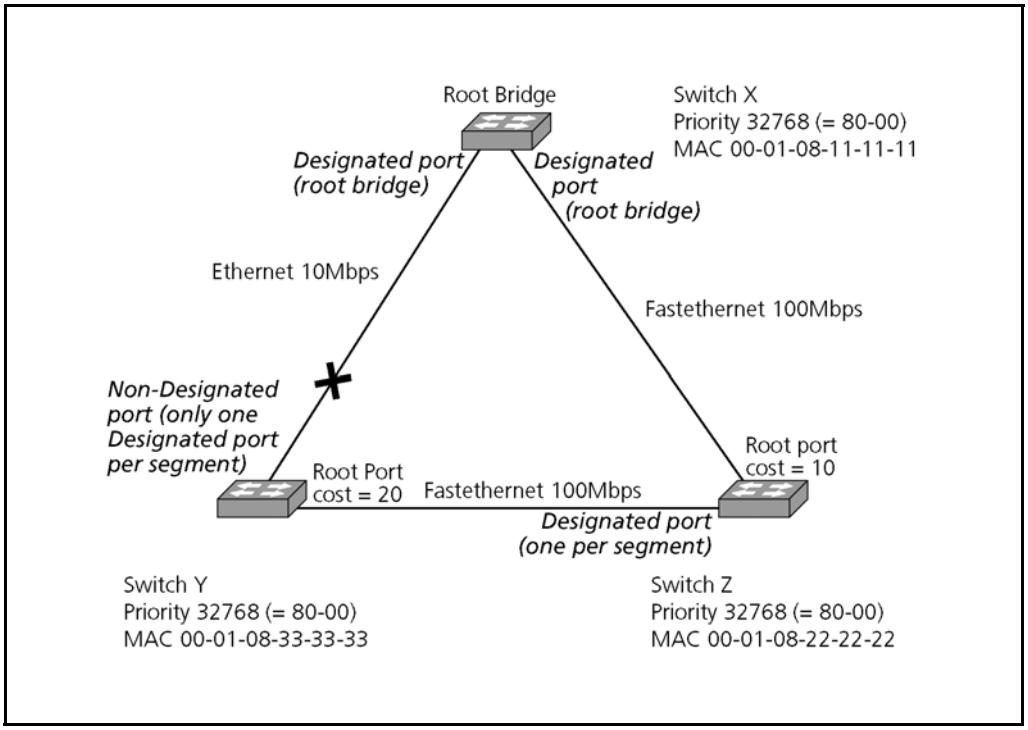
Chacun des bridges standards vont maintenant choisir leur root port. Ce port permet à chacun des bridges d'atteindre le root bridge au travers du chemin le plus avantageux.

Les coûts des liaisons sont codées sur la vitesse, les liens les plus rapides "coûtant" moins chers que les plus lents. Afin de calculer le coût total d'un chemin, il convient d'additionner tous les coûts des segments traversés.

A l'aide de cette règle, on voit que le bridge Z voit depuis l'un de ses ports le root bridge avec un coût de 10, alors que l'autre port lui offre un coût de 110. Dans ce cas de figure, le port offrant le coût de 10 sera élu root port.

La même règle appliquée au bridge Y nous donne un coût de 100 pour la liaison directe, mais un coût de 20 seulement si on traverse le bridge Z. C'est donc cette deuxième option qui est la moins couteuse. Le root port sera donc celui de droite.

4.3.4 Election des Designated Ports



Slide 4.19
Designated Ports

Pour la dernière élection, nous allons départager, au sein des ports restants, lesquels seront designated ports et lesquels seront non-designated ports.

Pour cette "élection" trois règles sont à respecter:

1. Tous les ports du root bridge sont des designated ports.
   Dans notre cas les deux ports du bridge X sont donc designated ports
2. Il y a un designated port par segment.
   Les ports du segment entre les bridges X et Z sont définis, il y a un designated port et un root port.

   Un des ports du segments entre les bridges Y et Z est un root port, l'autre sera donc un designated port

   Un des ports du segment entre les bridges X et Y est déjà un designated port (port du root bridge). L'autre port ne sera donc pas un port désigné.
3. Tous les ports qui ne sont pas désignés sont appelés non-designated port et seront bloqués.
   Dans notre exemple, un seul port est concerné, il s'agit du port en haut du bridge Y.

Dans cet exemple aucun conflit entre port n'est apparu. Quand un choix doit être fait, on désigne généralement le port qui possède le coût de liaison le plus bas vers le root bridge. On peut toutefois aussi jouer sur un paramètre de priorité.

4.3.5 IEEE : Path costs

Link Speed	IEEE Link Cost	
	Old IEEE Specification	Reratified IEEE Spec.
10 Gbps	1	2
1 Gbps	1	4
100 Mbps	10	19
10 Mbps	100	100

Slide 4.20
IEEE : Path costs

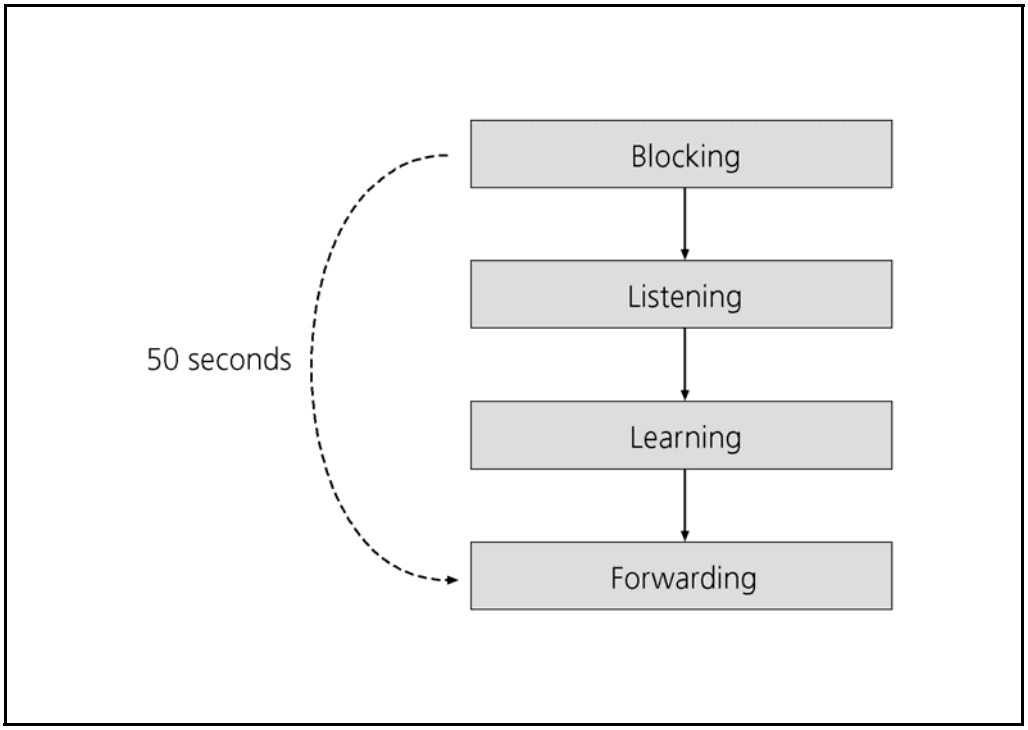
A l'origine, la norme IEEE 802.1d (Spanning Tree Protocol) codait les coûts des liaisons selon ce qui est indiqué dans la colonne centrale du tableau.

Ces codes de vitesses ne permettaient déjà pas de différencier les liens à 100 Mbit/s et ceux à 1 Gbit/s. L'arrivée de débits supérieurs n'aurait pas été gérable. Cette norme a donc été adaptée aux technologies émergantes, les nouvelles valeurs figurant dans la colonne de droite.

Il faudra faire attention, lorsqu'on relie entre eux des switches différents, à ce que leur codage interne des vitesses soient les mêmes. Dans le cas contraire, il faudra jouer sur les paramètres de priorité pour imposer au Spanning Tree des choix cohérents.

Cisco fait encore remarquer à fin 2001 que leurs switches de la série 1900 utilisent encore l'ancien codage, contrairement à tous les autres " Catalyst "...

4.3.6 Etats des ports durant le processus d'élection



Slide 4.21
Etats des ports

Blocking

Au départ du processus de Spanning Tree, tous les ports sont bloqués. De cette manière, les switches qu'on insert dans un réseau ne peuvent pas compromettre le fonctionnement de ce dernier. Le processus de Spanning Tree se déroule ensuite en plusieurs étapes.

Listening

Les ports passent dans un état d'écoute (listening), dans lequel seule les trames BPDU sont traitées.

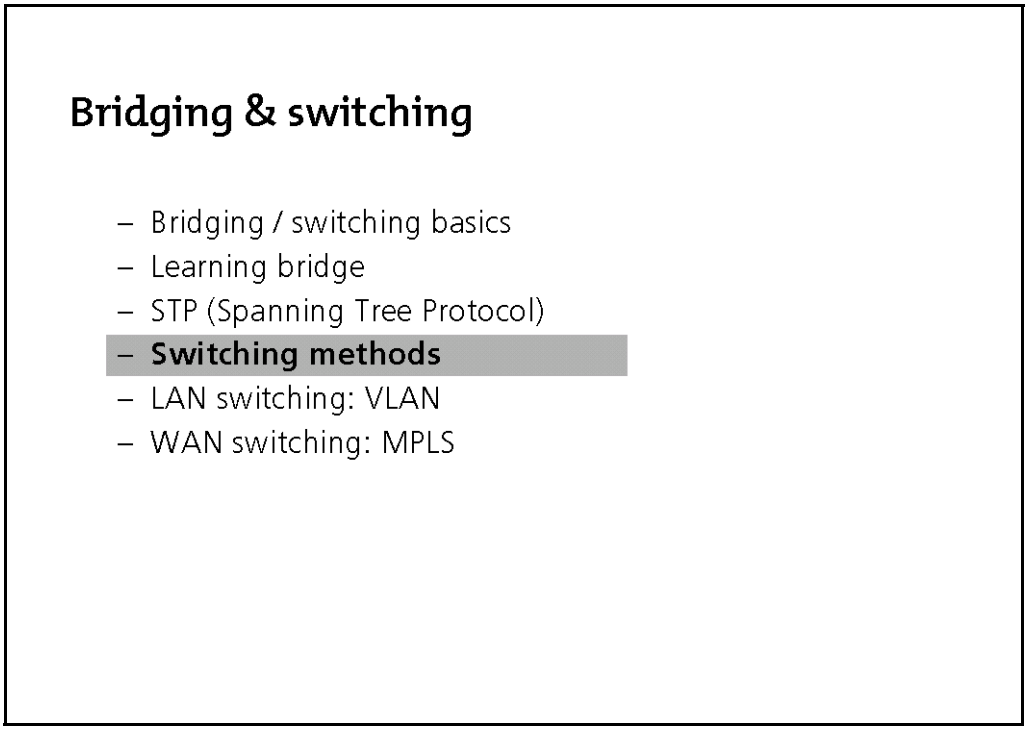
Learning

Dans un deuxième temps, le bridge passe en mode d'apprentissage (learning). Dans ce mode, le bridge reçoit déjà des trames, qu'il utilise pour remplir sa table de retransmission. Les ports étant toujours bloqués dans cette étape, il ne va naturellement pas encore retransmettre des trames.

Forwarding

Finalement, 50 secondes après la mise en route, les ports concernés vont passer en mode forwarding et le bridge commence son véritable travail.

4.4 Méthodes de switching



Slide 4.22
Méthodes de switching

Lorsque les bridges traditionnels, basés sur le software, ont laissé leur place aux switches, on a vu apparaître plusieurs procédés de retransmission des trames. Les pages suivantes proposent l'étude de deux procédés standards, ainsi que d'un procédé modifié par notre fournisseur, Cisco.

4.4.1 Store and Forward

Method

- Incoming frame is stored
- Checksum is calculated
- When outgoing port is free, frame is forwarded according to forwarding table

Pros / cons

- \+ Frames containing errors are discarded
- – Long forwarding delay (not relevant on very high-speed link)

Slide 4.23
Store and Forward

Store and forward

Les bridges traditionnels utilisent le principe du "store and forward" pour acheminer le trafic.

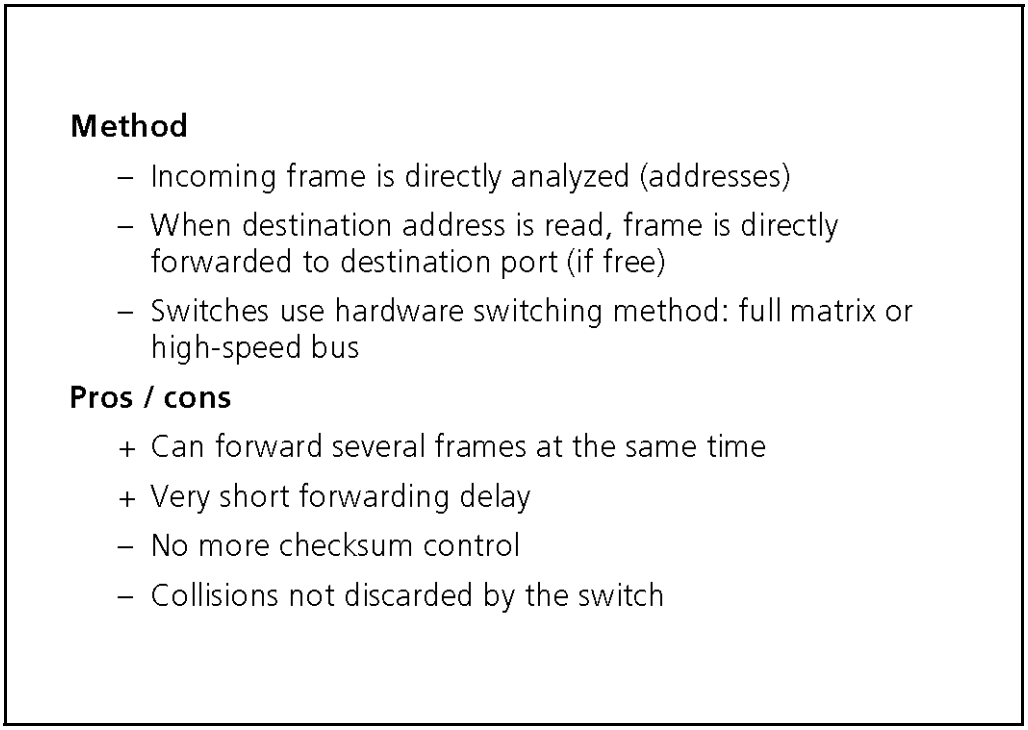
Le principe est de mémoriser entièrement la trame entrante. On peut ensuite contrôler sa validité (checksum). Si la trame contient des erreurs, elle sera détruite.

Sinon, elle est stockée jusqu'à ce que le port de sortie la concernant soit libre.

Les switches peuvent toujours utiliser cette méthode. Grâce au traitement matériel (hardware) de l'information, leur délai de traitement sera quand même meilleur que celui des bridges.

Cette méthode reste relativement longue, vu qu'on attend l'arrivée complète de la trame avant de la retransmettre. L'avantage est de ne retransmettre que les trames valides, grâce à la vérification du checksum.

4.4.2 Cut Through



Slide 4.24
Cut Through

Cut Through

Les switches peuvent mettre en œuvre un procédé appelé "Cut Through". Ils analysent alors le contenu des champs d'adresses au moment de leur arrivée. Si l'adresse de destination est connue et le port concerné libre, la trame y est directement conduite. Sinon une mémorisation intermédiaire est effectuée.

Les switches peuvent conduire simultanément plusieurs trames vers des ports de sortie différents.

Pour cela ils utilisent des méthodes de commutation matérielles (Hardware) : une matrice de commutation complète ou un bus interne à haute vitesse.

Ce principe offre un délai de retransmission très court. Par contre, la trame étant déjà en partie réémise lorsque le checksum se contrôle, on a plus la possibilité de détruire les trames éronnées.

4.4.3 Fragment free (Cisco)

Method

- Same as cut through
- Except that frame is forwarded after the 64th byte only

Pros / cons

- \+ After 64th byte no risk of collision
- – Latency is higher than cut through

Remarks

- – Not necessary with full duplex switched links

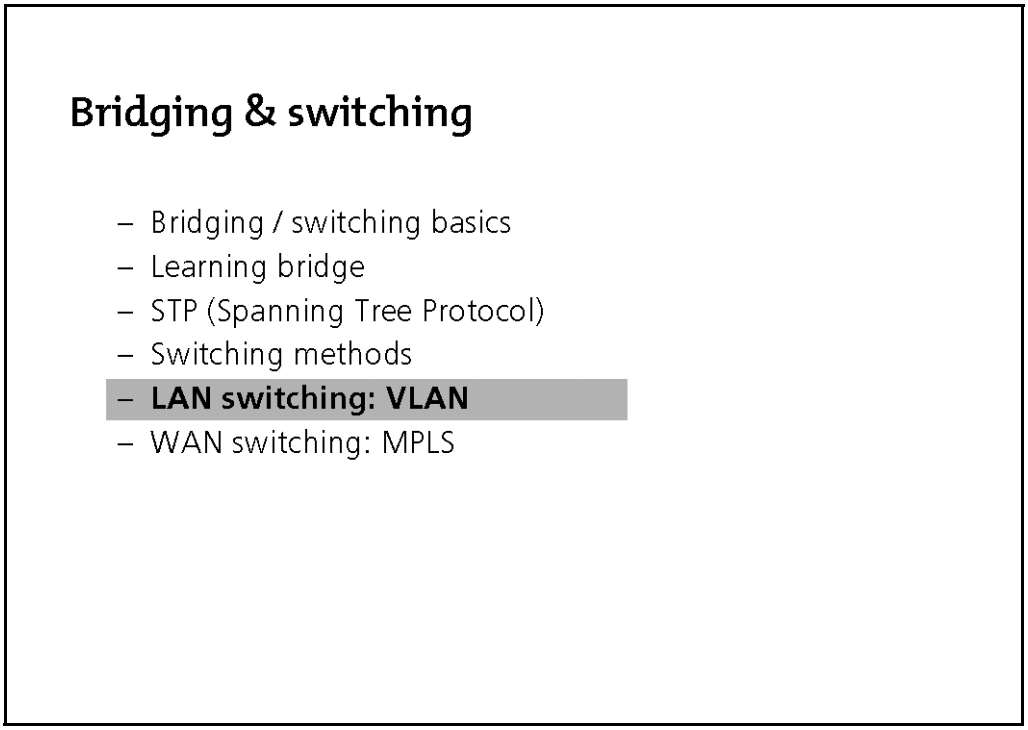
Slide 4.25
Fragment free (Cisco)

Cette solution se place entre le store and forward et le cut through en terme de performance. le Fragment Free, aussi appelé modified cut through, ne va pas directement retransmettre la trame dès réception de l'adresse de destination.

Dans ce cas de figure, on va attendre le 64ème octet, avant de démarrer la retransmission. L'expérience a montré que les risques de collision sont alors nuls. On évite ainsi de retransmettre des débuts de trames qui seront interrompues par les collisions.

Cette méthode n'a pas de raison d'être avec des LANs switchés récents, où chaque machine possède sa propre connexion au switch, rendant la probabilité de collision nulle. Rappelons aussi que dans le cas de liaison full-duplex le contrôle de collision est tout simplement désactivé !

4.5 LAN-Switching : VLAN

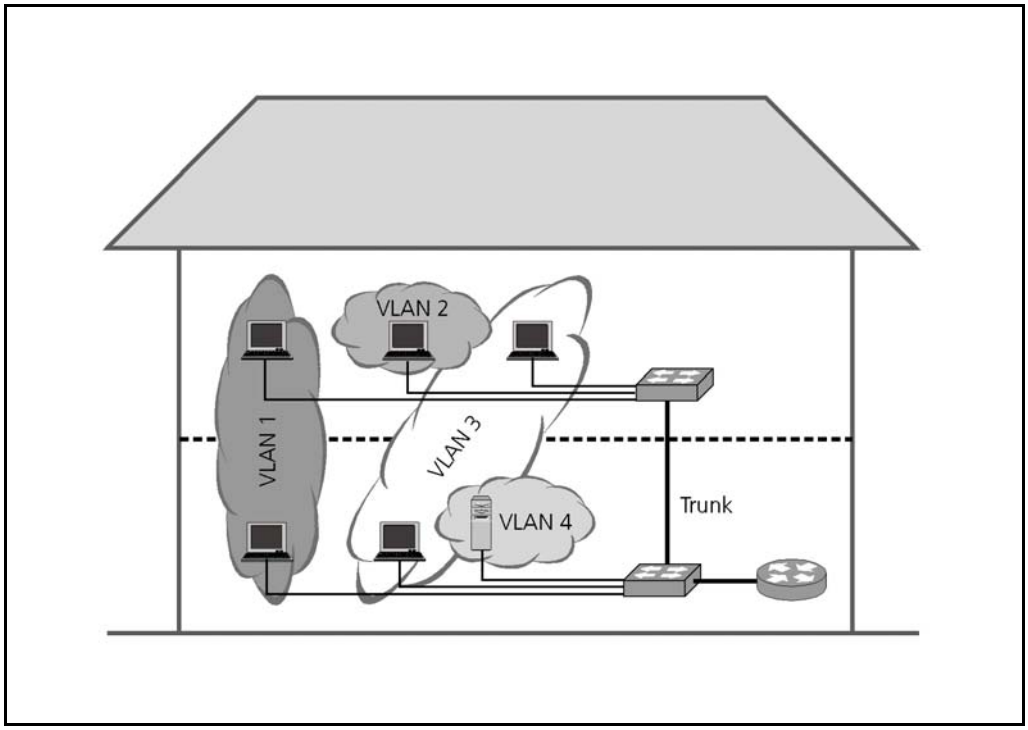


Slide 4.26
LAN-Switching : VLAN

Une fois qu'un réseau LAN est intégralement "switché", on peut franchir un pas de plus. Il s'agit d'isoler les machines dans des segments LAN virtuels.

On parle alors de VLAN (Virtual LAN), réseau local virtuel.

4.5.1 VLAN : Concept



Slide 4.27
VLAN : Concept

VLAN

Le principe du VLAN constitue à regrouper dans un réseau LAN des clients de ce réseau non plus par rapport à leur emplacement physique, mais en fonction de leur appartenance logique.

On va peut-être regrouper tous les PC des responsables de vente dans le même VLAN, alors qu'ils sont répartis dans les étages d'un bâtiment.

Les serveurs seront isolés dans leur propre réseau, lequel sera certainement équipé de fonctions de sécurité spéciales.

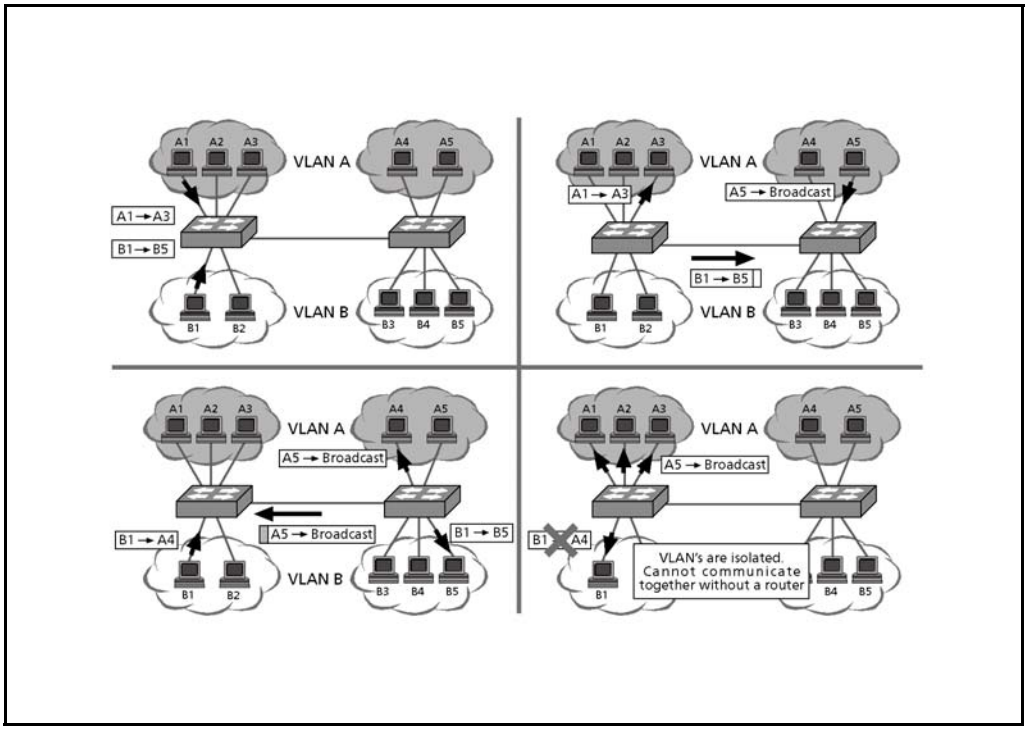
La solution du VLAN est de plus en plus utilisée, elle permet d'augmenter la flexibilité, la sécurité, ainsi que la capacité d'extension du réseau (scalability).

Les liaisons entre les switches, appelées trunk, véhiculent le trafic de plusieurs VLANs. Afin de ne pas confondre les différents trafics, chaque trame d'un VLAN sera étiquettée (Tag) d'un identificateur propre à son réseau virtuel.

Le switches ajoutent et suppriment ces étiquettes lors des entrées / sorties dans le trunk. Les équipements terminaux traitent des trames Ethernet classiques.

Plusieurs standards ainsi que de nombreuses solutions propriétaires existent pour réaliser cet étiquetage. Contrairement aux équipements terminaux, les interfaces "trunk" des équipements doivent supporter l'encapsulation spécifique à la technologie du VLAN.

4.5.2 VLAN : Fonctionnement



Slide 4.28
VLAN : Fonctionnement

Dans cet exemple, on observe différents trafics au sein de deux LAN virtuels isolés. Le trafic circulant de A1 à A3 ne passe pas le trunk, alors qu'une trame de B1 à B5 va utiliser le trunk pour atteindre la destination "éloignée".

On voit également apparaître l'étiquette sur les trames qui franchissent le trunk. Elle est ici représentée par un en-tête de la "couleur" du VLAN.

Les deux VLANs sont isolés. Le trafic de diffusion émis par A5 n'atteindra que les stations du VLAN A.

Pour que du trafic puisse s'écouler entre les VLAN's (par exemple de B1 à A4) il est nécessaire qu'un routeur les interconnecte. Du point de vue IP, ces stations seront dans des (sous-)réseaux différents.

Switch

4.5.3 VLAN : Standards

VLAN tagging

- IEEE 802.10 header between MAC and LLC headers
- IEEE 802.1q
- ISL (Cisco)

VLAN configuration and management

- Static (which port belongs to one VLAN)
- Dynamic (uses a VLAN server, like VMPS)
- Distributes VLAN info through VTP (VLAN trunk Protocol)

Slide 4.29
VLAN : Standards

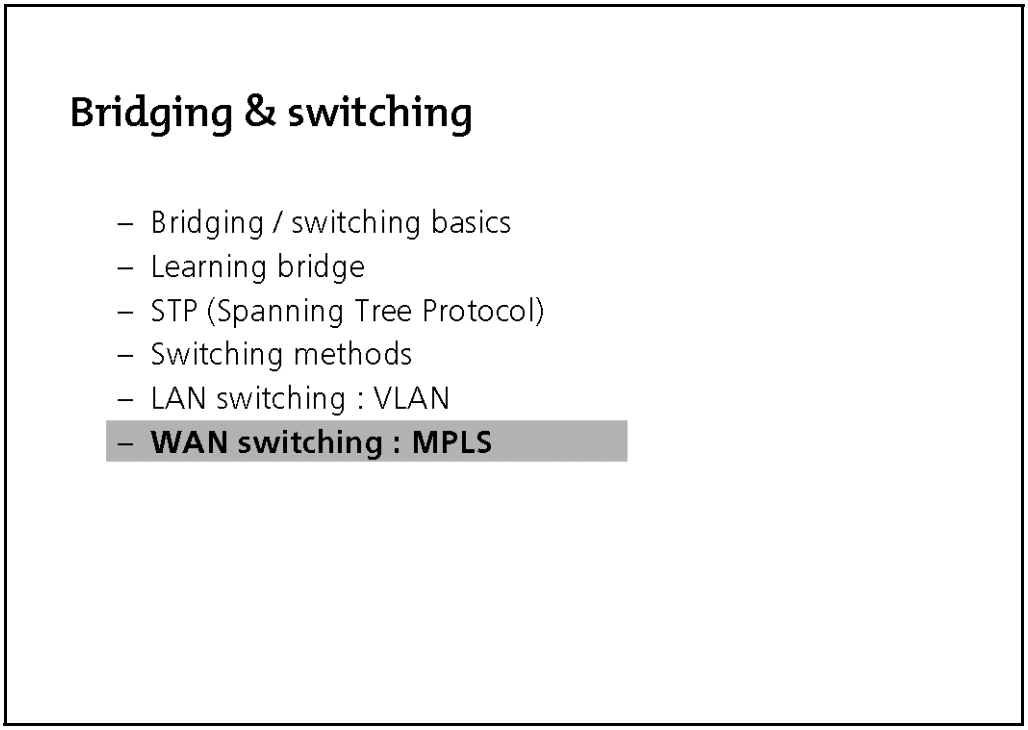
Les normes IEEE802.10 et 802.1q définissent le fonctionnement de VLAN normalisé. Cisco utilise un format propriétaire nommé ISL.

On peut configurer les VLANs de manière statique sur chaque switch séparément. Cette solution, en raison du temps qu'elle nécessite, ne sera mise en oeuvre que dans des réseaux de taille réduite.

Pour les réseaux plus grand, on utilisera des solutions dynamiques, pour lequelles un serveur de VLAN est nécessaire. VMPS (VLAN Membership Policy Server) est la solution préconisée par Cisco.

Les switches se distribuent les informations relatives aux VLANs à travers un protocole dédié. On peu encore ici citer le protocole propriétaire de Cisco, VTP (VLAN Trunking Protocol).

4.6 WAN-Switching : MPLS



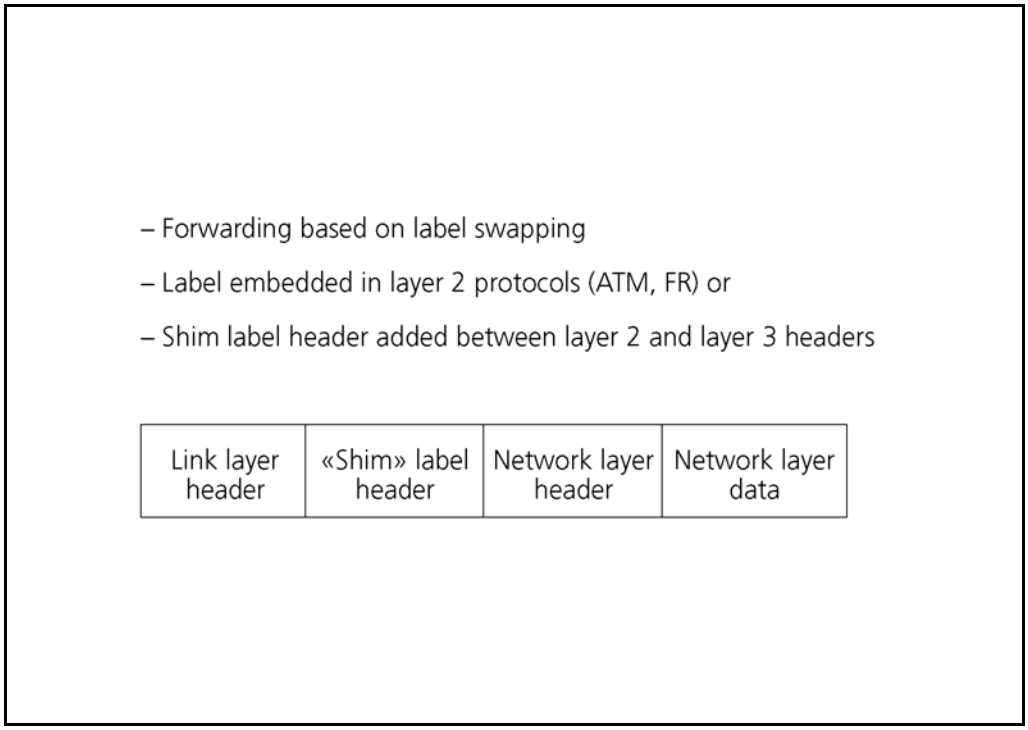
Slide 4.30
MPLS (Multi Protocol Label Switching)

MPLS

MPLS est une méthode d'acheminement de paquets perfomante. Elle résulte d'une évolution de différentes technologies du milieu des années 90. Les plus connues de ces technologies étaient : Ipsilon IP Switching, Toshiba Cell Switching, Cisco Tag Switching, IBM ARIS (Aggregate Route-based IP Switching). Toutes ces méthodes ont un point commun : elles utilisent le principe de translation d'étiquette (Label Swapping) pour acheminer les données. MPLS est le nom qui a été donné au groupe de l'IETF chargé de définir une approche commune à toutes ces techniques d'acheminement.

Le choix de l'acheminement se fait au travers des protocoles de routages traditionnels. Une fois les chemins établis, on crée un tunnel MPLS "switché" au travers du réseau IP. Il 's'agit d'étudier ici le principe de la commutation MPLS.

4.6.1 Principes et caractéristiques de MPLS

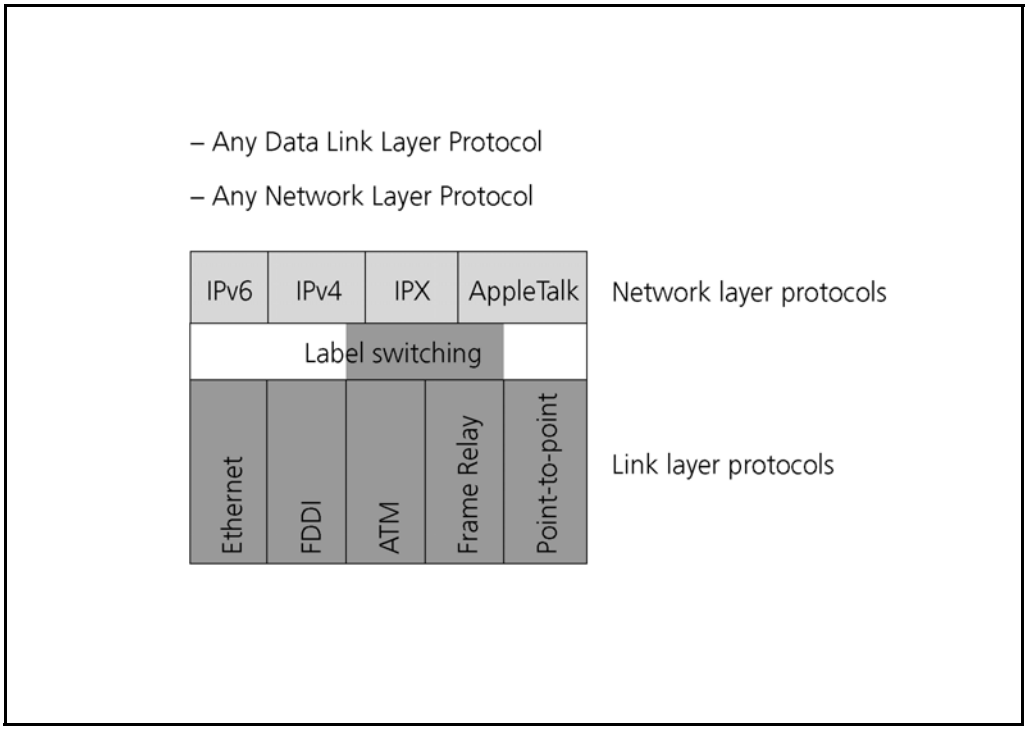


Slide 4.31
Principes et caractéristiques de MPLS

Label

L'acheminement d'un paquet dans un réseau MPLS est basé sur l'analyse d'une étiquette (Label). Dans certaines technologies, comme Frame Relay ou ATM, cette étiquette peut être représentée par les identificateurs de connexion virtuelle (DLCI pour Frame Relay, VPI/VCI pour ATM). Pour certains autres protocoles de couche 2 (par exemple Ethernet, liaisons point à point) cette possibilité n'existe pas. Il est alors nécessaire d'introduire une entête supplémentaire (Shim Label Header) entre l'entête de couche 2 et l'entête de couche 3.

4.6.2 Architecture de MPLS

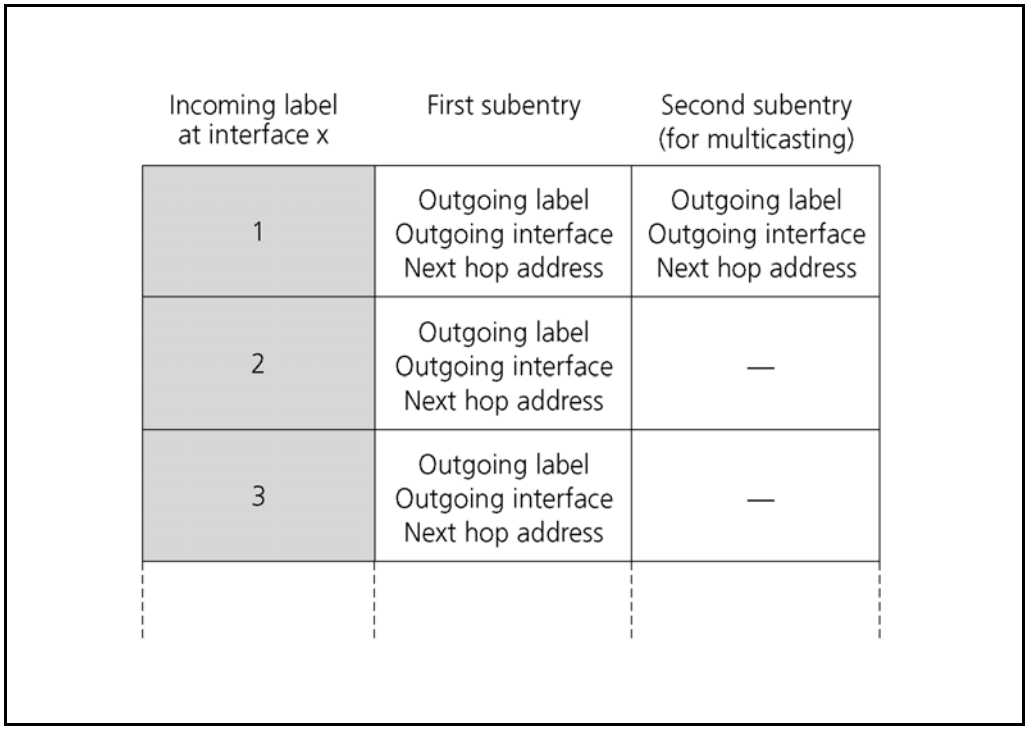


Slide 4.32
Architecture de MPLS

Multiprotocol

Le principe de l'acheminement par "Label Switching" n'est ni lié à une technologie de couche 2 (Link Layer) ni à un protocole de couche réseau. C'est pourquoi on parle de "Multiprotocol" dans la dénomination MPLS.

4.6.3 Table de retransmission



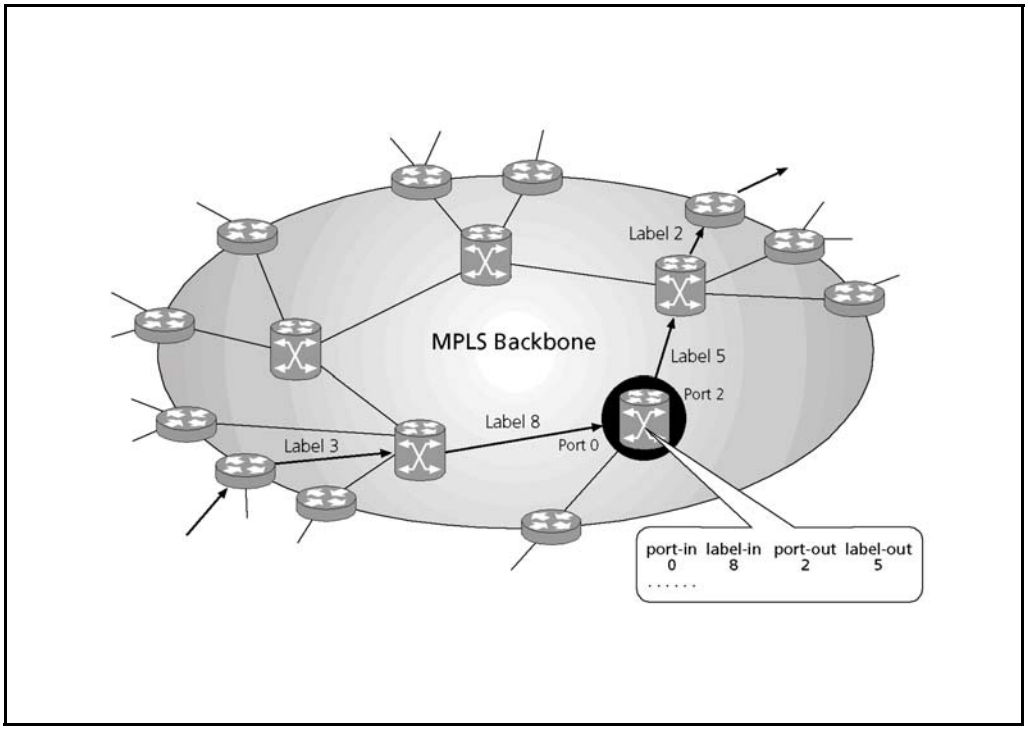
Slide 4.33
Table de retransmission

LSR

Lorsqu'un LSR (Label Switch Router) reçois un paquet, il utilise le Label du paquet pour rechercher l'entrée correspondante dans la table d'acheminement. Une fois l'entrée trouvée, il utilise les informations des sous-entrées (Subentry) pour déterminer sur quelle interface et avec quel Label le paquet doit être acheminé.

La table d'acheminement peut avoir une sous-entrée (unicast) ou plusieurs sous-entrées dans le cas de l'acheminement multicast.

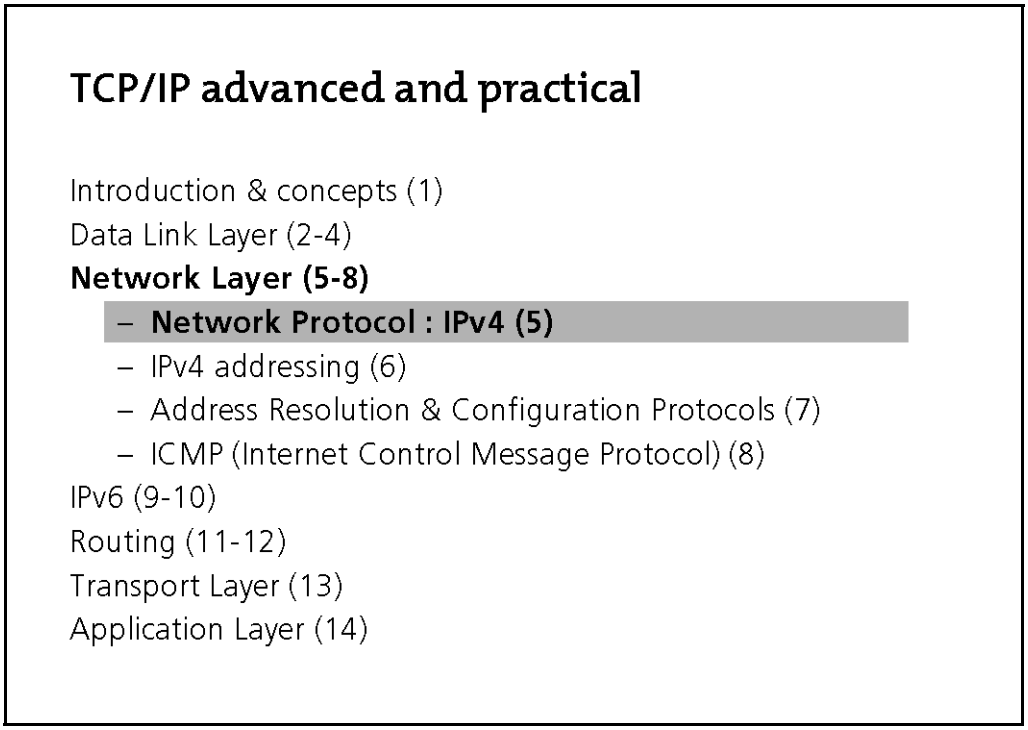
4.6.4 Exemple MPLS



Slide 4.34
Exemple MPLS

Dans cet exemple de Backbone, chacun des LSR (Label Switch Router) associe un couple "port-in / label-in" à un couple "port-out / Label-out". Des liaisons virtuelles sont ainsi créées pour chacune des FEC (Forwarding Equivalent Class), les routes MPLS, au travers de ce réseau.

5 Protocole réseau : IPv4



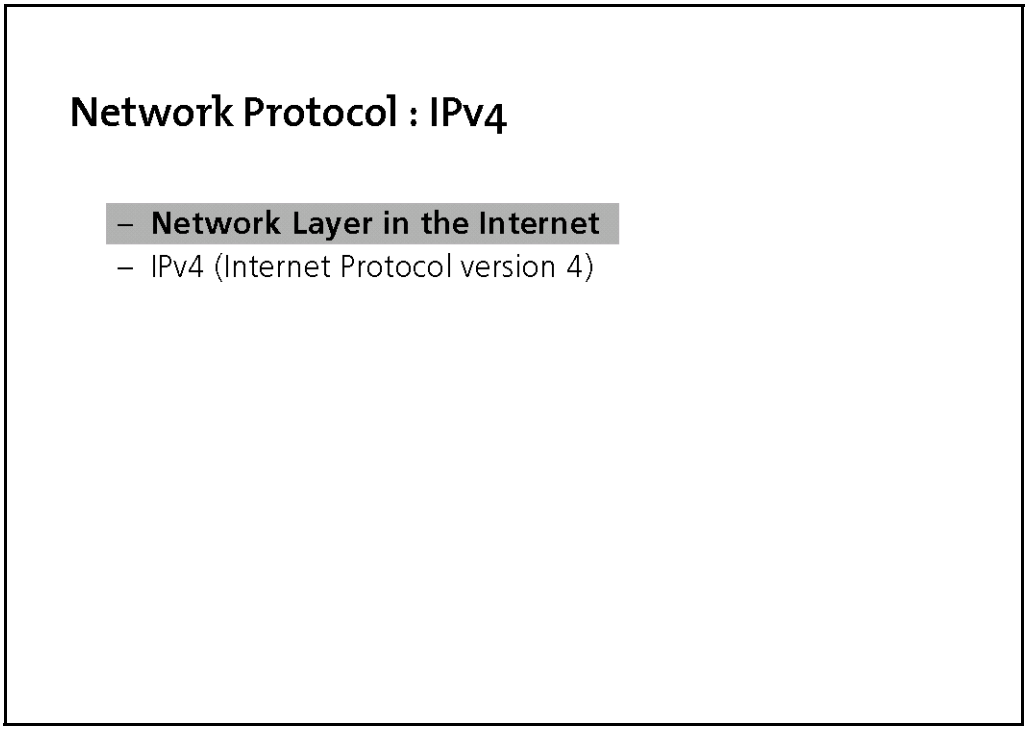
Slide 5.1
Protocole réseau : IPv4

Après un aperçu des fonctions de base de la couche réseau, ce chapitre traite du protocole réseau actuellement utilisé dans l'Internet, IP version 4.

Objectifs

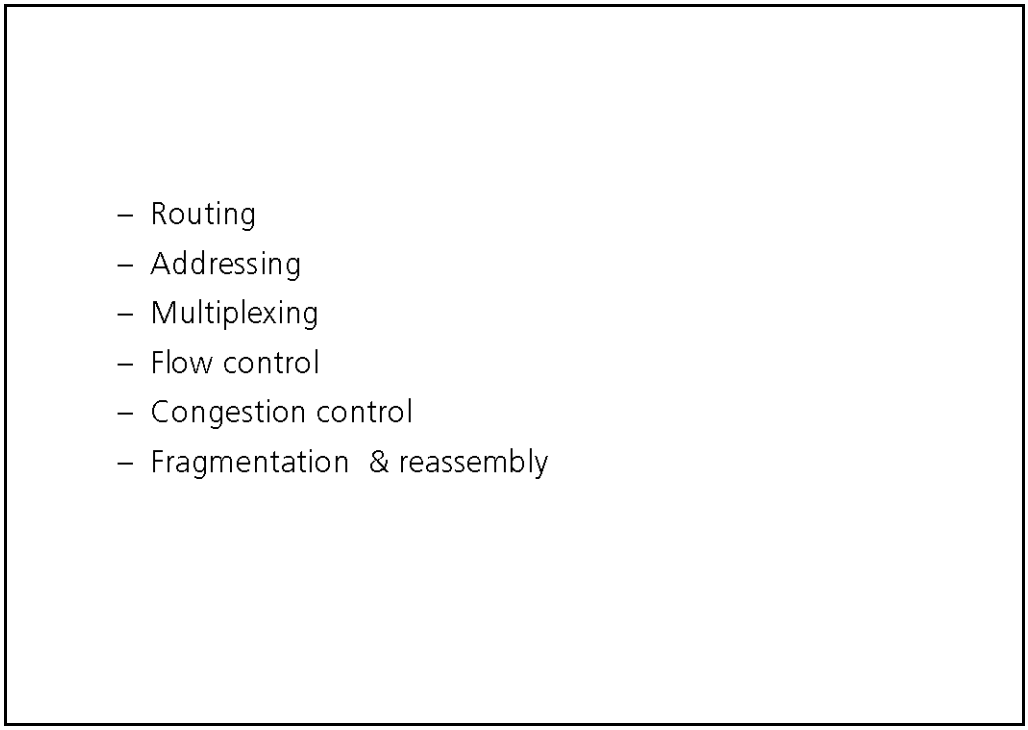
A l'issue de ce chapitre, les participants sont capables de reconnaître en entête IP version 4, d'expliquer la fonction des principaux champs de cet entête et le principe de fonctionnement de ce protocole.

5.1 Couche réseau dans l'internet



Slide 5.2
Couche réseau dans l'Internet

5.1.1 Fonctions de base

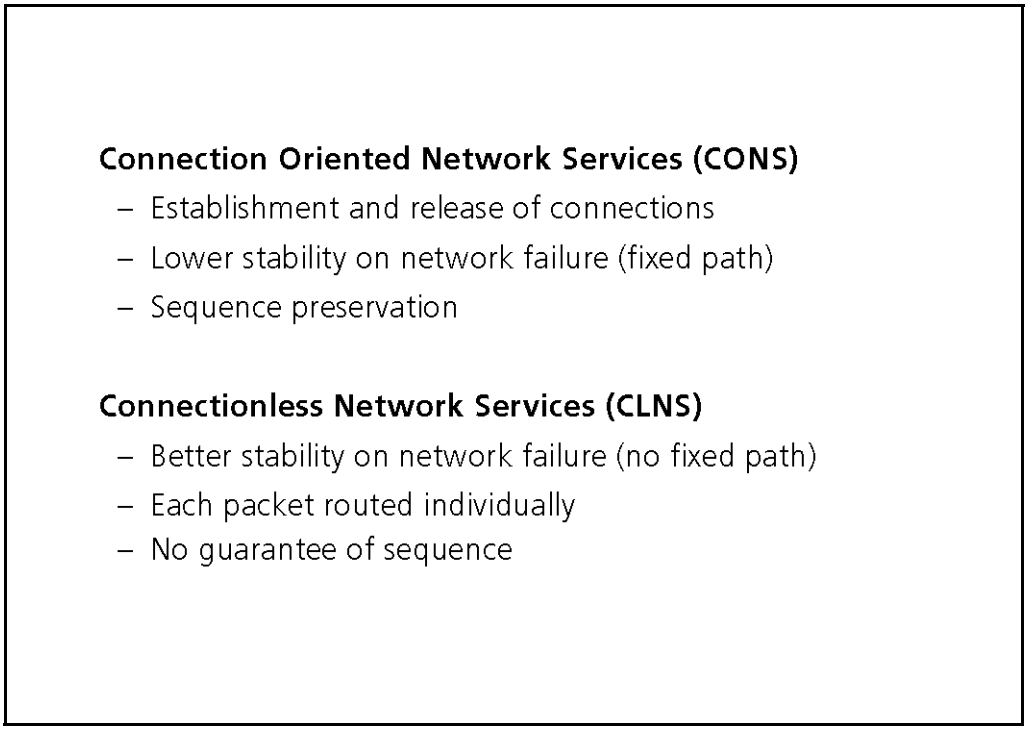


Slide 5.3
Fonctions de base

Une des fonctions clés de la couche réseau est le routage. Il s'agit de déterminer, pour chaque information, quelle est sa destination et quelle direction prendre pour l'atteindre. On utilise pour cela les données d'adressage, contenue dans les entêtes de protocoles et on les compare aux données présentent dans les tables des routeurs.

Une couche réseau peut également mettre en œuvre des principes de contrôle de flux ou de congestion, s'occuper de multiplexer des flux d'information, ou encore de fragmenter, respectivement réassembler, des informations dont la taille dépasserait les capacités du réseau à traverser.

5.1.2 Avec ou sans connexion



Slide 5.4
Avec ou sans connexion

Une couche réseau peut travailler avec ou sans connexion. Un réseau orienté connexion (CONS Connection Oriented Network Services) choisi, au moment de la connexion, un itinéraire pour relier les partenaires de la communication. A l'inverse, un réseau orienté sans connexion (CLNS Connectionless Network Service) va devoir prendre une décision d'acheminement pour chaque élément transmis au partenaire.

La méthode sans connexion, utilisée dans l'Internet, permet de ne pas perdre le contact, même lorsqu'une modification de réseau intervient (panne, saturation, etc.). Il en résulte par contre une diminution de performance car chaque élément transmis (paquet de données) contient toute l'information nécessaire à son acheminement.

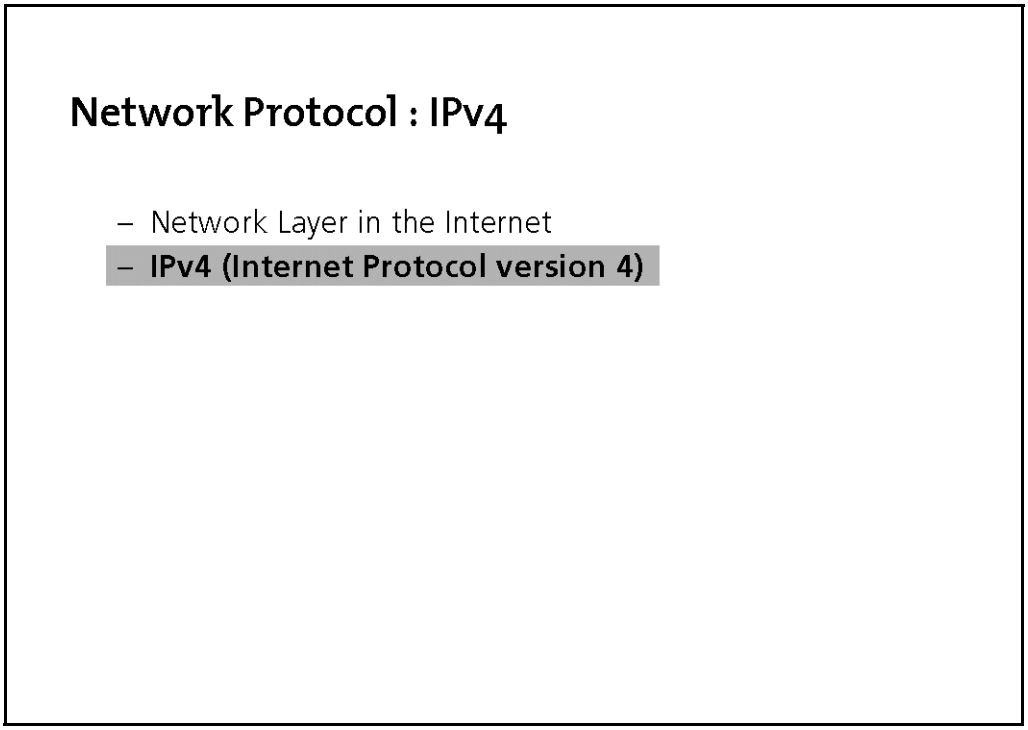
5.1.3 Qualité de service

Slide 5.5
Qualité de service

La couche réseau peut offrir différentes qualités de services. On peut exiger des contraintes temporelles, délai de transmission, variation de celui-ci. Des attentes sémantiques sont également possibles. La transparence de la couche réseau quant aux services et aux données doit souvent être garanti. On peut encore exiger que le réseau soit disponible lorsqu'on en a besoin.

Ces différentes qualités de service ne sont pas acquises. En fonction de la technologie réseau, on peut ne pas avoir de qualité de service, pouvoir en obtenir à la demande (paramétrable selon contrat client) ou encore bénéficier de ces qualités intrinsèquement à la technologie choisie.

5.2 IPv4 (Internet Protocol version 4)



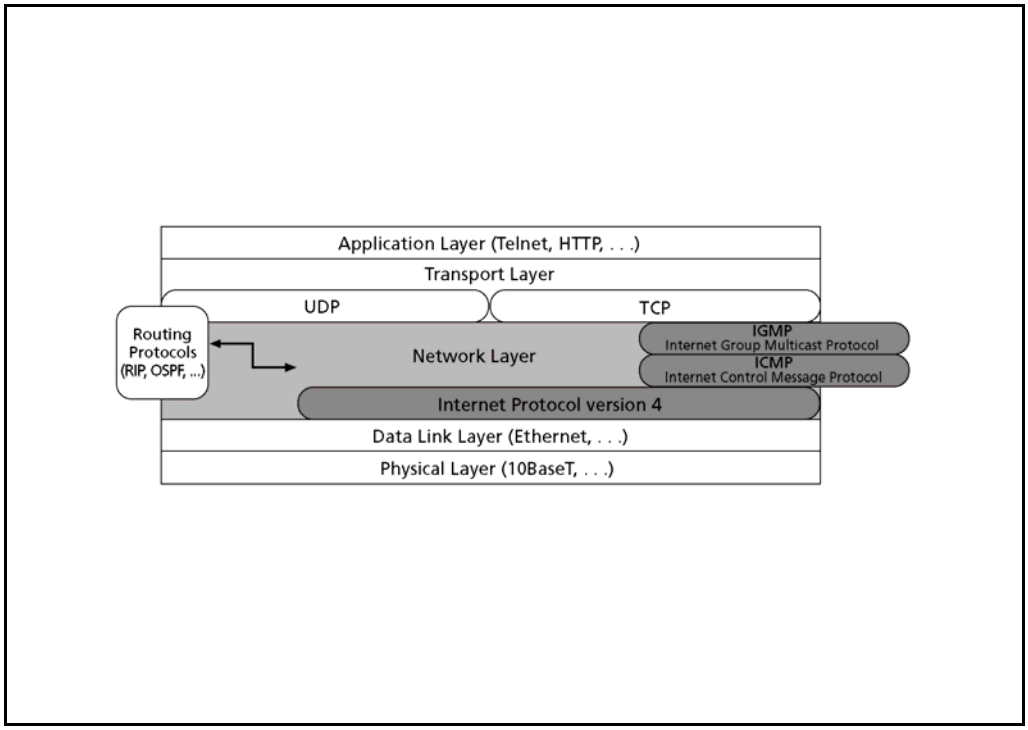
Slide 5.6
IPv4 (Internet Protocol version 4)

Le protocole IP se trouve en couche 3 du modèle de référence OSI. Il s'agit du protocole réseau utilisé dans l'Internet.

Il est décrit dans [RFC 791]

On peut dire qu'il est l'élément central d'articulation de toute la pile ARPA (TCP/IP).

5.2.1 Architecture d'IPv4



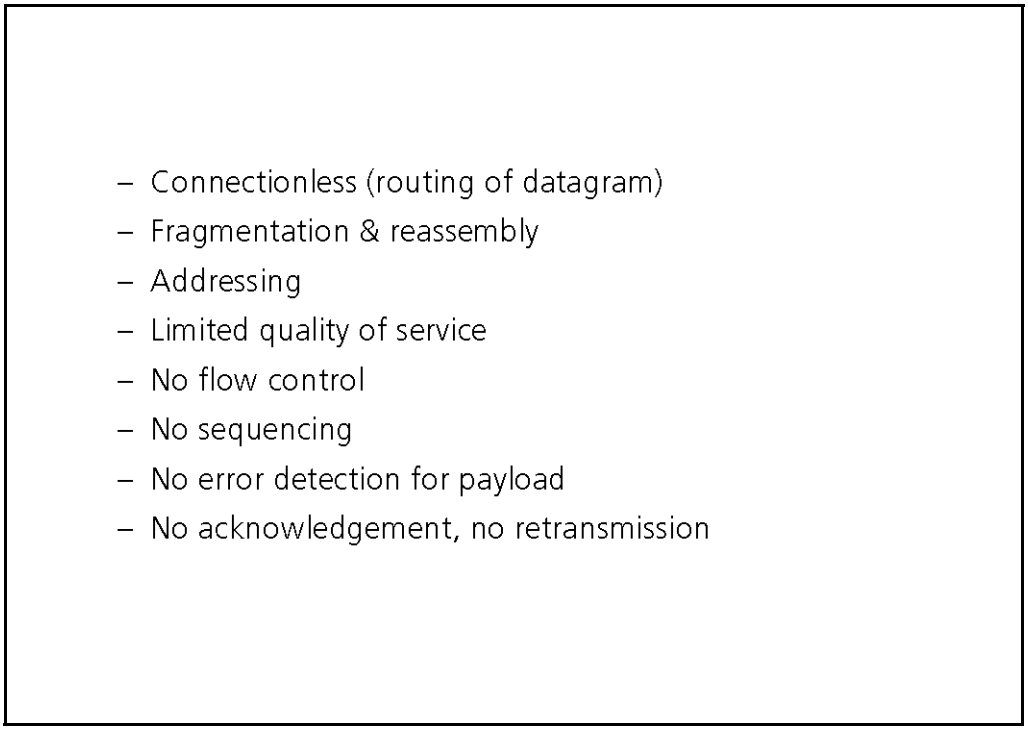
Slide 5.7
Architecture d'IPv4

IP peut fonctionner sur une large plage de protocoles de couche 2, donnant ainsi accès à toutes sortes de supports physiques.

En couche 3, il est associé à deux protocoles, considérés comme étant de ses composantes. Il s'agit de ICMP (messages de contrôle) et de IGMP (Gestion des groupes multicast).

Il transporte indifféremment les deux protocoles de transport de cette famille ARPA, UDP (User Datagram Protocol) et TCP (Transmission Control Protocol).

5.2.2 Fonctions et propriétés IPv4



Slide 5.8
Fonctions et propriétés IPv4

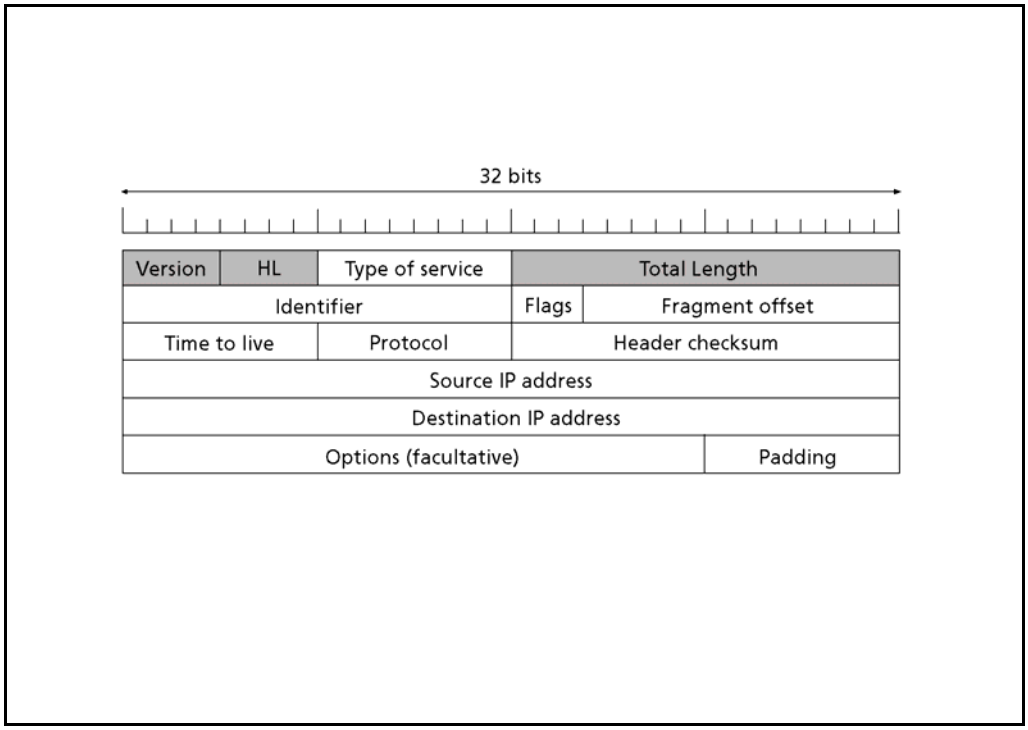
Le protocole IP est un protocole sans connexion.

Un adressage est utilisé pour l'acheminement correct des paquets. Il est structuré et peut être divisé en sous-réseaux.

IP peut offrir une certaine qualité de service mais elle n'est pas implémentée dans l'épine dorsale d'Internet. Toutefois, on commence à trouver des réseaux locaux (LAN, Local Area Network) qui offrent ces qualités de service.

IP ne contrôle pas le flux, ne garantit pas le séquencement des informations. Il ne possède pas de détection d'erreur pour les données utiles transportées et ne procède pas à la retransmission de paquets perdus.

5.2.3 Format de paquet IPv4



Slide 5.9
Format de paquet IPv4

Voici le format du paquet IP. Tout d'abord nous trouvons un champ Version qui, sur 4 bits, définit la version du protocole IP utilisée. Il s'agit pour nous de la version 4.

HL, Header Length

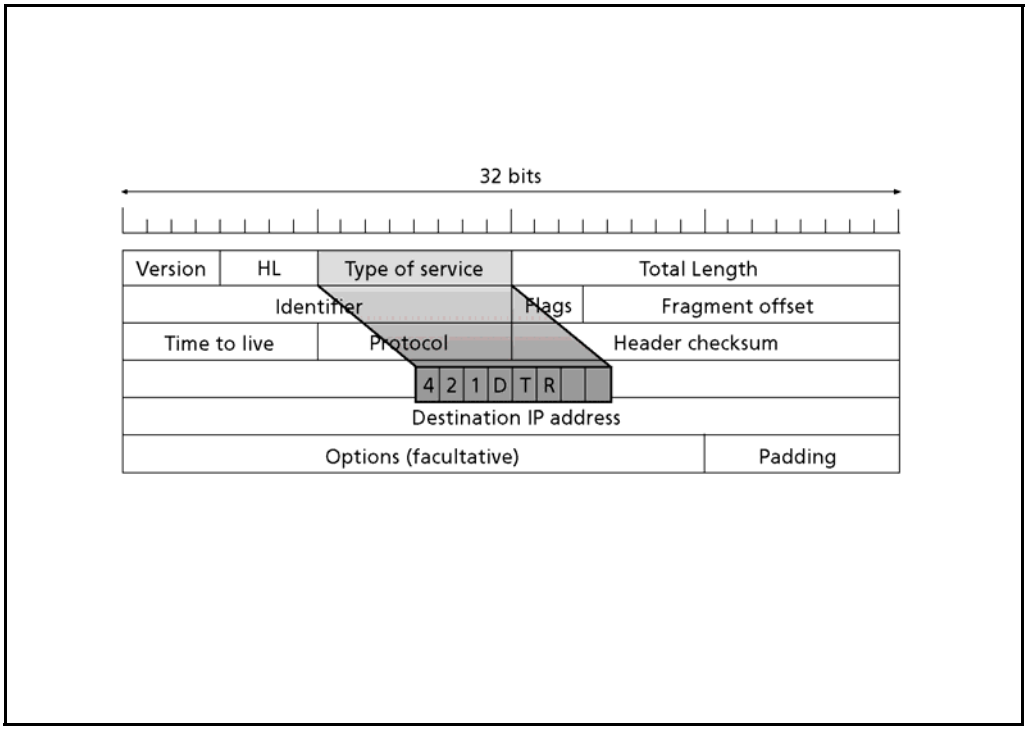
Le champ, HL (Header Length) indique la longueur de l'entête, en mots de 32 bits. Un entête habituel ne possède pas d'option et possède par conséquent 20 octets, soit 5 fois 32 bits.

Type of service est décrit en détail à la page suivante.

Total Length

La longueur totale du paquet IP est indiquée dans le dernier champ de cette première ligne, "Total Length".

5.2.4 Format de paquet : TOS, qualité de service IPv4



Slide 5.10
Format de paquet : TOS, qualité de service

TOS, Type of service

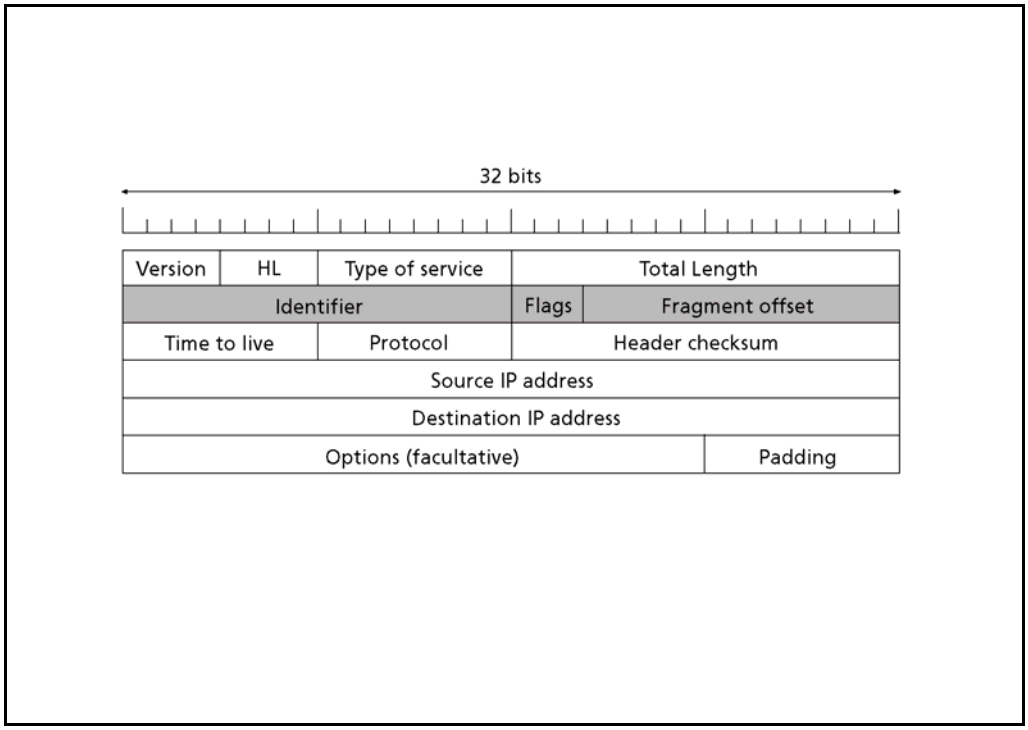
Le champ "Type of service" a une longueur d'un octet. Les trois premiers bits représentent une priorité (421 indique le poids des bits). Les bits D, T et R représentent chacun un type de service différent.

Delay, Throughput, Reliability

D activé (Delay) demande un délai de transmission court. Cela est important pour toutes les communications "temps réel", comme la téléphonie sur Internet. Le bit T (Throughput) demande transmission à haut débit. On l'utilise lorsque des données vidéo devront être transmises. La fiabilité nécessaire aux transmissions de données pourra être sollicitée en activant le bit R (Reliability).

Il faut pour cela que les routeurs puissent offrir des routes alternatives ayant des caractéristiques connues et maîtrisées. Ce n'est aujourd'hui pas le cas d'Internet.

5.2.5 Format de paquet IPv4 : Fragmentation



Slide 5.11
Format de paquet IPv4 : Fragmentation

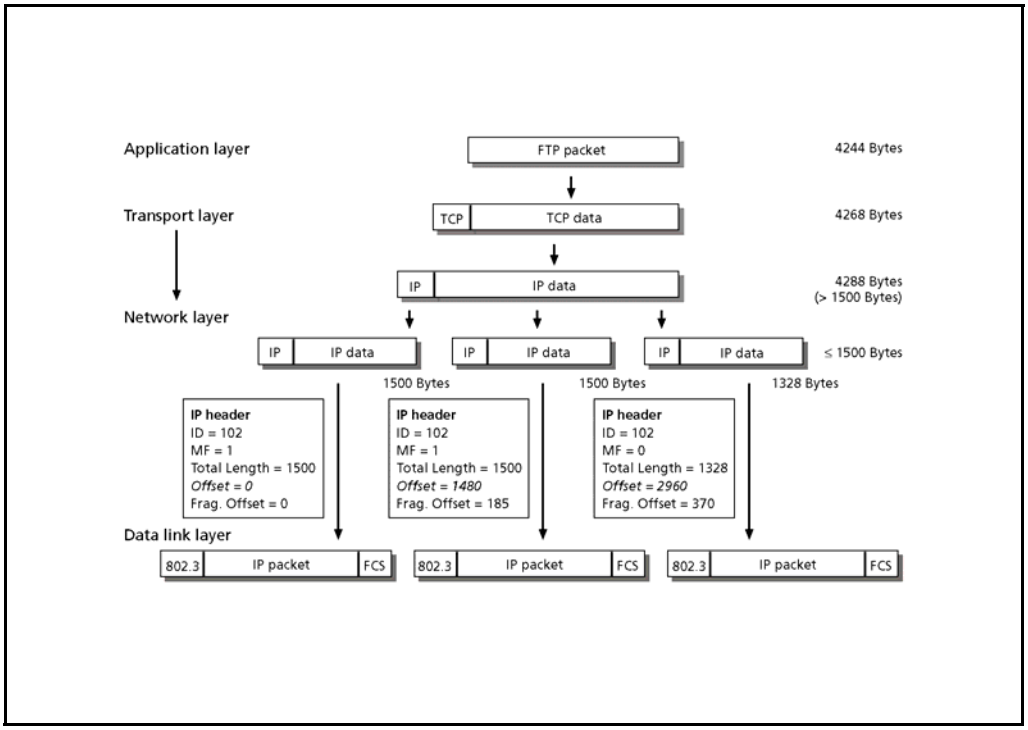
Identifier, Fragment offset

Si un paquet IP doit traverser un réseau qui ne supporte pas sa longueur, le routeur confronté au problème devra le fragmenter en paquets plus petits, compatibles avec la technologie à disposition. Chaque fragment aura la même identification, un "fragment offset" se chargeant de fournir le numéro du premier octet transmis. Il est possible qu'un des fragments suive un autre chemin et doive à nouveau être fragmenté. Seule la destination s'occupe du réassemblage.

Flags

Le 1er bit des flags n'est pas utilisé. Le 2ème, "DF" (D'ont Fragment) interdit la fragmentation du paquet. "MF" (More fragment), le 3ème et dernier bit, indique que d'autres fragments de ce paquet viennent encore.

5.2.6 Fragmentation IPv4 : Exemple

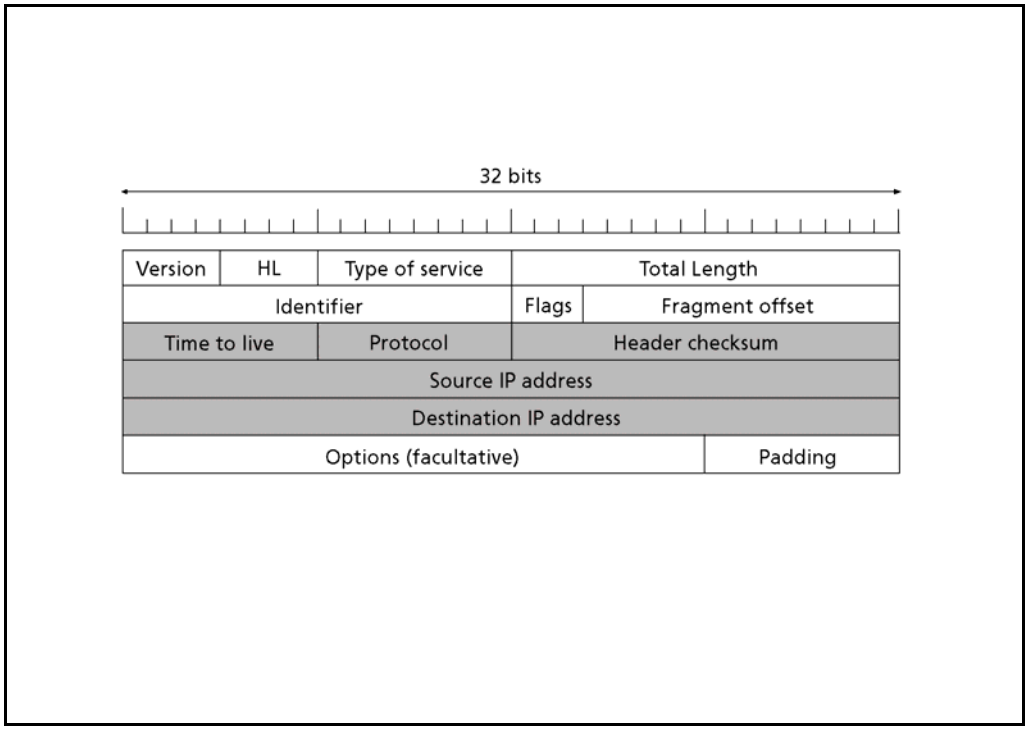


Slide 5.12
Fragmentation IPv4 : Exemple

Fragmentation

Prenons, par exemple un paquet IP de 4288 octets. Il ne peut pas traverser un réseau Ethernet n'acceptant qu'une taille max. de 1 500 o. Ce paquet va donc être fragmenté en 3 paquets de 1 500, 1 500 et 1 328 o. Cela donne un total de 4328 octets, représentant nos 4288o de départ plus 2 en-têtes IP de 20 octets (2 et 3ème frag). Dans le 1er fragment, on transporte 1480 octets de données (0 à 1 479). Il est donc logique de trouver l'octet N°1480 dans l'offset du 2ème fragment (respectivement 2960 dans le 3ème). Le champ "Fragment offset" n'est codé que sur 13 bits, cela le rend huit fois plus petit que "Total Length". On range dans le champs "Fragment offset" l'offset réel divisé par huit. Les données contenues dans les premiers fragments seront toujours longues d'un multiple de huit octets.

5.2.7 Format de paquet IPv4 : Protections et adressage



Slide 5.13
Format de paquet IPv4 :Protections et adressage

TTL

Le champ "Time to Live" (TTL) est un décompteur. Chaque routeur traversé va décrémenter le TTL. Si un routeur parvient à la valeur 0, il détruit le paquet. C'est notre sécurité contre les paquets qui tournent en rond dans le réseau.

"Protocol" sert à indiquer quel est le protocole transporté dans les données (TCP=6, UDP=17, ICMP=1).

Protocol

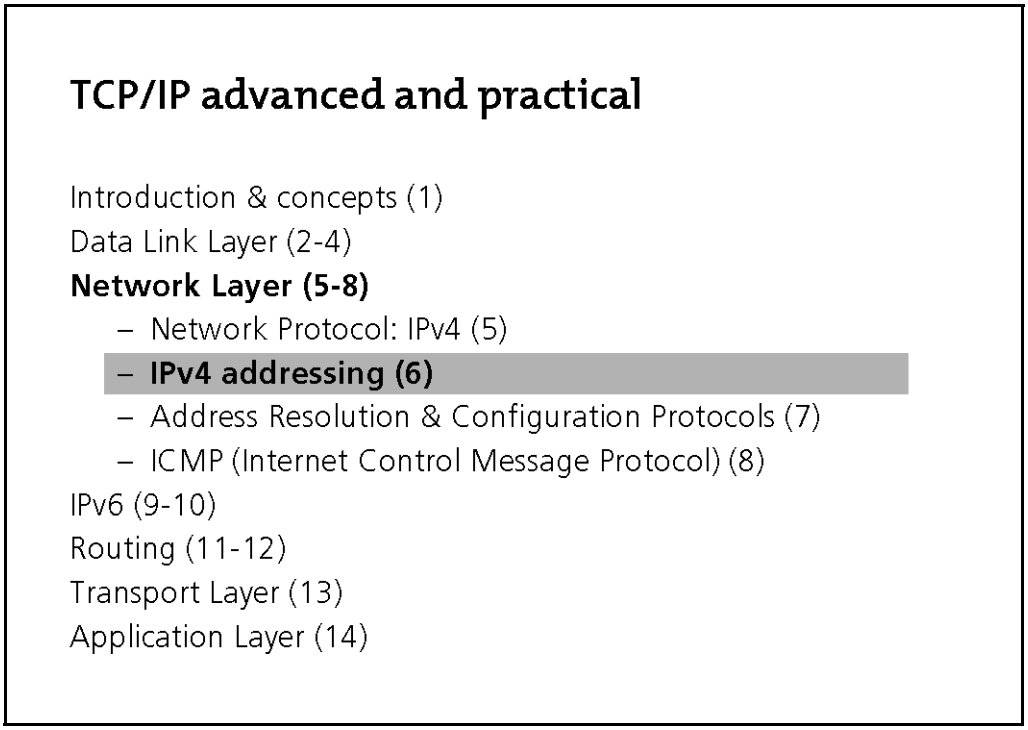
Un champ est prévu pour le checksum de l'entête. Aujourd'hui beaucoup de routeurs ne calculent plus cette somme, par manque de temps.

IP Address

Ensuite viennent Les adresses source et destination nécessaires à l'acheminement.

Parfois des options de déboguage peuvent terminer notre entête

6 Adressage IPv4



Slide 6.1
Adressage IPv4

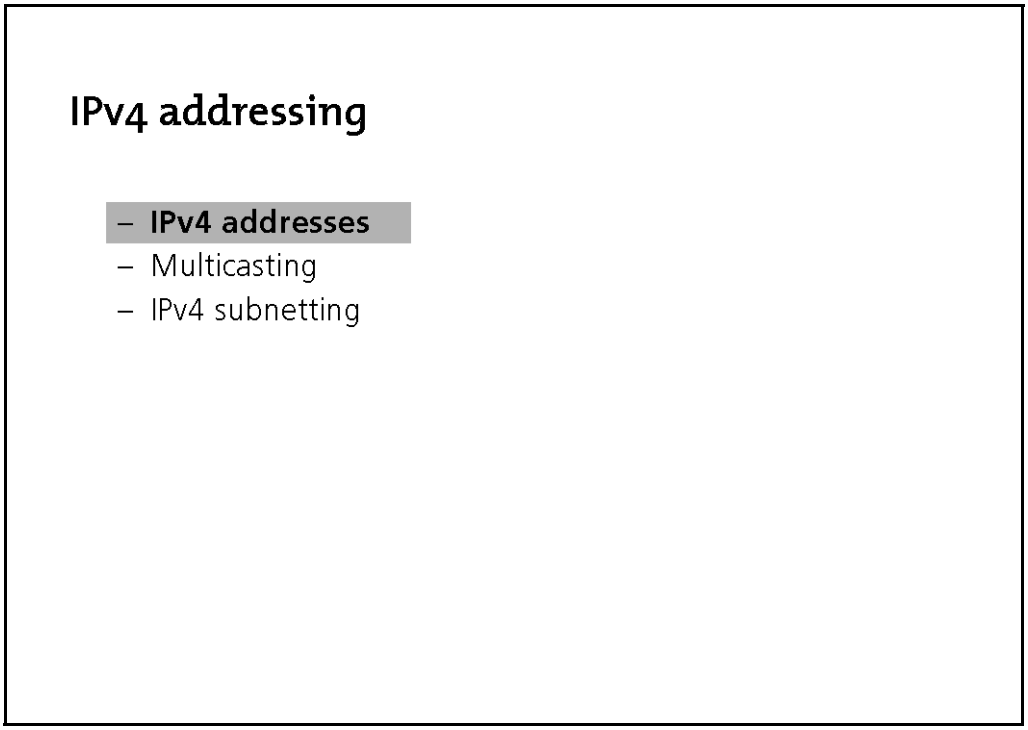
Ce chapitre traite de l'adressage IPv4. On y parle des différents types et classes d'adresses, ainsi que du subnetting.

Objectifs

A l'issue de ce chapitre, les participants sont capables de différencier les différentes classes d'adresses IP, ainsi que l'unicasting du multicasting.

Ils sont en outre capables de calculer des sous-réseaux, de reconnaître les adresses broadcast et de sous-réseaux des adresses utiles. Ils peuvent nommer le supernetting avec l'utilisation de CIDR.

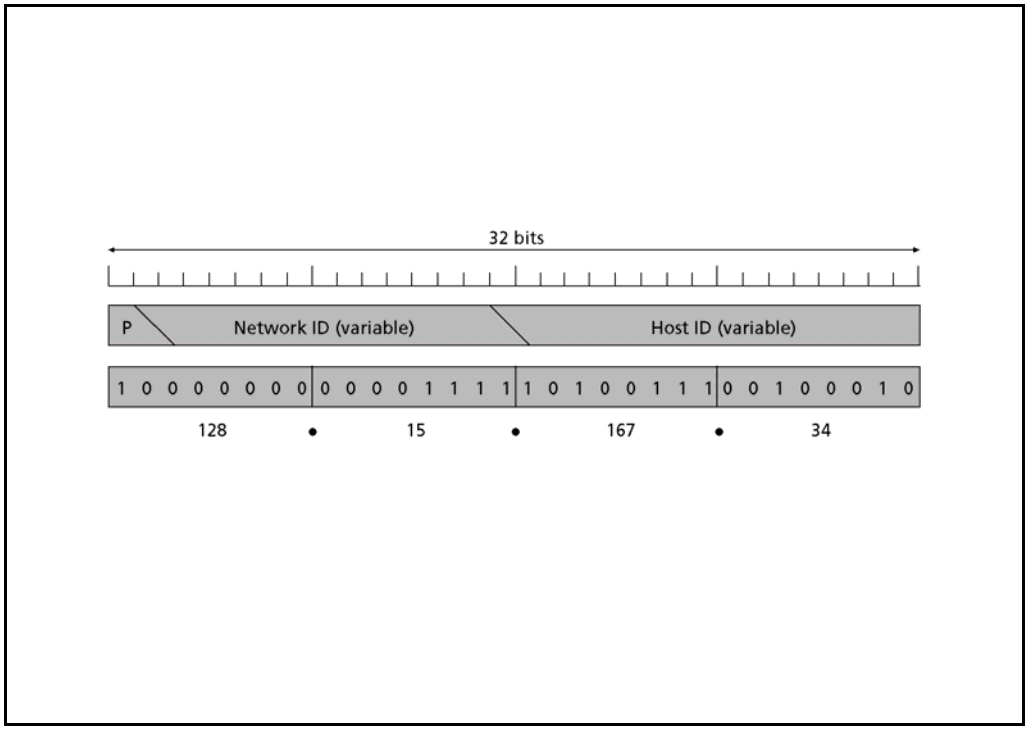
6.1 Adresses IPv4



Slide 6.2
Adresses IPv4

Nous allons maintenant étudier la structure de l'adresse IP.

6.1.1 Format d'adresse IPv4



Slide 6.3
Format d'adresse IPv4

L'adresse IP est composée de 32 bits. Elle est structurée en réseaux (Network ID) et clients (Host ID).

Des réseaux de tailles différentes sont disponibles, on les reconnaît à un préfixe défini (P).

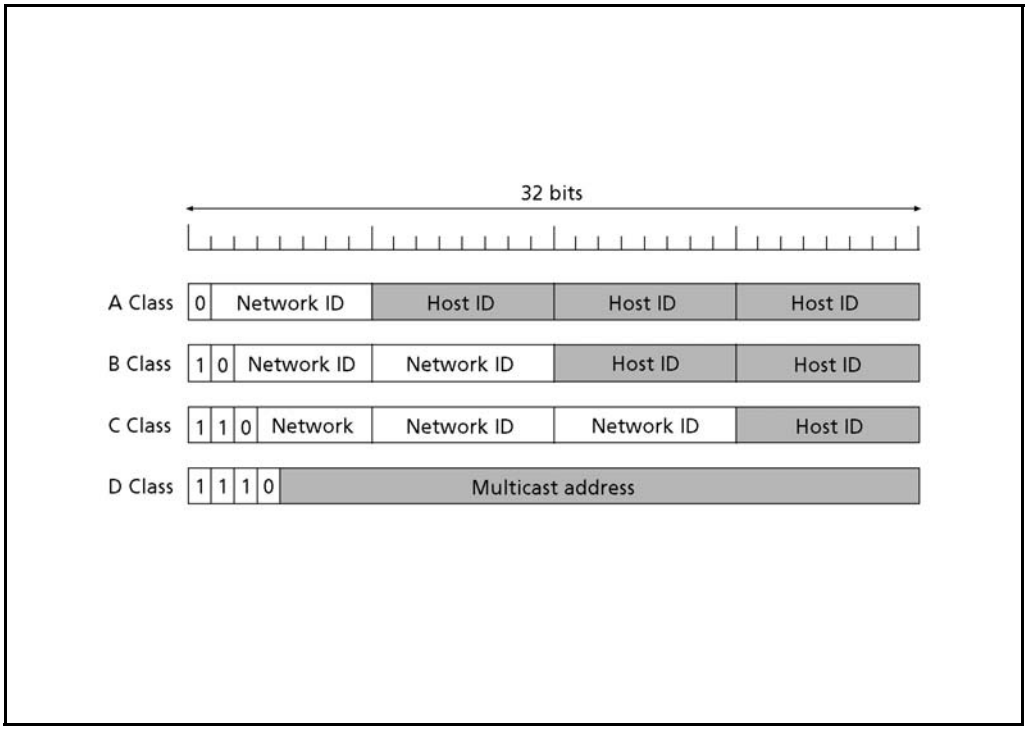
Pointé décimal

Chacun des 4 octets composant l'adresse IP est exprimé en décimal. On représente l'adresse IP en séparant ces 4 octets par des points. On parle de représentation "pointé décimal".

Par conséquent, les valeurs que l'on peut trouver seront comprises entre 0 et 255.

Une adresse IP "12.345.67.891" ne peut pas exister.

6.1.2 Classes d'adresses IPv4



Slide 6.4
Classes d'adresse IPv4

Une adresse de classe A commence par un 0, les 7 bits suivants permettent de définir 128 réseaux (126 utilisés). Ils contiennent chacun > 16 millions de clients (hosts) potentiels.

Classe A

"10" est le préfixe d'un réseau de classe B. Au nombre de 16 384, ils peuvent adresser 65 534 hosts

Classe B

Les ~2 millions de réseaux de classe C (préfixe = 110) ne peuvent contenir plus que 254 hosts. Seuls ces réseaux, trop petits pour les sociétés, sont encore disponibles.

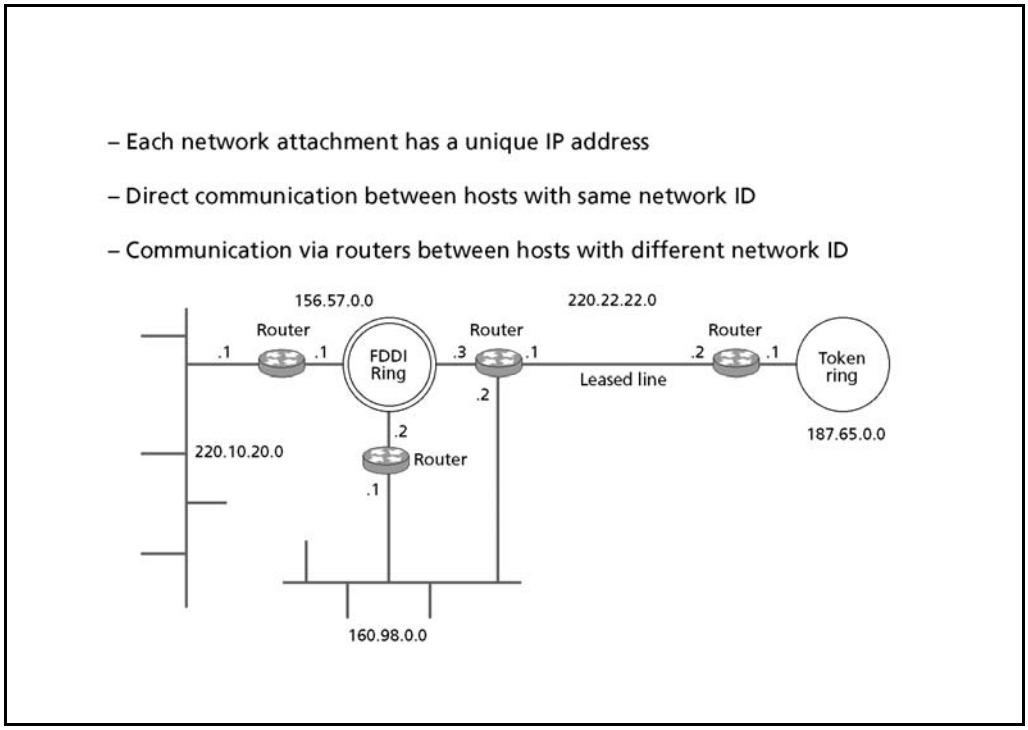
Classe C

Les adresses multicast classe D se reconnaissent au préfixe "1110"

Classe D

Le reste des adresses (préfixe 1111) s'appelle classe E (utilisation expérimentale).

6.1.3 Adressage IPv4



Slide 6.5
Adressage IPv4

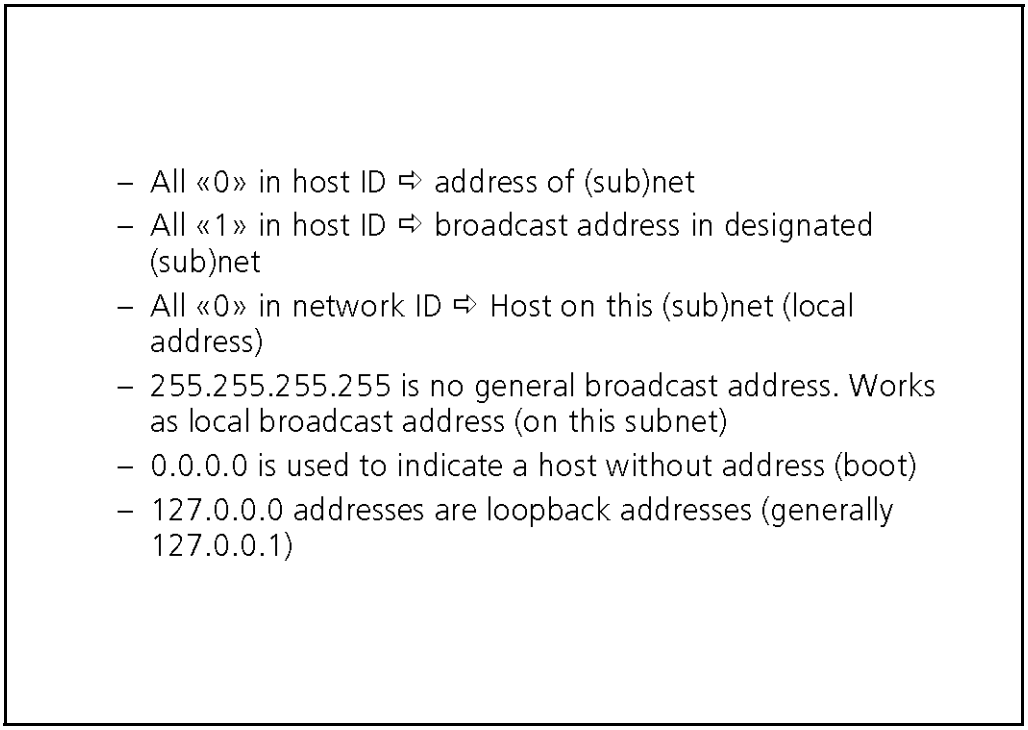
Chaque connexion physique au réseau possède sa propre adresse IP unique. Les routeurs vont donc posséder autant d'adresses qu'ils ont d'interfaces.

Deux clients dont l'identificateur (sous-)réseau est le même, partagerons le même "câble". Ils pourront communiquer directement entre eux, sans utiliser les compétences d'un routeur.

A l'inverse, deux clients ne possédant pas la même identification de réseau devront confier leur message au routeur. C'est lui qui s'occupera de l'acheminer dans la bonne direction, au prochain routeur. Ainsi de suite, de routeur en routeur, notre message va transiter à travers le réseau, jusqu'à notre destination finale.

Seul le dernier routeur connaîtra l'emplacement de la destination.

6.1.4 Adresses spéciales IPv4



Slide 6.6
Adresses spéciales IPv4

Lorsque tous les bits de la partie "Host" d'une adresse sont à "0", cette adresse désigne le (sous-)réseau lui-même. Lorsque tous ces bits sont à " 1 " on trouve l'adresse de diffusion (broadcasting) du (sous-)réseau. Ces deux adresses sont réservées et ne peuvent être attribuées à un client ou à un routeur.

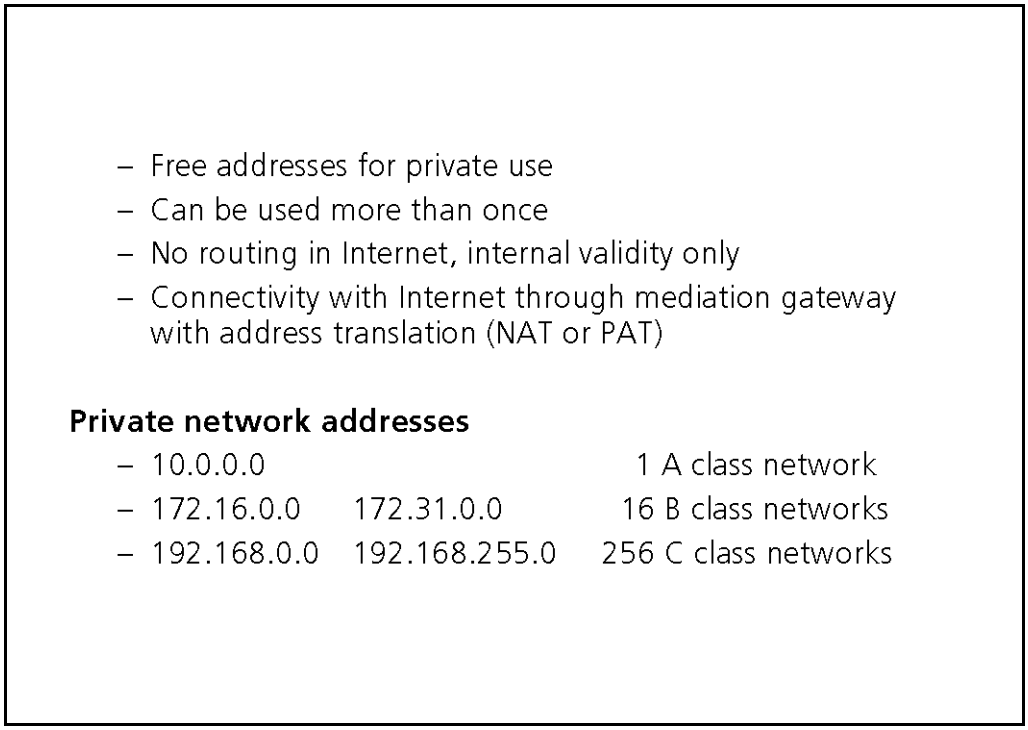
Les bits réseau à "0" signifie qu'on reste à l'intérieur du réseau (adresse locale).

255.255.255.255 ne permet heureusement pas de faire une diffusion générale, les routeurs ne routant pas cette adresse, elle correspond à une diffusion locale. Broadcast

0.0.0.0 indique une machine ne possédant pas (encore) d'adresse IP.

les adresses 127.0.0.0 sont utilisées pour des tests de boucle (gén.127.0.0.1) Loopback

6.1.5 Adresses privées IPv4



Slide 6.7
Adresses privées IPv4

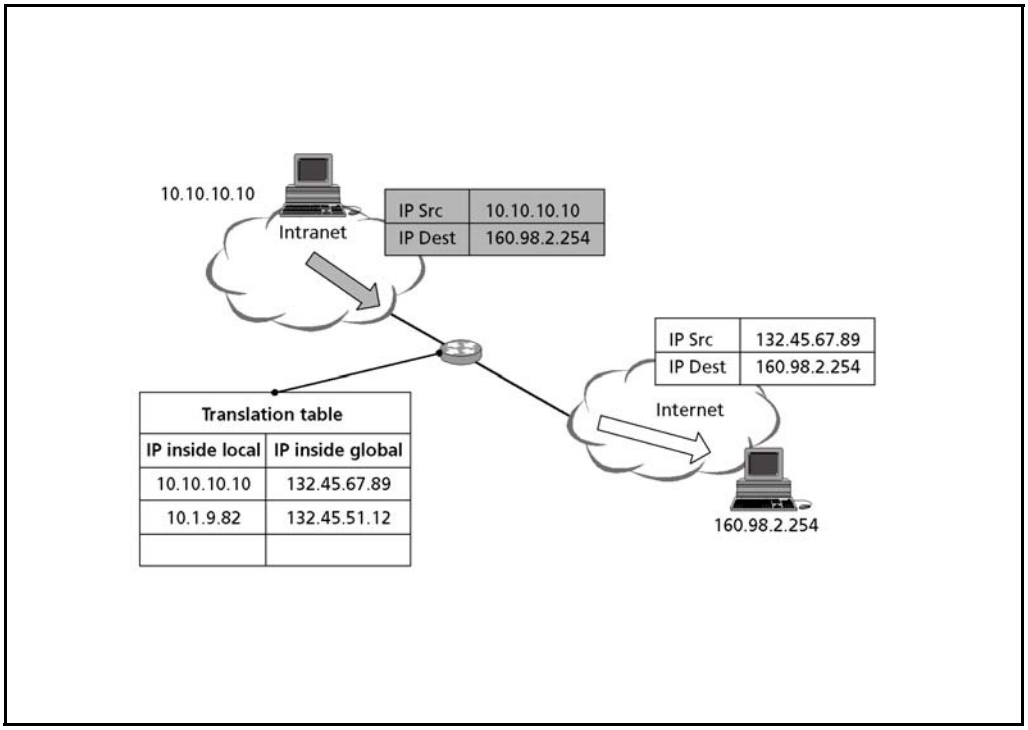
Une autre solution à la saturation des adresses IP est l'utilisation d'adresses privées. Ces adresses sont libres d'utilisation pour les réseaux locaux (LAN). Elles vont donc pouvoir être utilisées plusieurs fois dans le monde. [RFC 1918]

NAT, PAT

Elles ne sont pas supportées par Internet, mais la connectivité peut être assurée par une translation d'adresse (NAT, Network Address Translation) ou une translation de ports et d'adresses (PAT, Port Address Translation).

Ces solutions permettent d'utiliser un grand réseau en interne (A ou B) est de n'avoir qu'un réseau plus modeste pour la connectivité. Le PAT permet même de n'utiliser qu'une seule adresse pour toute une entreprise (Intranet de Swisscom).

6.1.6 Translation d'adresse, NAT



Slide 6.8
Translation d'adresse, NAT

Un paquet IP est émis par le PC 10.10.10.10 à destination d'une machine distante 160.98.2.254. Il traverse son intranet sans problème, jusqu'au routeur de sortie. Là un problème se pose : son adresse source n'est pas valable dans l'Internet.

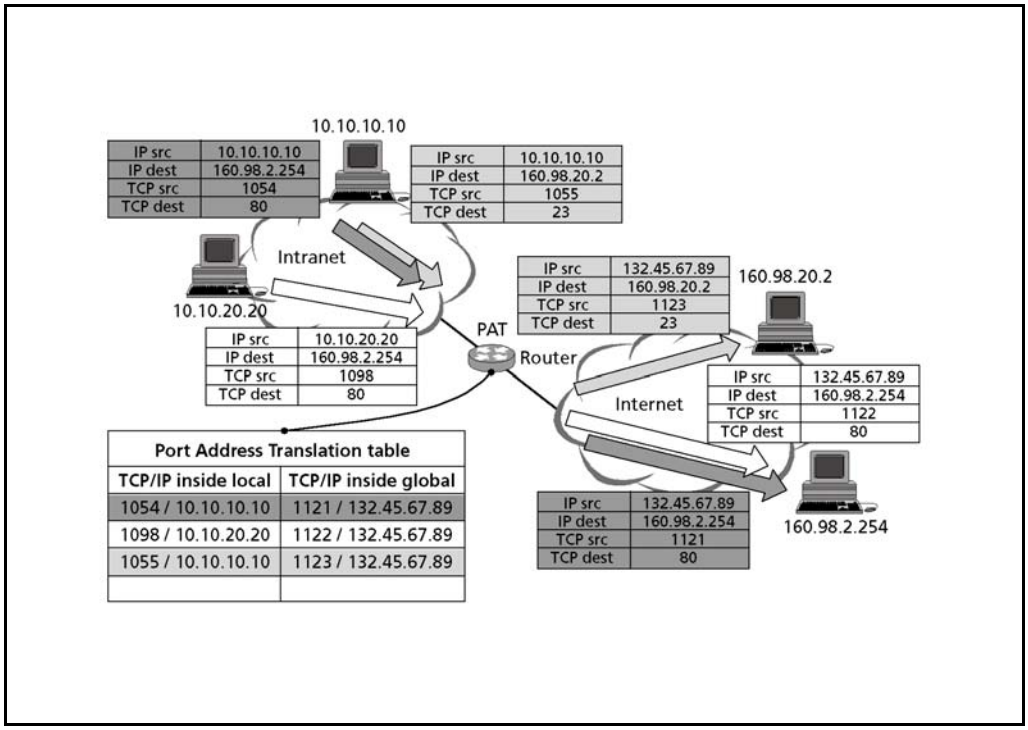
Le routeur modifie le paquet en affectant une adresse publique disponible à l'adresse interne. Il mémorise la correspondance dans sa table de translation. Ceci réserve l'adresse publique. Le paquet peut ensuite traverser l'Internet.

L'affectation d'une adresse externe à une adresse interne est univoque, les réponses subiront la modification inverse. Lorsque le PC n'engendre plus de trafic, l'entrée de la table est effacée et l'adresse libérée. [RFC 1631, 2663]

Dans le cas où notre adressage interne utilise un réseau A, seuls 65534 clients pourront simultanément sortir dans l'Internet. Ceci parce que nous utilisons un réseau B pour la translation des adresses.

Le détail de la terminologie sur le NAT sera vu dans la pratique, au chapitre 16.6.3.

6.1.7 Translation d'adresse de port , PAT



Slide 6.9
Translation d'adresse de port, PAT

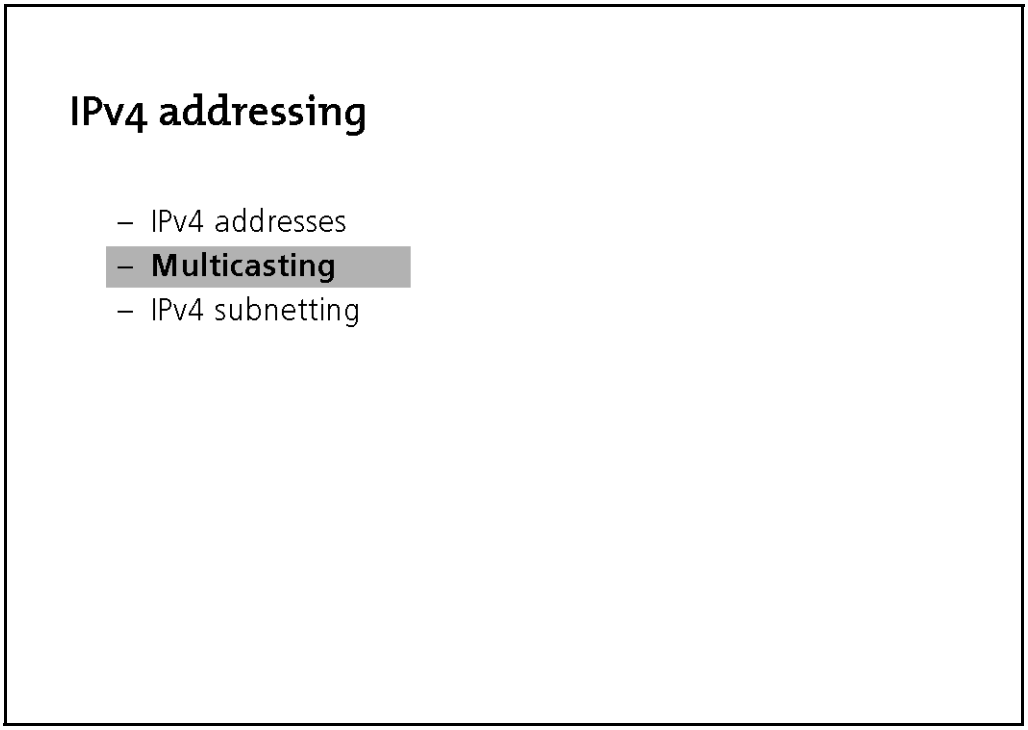
La translation d'adresse de port (PAT, Port Address Translation) permet d'utiliser minimum une seule adresse IP. Le routeur affecte pendant la durée de transmission un couple "adresse externe / port TCP libre" à "adresse interne / port TCP source" de l'initiateur de la communication. Ces couples sont nommés "sockets".

Socket

Chaque socket est unique. Côté Internet c'est uniquement la valeur du port qui différencie ces sockets, alors que dans l'Intranet on doit analyser les deux grandeurs port et adresse pour les reconnaître.

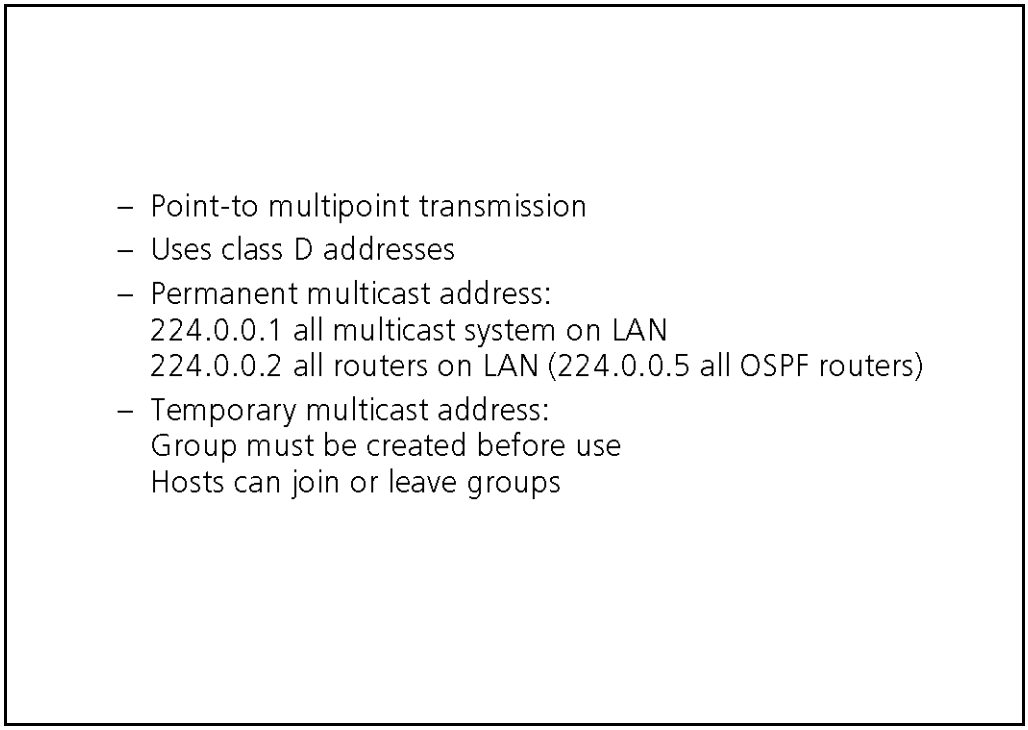
A noter que le routeur PAT est en fait un gateway, travaillant sur la couche transport. Généralement, le PAT est intégré dans l'application "Proxy".

6.2 Multicasting



Slide 6.10
Multicasting

6.2.1 IPv4 Multicasting



Slide 6.11
IPv4 Multicasting

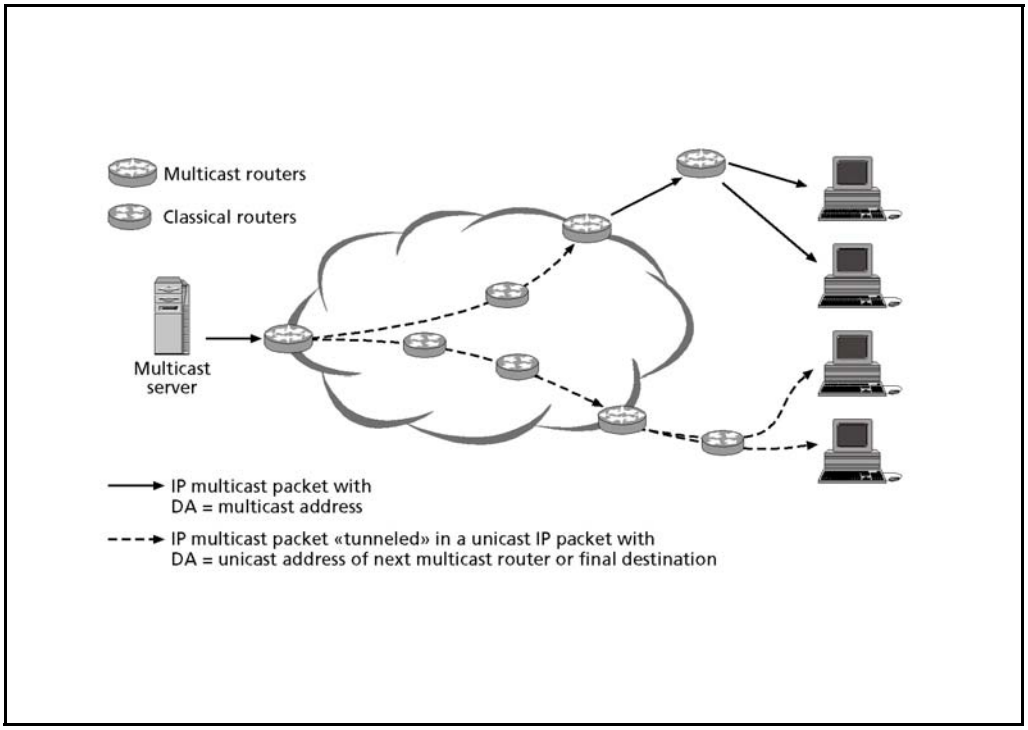
Classe D

Le multicasting consiste à envoyer un paquet IP à plusieurs hosts de manière simultanée. Les routeurs multicast possèdent plusieurs directions pour une adresse multicast (adresses de classe D) et dupliquent le paquet pour chacune d'elles.

Des adresses permanentes ont étés définies (224.0.0.1/.2/.5) représentant un "public cible" défini.

Les autres adresses peuvent être utilisées afin de créer des groupes dédiés, par exemple pour une audio ou vidéo conférence. Le groupe devra être créé avant d'être utilisé. Une fois le groupe disponible, les hosts peuvent à tout moment s'y joindre ou s'en retirer.

6.2.2 IPv4 Multicasting : Tunneling



Slide 6.12
IPv4 Multicasting : Tunneling

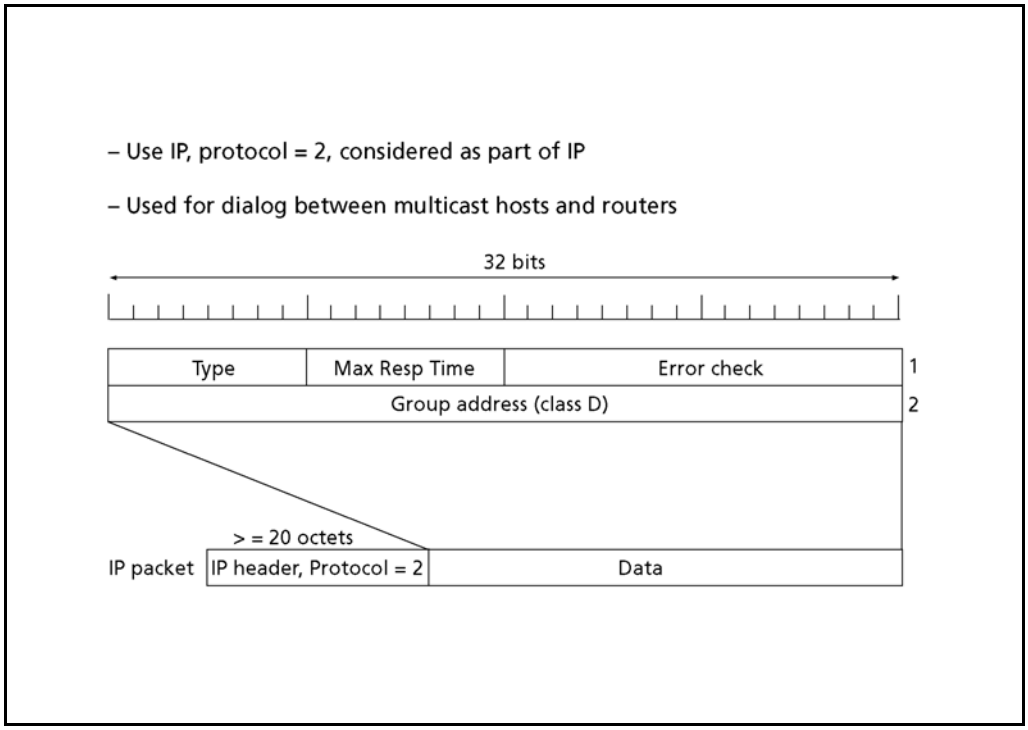
Tunneling

Tous les routeurs ne supportent pas les adresses multicast. Pour contourner cette difficulté, on crée un tunnel entre les routeurs multicast.

On procède en encapsulant le paquet IP multicast dans un paquet IP unicast, dont la destination est le prochain routeur multicast. De cette manière, les routeurs unicast acheminent un paquet IP classique, sans travaux de duplication, au prochain routeur multicast.

Une fois ce paquet reçu, le routeur multicast le "déballe" est voit le paquet multicast. Il peut donc le renvoyer partout où cette information est attendue. Les routeurs multicast dialoguent entre eux à l'aide de protocoles de routage spécifiques (DVMRP, MOSPF).

6.2.3 IGMP (Internet Group Management Protocol)



Slide 6.13
IGMP (Internet Group Management Protocol)

IGMP

IGMP est le protocole utilisé par les routeurs multicast pour dialoguer avec les hosts.

Il est directement transporté par IP (protocol=2) et est considéré comme une de ces parties. Il est décrit dans [RFC 2236]

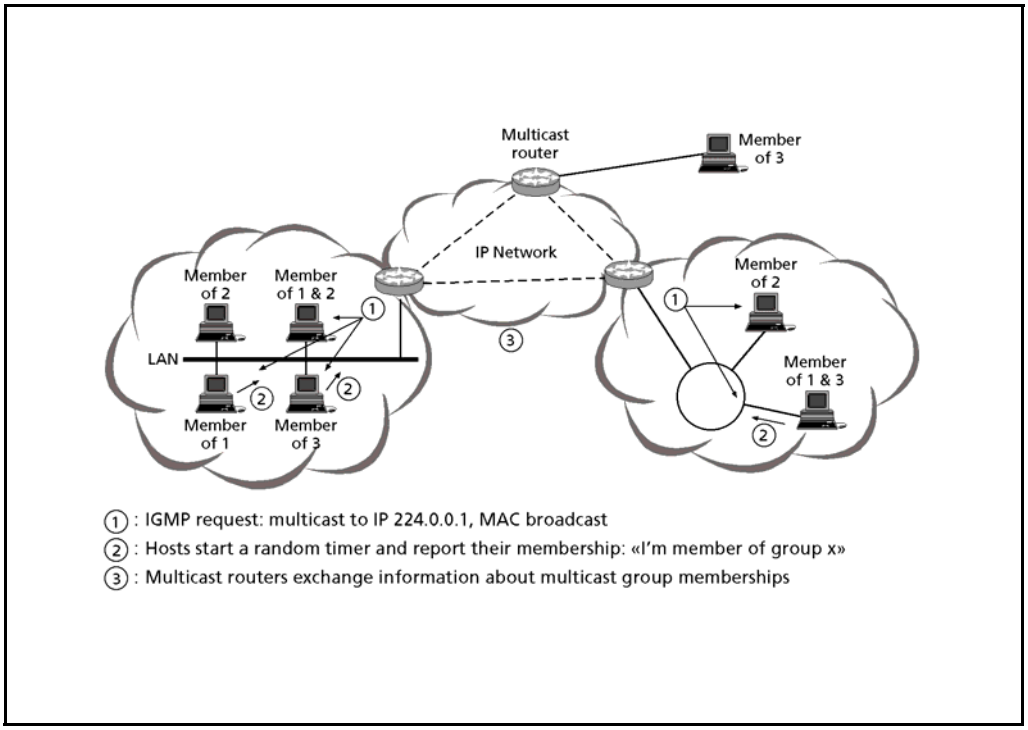
Type définit s'il s'agit d'une question, réponse ou encore annonce de retrait.

Max resp time est le temps (en 10èmede sec.) laissé par le routeur aux hosts pour répondre. Ce champ n'est utilisé que dans les questions.

Error check est une somme de contrôle.

Group address contient la réponse du host, sous forme d'une adresse de classe D.

6.2.4 Exemple IGMP



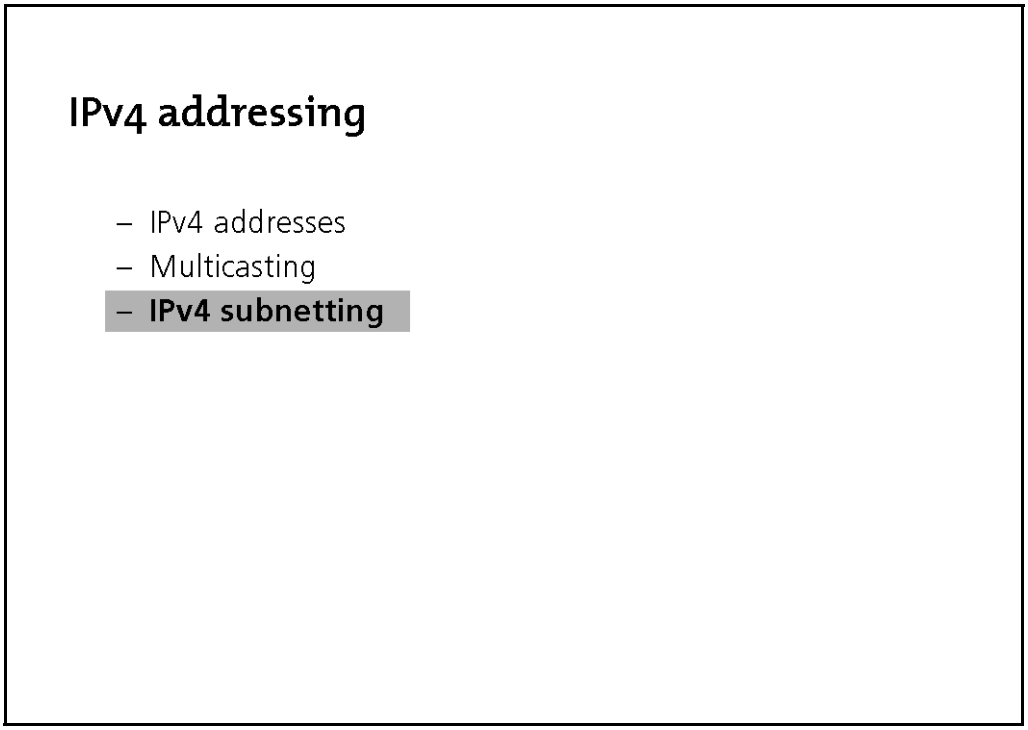
Slide 6.14
Exemple IGMP

Les routeurs multicast questionnent régulièrement les hosts sur leur appartenance à un groupe multicast. Ils utilisent alors une question IGMP (query, type=0x11), qu'ils envoient à l'adresse 224.0.0.1 (en broadcast MAC).

Les hosts appartenant à un groupe répondent au routeur (report, type=0x16), en indiquant l'adresse de classe D correspondante. Cette réponse est donnée après un temps aléatoire mais avant le délai imposé. Un host appartenant à plus d'un groupe donnera autant de réponses. Ces informations sont ensuite échangées entre les routeurs multicast par les protocoles de routage multicast.

Un host quittant un groupe l'indiquera à son routeur multicast par un message IGMP "leave group" (Type=0x17).

6.3 IPv4 Subnetting



Slide 6.15
IPv4 Subnetting

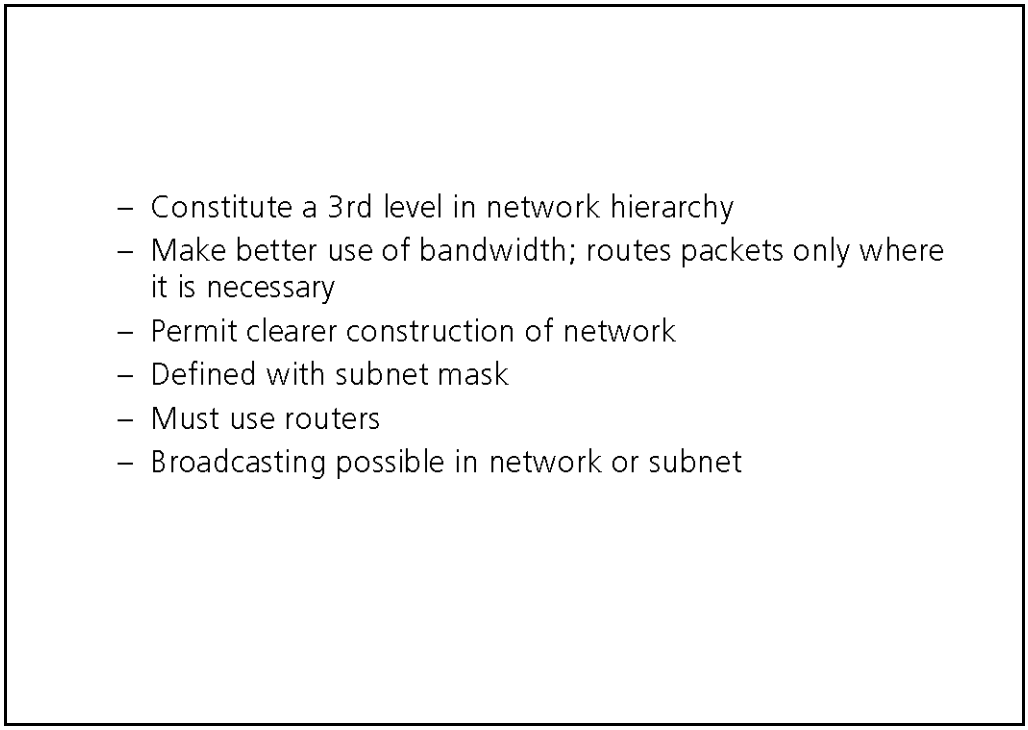
Subnet

Afin de simplifier la gestion d'un réseau, on peut partager ce réseau en entités plus petites, appelées sous-réseaux (subnets).

Nous allons étudier ici le fonctionnement et la construction de ces sous-réseaux.

Ceci est décrit dans [RFC 950]

6.3.1 Sous-réseaux



Slide 6.16
Sous-réseaux

L'utilisation de sous-réseaux crée un troisième niveau hiérarchique, entre le réseau et le client. Elle permet une meilleure utilisation de la bande passante. En effet, les paquets IP ne vont circuler que là où c'est nécessaire, libérant ainsi les ressources des autres sous-réseaux.

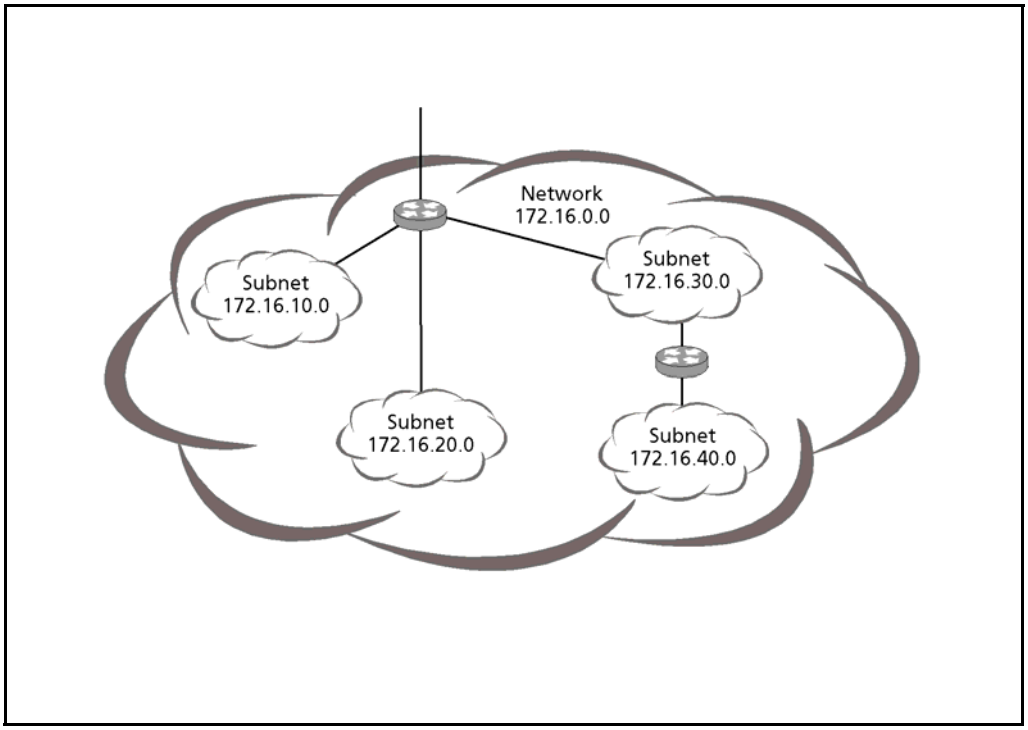
On peut, grâce aux sous-réseaux, construire notre réseau à l'image du bâtiment qui l'abrite, rendant les travaux d'entretien et d'extension plus simples.

Subnet mask

Les sous-réseaux sont définis à l'aide d'un masque spécifique (Subnet mask), ils nécessitent l'utilisation de routeurs.

La diffusion dans le réseau reste possible. On ajoute à cela une diffusion propre aux sous-réseaux.

6.3.2 Sous-réseaux : Exemple



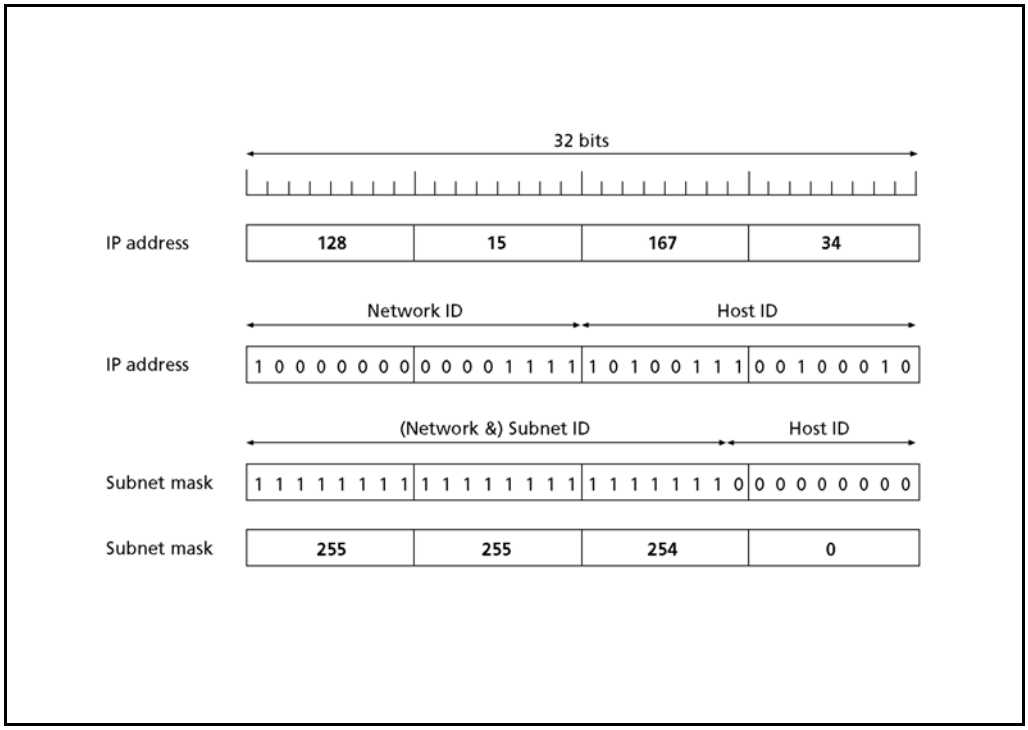
Slide 6.17
Sous-réseaux : Exemple

Pour construire une adresse de sous-réseau on doit utiliser une partie de l'adresse client.

Dans notre exemple un réseau de classe B (172.16.0.0) est divisé en quatre sous-réseaux. Ils se différencient par le 3ème octet de leur adresse IP (172.16.XX.0). Cet octet fait pertie de la partie client d'une adresse "B".

Un paquet qui arrive de l'Internet dans le routeur d'entrée sera directement acheminé par celui-ci dans le bon sous-réseau. Notons qu'il devra toutefois traverser le sous-réseau 172.16.30.0 afin d'atteindre un client de 172.16.40.0

6.3.3 Masque de sous-réseau



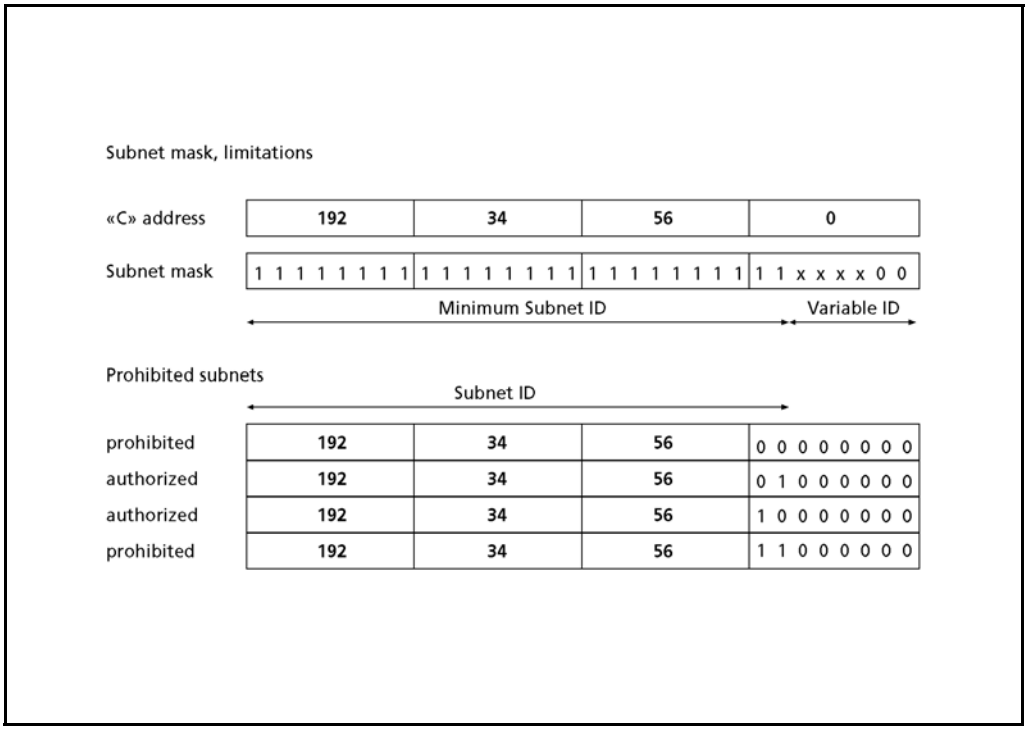
Slide 6.18
Masque de sous-réseau

Le masque de sous-réseau est, à l'instar d'une adresse IP, long de 32 bits. C'est d'abord une succession de "1", qui montrent la présence des bits réseau et sous-réseau. C'est ensuite, dès le passage de "1" à "0", des "0" qui indiquent la partie client de l'adresse.

Cela implique que seules les valeurs : 255, 254, 252, 248, 240, 224, 192, 128 et 0 sont possibles pour le masque.

On notera que dans cet exemple on a allongé de 7 bits l'adresse réseau pour en faire une adresse sous-réseau, ne laissant au client que 9 bits, à cheval entre deux octets. On a ici à faire au PC 0.0.1.34 du sous-réseau 128.15.166.0. Dans ce cas la lisibilité de l'adresse n'est pas évidente, ceci est du à la notation "pointé décimal".

6.3.4 Sous-réseaux : Limitations



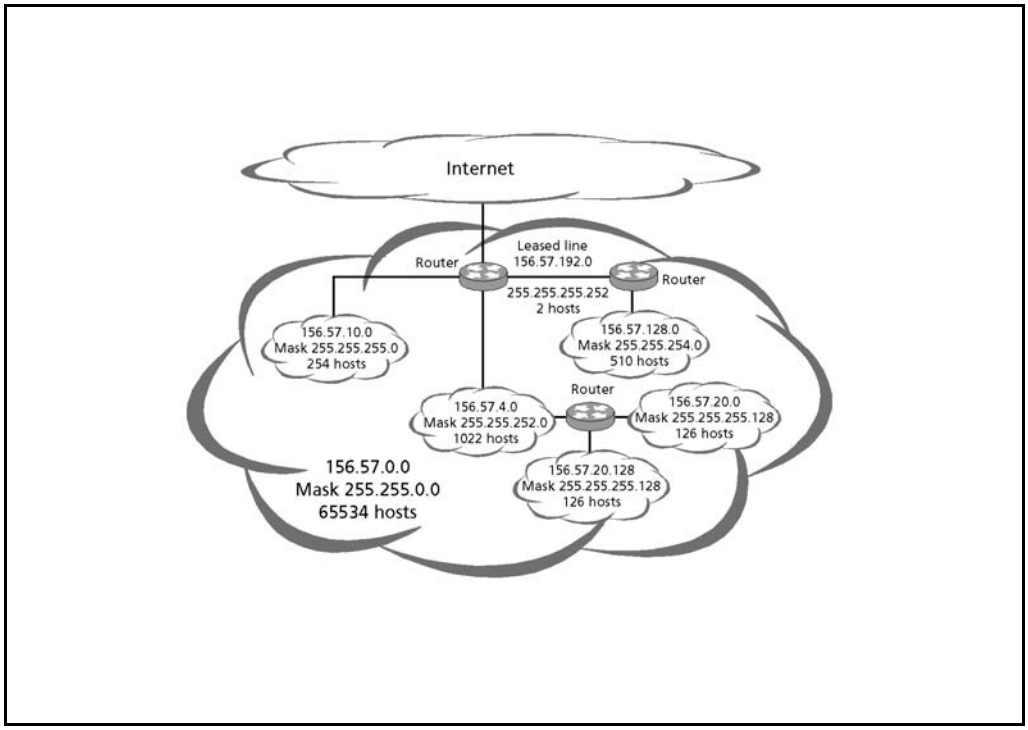
Slide 6.19
Sous-réseaux, limitations

Deux limites se posent à la définition d'un masque de sous-réseaux :

1. Il faut laisser au minimum 2 bits pour les clients, de manière à trouver 4 adresses, le sous-réseau, l'adresse de diffusion et deux adresses "client" utiles. Avec 1 bit nous n'aurions pas d'adresses utiles !
2. la partie sous-réseau doit avoir au minimum 2 bits de long. En effet, comme indiqué dans la 2ème figure, le 1er et le dernier sous-réseaux créés ne sont pas autorisés. Le 1er possède la même adresse que le réseau et dans le cas du dernier, c'est l'adresse de diffusion qui est commune. Avec 1 bit on ne créerait que les deux sous-réseaux interdits !

On peut toutefois relever que le premier sous-réseau est de plus en plus utilisé avec des protocoles et algorythmes de routage modernes. L'utilisation du dernier sous-réseau, quant à elle, reste encore aujourd'hui un sujet "tabou".

6.3.5 Masques de sous-réseau : Exemple



Slide 6.20
Masques de sous-réseau : Exemple

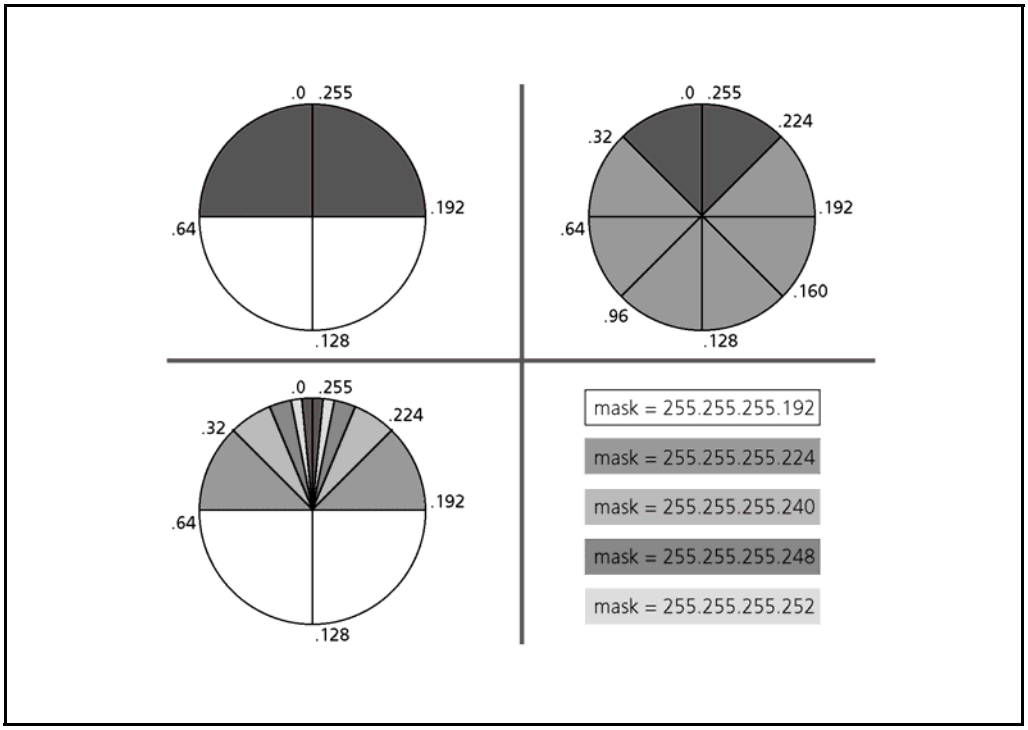
Nous pouvons définir des masques de sous-réseau différents pour chaque sous-réseau, à condition qu'il n'y ait pas de recoupement dans les zones d'adressage.

En haut à droite, on trouve une ligne louée, c'est à dire une ligne point à point sur laquelle il ne peut y avoir que deux clients. Il est donc logique de trouver ici un masque forçant l'étendue réseau à deux clients seulement, dans l'esprit d'économiser au maximum l'espace d'adressage disponible.

On notera encore que les deux réseaux en bas à droite sont directement consécutifs.

Afin de contrôler l'absence de recoupement, on aimera certainement recourir à une représentation graphique. La page suivante représente, sous forme graphique, plusieurs possibilité de "découper" un réseau de classe C.

6.3.6 Subnetting avec masque variable



Slide 6.21
Subnetting avec masque variable

Dans le cas des réseaux de classe C, l'espace d'adressage est très limité. Seul un octet est disponible à l'utilisateur pour construire ses sous-réseaux et adresser ses machines.

mask 255.255.255.192

Avec un masque de 255.255.255.192, on fabrique deux (4-2) sous-réseaux pour 62 machines. Malheureusement, avec les restrictions d'utilisation des sous-réseaux, la moitié de l'espace d'adressage se trouve être dans des sous-réseaux "interdits" (gris foncé).

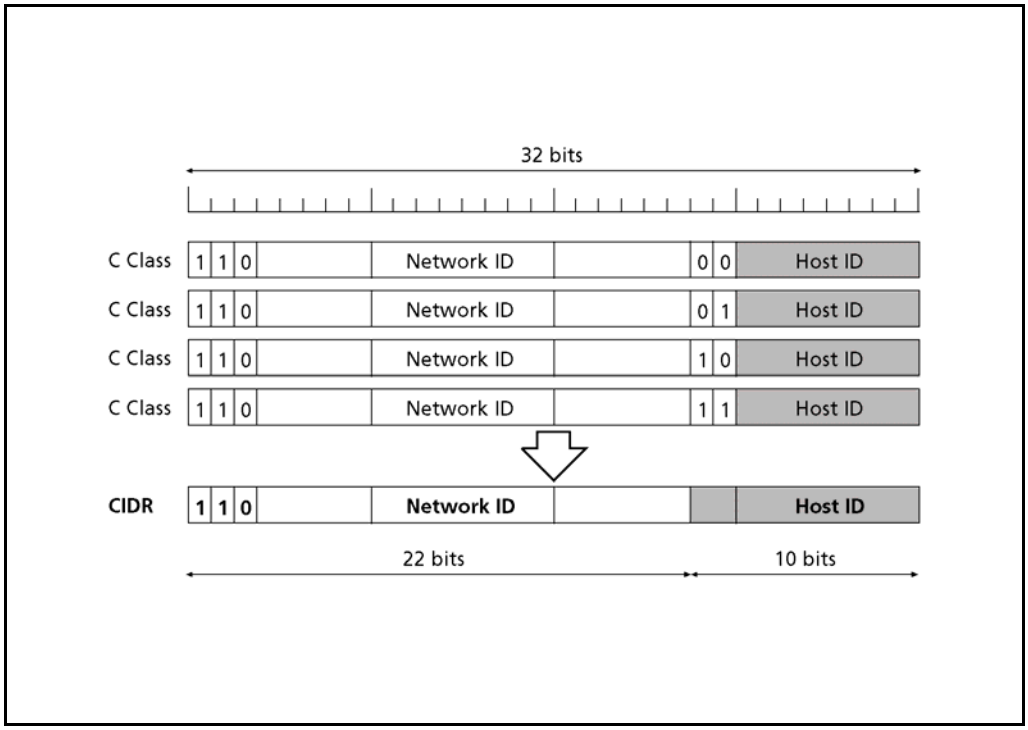
mask 255.255.255.224

Avec 255.255.255.224, les six (8-2) sous-réseaux acceuillent 30 machines. Ce sont des sous-réseaux plus petits, mais qui occupent cette fois les 3/4 de l'espace d'adressage.

variable mask

Afin d'utiliser au maximum l'espace d'adressage d'un tel réseau, nous utiliserons volontiers la possibilité des masques de sous-réseaux variables. La dernière représentation montre comment faire les plus grands sous-réseaux, en utilisant la plus grande proportion de l'espace d'adressage. Cet exemple est disponible de manière complète dans l'annexe 19.7.

6.3.7 Supernetting : CIDR (Classless Interdomain Routing)



Slide 6.22
Supernetting, CIDR

CIDR, Classless Interdomain Routing

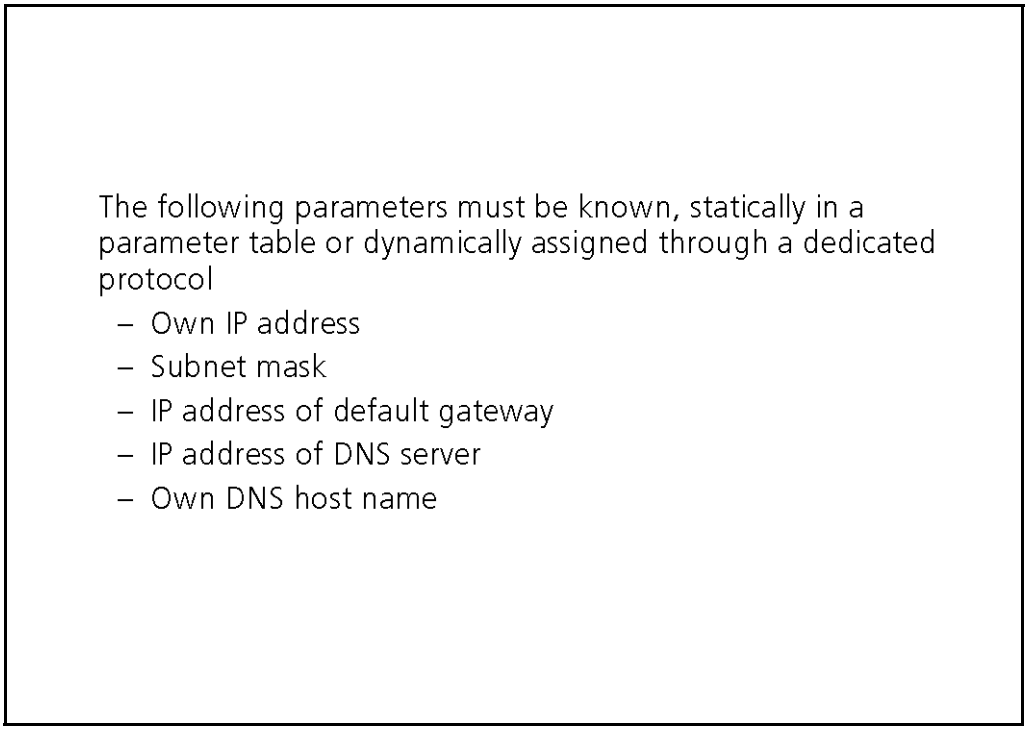
Afin de rendre les réseaux de classe C plus attractifs, on a autorisé la distribution de réseaux C successifs. Dans notre exemple, un bloc de 4 réseaux C sont regroupés en une seule adresse réseau de 22 bits. ces nouveaux réseaux, appelés CIDR, ont une capacité de 1 022 hosts, ce qui devient suffisant pour un grand nombre de sociétés. [RFC 1518, 1519]

Supernetting

On utilise un masque de réseau exceptionnellement plus court afin de partager les réseaux C des réseaux CIDR. Ce principe s'appelle le supernetting.

La grande quantité de réseau C ou CIDR à router auraient pu poser des problèmes à nombreux routeurs. Afin de faciliter le routage de ces réseaux, on a attribué les adresses restantes par continent et par pays. Cela permet de router par groupe d'adresse plutôt que par adresses individuelles, réduisant d'autant la taille des tables des routeurs.

6.3.8 Configuration IP d'un host



Slide 6.23
Configuration IP d'un host

IP Config

Afin de pouvoir communiquer sur son réseau, un host Internet doit connaître sa propre adresse IP et le masque de son sous-réseau. L'adresse de son routeur de sortie est nécessaire également. Sans cette adresse, le host est confiné à l'intérieur de son sous-réseau.

En outre, afin de pouvoir "surfer" sur le net, l'utilisateur appréciera de travailler avec les noms des machines (www.swisscom.com, par exemple). Pour cela il faut que sa machine connaisse son nom DNS et l'adresse de celui qui va lui traduire les noms logiques en adresses IP, le serveur DNS local.

Ces paramètres peuvent être enregistrés de manière statique dans la machine, ou lui être livré par un protocole spécialisé lors de son démarrage (boot).

7 Résolution et configuration d'adresses

TCP/IP advanced and practical

Introduction & concepts (1)
Data Link Layer (2-4)
Network Layer (5-8)
- Network Protocol IPv4 (5)
- IPv4 addressing (6)
- **Address Resolution & Configuration Protocols (7)**
- ICMP (Internet Control Message Protocol) (8)

IPv6 (9-10)
Routing (11-12)
Transport Layer (13)
Application Layer (14)

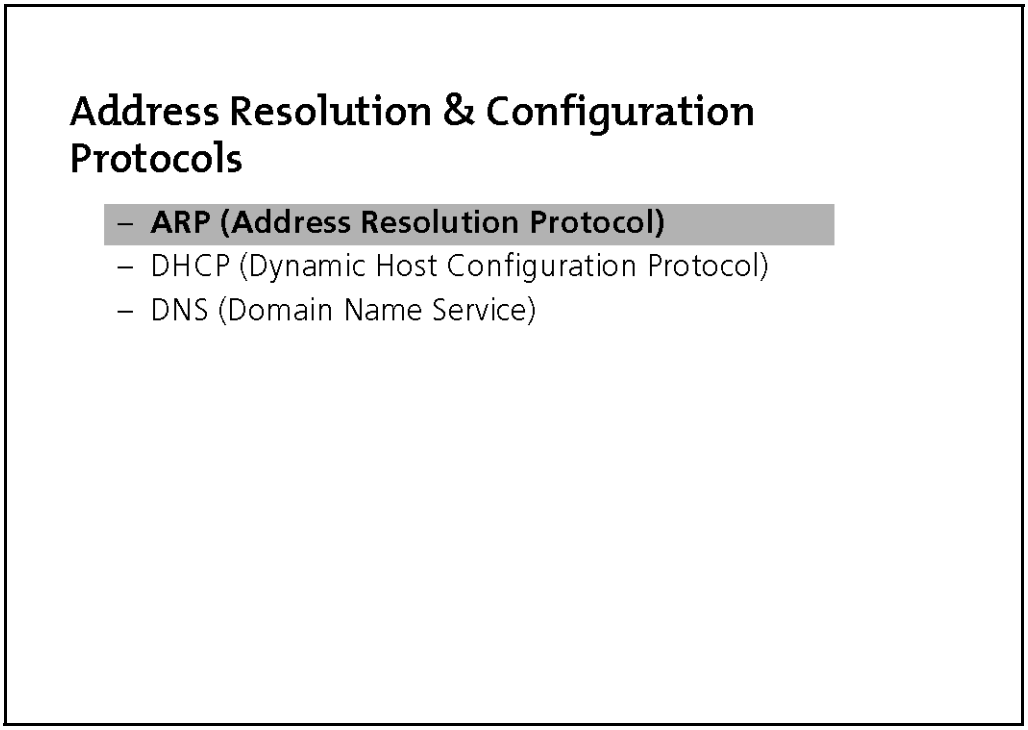
Slide 7.1
Résolution et configuration d'adresses

Ce chapitre traite des différents protocoles permettant de résoudre une adresse IP, depuis des infos de couches inférieures ou supérieures.

Objectifs

A l'issue de ce chapitre, les participants sont capables d'expliquer le fonctionnement d'une requête ARP ou DNS. Ils sont en outre capable de d'identifier le fonctionnement d'une configuration dynamique à l'aide de DHCP.

7.1 ARP (Address Resolution Protocol)



Slide 7.2
ARP (Address Resolution Protocol)

La tâche de ARP (Address Resolution Protocol) est de fournir l'adresse MAC d'un host connu seulement par son adresse IP.

C'est généralement le cas du routeur de sortie.

ARP est décrit dans [RFC 826]

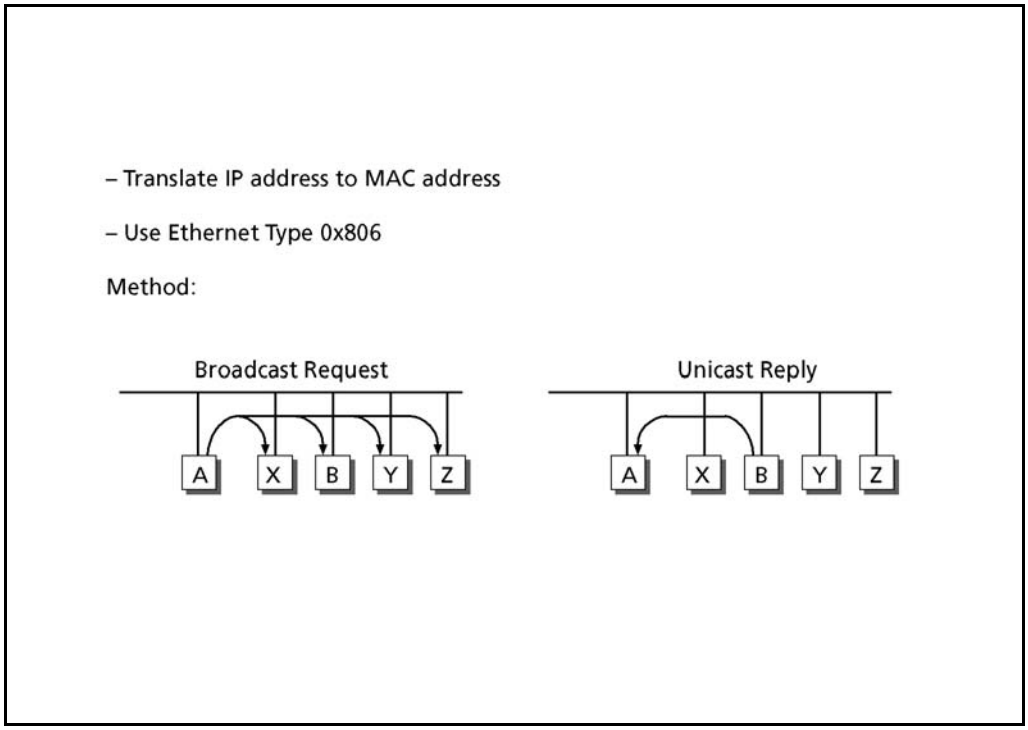
ARP

On regardera le principe de fonctionnement de RARP, effectuant le travail inverse.

RARP est décrit dans [RFC 903]

RARP

7.1.1 Protocole de résolution d'adresse : ARP



Slide 7.3
Protocole de résolution d'adresse : ARP

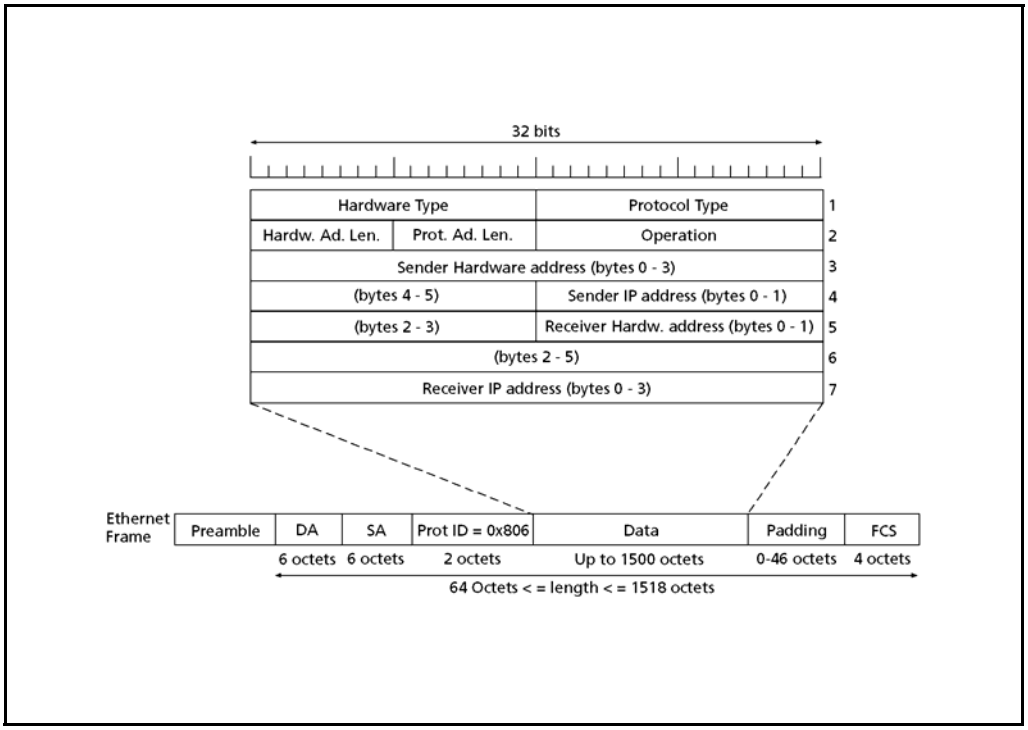
ARP est directement transporté par une trame Ethernet, où il est identifié par la valeur héxadécimale 806h.

MAC

Une requête est envoyée en diffusion générale dans notre sous-réseau (broadcast MAC). Cette requête peut être vue comme la question "Quelle est l'adresse MAC de celui qui s'appelle IP : xx.xx.xx.xx ?".

Toutes les machines du sous-réseau entendent cette question. Seule la machine qui reconnaît son adresse IP répond. Cette réponse est envoyée de manière unicast (adresses fournies dans la requête). Ces adresses sont stockées quelques minutes dans une table ARP (sous DOS, taper "arp -a" pour afficher cette table).

7.1.2 Format de paquet ARP



Slide 7.4
Format de paquet ARP

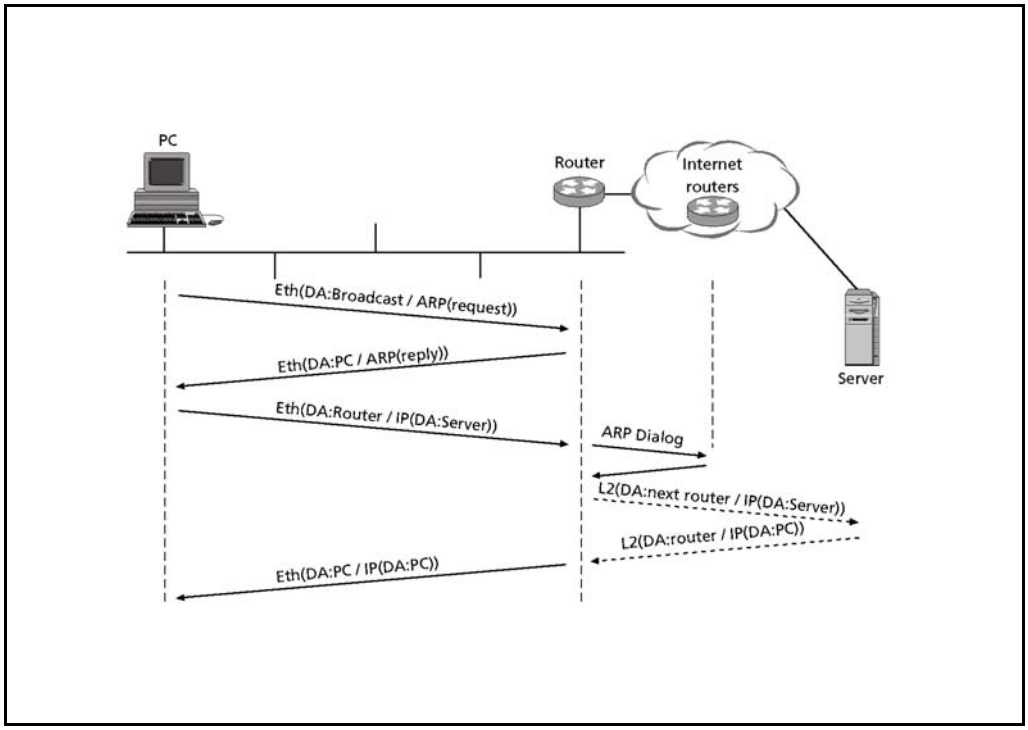
Le paquet ARP commence par une définition du hardware (couche 2, pour nous Ethernet) et du protocole (couche 3, pour nous IP) utilisés. Les champs suivants "x.Ad.Len" sont là pour préciser quelles sont les longueurs respectives de ces adresses (6 et 4 octets dans notre cas).

Le champ "OP" indique une requête ou une réponse (request=1, reply=2).

La fin du paquet ARP est un tableau contenant les 4 adresses concernées par cette requête (MAC et IP, de chacun des partenaires).

Dans la requête, le champ "Receiver Hardw. address" est laissé à "0". Il sera complété dans la réponse.

7.1.3 Exemple ARP



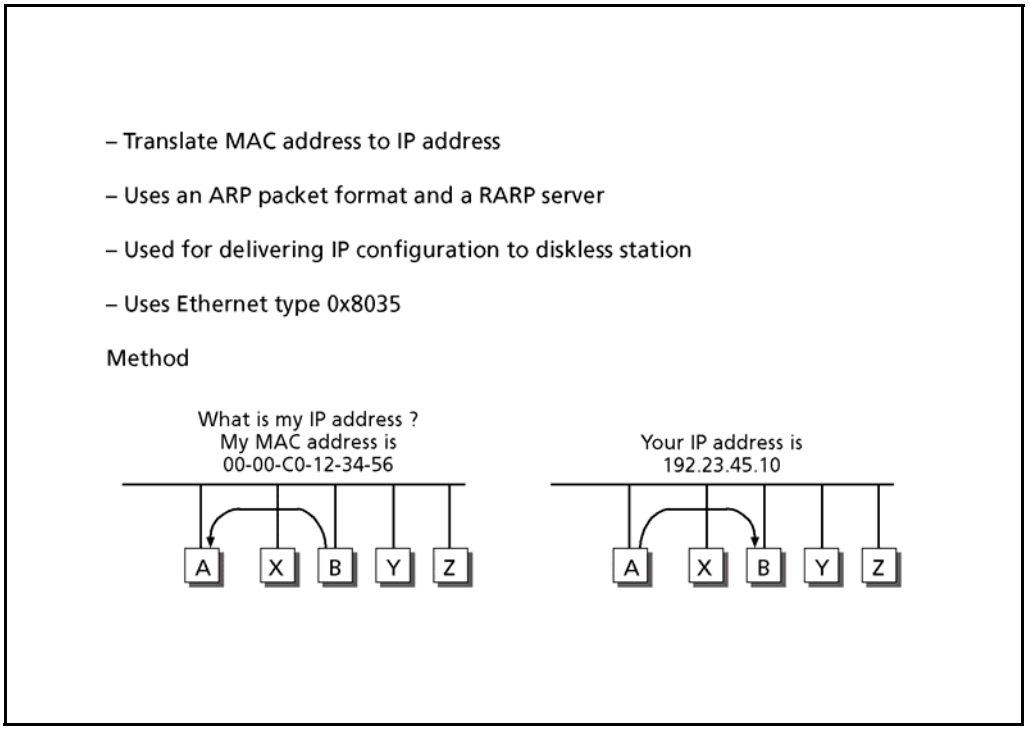
Slide 7.5
Exemple ARP

Un PC doit émettre un paquet IP à destination d'un serveur, à travers l'Internet. Afin de pouvoir le transmettre sur une trame Ethernet à son routeur, il doit en connaître l'adresse MAC. Or, dans sa configuration, il ne possède que son adresse IP. Il doit donc résoudre son adresse MAC. Pour cela, il utilise une requête ARP. Envoyée en broadcast, elle est reçue par le routeur. Il va répondre de manière unicast.

Une fois l'adresse MAC connue, notre paquet IP peut être émis en direction de notre serveur (couche 3 :IP), porté sur une trame à destination de notre routeur (couche 2 :MAC). Le routeur devra procéder de manière identique vis-à-vis du routeur suivant, et ainsi de suite.

Les éventuelles réponses "IP" n'engendreront pas ce trafic ARP, les adresses sont alors encore connues dans les tables.

7.1.4 Protocole inverse de résolution d'adresse : RARP

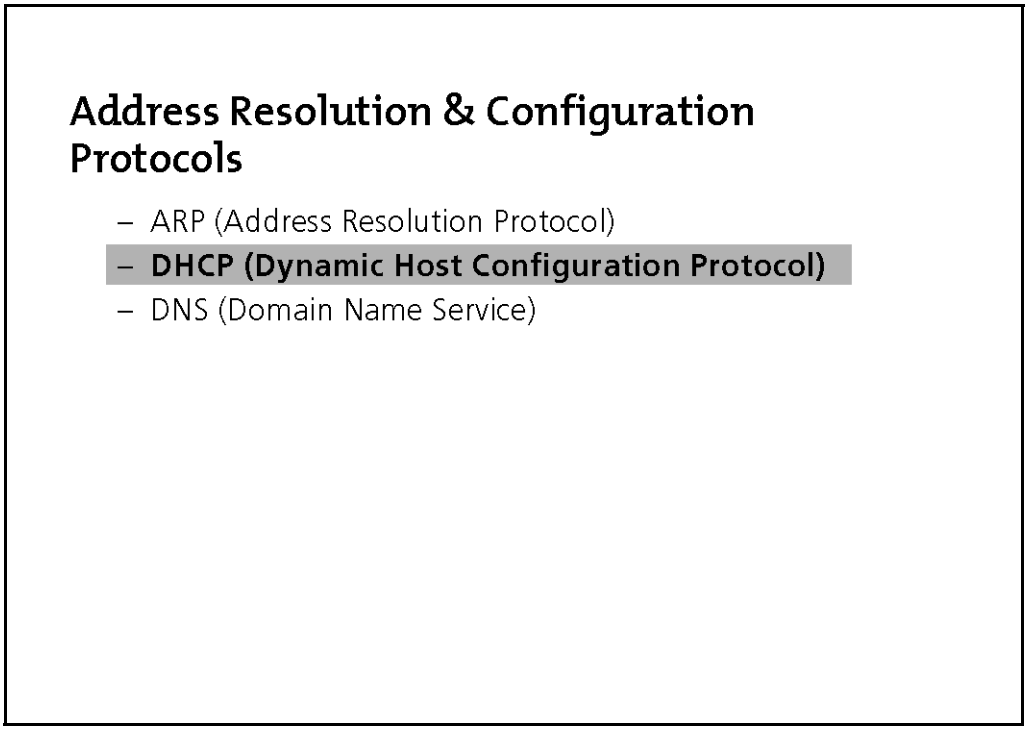


Slide 7.6
RARP

RARP est utilisé pour des machines sans disque. Au boot, ces machines ne connaissent que leur adresse MAC. Elles questionnent un serveur RARP, présent dans le sous-réseau, afin de connaître leur adresse IP. Le serveur RARP connaît les adresses IP des machines dont il est responsable. Il les reconnaît grâce à leur adresse MAC. Il leur répond en livrant leur adresse IP.

RARP utilise le format de paquet ARP. Les valeurs des requêtes et des réponses sont différentes (request=3, reply=4).

7.2 DHCP (Dynamic Host Configuration Protocol)



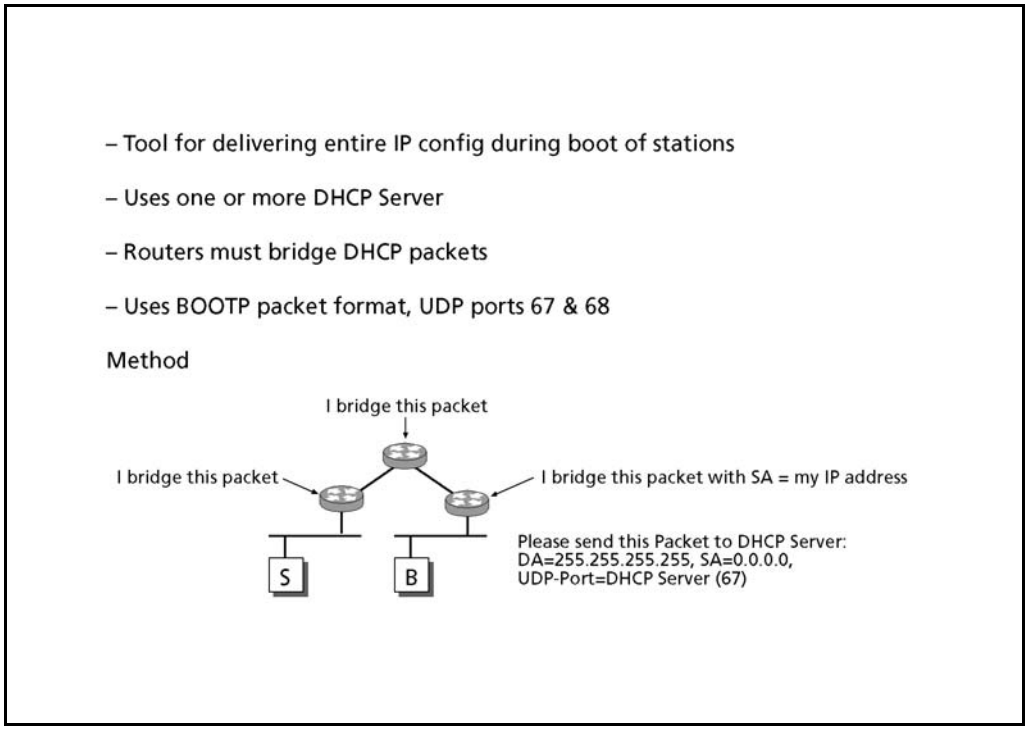
Slide 7.7
DHCP (Dynamic Host Configuration Protocol)

DHCP, BOOTP

DHCP (Dynamic Host Configuration Protocol) est un protocole servant à livrer dynamiquement des configurations à des machines. Il est une évolution d'un protocole appelé BOOTP et utilise son format de paquet.

Il est décrit dans [RFC 2131, 2132]

7.2.1 Configuration dynamique : DHCP



Slide 7.8
Configuration dynamique : DHCP

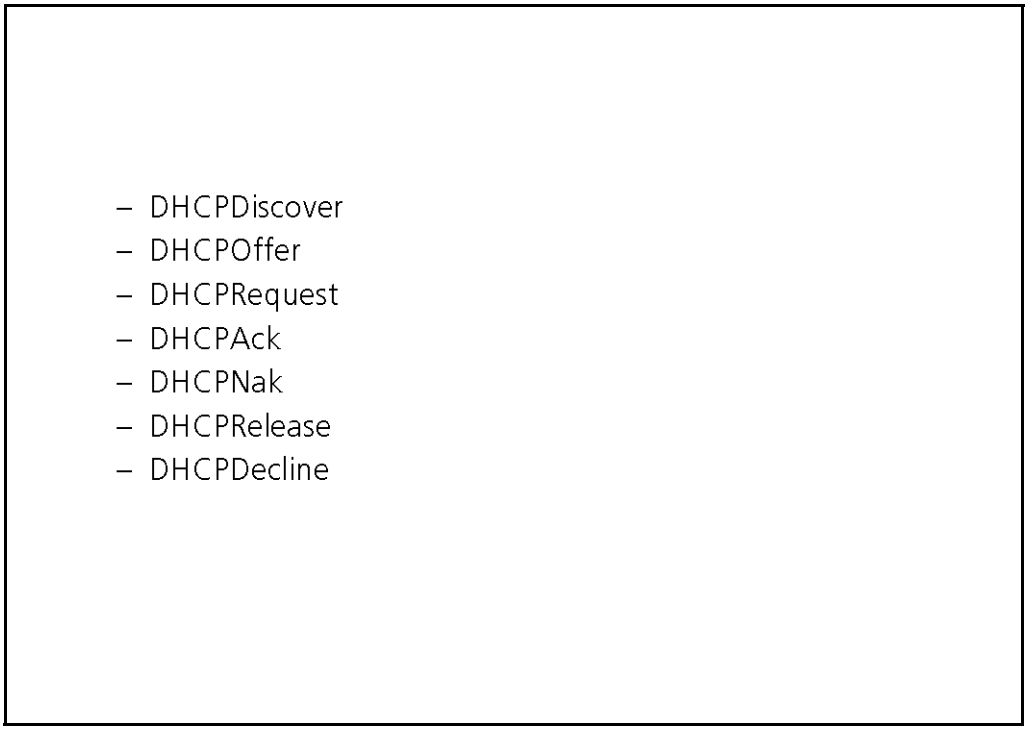
La machine pose la question "Quelle est ma config ?". Les routeurs bridgent cette requête en direction des différents serveurs DHCP. Chaque serveur va proposer une configuration.

La machine choisira une de ces configurations, libérant ainsi les autres propositions.

BOOTP Relay Agents

Les routeurs qui doivent bridger les paquets DHCP doivent être configurés de manière particulière. On les appelle des "BOOTP Relay Agents".

7.2.2 Messages DHCP



Slide 7.9
Messages DHCP

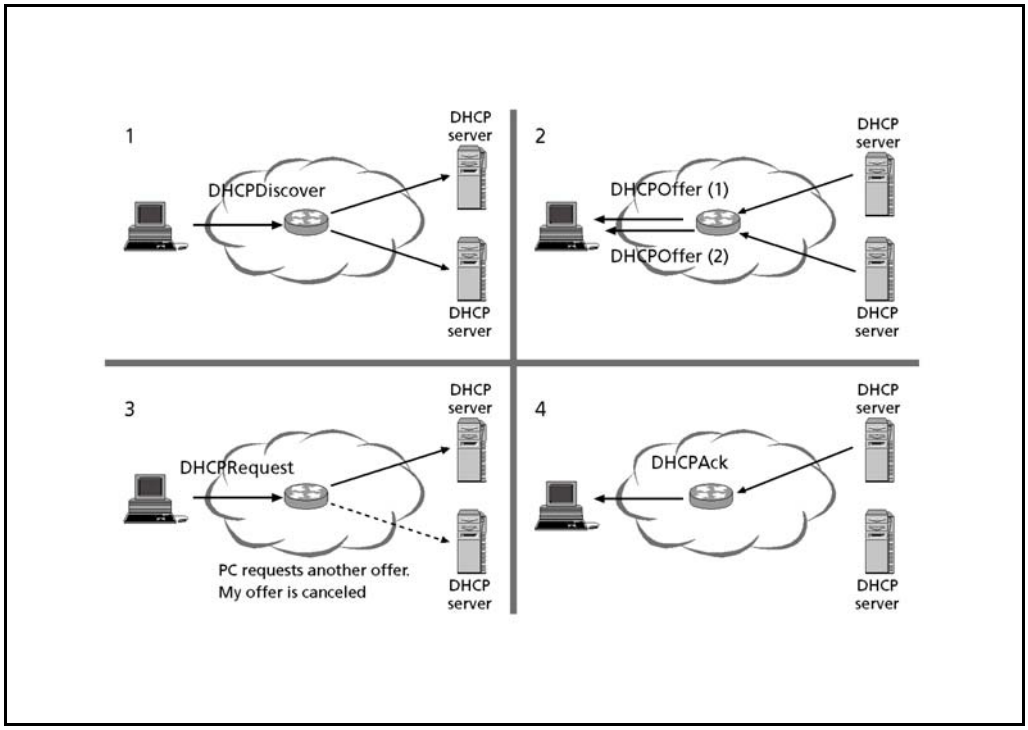
Les clients DHCP dialoguent avec les serveurs à l'aide d'une collection de messages.

DHCPDiscover demande une nouvelle config IP. DHCPOffer, sa réponse, propose une configuration. Généralement plusieurs configurations sont proposées par autant de serveurs. Notre machine va demander le droit d'utiliser l'une d'elles avec DHCPRequest. Cela lui sera accordé avec DHCPAck, ou refusé avec DHCPNak.

Au "shutdown", notre machine peut gracieusement rendre sa configuration avec DHCPRelease (non utilisé par Microsoft).

DHCPDecline sera utilisé par le PC pour signaler au serveur DHCP que la config proposée est déjà utilisée par une autre machine.

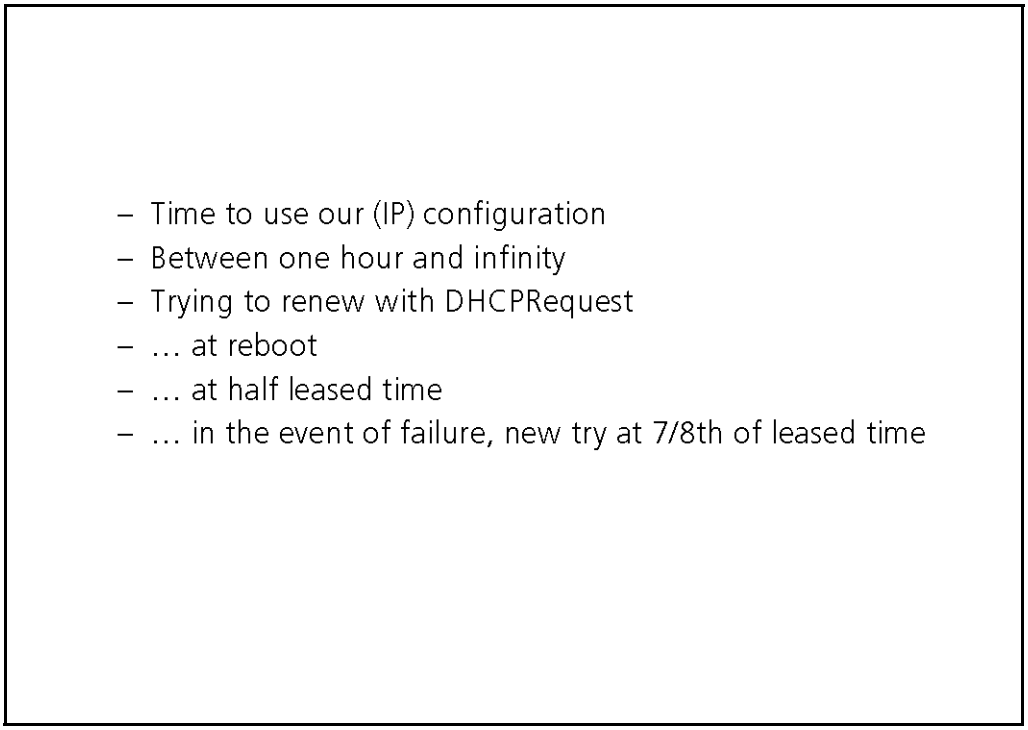
7.2.3 1ère initialisation DHCP : Exemple



Slide 7.10
1ère initialisation DHCP : Exemple

Le PC envoie un message DHCPDiscover pour demander une nouvelle configuration. Ce message est relayé par les "BOOTP Relay Agents" jusqu'aux serveurs DHCP. S'il leur reste des ressources, chacun d'eux va faire une proposition de configuration (DHCPOffer). Le PC attend que toutes les propositions soient arrivées avant d'en choisir une. Il demande le droit d'utilisation de cette configuration au serveur concerné avec DHCPRequest. Cette requête parvient également aux autres serveurs, qui en déduisent que leur offre est rejetée. Normalement, une confirmation DHCPAck est retournée au PC. Il se peut toutefois que la ressource proposée ait été attribuée entre temps. La norme DHCP n'impose pas au serveur de réserver une config. proposée. Le PC recevrait alors un DHCPNak.

7.2.4 Bail DHCP



Slide 7.11
Bail DHCP

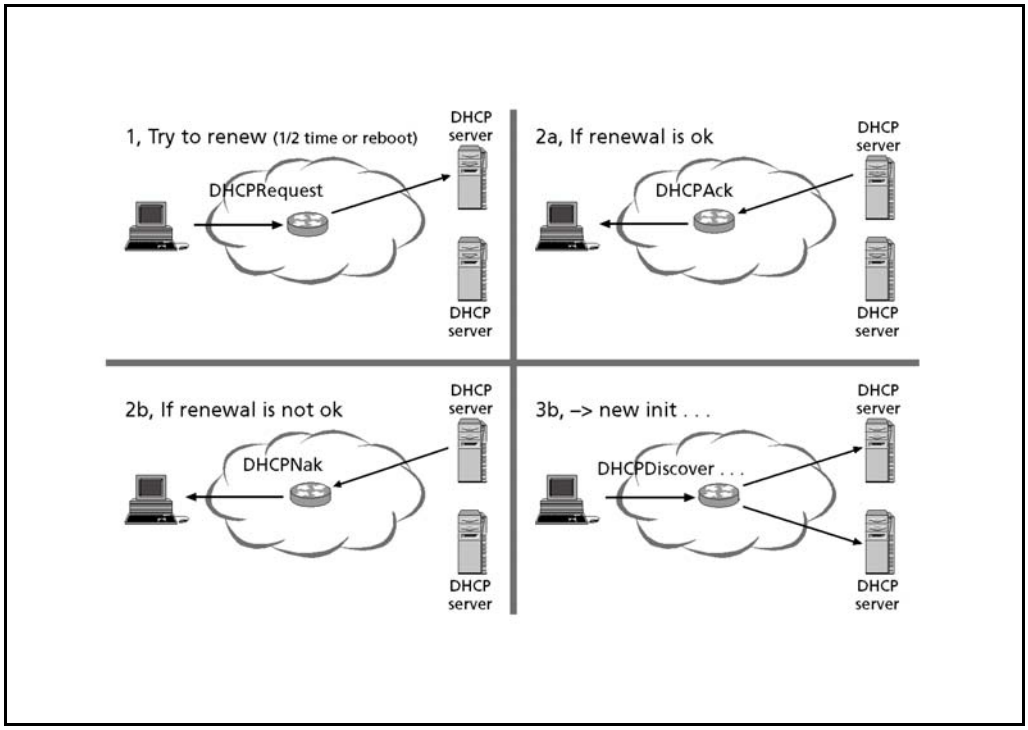
DHCP Lease

Chaque configuration DHCP est accompagnée d'un "bail". Il représente la durée durant laquelle on peut utiliser cette config. Pour palier aux problèmes de glissement entre les horloges des systèmes, le serveur enregistre un bail plus long que celui indiqué. Ce bail peut varier entre 1h et ~136ans (défini en seconde) !

Les machines vont tenter de renouveler leur bail au milieu de sa durée. En cas de non-réponse, elles continuent de l'utiliser jusqu'à 7/8ème du temps final. A ce moment, elles tentent une deuxième fois de le renouveler. En cas d'échec ou de non-réponse, les machines redémarrent une initialisation DHCP.

Lors du boot, les PC vont aussi tenter renouveler leur bail, avant de recommencer, en cas d'échec, une initialisation DHCP complète.

7.2.5 Renouvellement de bail DHCP : Exemple



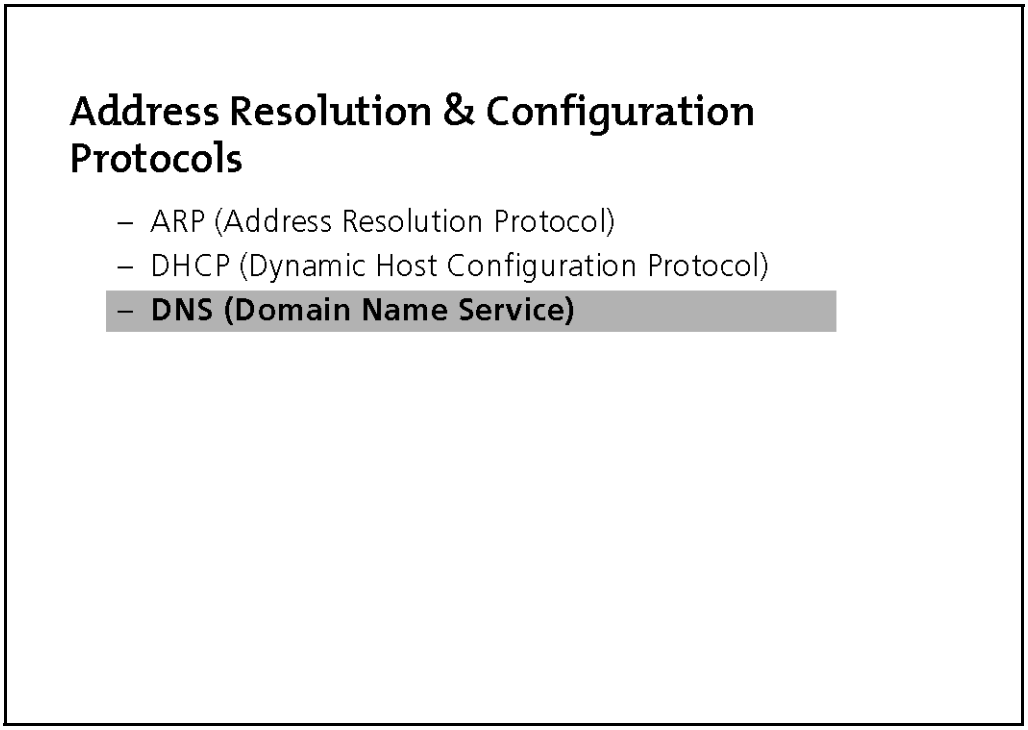
Slide 7.12
Renouvellement de bail DHCP : Exemple

Le renouvellement du bail se fait directement à l'aide du message DHCPRequest. Le bail sera renouvelé avec le message DHCPAck. Cependant une nouvelle durée peut être imposée.

Si le serveur détecte une incompatibilité (par ex. si le PC a été déplacé), il envoie un message DHCPNak. Ce dernier impose au PC de reprendre une procédure d'initialisation complète.

En cas de non-réponse, le PC peut continuer de travailler avec son adresse actuelle. Cependant on conseille d'envoyer un DHCPRelease et de recommencer une procédure d'initialisation.

7.3 DNS (Domain Name Service)



Slide 7.13
DNS (Domain Name Service)

Logical Name, IP Address

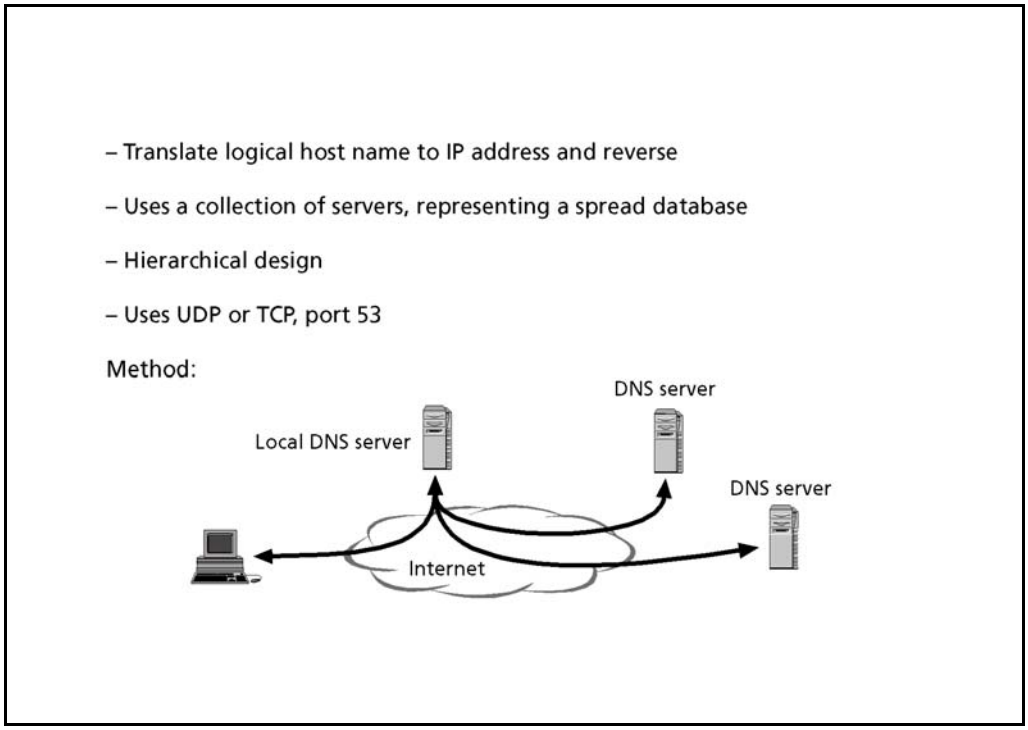
Afin de simplifier l'utilisation d'Internet, des noms logiques ont été attribués aux différentes machines présentes. Si pour nous l'utilisation de noms est plus claire que celle d'adresses IP, celles-ci sont toujours requises dans le réseau.

DNS

DNS définit la structure de ces noms, ainsi que la manière de lier un nom logique à une adresse IP (et inversement).

Il est décrit dans [RFC 1034, 1035] et complété par plusieurs autres RFC's.

7.3.1 DNS : Service de nom de domaine



Slide 7.14
DNS : Service de nom de domaine

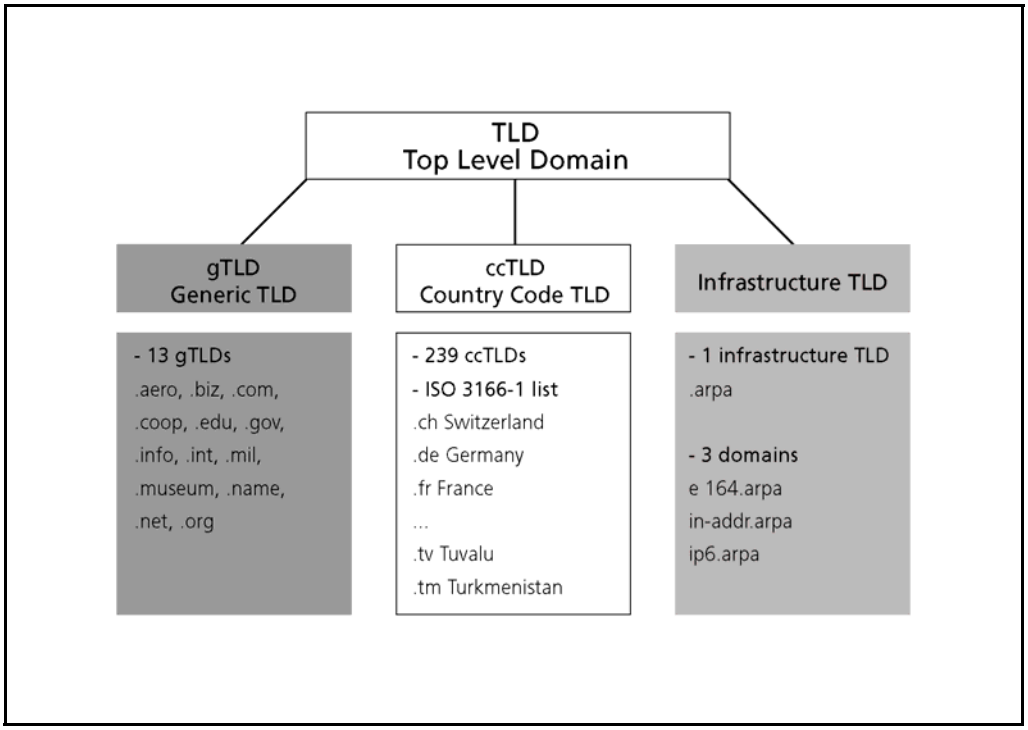
La quantité de noms à gérer est telle que seule une base de donnée répartie dans une collection de serveurs dédiés peut répondre au problème.

Chaque "host" connaît un point d'accès à cette base de donnée, son serveur DNS local. C'est lui qui assumera la recherche des adresses pour le host.

UDP, TCP

Il utilise UDP ou TCP, en fonction de l'implémentation choisie et du nombre d'informations à transporter

7.3.2 DNS : Noms des domaines racines



Slide 7.15
DNS : Noms des domaines racines

DNS connaît aujourd'hui 13 domaines racines génériques (gTLD : Generic Top Level Domain) : les domaines " aero, biz, com, coop, edu, gov, info, int, mil, museum, name, net et org ".

gTLD (Generic Top Level Domain)

Parallèlement 239 domaines racines nationaux (ccTLD :Country Code TLD) sont définis. Ces derniers, codés sur 2 lettres, utilisent la normalisation de codes de pays ISO3166, plus précisement la liste ISO3166-1.

ccTLD (Country code Top Level Domain)

Un dernier domaine (arpa) est utilisé pour les problèmes d'infrastructure. Ce dernier est composé de trois domaines. le domaine in-addr.arpa sert à la résolution DNS inverse. IP6 fait de même pour les adresses IPv6 et e164 permet d'établir le lien entre les adresses OSI e164 et les adresses IP.

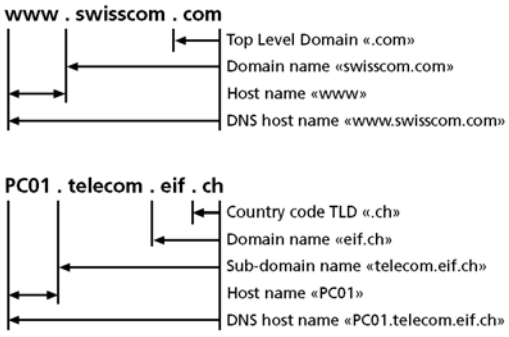
Infrastructure TLD

Sous ces domaines principaux, on peut créer autant de domaines et de sous-domaines que l'on veut. On ne peut toutefois pas dépasser la longueur de 255 caractères pour le nom DNS complet.

Des informations sur la gestion et l'utilisation de ces domaines sont disponibles sous www.icann.org (The Internet Corporation for Assigned Names and Numbers).

ICANN

7.3.3 DNS : Structure d'un nom logique



Slide 7.16
DNS : Structure d'un nom logique

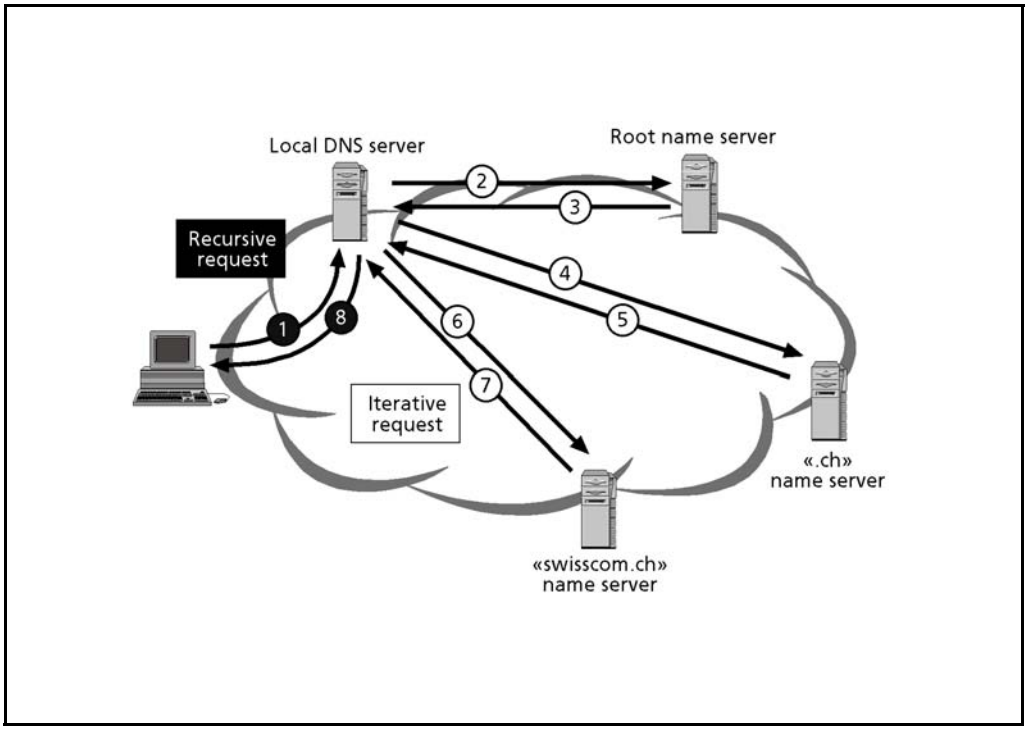
Un nom DNS est construit de manière hiérarchique, en partant du suffixe de domaine principal (TLD). On note ensuite, séparés par des points, le nom du domaine et celui de la machine.

www

Notons que "WWW" est généralement le nom de la machine qui fait serveur Web. Cette appellation est une coutume, elle n'est pas obligatoire. Le serveur mail ne possède souvent pas de nom, l'absence de nom est un nom particulier reconnu.

On peut aussi construire des sous-domaines, comme dans le deuxième exemple. Plusieurs niveaux de sous-domaines peuvent être créés, dans la limite des 255 caractères maximum pour le "DNS host name".

7.3.4 DNS : Requête



Slide 7.17
DNS : Requête

DNS Local

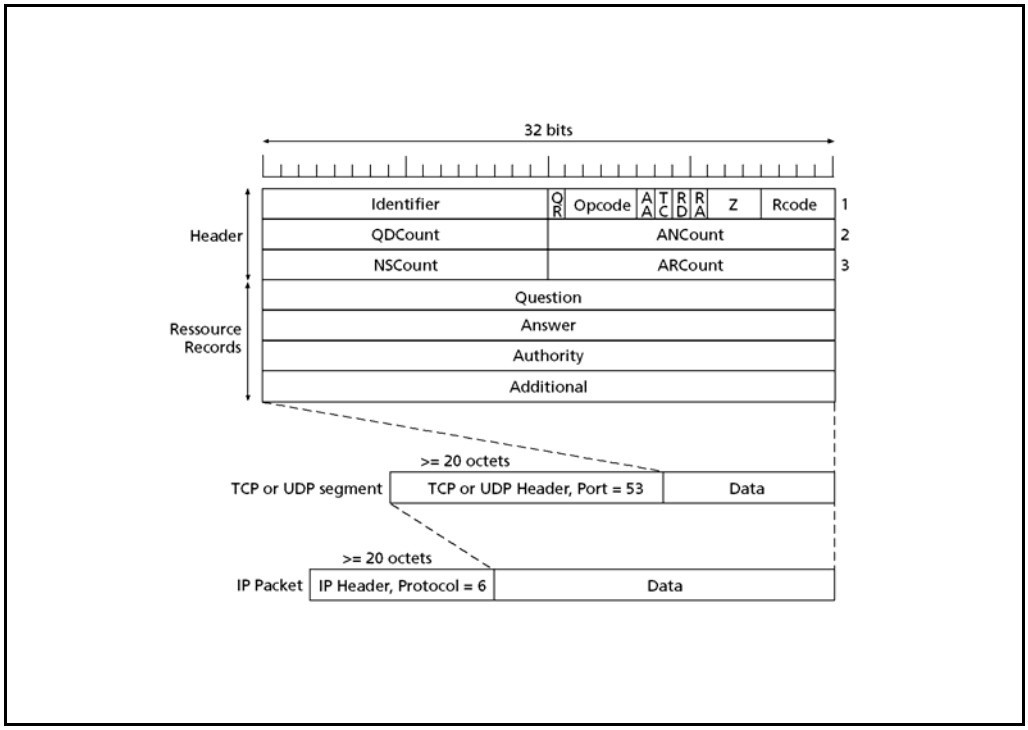
Chaque host connaît un serveur DNS local. Il le mandate, à travers une requête récursive (qui l'oblige à répondre), pour traduire un nom logique (www.swisscom.ch) en adresse IP.

DNS Root

Le serveur DNS local va relayer cette question à un serveur DNS root. Celui-ci ne connaît pas notre adresse, mais donne l'adresse du DNS responsable de ".ch". Notre question lui sera posée. Lui non plus ne connaît pas la réponse, il nous rend l'adresse du DNS responsable du domaine " swisscom.ch ". Ce DNS va pouvoir répondre à notre question, il est responsable de toutes les adresses ".swisscom.ch". Le DNS local pourra alors nous fournir notre réponse.

A noter que notre DNS local aurait pu aller directement sur un DNS plus "proche" de la solution, s'il en connaissait déjà l'adresse.

7.3.5 DNS : Format de paquet



Slide 7.18
DNS : Format de paquet

Le paquet DNS se compose d'un identificateur, permettant de lier les réponses aux requêtes effectuées. QR permet de spécifier s'il s'agit d'une requête ou d'une réponse. OPcode indique le type de requête. AA indique que la réponse est donnée par un serveur faisant autorité. TC indique que le message a du être tronqué. RD force une requête récursive. RA indique si la récursivité est disponible. Z est réservé est doit être à "0". Rcode peut transporter des codes d'erreurs avec les réponses.

XXCount indiquent le nombre de questions, réponses, serveurs faisant autorité et parties additionnelles dont est composé la fin du paquet.

8 ICMP (Internet Control Message Protocol)

TCP/IP advanced and practical

Introduction & Concepts (1)
Data Link Layer (2-4)
Network Layer (5-8)
- Network Protocol IPv4 (5)
- IPv4 Addressing (6)
- Address Resolution & Configuration Protocols (7)
- **ICMP (Internet Control Message Protocol) (8)**

IPv6 (9-10)
Routing (11-12)
Transport Layer (13)
Application Layer (14)

Slide 8.1
ICMP (Internet Control Message Protocol)

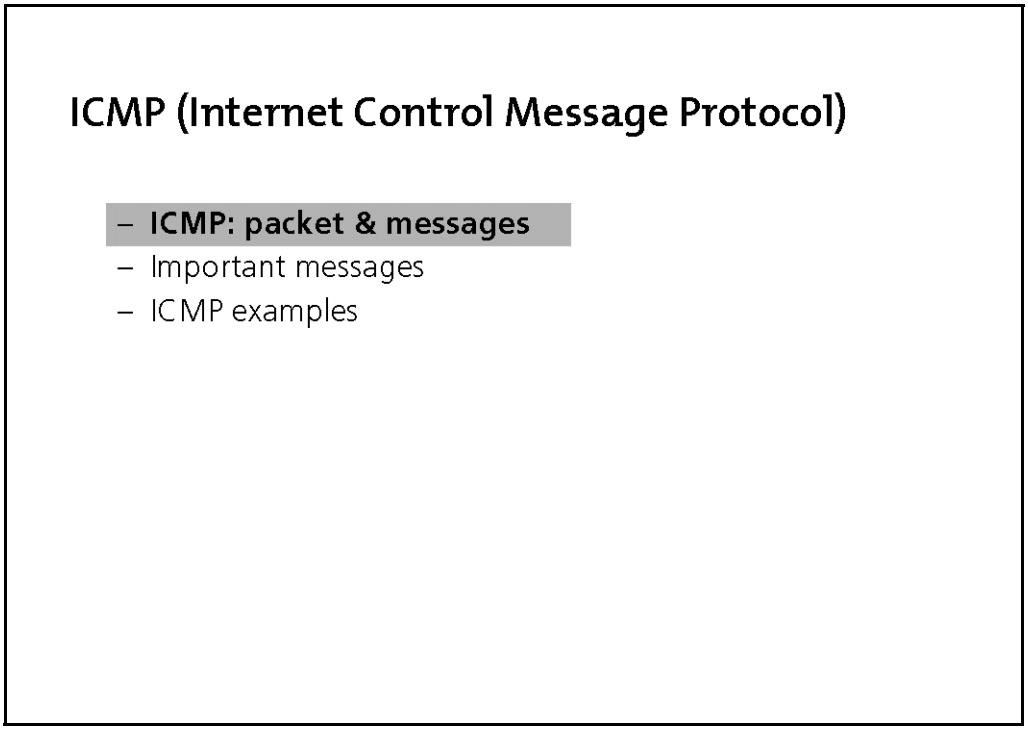
Ce chapitre traite du protocole ICMP. Placé en couche 3, il permet l'échange de messages de contrôle et d'erreur au travers du réseau.

Il est directement véhiculé par IP dont il est considéré comme étant une de ses composantes. Il est décrit par [RFC 792] et complété par une partie de [RFC 950]

Objectifs

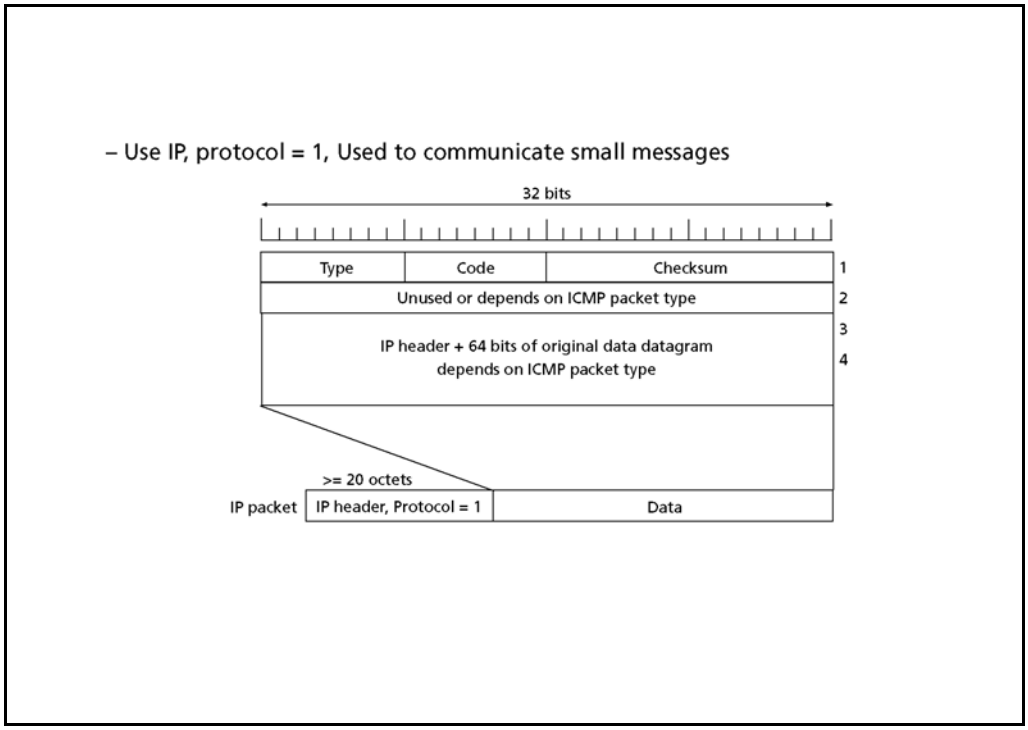
A l'issue de ce chapitre, les participants sont capables de nommer les principaux messages ICMP, d'utiliser ce protocole au travers des applications DOS "Ping" et "Tracert".

8.1 ICMP : Paquets et messages



Slide 8.2
ICMP : Paquets et messages

8.1.1 Format de paquet ICMP



Slide 8.3
Format de paquet ICMP

ICMP

Le format de paquet ICMP contient une entête de 8 octets. Le premier définit le type du message. Code, l'octet suivant, contient souvent des précisions concernant le message. Il n'est pas toujours utilisé. La Checksum de 16 bits protège le paquet ICMP complet. Les 4 octets suivants ont des fonctions variant selon le type de message. Après l'entête, on peut trouver des données. Il s'agit souvent d'une copie du début du paquet IP dans lequel on signale une erreur.

Aucun paquet ICMP erroné ne doit déclencher d'autres paquets ICMP (avalanche).

8.1.2 Messages ICMP

Type	Message Type	Remarks
0	Echo reply	See Echo request
3	Destination unreachable	Detailed in this chapter
4	Source quench	Generally not used
5	Redirect	Detailed in this chapter
8	Echo request	Detailed in this chapter
11	Time exceeded	Detailed in this chapter
12	Parameter problem	
13	Timestamp request	«Echo» without data, with timestamp.
14	Timestamp reply	
15	Information request	not use any more
16	Information reply	
17	Address mask request	Tool for discovering address mask
18	Address mask reply	

Slide 8.4
Messages ICMP

Certains de ces messages seront traités en détails par la suite. Les autres sont les suivants :

Source Quench peut être utilisé par les équipements pour demander à la source de ralentir le rythme de ses envois (protection contre la saturation).

Source quench

Parameter problem indique à la source qu'une valeur de champ n'est pas comprise (protocol par exemple).

Parameter problem

Le couple Timestamp permet de faire une demande d'écho en indiquant l'heure des systèmes.

Timestamp request, Timestamp reply

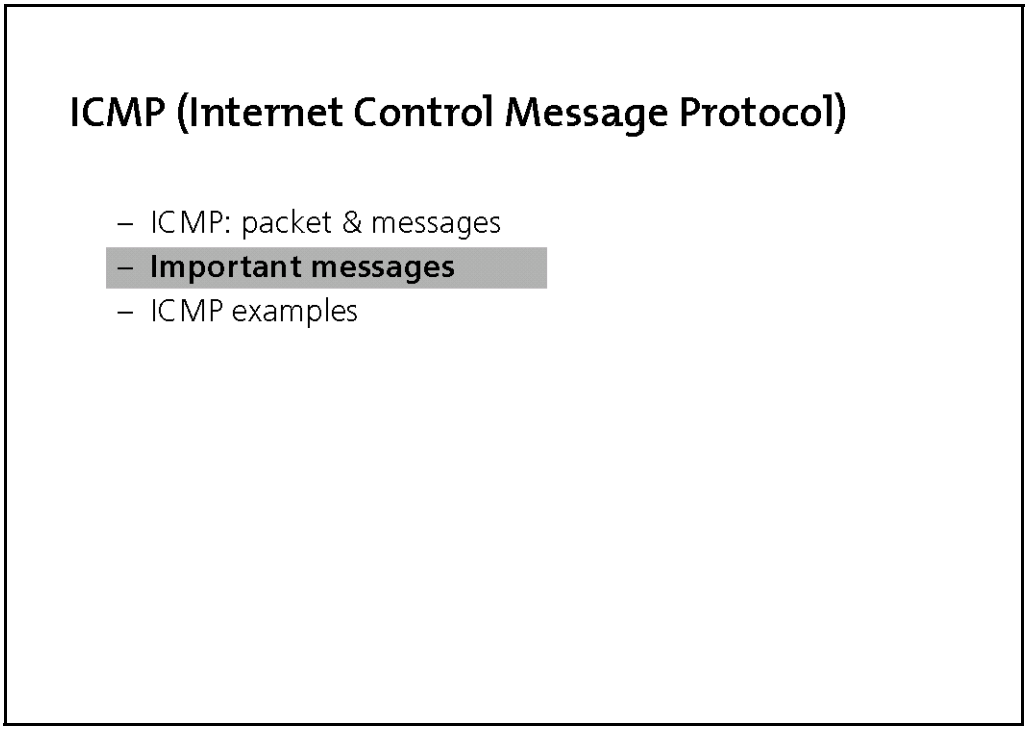
Une machine ne connaissant que son adresse IP locale servait Information request pour résoudre son adresse réseau.

Information request, Information reply

Address Mask permet de découvrir quelle est le masque de notre sous-réseau.

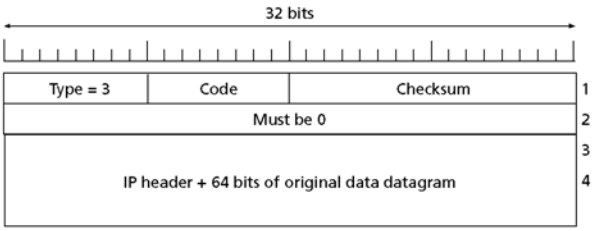
Address mask request, Address mask reply

8.2 Messages importants



Slide 8.5
Messages importants

8.2.1 ICMP Destination unreachable



Code	Meaning	Normal sender
0	Network unreachable	Router
1	Host unreachable	Router
2	Protocol unreachable	Host
3	Port unreachable	Host
4	Fragmentation needed and DF set	Router
5	Source route failed (IP option)	Router

Slide 8.6
ICMP Destination unreachable

Destination Unreachable

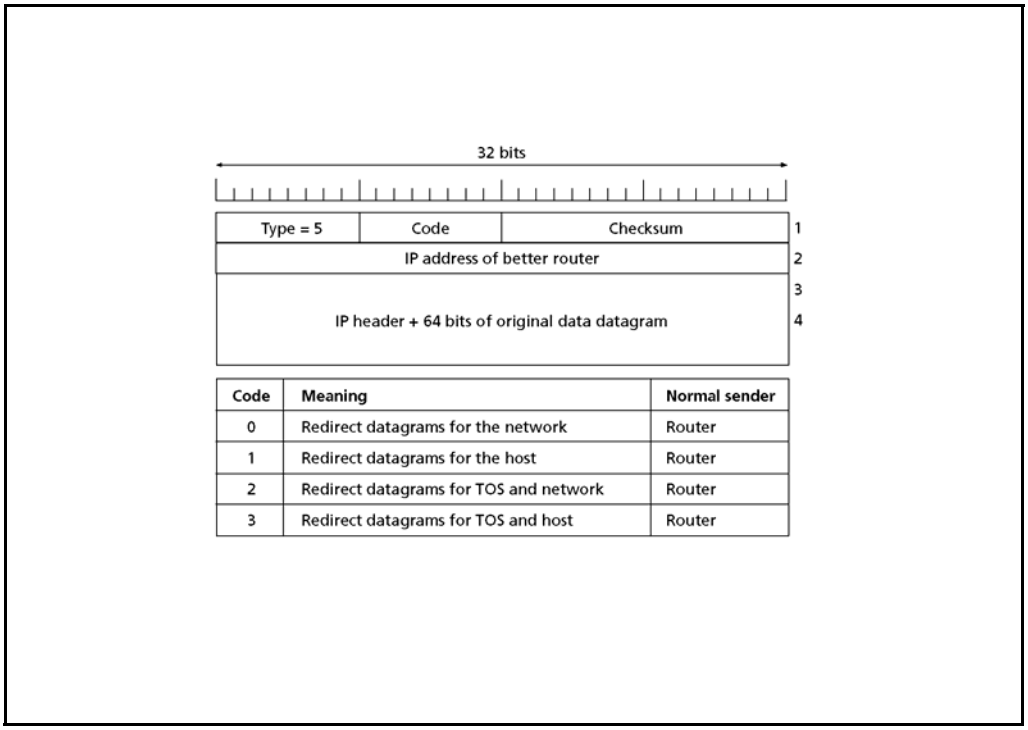
Le message ICMP "Destination unreachable" indique que la destination ne peut pas être atteinte. Différents codes précisent ce qui ne peut pas être atteint : le réseau de destination (0), le host lui-même(1), …

Les messages codés 2 et 3 proviennent du host destinataire, qui se plaint de ne pas connaître le protocole transporté (2) ou le port (TCP ou UDP) de destination (3).

Si on interdit la fragmentation d'un paquet et que celui-ci est trop grand, on recevra aussi ce message ICMP (4).

Le dernier message est plus particulier. Il informe d'un problème avec une option de l'entête IP. Celles-ci étant rares, on ne risque pas de croiser ce type de message en chemin…

8.2.2 ICMP Redirect



Code	Meaning	Normal sender
0	Redirect datagrams for the network	Router
1	Redirect datagrams for the host	Router
2	Redirect datagrams for TOS and network	Router
3	Redirect datagrams for TOS and host	Router

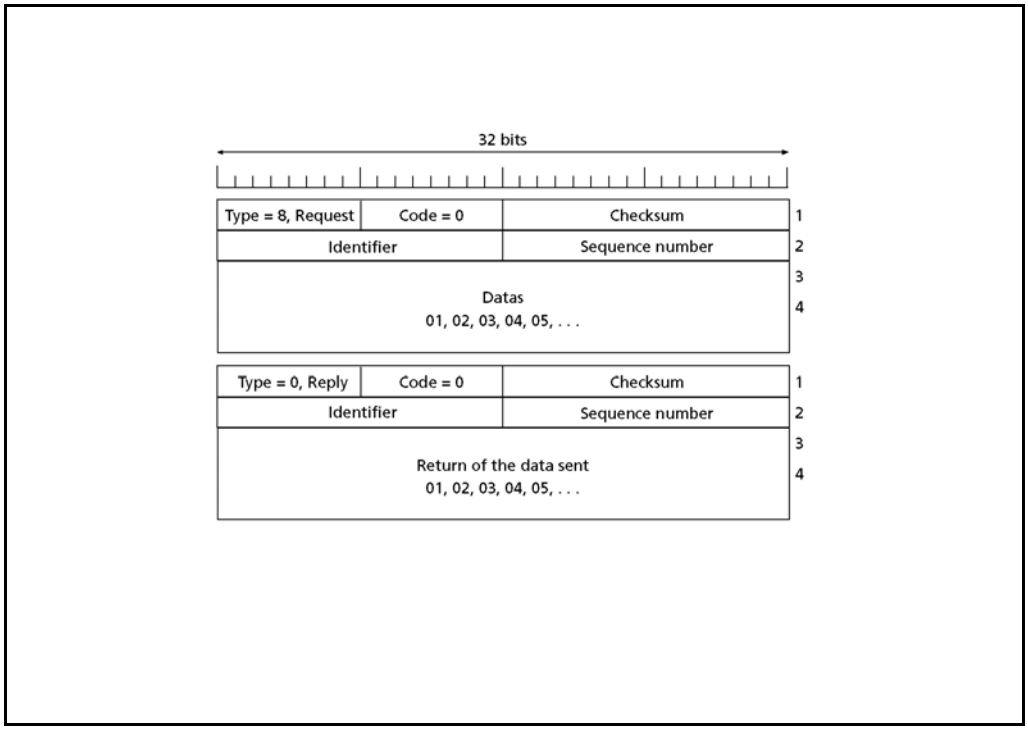
Slide 8.7
ICMP Redirect

Le message Redirect est envoyé par un routeur à un host. Le routeur constate que le prochain routeur nécessaire à l'acheminement du paquet est dans le même sous-réseau que le host "source". Il va donc l'informer de s'adresser directement à cet autre routeur par la suite. Le paquet ayant déclenché ce message n'est pas détruit, il sera routé.

Redirect

On constate que les codes permettent de différencier les changements de route pour un host unique ou pour tout son réseau. Ils permettent également de préciser que la route proposée est meilleure pour le type de service exigé. On gardera alors le premier routeur pour les autres types de services.

8.2.3 ICMP Echo request et Echo reply



Slide 8.8
ICMP Echo request et Echo reply

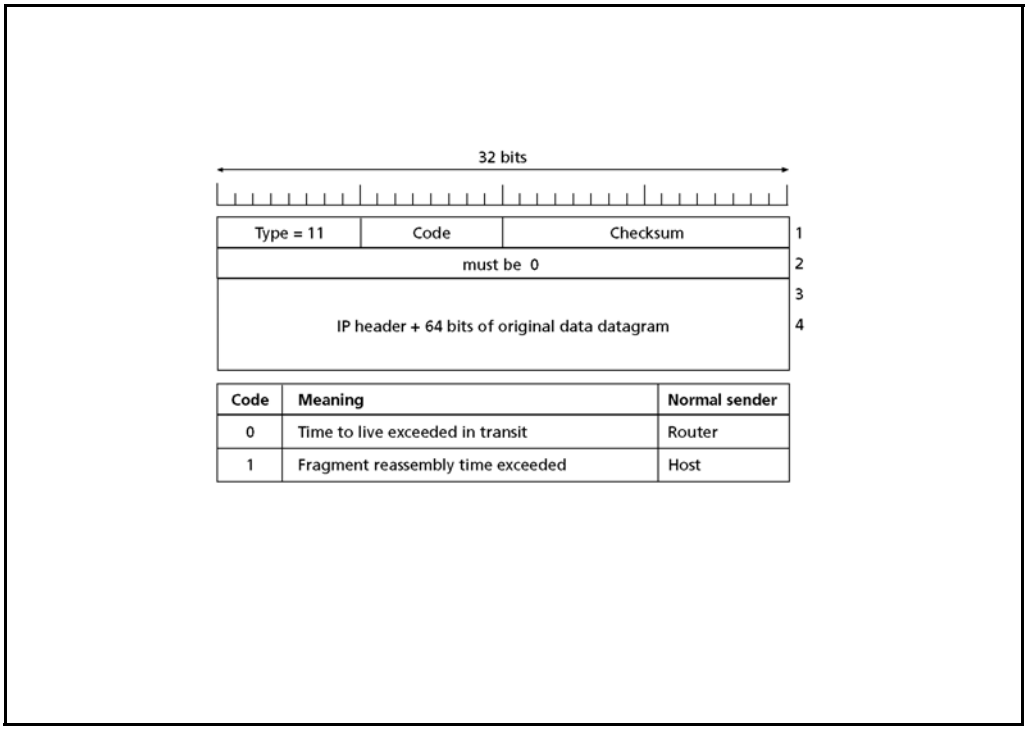
Echo request, Echo reply

Echo request est un message auquel le destinataire doit répondre par un Echo reply. Ce message est utilisé afin de vérifier si notre partenaire est présent (si la machine est allumée par exemple).

On peut adjoindre des données à une requête dans les limites de taille du paquet IP. Ces données seront retransmises dans la réponse. Ca permet donc de tester le réseau en le "chargeant" avec des paquets de taille imposée.

Echo reply est différencié d'Echo request par la valeur du type de message. Actuellement code doit être laissé à 0. Un identificateur et un numéro de séquence peuvent être ajouté. Ils ne sont pas obligatoires, mais permettent de lier les réponses aux questions lors de test "en rafales".

8.2.4 ICMP Time exceeded



Code	Meaning	Normal sender
0	Time to live exceeded in transit	Router
1	Fragment reassembly time exceeded	Host

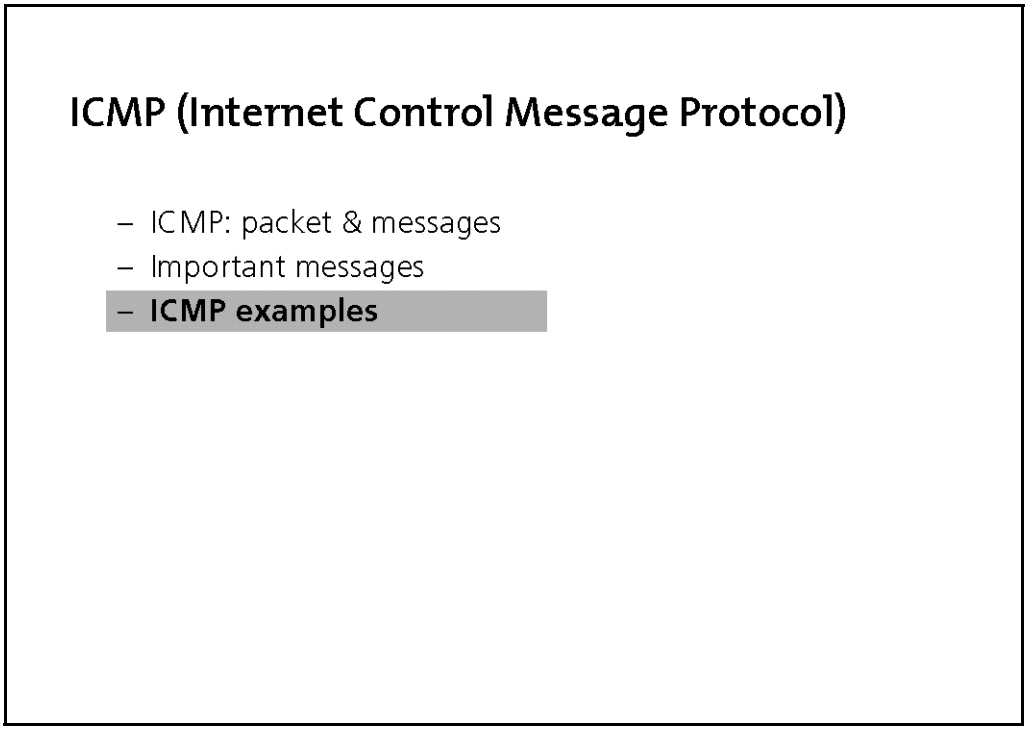
Slide 8.9
ICMP Time exceeded

Time exceeded, TTL

On sait que l'entête IP contient un champ appelé "Time to Live", décrémenté par chaque routeur, jusqu'à atteindre la valeur 0. A ce moment le routeur concerné détruit le paquet et émet un message ICMP "time exceeded, code 0" à destination de la source. Afin qu'elle puisse savoir de quel paquet il s'agissait, l'entête du-dit paquet est copiée dans les données du message ICMP.

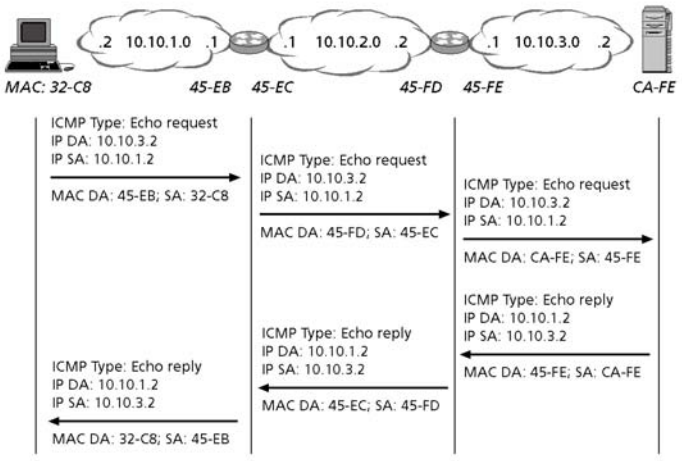
Le message de code 1 est beaucoup moins courant. Il informe la source que son paquet a été fragmenté est que le "time-out" pendant lequel on attend les fragments est terminé, sans qu'ils ne soient tous arrivés.

8.3 Exemples ICMP



Slide 8.10
Exemples ICMP

8.3.1 Ping



Slide 8.11
Ping

"Ping" est un logiciel, disponible sous DOS (syntaxe Ping [nom ou adresse IP]) et sous pratiquement tous les systèmes d'exploitation, y compris ceux des routeurs.

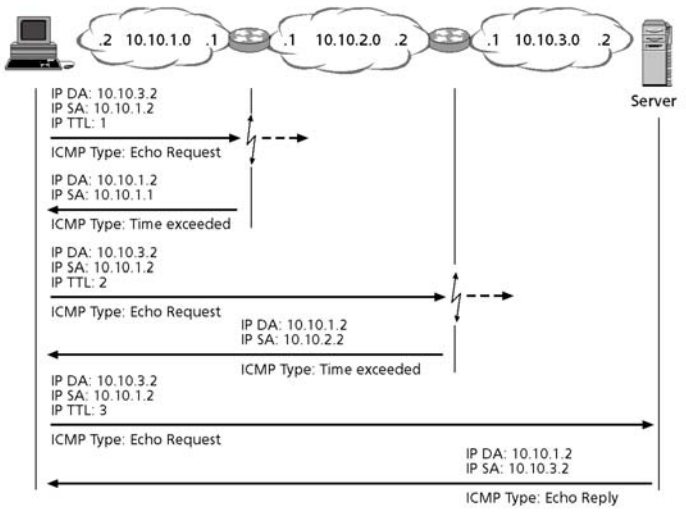
Echo request, Echo reply

ICMP est la base du fonctionnement de Ping. L'ordinateur "Pingueur" envoie un Echo Request à travers le réseau jusqu'à la destination "Pinguée", qui va répondre avec un Echo Reply.

La version DOS va d'abord commencer par traduire en adresse IP le nom de la machine à "Pinguer" (DNS) puis fait successivement 4 fois le dialogue représenté, en emportant à chaque fois 32 octets de données. En outre le temps entre l'envoi de la requête et l'arrivée de la réponse est indiqué à l'écran.

On peut faire varier tous les paramètres (TTL, taille des données, nombre d'essais).

8.3.2 Traceroute



Slide 8.12
Traceroute

Tracert

Tracert est un logiciel DOS, permettant de tracer la route entre le point de départ et la destination.

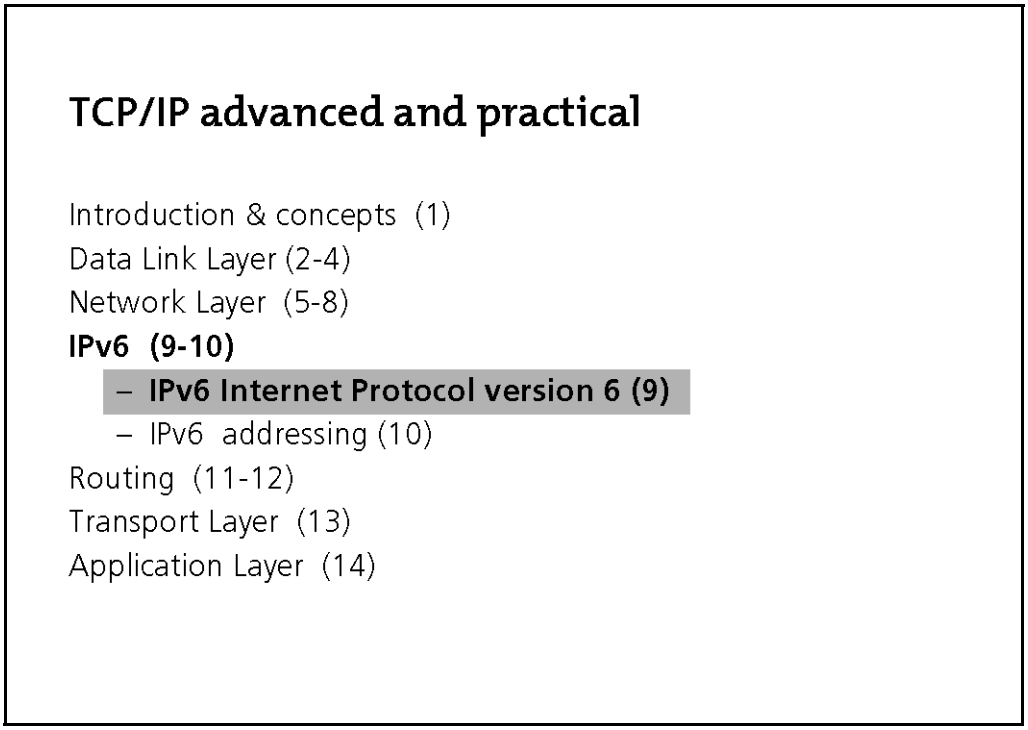
Echo request, Time exceeded

L'astuce du fonctionnement est assez simple. On envoie un Echo request en direction de la cible, mais en limitant la vie du paquet IP au 1er routeur (TTL =1). Celui-ci décrémente le TTL et doit détruire le paquet. Il informe la source de la destruction avec un message ICMP "Time exceeded". Ce message est porté par un paquet IP contenant l'adresse du routeur. On découvre ainsi notre 1er routeur.

Echo reply

Un même Echo Request est ensuite envoyé avec un TTL = 2. Celui-ci ira jusqu'au 2ème routeur et ainsi de suite jusqu'à la destination, qui répondra avec un Echo reply. Des requêtes DNS sont insérées entre chaque envoi afin de trouver le nom du routeur.

9 IPv6 (Internet Protocol version 6)



Slide 9.1
IPv6 : Internet Protocol version 6

Ce chapitre traite de la nouvelle génération de protocole Internet, IP version 6.

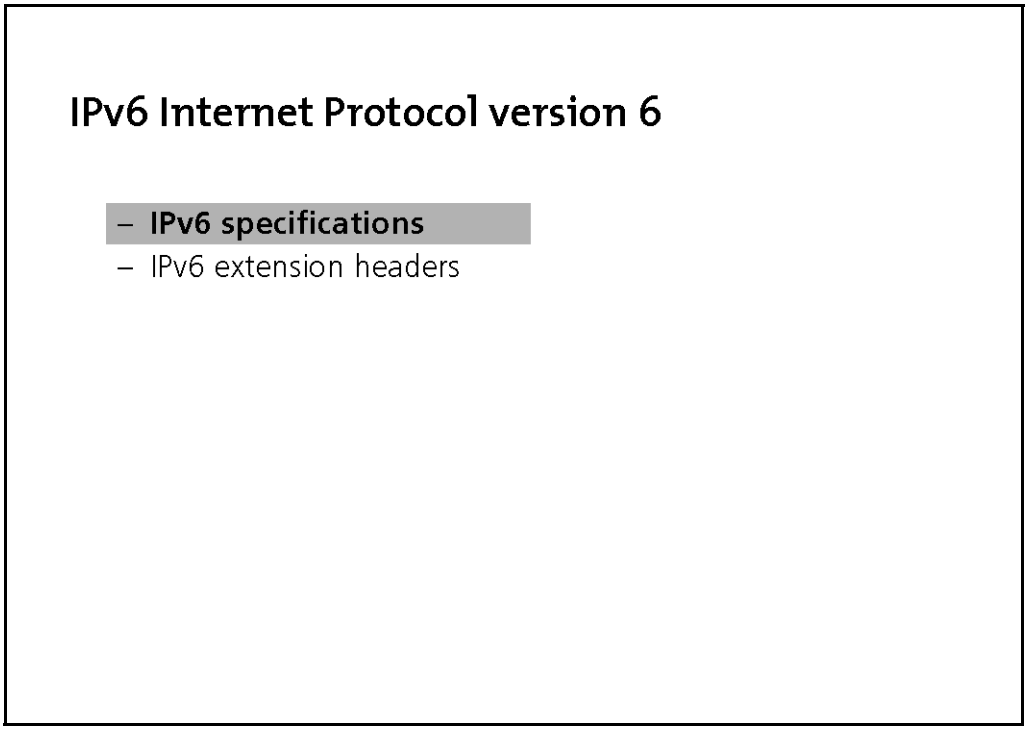
Connu également sous le nom de IPng (Internet Protocol next generation), IPv6 est un protocole de couche réseau. Il est prévu comme étant le successeur de IPv4.

Il est décrit dans [RFC 2460]

Objectifs

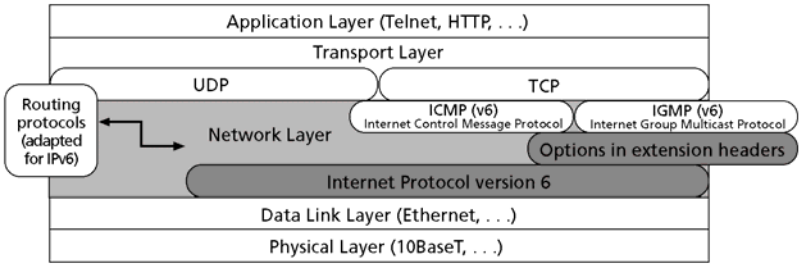
A l'issue de ce chapitre, les participants sont capables de reconnaître un entête IPv6, de nommer les avantages par rapport à IPv4, ainsi que de différencier les entêtes optionels d'IPv6.

9.1 IPv6 : Spécifications



Slide 9.2
IPv6 : Spécifications

9.1.1 Architecture d' IPv6



Slide 9.3
Architecture d'IPv6

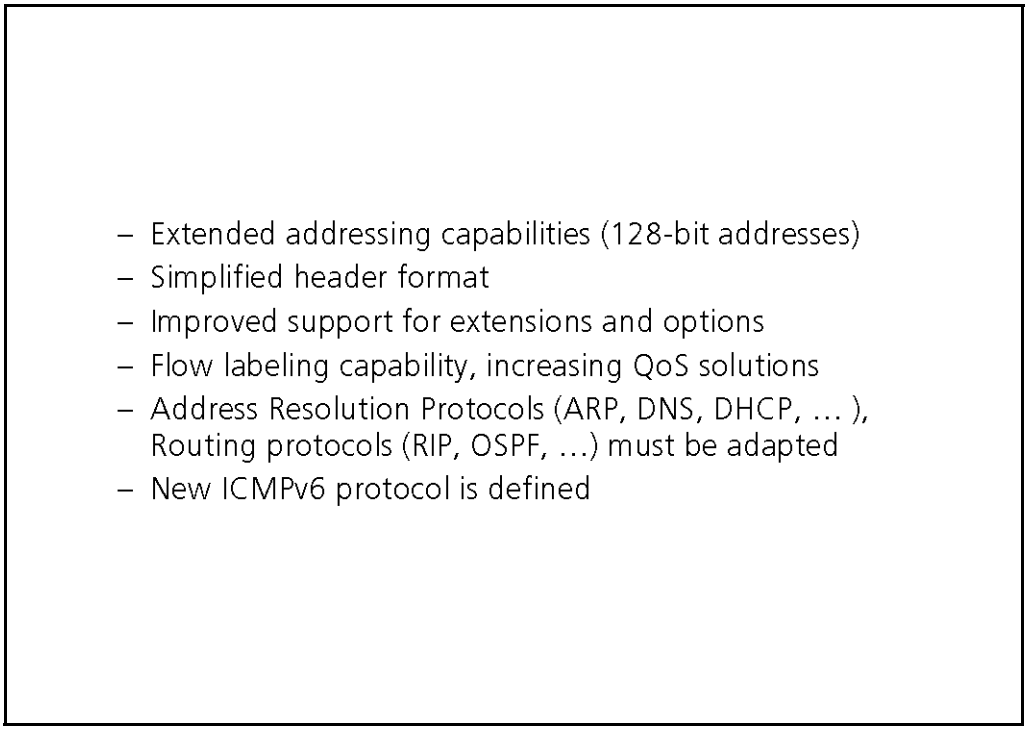
IPv6

A l'instar d'IPv4, il est utilisé par les protocoles de transports TCP et UDP. Ceux-ci ne seront que peu modifiés pour l'utilisation d'IPv6 (pseudo-header, etc.). IPv6 peut lui aussi fonctionner sur un grand nombre de protocoles de couche 2.

Il offre les mêmes services que IPv4. Cependant son adressage est plus étendu, et ses options sont traitées de manière plus intéressante.

Il est actuellement "draft standard" et peut être utilisé. Les adresses IPv6 sont disponibles auprès des providers.

9.1.2 Fonctions et propriétés IPv6, différences avec IPv4



Slide 9.4
Fonctions et propriétés IPv6, différences avec IPv4

Les principaux changements par rapport à IPv4 sont d'abord l'extension des adresses. Celles-ci ont maintenant 128 bits de longueur.

Une simplification de l'entête a été effectuée. Les champs qui ne sont pas utilisés fréquemment sont passés en options. L'intégration de ces dernières ce fait par ajout d'entêtes d'extension, optionnelles, après l'entête IPv6.

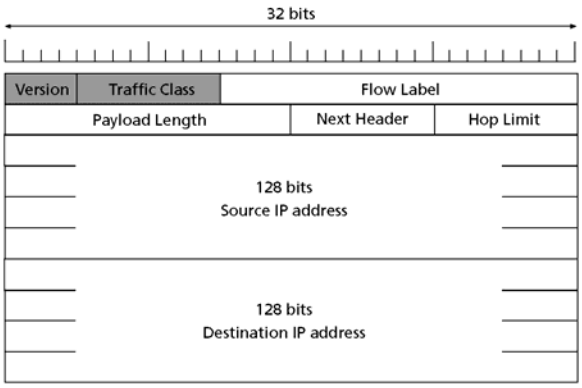
QOS

Une prise en charge particulière de flux de paquets permet de mieux répondre aux besoins en QOS.

ICMPv6

Les différents protocoles utilisant les adresses IP, comme les protocoles de résolution ou encore les protocoles de routage devront être adaptés à la taille et au format des adresses IPv6. En outre un nouveau protocole ICMPv6 a été créé.

9.1.3 Format de paquet IPv6



Slide 9.5
Format de paquet IPv6

Le paquet IPv6 possède une entête de longueur fixe de 40 octets.

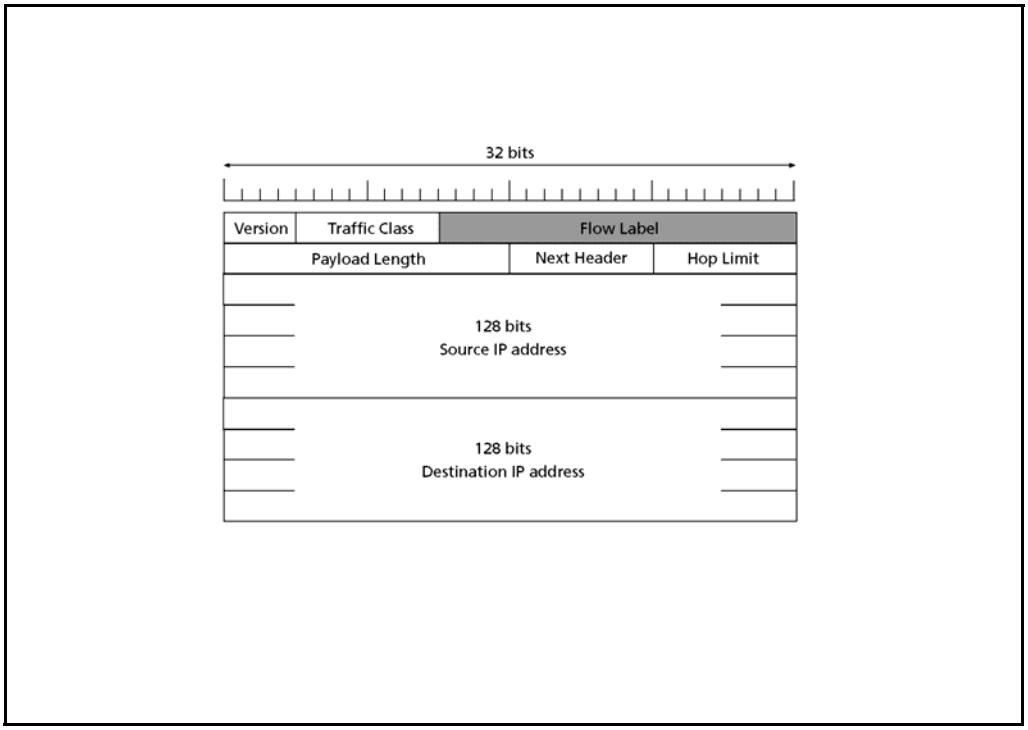
Version

Cette entête commence par un champ Version, long de 4 bits, correspondant à celui d'IPv4. Dans notre cas il aura la valeur 6.

Traffic Class, TOS

Traffic Class est un octet fournissant les mêmes services que TOS de IPv4. La construction de cet octet n'est pas compatible avec TOS, cependant les infos TOS pourront y être codées. On envisage même d'utiliser Traffic Class à la place de TOS dans les paquets IPv4.

9.1.4 Format de paquet IPv6 : Etiquette de flux



Slide 9.6
Format de paquet IPv6, étiquette de flux

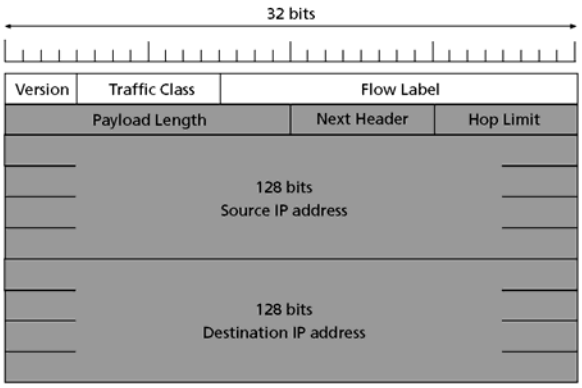
Flow Label

L'étiquette de flux, Flow label, permet aux routeurs de reconnaître un paquet IP comme faisant partie d'un ensemble.

Un flux est un ensemble de paquets devant bénéficier d'une certaine qualité de service. Un flux est défini par les adresses IP source et destination et par le flow label. On ne peut pas envoyer des paquets à des adresses destinations différentes avec la même étiquette de flux.

Chaque flux doit être négocié avant d'être utilisé. La valeur "0" le flow label définit un paquet isolé, ne faisant pas partie d'un flux. Si le protocole IPv6 est aujourd'hui "draft standard", la gestion des flux est encore expérimentale. Des étiquettes de flux "0" seront les plus utilisées à l'introduction de IPv6.

9.1.5 Format de paquet IPv6 : Protections et adressage



Slide 9.7
Format de paquet IPv6, protections et adressage

Payload length définit la longueur des données IP, c'est à dire la longueur du paquet sans cette entête, mais avec les éventuelles entêtes d'extensions.

Next Header

Next header reprend les valeurs du champ Protocol de IPv4 (TCP=6, UDP=17, ...). Dans le cas d'IPv6, on peut aussi trouver ici l'annonce d'une entête optionnelle. Celle-ci comprendra aussi un champ Next header.

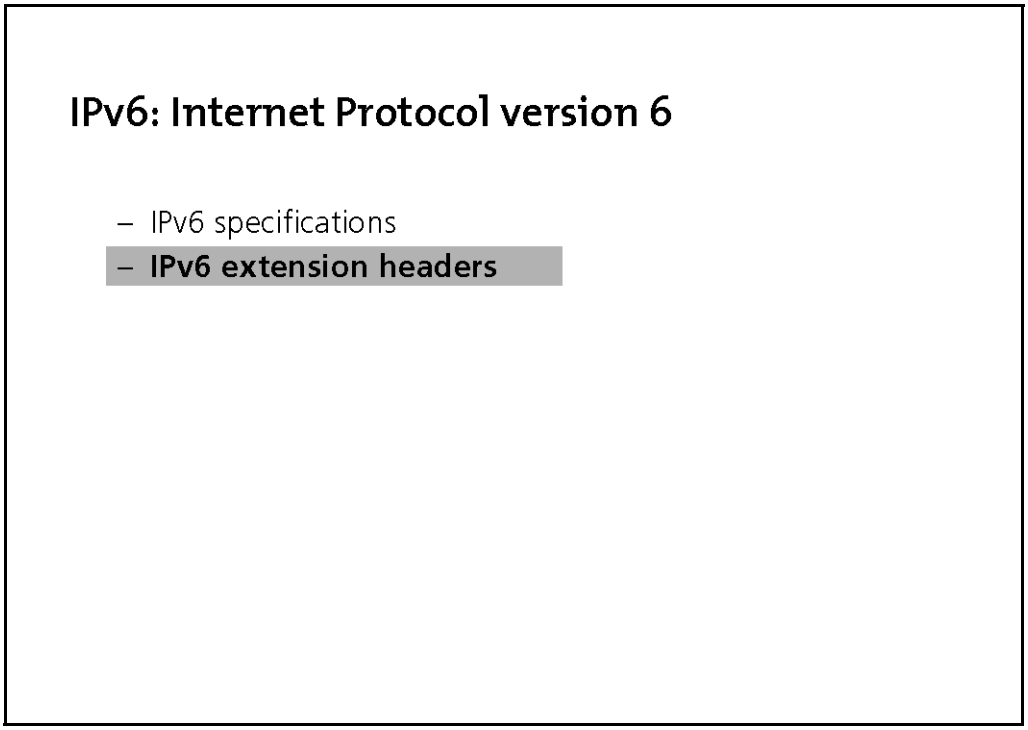
Hop Limit

Hop limit correspond à Time-to-live IPv4. Il sera décrémenté par les routeurs en chemin.

IPv6 Address

On trouve ensuite les adresses source et destination. Elles ont chacune une longueur de 128 bits (contre 32 à IPv4).

9.2 IPv6 : Entêtes d'extension



Slide 9.8
IPv6, entêtes d'extention

Extensions Headers

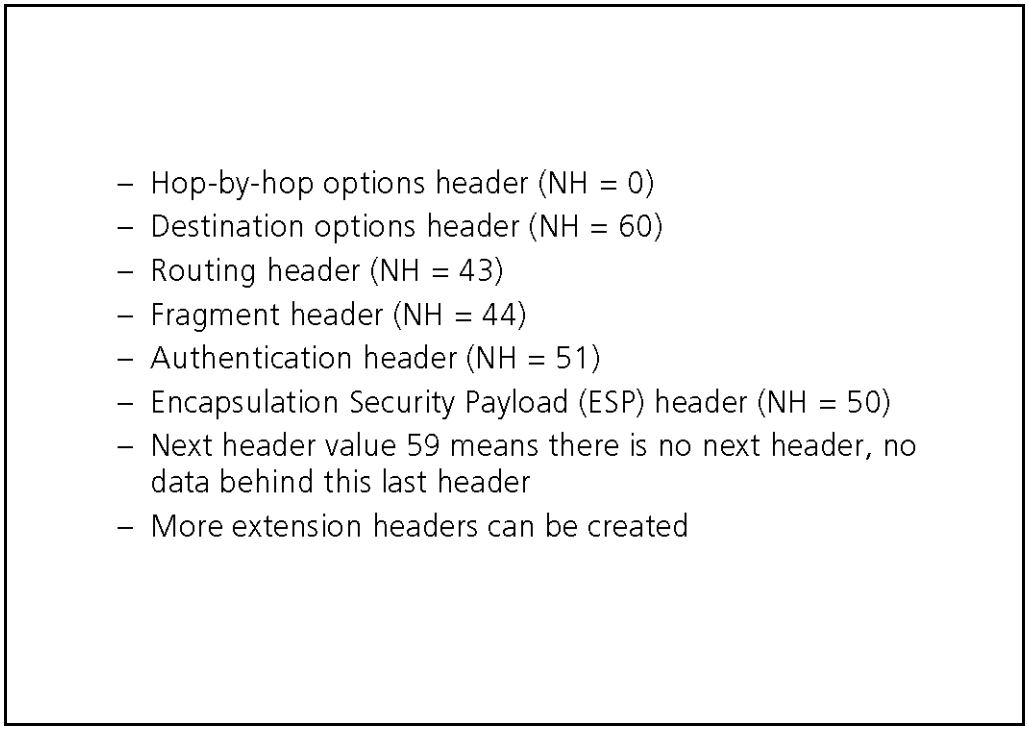
Tout ce qui n'est pas nécessaire à l'acheminement d'un paquet IP à travers l'Internet, et traiter sous forme optionnelle dans des entêtes séparées.

Leur fonction est de transporter avec le paquet des informations dédiées à des protocoles spécifiques.

Elles transportent des informations relatives à l'authentification, au cryptage, au routage spécifique, à la fragmentation ou encore des options particulières.

Elles sont décrites dans [RFC 2460, 2402, 2406]

9.2.1 Entêtes d'extensions IPv6

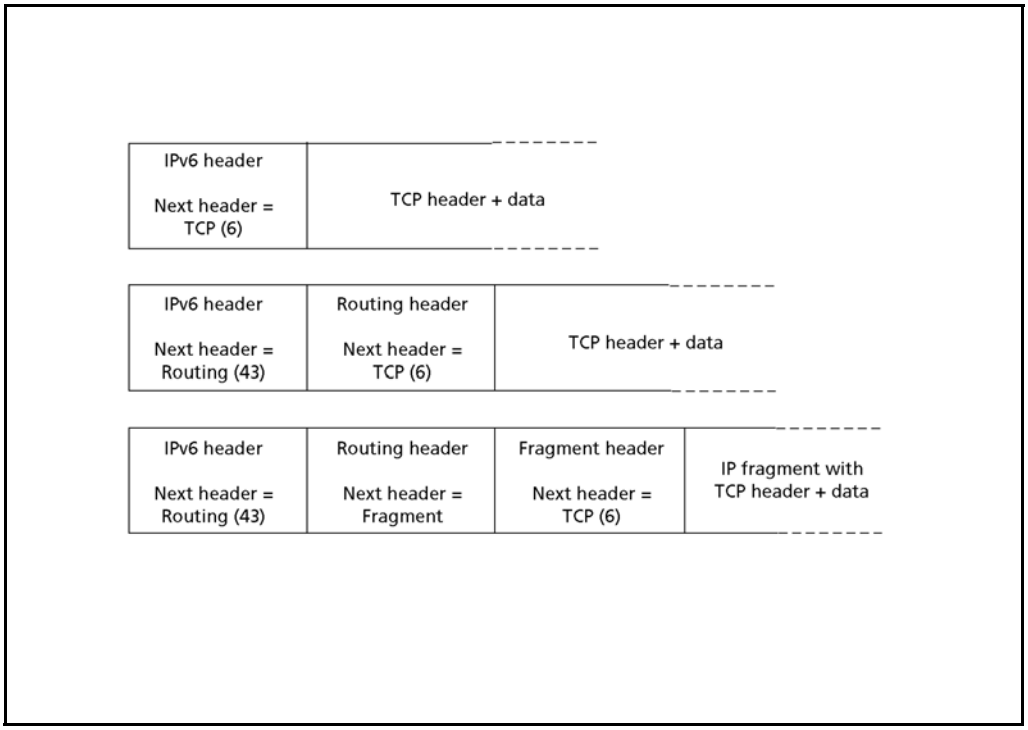


Slide 9.9
Entêtes d'extensions IPv6

A l'exception de "Hop-by-hop options header", toutes ces entêtes ne sont pas traitées par les routeurs en chemin, mais seulement à la destination.

- **Hop-by-hop** et **Destination options header** sont des "containers" prévus pour transporter des options (à définir) traitées à chaque saut ou à destination.
- **Routing header** contient une liste des hosts devant être "visités" en parcours.
- **Fragment header** va permettre de gérer la fragmentation d'un paquet IP.
- **Authentication header** permet d'assurer l'authentification de la source.
- **ESP header** permet le cryptage des données.
- **Next header = 59** indique qu'il n'y a rien après cette entête. On peut utiliser un paquet IP pour ne transmettre que des options, par exemple.

9.2.2 Entête d'extensions : Méthode



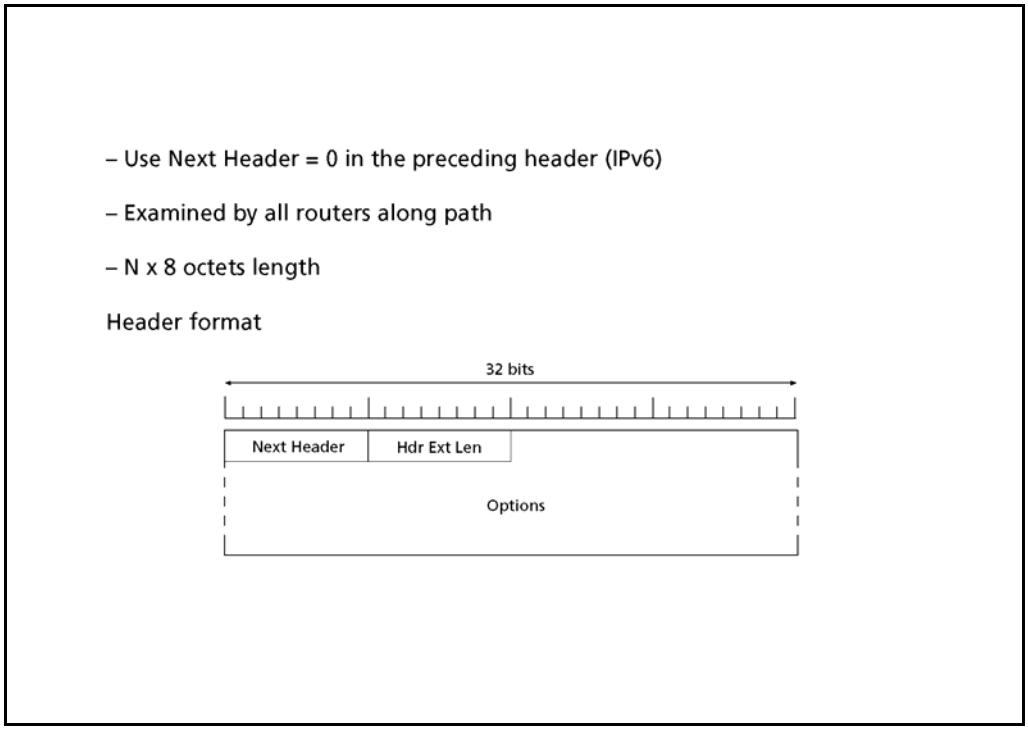
Slide 9.10
Entête d'extensions, méthode

Celles-ci contiennent toutes un champ next header, ce qui permet de les "empiler" avant les informations utiles. Chaque entête annoncera la suivante. La dernière indiquera l'entête du protocole supérieur (TCP, UDP, …).

Ces entêtes seront traitées dans l'ordre dans lequel elles sont empilées. Toutefois, un ordre est conseillé entre ces différentes entêtes.

Nous allons regarder le format de ces différentes entêtes, ainsi que le principe de fonctionnement de quelques-unes.

9.2.3 Entête IPv6 pour option "hop by hop"



Slide 9.11
Entête IPv6 pour option "hop by hop"

Hop by hop Options Header

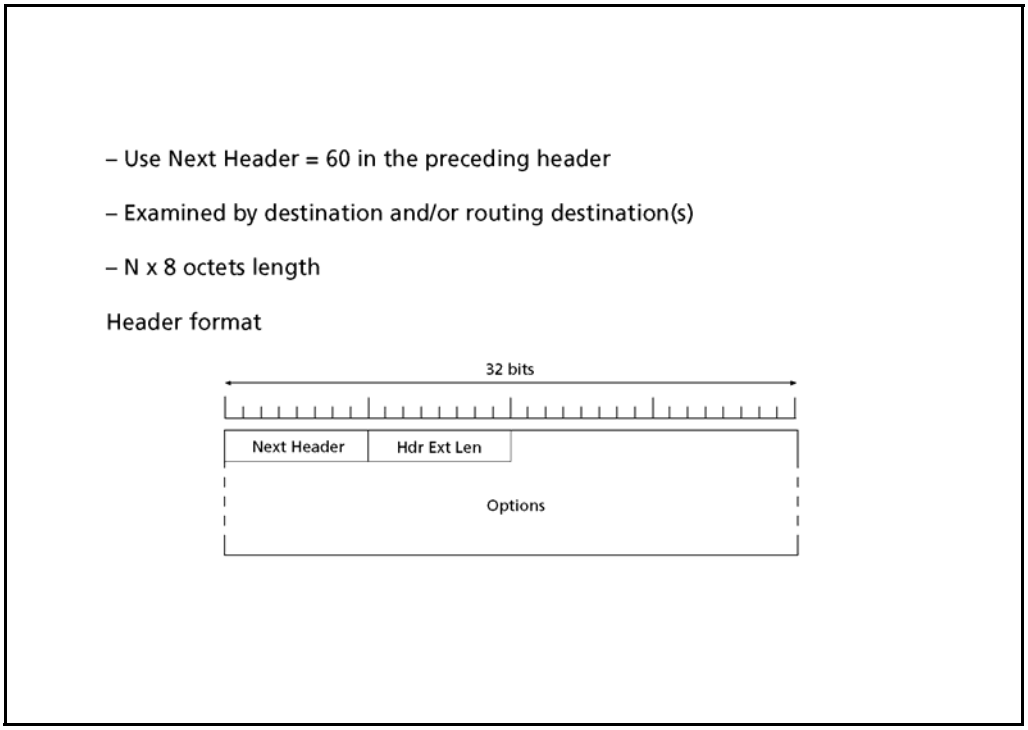
Cette entête sert de container pour transporter des options devant être traitées par les routeurs en chemin. Le fait que cette entête est la seule traitée par les routeurs lui impose d'être la première entête après IPv6. Les autres entêtes d'extension seront traitées à la destination uniquement.

Next header contiendra la valeur de la prochaine entête, optionnelle ou traditionnelle (TCP, UDP, ...).

Hdr Ext Len (Header Extension Length) contient la longueur de cette entête. Il compte les groupes de 8 octets (64 bits) composant cette entête, sans les premiers 8 octets. Une entête hop-by-hop de 24 octets aura une "longueur" de 2.

Ensuite on trouve le champ pouvant contenir une ou plusieurs options.

9.2.4 Entête IPv6 pour options de destination



Slide 9.12
Entête IPv6 pour options de destination

Destination Options Header

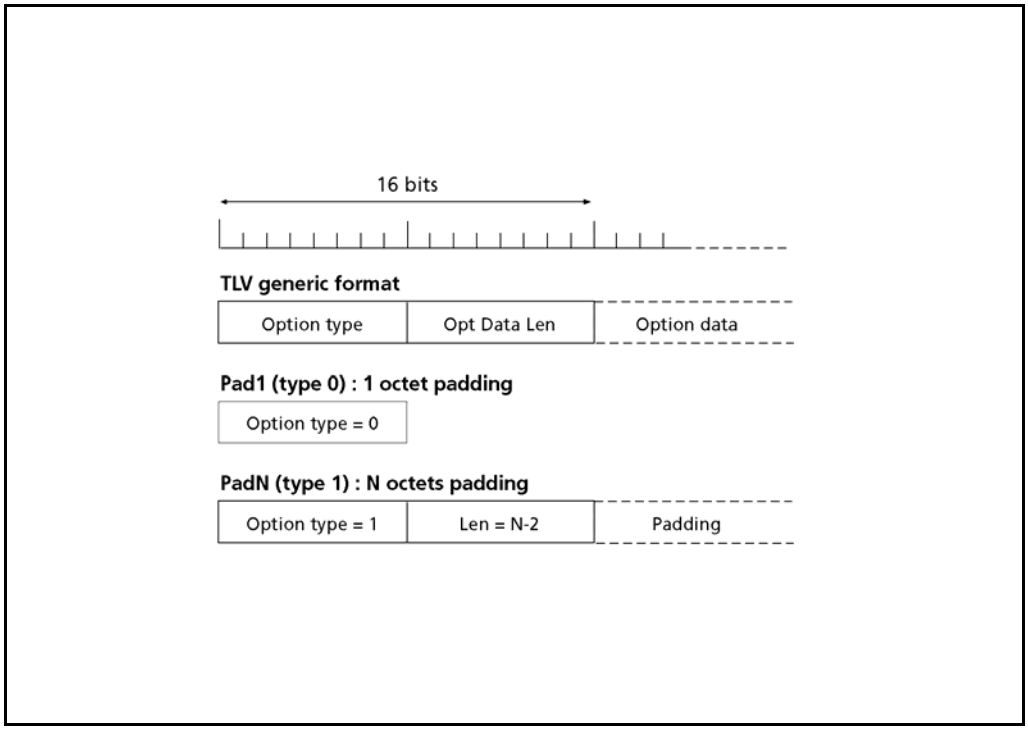
A l'instar de "hop-by-hop options header", destination options header est un container permettant d'amener des options à la destination. La différence réside dans le fait qu'ici les routeurs ne sont pas concernés par les options transportées.

L'entête est identique aux deux containers, la manière d'y stocker les options également.

Les options sont définies par un type, suivi d'un champ spécifiant leur longueur. Elles doivent être construites sous forme de champs de 1, 2, 4 ou 8 octets qui seront rangés de manière spécifique dans l'entête.

Actuellement il n'existe pas d'options standardisées. (Exception : "padding")

9.2.5 Format des options



Slide 9.13
Format des options

TLV Options Format

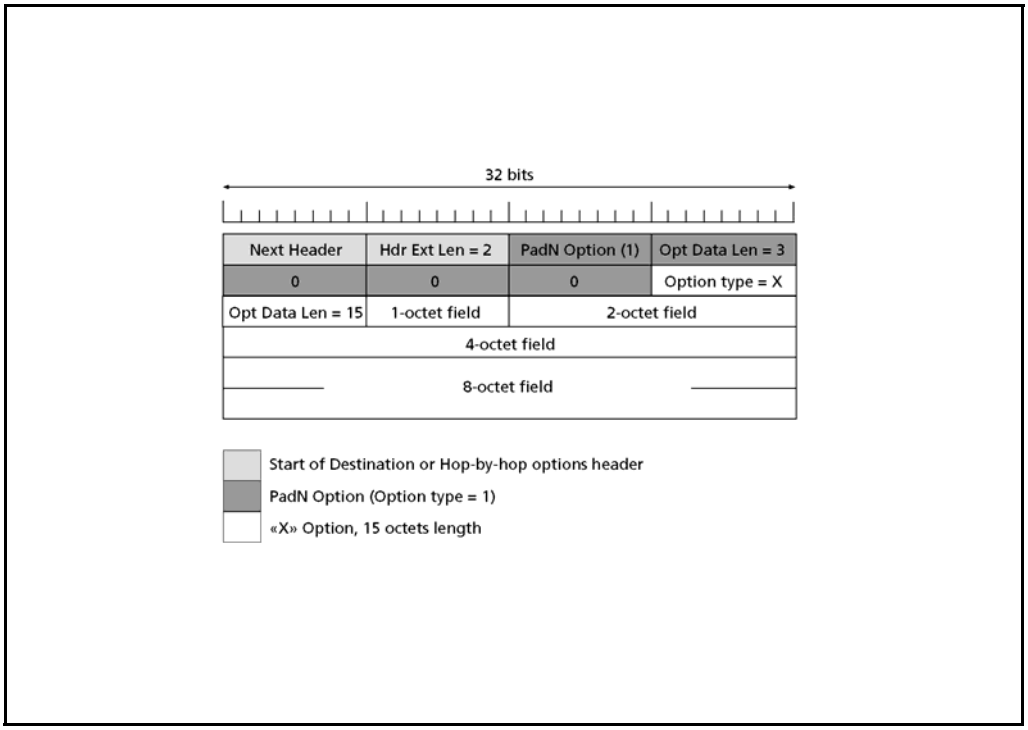
Option type indique le type d'option (à définir). Le champ suivant donne la longueur de l'option, sans les deux premiers octets.

Afin de traiter rapidement ces options, des critères d'alignement de leurs données ont été imposés. Ceci entraîne que du padding et nécessaire pour aligner, respectivement remplir les octets placés entre les options.

Deux options de padding ont été créées. Pad1 (type 0) a un format particulier. C'est la seule option à ne pas avoir d'octet de longueur. Elle a pour but de remplir un "trou" d'un octet. A partir de 2 octets on trouve l'option PadN (type 1).

Le principe d'alignement veut que le 1er octet des champs de données des options soit placé à un multiple de leur longueur, depuis l'origine de l'entête (n x 8 pour un champ de 8 octets).

9.2.6 TLV Conditions d'alignement : Exemple

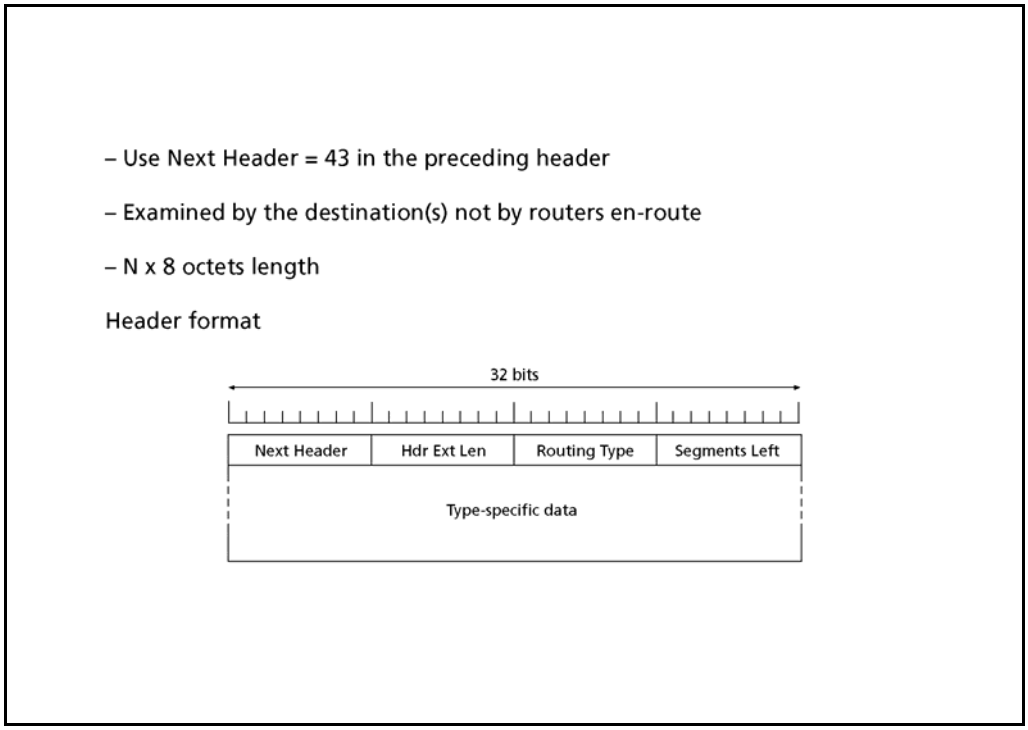


Slide 9.14
TLV conditions d'alignement, exemple

Dans cet exemple, une option d'une longueur de 15 octets de données est introduite dans une entête hop-by-hop ou destination. Les 15 octets sont décomposés en champs de 1, 2, 4 et 8 octets. L'alignement le plus critique correspond au champ de 8 octets. Son 1er octet doit se trouver à un emplacement numéroté d'un multiple de 8. Le 1er octet de l'entête étant l'octet 0, le 8 est le 1er de la 3ème ligne, le 16 le 1er de la 5ème ligne, etc. Dans notre cas, on devra aligner ce champ sur le n°16. Les autres champs doivent tous être placés à un multiple de leur longueur, ce qui est le cas ici.

Il ne reste qu'à mettre du padding entre le début de l'entête et notre option. Celui-ci sera fait à l'aide d'une option PadN longue de 5 octets (2+3).

9.2.7 Entête IPv6 de routage



Slide 9.15
Entête IPv6 de routage

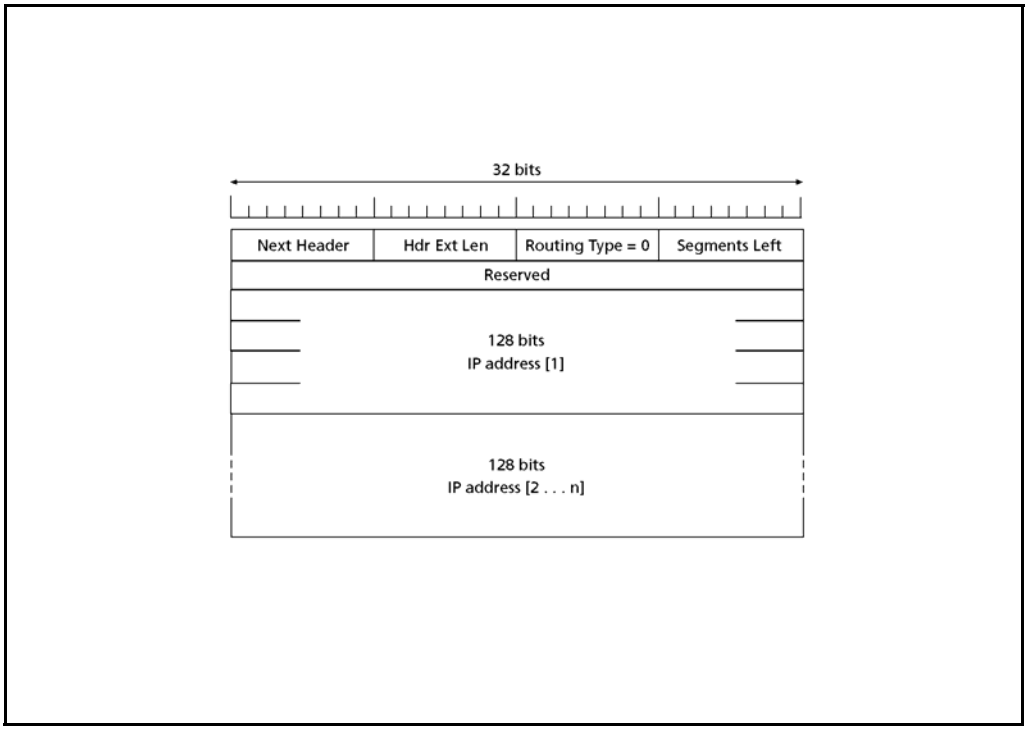
Routing Header

L'entête de routage correspond aux options IPv4. Elle permet de dresser la liste des hosts devant être "visités" en chemin vers une destination finale.

Les deux premiers champs sont déjà connus. Routing type permet de définir différents type de routage. Seul le type 0 est défini actuellement. Segments left indique le nombre de hosts qu'il faut encore "visiter", c'est à dire la position de la prochaine adresse dans la table.

Type-specific data contient la table des adresses des hosts à "visiter". Son format va dépendre du choisi.

9.2.8 Entête de routage type 0



Slide 9.16
Entête de routage type 0

Type 0 Routing Header

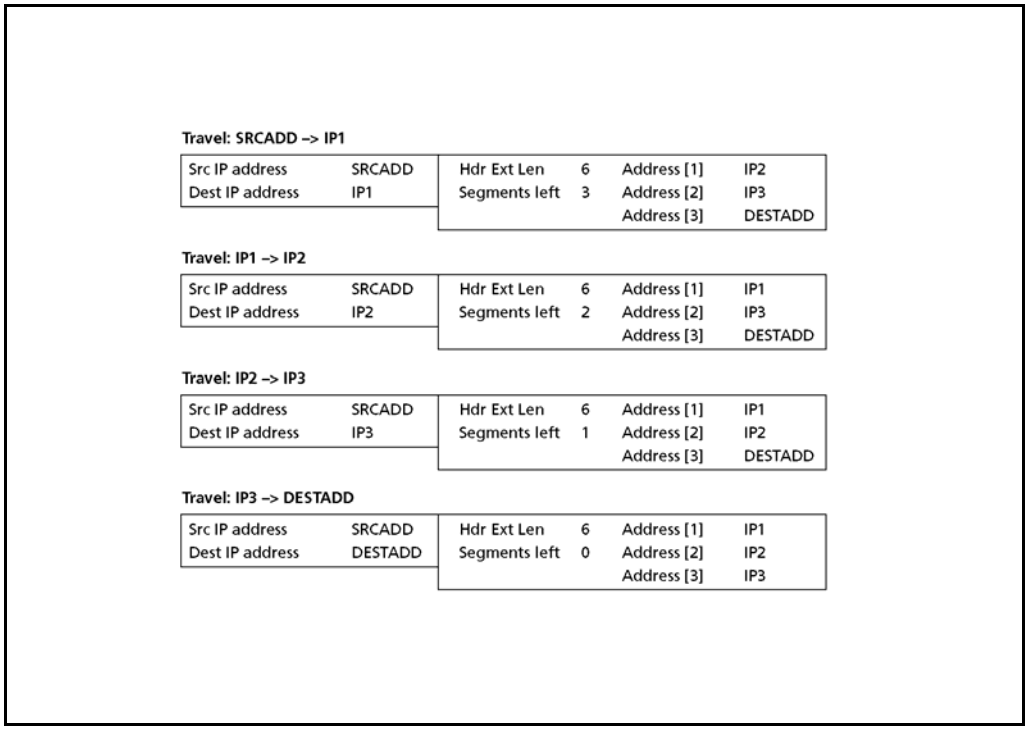
Cette entête de routage type 0 est assez simple.

Après la 1ère ligne d'entête, on trouve une ligne réservée à un usage futur.

En fait, les adresses IP qui suivent sont stockées dans des deux champs de 8 octets consécutifs. Il fallait aligner le premier champ sur un octet numéroté d'un multiple de 8, comme pour les "containers" à options.

Cette liste comprendra, au départ, toutes les adresses devant être visitée, sauf la première qui se trouvera déjà dans le champ "Destination address" de l'entête IP (selon exemple page suivante).

9.2.9 Entête de routage type 0 : Exemple



Slide 9.17
Entête de routage type 0, exemple

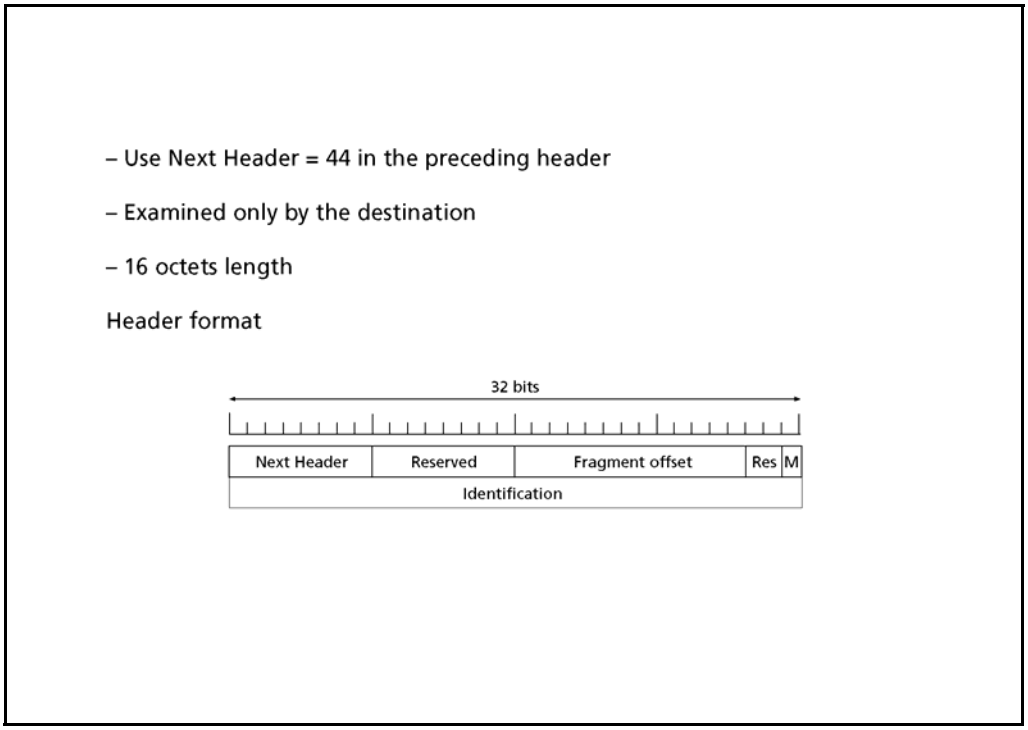
Dans cet exemple on voit les modifications de la liste d'adresses en fonction du segment parcouru. L'adresse de source sera toujours la source initiale du paquet.

A la première destination, le host concerné va aller chercher l'adresse de la destination suivante dans la table à la 3ème ligne (Segments left) depuis le bas. Elle sera placée dans le champ "Destination address" du paquet IP

Il copiera ensuite sa propre adresse IP dans la table d'adresses, à la place de celle qu'il vient de prendre. Une petite décrémentation de "Segments left" et le paquet peut être réémis dans le réseau.

Chaque host "étape" procédera à la même réflexion, en montant de moins en moins haut dans la table d'adresses, jusqu'à la destination finale.

9.2.10 Entête IPv6 de fragmentation



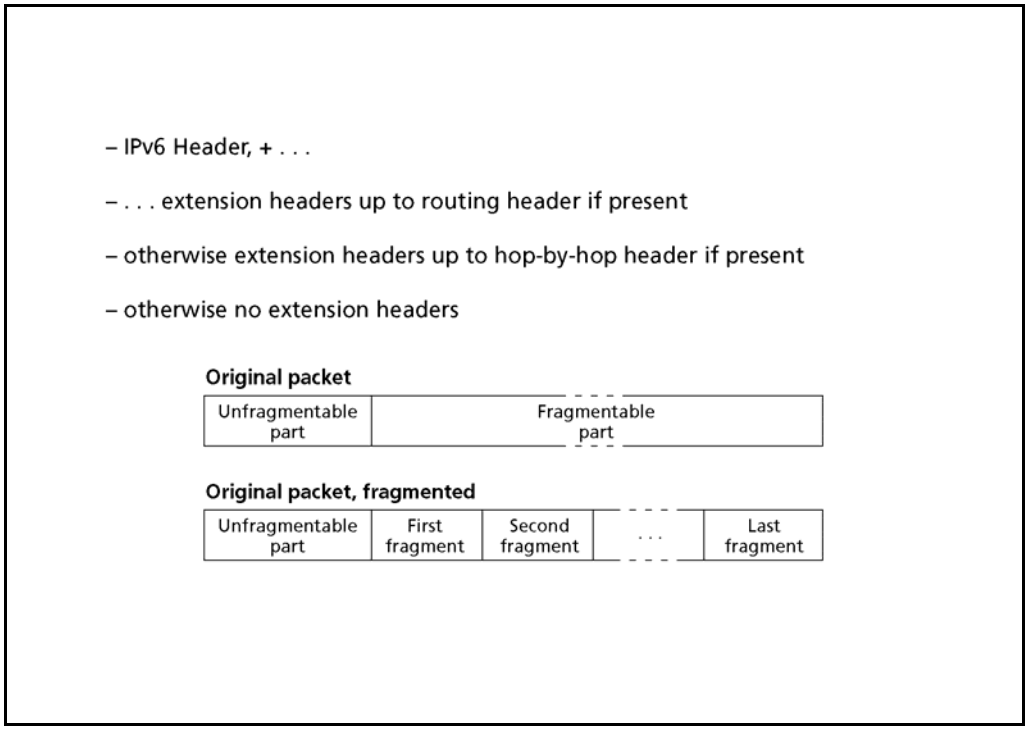
Slide 9.18
Entête IPv6 de fragmentation

Fragmentation Header

Lorsqu'un paquet est trop grand pour passer dans un réseau, il doit être fragmenté. Avec IPv6 seule la source peut fragmenter un paquet. Un routeur confronté au problème va détruire le paquet et indiquer à la source le besoin de fragmenter.

Next Header indique la prochaine entête. Reserved doit être laissé à 0. Fragment offset code le numéro du premier octet par rapport à l'entête du paquet original, divisé par 8. L'offset indique donc le numéro du 1er groupe de 8 octets composant le fragment. Res est réservé est doit être à 0. M indique s'il y a encore des octets (M=1, More fragments). Identification sert à identifier tous les fragments d'un même paquet original.

9.2.11 Partie infragmentable



Slide 9.19
Partie infragmentable

La fragmentation est effective entre la source et la destination finale. Certaines entêtes doivent être traitées dans les routeurs (hop-by-hop) ou dans les stations "visitées" en chemin (routing et entêtes la précédant).

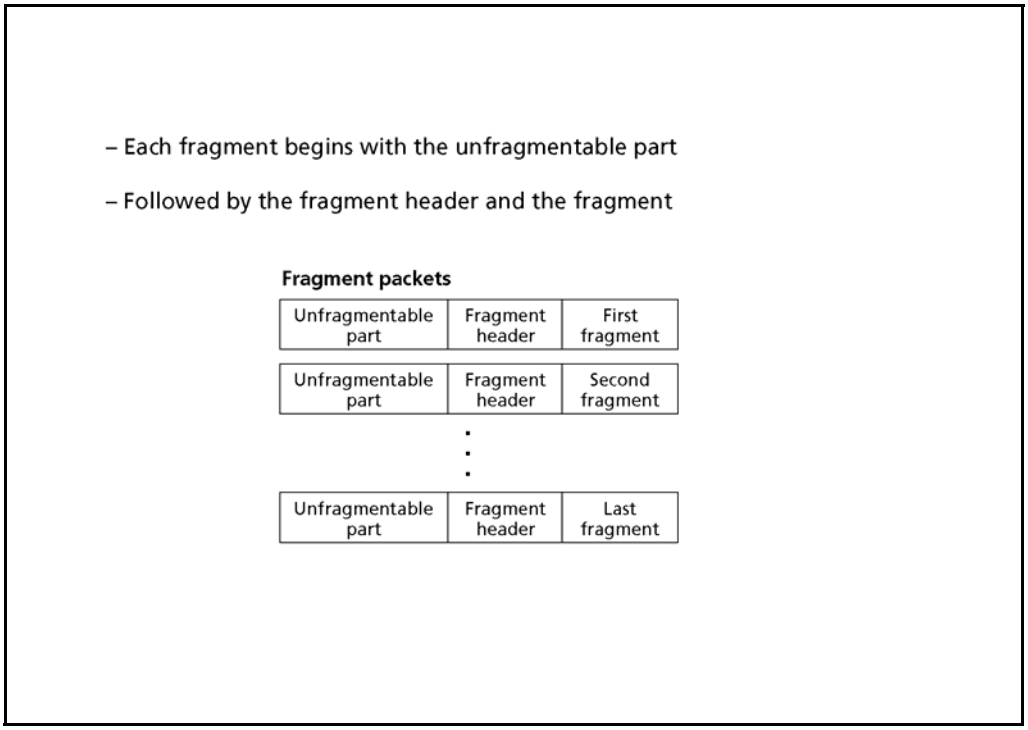
Unfragmentable Part

Ces entêtes doivent rester "lisibles" et ne peuvent, par conséquent, pas être fragmentées. Elles forment la partie infragmentable du paquet original.

Cela donne toutes les entêtes jusqu'à et y compris l'entête de routage. Si elle n'est pas présente, l'entête d'extension Hop-by-hop seulement accompagnera l'entête IPv6 dans la partie infragmentable. Si Hop-by-hop manque également, seule l'entête IPv6 se trouvera dans la partie infragmentable.

Les autres entêtes d'extensions peuvent être fragmentées.

9.2.12 Construction du fragment



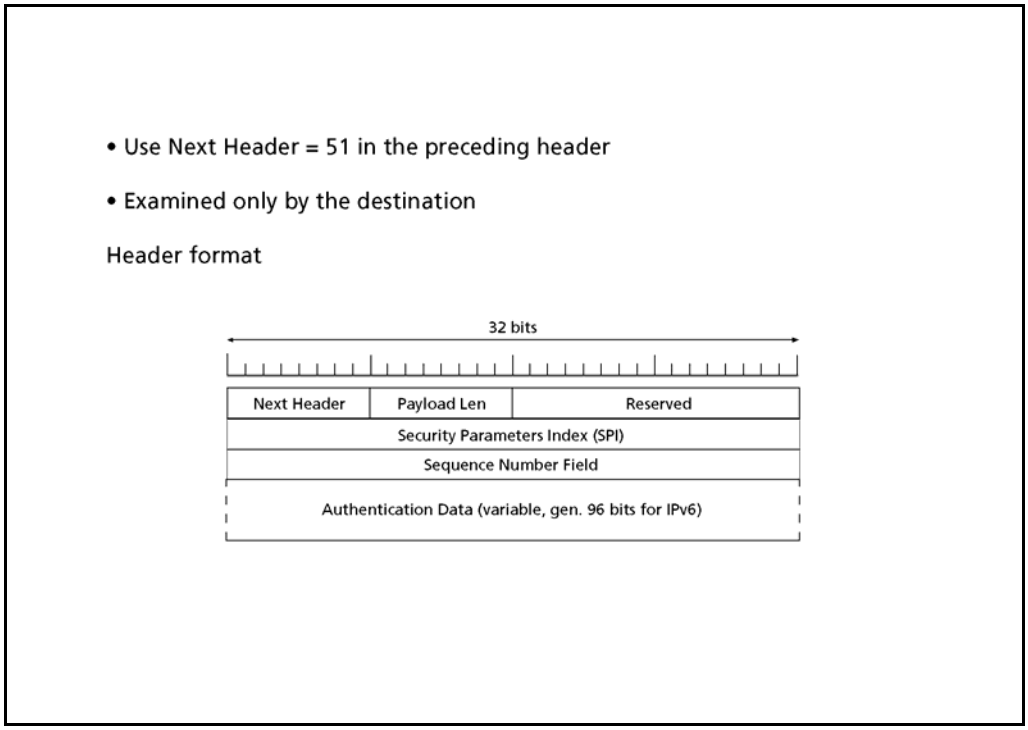
Slide 9.20
Construction du fragment

Chaque nouveau paquet contiendra la partie infragmentable du paquet original. Seuls les champs de longueur IPv6 et Next header de la dernière entête sont modifiés. IPv6 Payload Length correspondra à la longueur du paquet créé (fragment packet). Next Header de la dernière entête de la partie infragmentable passe à 44, indiquant ainsi la présence de l'entête de fragmentation.

Celle-ci va donc directement suivre la partie infragmentable. Elle précède le fragment lui-même.

Les valeurs fragment offset et M-flag s'utilisent comme leurs homologues de IPv4. Ces fragmentations sont compatibles.

9.2.13 Entête IPv6 d'authentification



Slide 9.21
Entête IPv6 d'authentification

Authentication Header

Cette entête permet d'authentifier l'auteur du paquet. [RFC 2402]

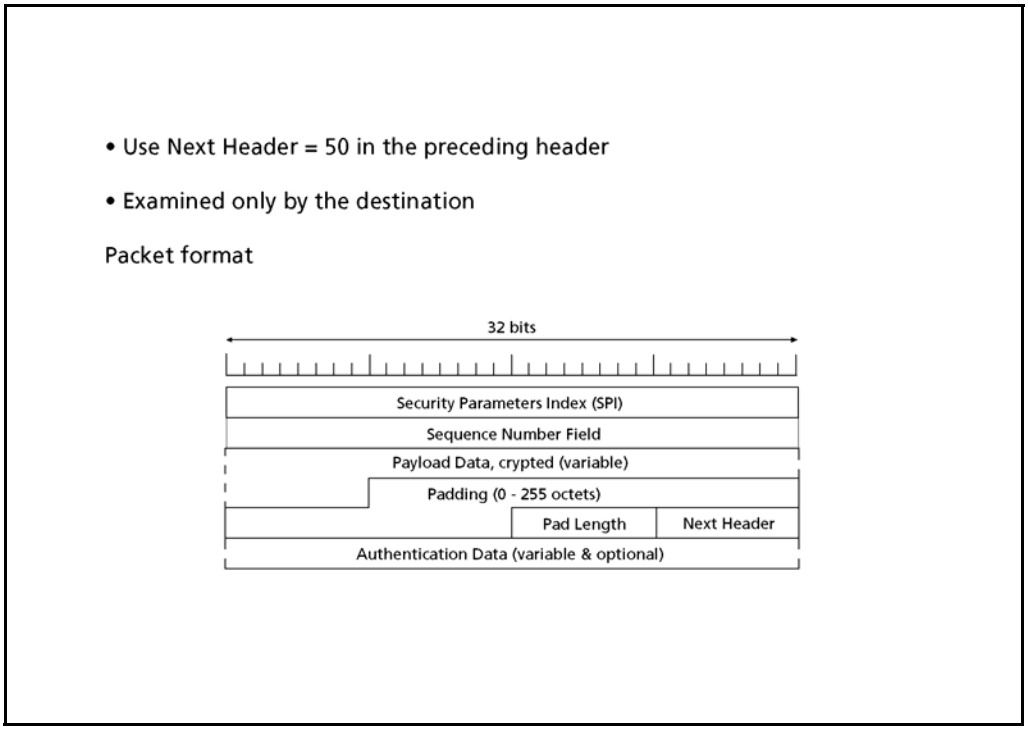
Next Header représente la prochaine entête.

Payload length est exprimé en mot de 32 bits. Il représente la longueur totale, sans les 64 premiers bits. Ce format particulier permet d'être compatible avec les formats IPv4 (longueur N x 4 octets) et IPv6 (longueur N x 8 octets).

SPI est un nombre arbitraire qui, associé à l'adresse IP destination et au protocole d'authentification, permet de calculer une valeur placée dans Authentication Data. C'est ce résultat, connu seulement des deux côtés, qui assure l'authentification de la source.

Sequence Number part de 0 et sera incrémenté dans les paquets successifs.

9.2.14 Cryptage IPv6, format de paquet



Slide 9.22
Cryptage IPv6 : Format de paquet

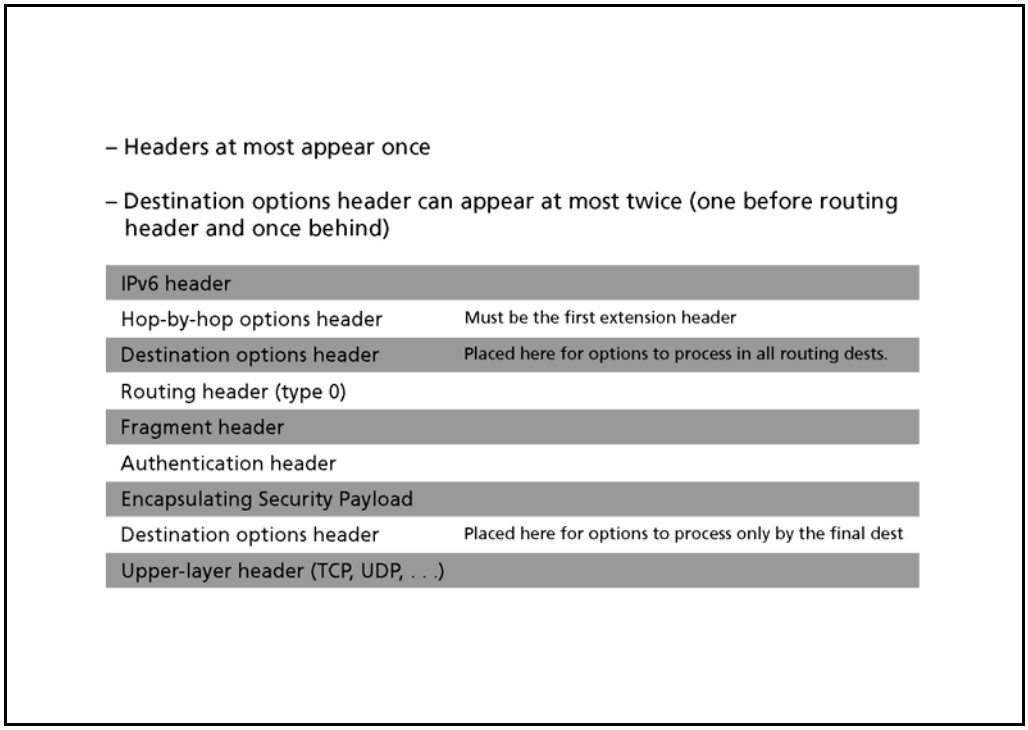
Ici la notion d'entête est un peu dépassée. La "suite" du paquet IP se trouve en fait au milieu du paquet de cryptage, dans le champ Payload Data. Les champs suivants ne sont plus cryptés et terminent le paquet IP. [RFC 2406]

ESP (Encapsulating Security Payload)

Les champs SPI et Sequence Number ont les mêmes fonctions que pour l'entête d'authentification. Suivant le protocole de cryptage (encoding) et la longueur des données IP, du padding peut-être nécessaire. Sa longueur est définie dans le champ Pad Length. Next Header représente la prochaine entête. Celle-ci se trouve en fait dans le champ Payload data.

En fonction du protocole de cryptage un calcul d'authentification peut être fait, son résultat sera stocké dans le champ Authentication Data.

9.2.15 Entête d'extension IPv6, ordre d'apparition



Slide 9.23
Entête d'extension
IPv6, ordre d'apparition

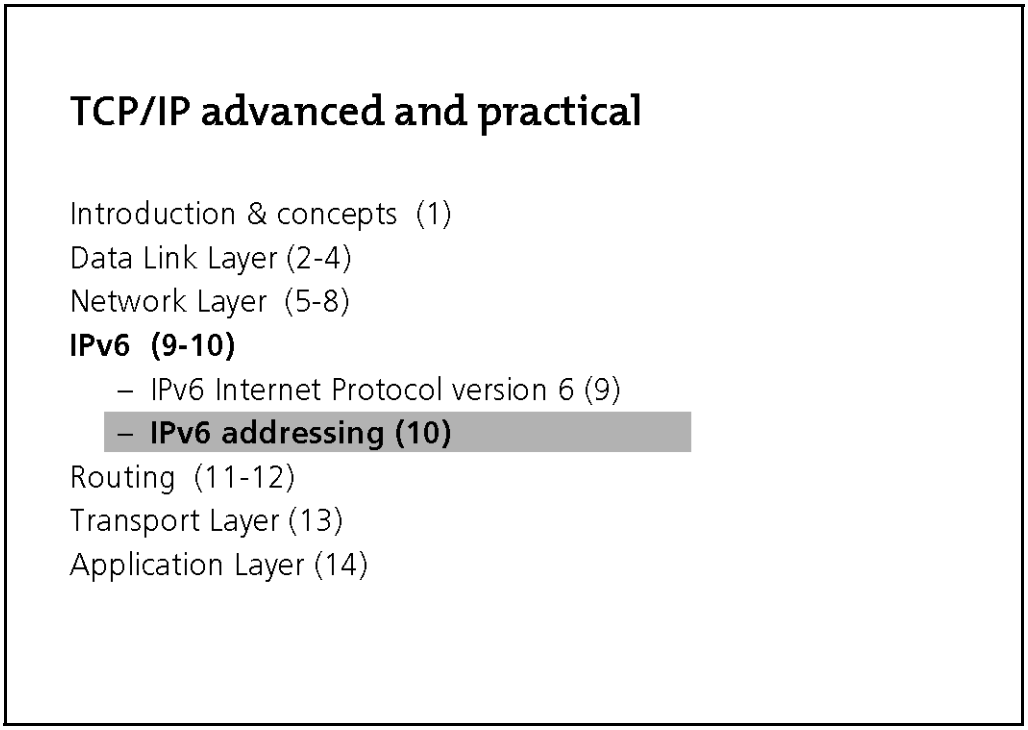
Chaque entête ne doit pas apparaître plus d'une fois dans un paquet IP.

L'entête Destination Options peut apparaître au maximum deux fois, une fois avant l'entête de routage (pour les options traitées par toutes les "étapes visitées") et une fois après (pour les options traitées uniquement par la destination finale).

L'entête hop-by-hop options doit toujours être placée en tête, directement après l'entête IPv6. Les routeurs devant traiter ces options ne "scannent" pas tout le paquet à sa recherche.

Les entêtes sont traitées dans leur ordre d'apparition. Cet ordre permet à toutes les options d'être prises en compte. On peut toutefois changer l'ordre d'apparition si notre configuration nous l'autorise (sans déroger aux règles ci-dessus).

10 Adressage IPv6



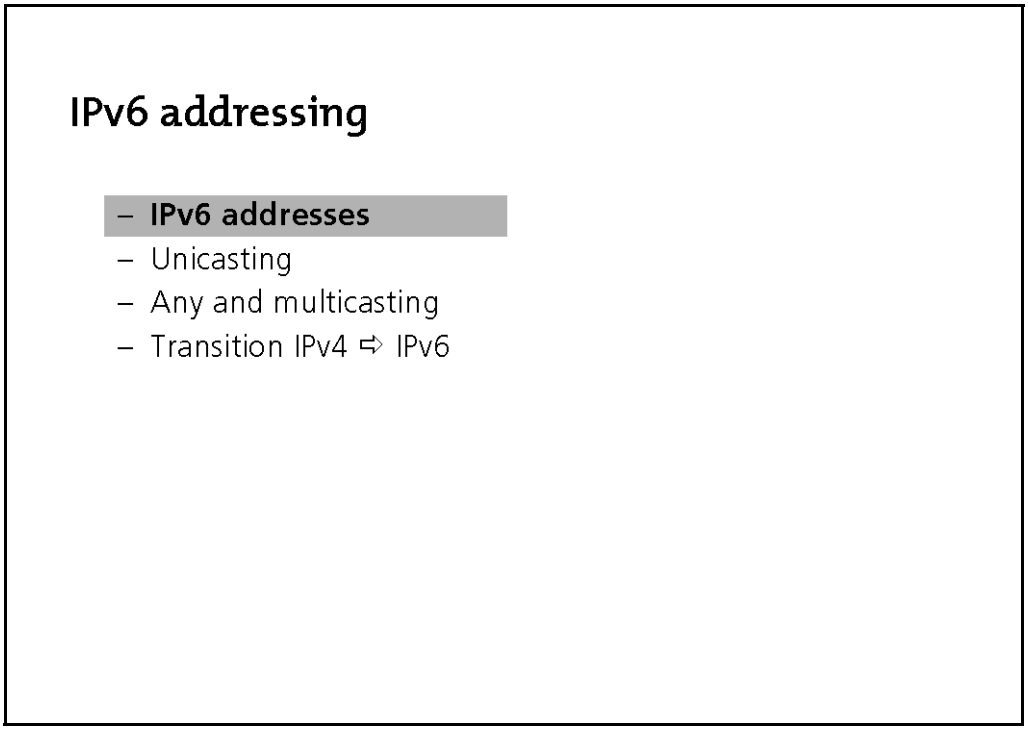
Slide 10.1
Adressage IPv6

Ce chapitre traite spécifiquement de l'adressage dans un réseau IPv6.

A l'issue de ce chapitre, les participants sont capables de reconnaître les catégories d'adresses IPv6 et d'en nommer les avantages par rapport à IPv4.

Objectifs

10.1 Adresses IPv6

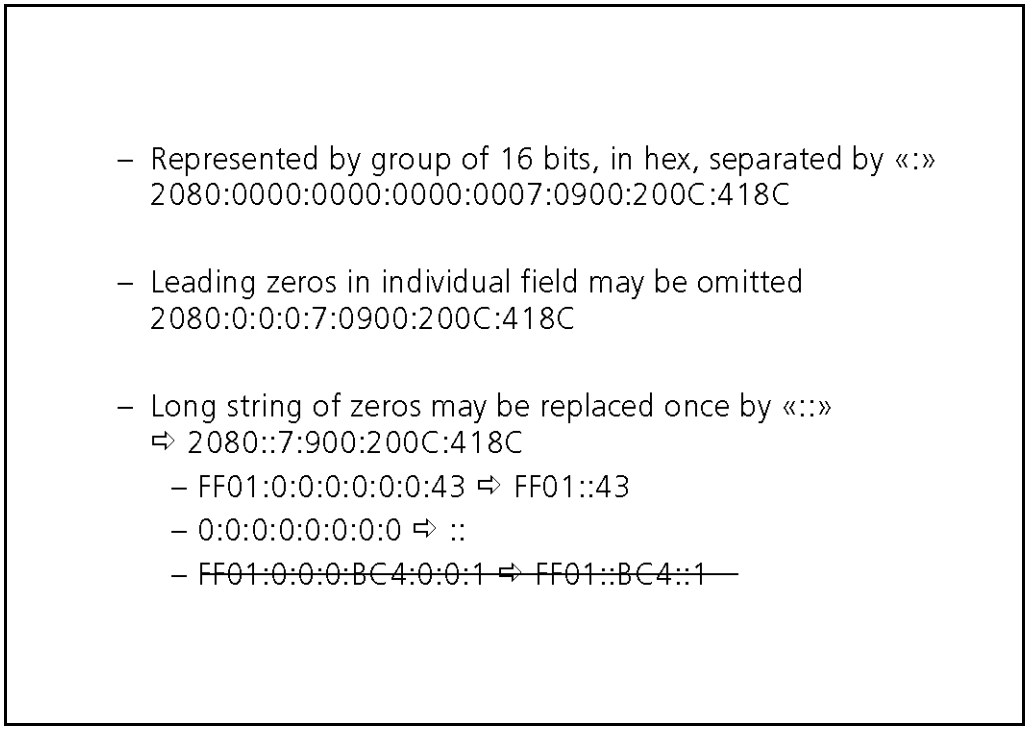


Slide 10.2
Adresses IPv6

La structure de l'adressage IPv6 est décrit dans [RFC 2373].

Le format d'adresse utilisé pour le unicasting global, l'adresse agrégée globale (Aggregatable Global Unicast Address) est décrite dans [RFC 2374]

10.1.1 Représentation des adresses IPv6



Slide 10.3
Représentation des adresses IPv6

IPv6 Address

L'adresse IPv6 se note en hexadécimal. Elle se représente sous forme de 8 groupes de 16 bits chacun, séparés par le caractère ":".

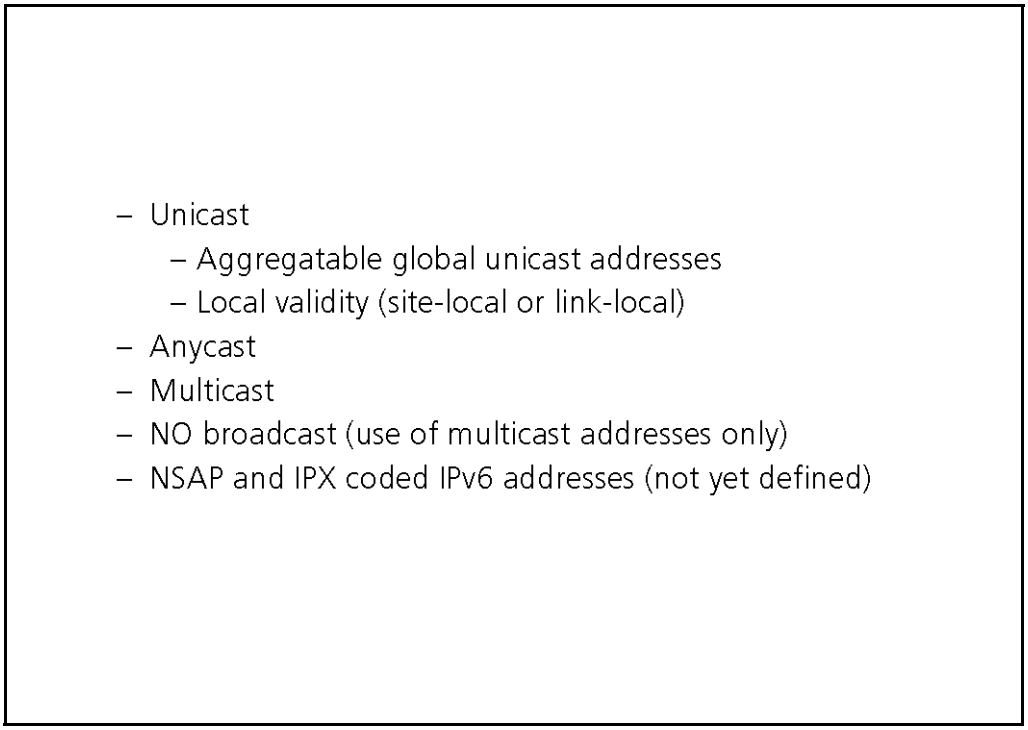
Héxadecimal

La forme hexadécimale code 4 bits par caractère. Ceci simplifie la lecture de l'adresse par rapport au binaire.

Les zéros non significatifs peuvent être omis individuellement dans chaque champ.

Une suite de champs consécutifs à zéro peut être remplacée par un "::". Ce symbole ne peut apparaître qu'une fois dans l'adresse, afin de ne pas perdre la position des champs placés entre ces symboles.

10.1.2 Types d'adresses IPv6



Slide 10.4
Types d'adresses IPv6

Les adresses IPv6 se déclinent en plusieurs formats.

Les adresses unicast, permettant une liaison point à point entre deux partenaires, peuvent avoir une validité globale ou locale.

Unicast

Les adresses anycast sont attribuées à plusieurs interfaces. Un paquet à destination d'une adresse anycast atteindra l'interface la plus proche possédant cette adresse.

Anycast

Les adresses multicast ont plus d'importance que pour IPv4. Ce sont ces adresses qui seront utilisées pour la diffusion dans le réseau. Les adresses traditionnelles de diffusion (broadcast) n'existent pas dans le schéma d'adressage de IPv6.

Multicast

En outre, on prévoit de coder les adresses NSAP et IPX au format IPv6.

NSAP, IPX

10.1.3 Préfixes d'adresses IPv6

Allocation	Prefix (binary)	Fraction of address space
Reserved (unspecified, loopback, . . .)	0000 0000	1/256
Unassigned	0000 0001	
Reserved for NSAP allocation	0000 001	
Reserved for IPX allocation	0000 010	1/128
Unassigned	0000 011	
Unassigned	0000 1	1/32
Unassigned	0001	1/16
Aggregatable global unicast addresses	001	
Unassigned	010	
Unassigned	011	1/8
Unassigned	100	
Unassigned	101	
Unassigned	110	
Unassigned	1110	1/16
Unassigned	1111 0	1/32
Unassigned	1111 10	1/64
Unassigned	1111 110	1/128
Unassigned	1111 1110 0	1/512
Link-local unicast addresses	1111 1110 10	1/1024
Site-local unicast addresses	1111 1110 11	1/1024
Multicast adresses	1111 1111	1/256

Slide 10.5
Préfixes d'adresses IPv6

Aggregatable Global Unicast

L'espace d'adressage de IPv6 a été entièrement divisé. Actuellement seul une partie de ce domaine d'adressage est défini. La partie la plus importante (1/8) est utilisée par les adresses unicast "Aggregatable Global Unicast".

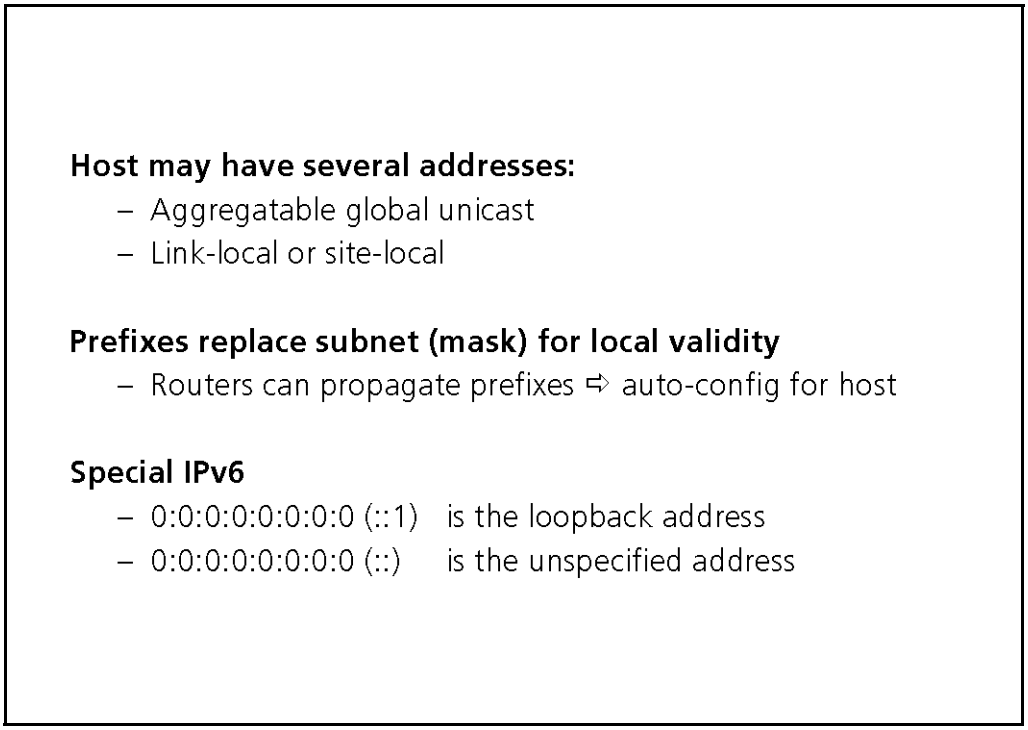
Link local, Site local

On découvre deux niveaux d'adressage locaux : link et site local. Il suffit de placer ce préfixe devant la partie "host" de l'adresse IPv6 pour lui donner une validité locale.

EUI-64

Les adresses préfixées de 001 à 111, sans les adresses multicast (1111 1111), possèdent toutes une partie "host" de 64 bits. Cette partie sera codée selon le standard EUI-64.

10.1.4 Adressage IPv6



Slide 10.6
Adressage IPv6

Les clients d'un réseau IPv6 peuvent avoir plusieurs adresses, leur adresse à validité globale et leurs adresses à validité locale (link + site).

Link, Site

La validité locale étant assurée par un préfixe, aucun masque de sous-réseau n'est nécessaire pour envoyer des paquets dans notre réseau. On peut facilement atteindre un routeur, qui peut nous indiquer quel est le préfixe de notre link ou site. C'est une manière simple pour découvrir l'adresse de notre réseau. Ceci permet donc une configuration automatique des adresses.

Configuration automatique

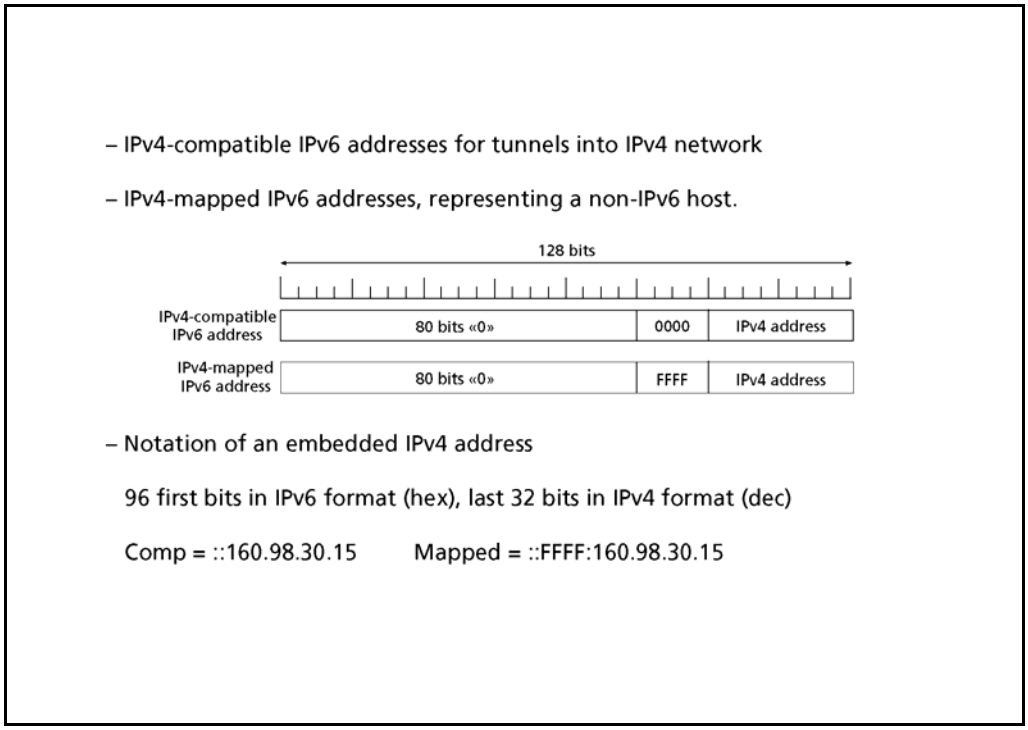
"::1" est l'adresse de loopback, elle correspond à l'adresse IPv4 127.0.0.1.

Loopback Address

"::" est l'adresse non spécifiée. Elle sera utilisée par une machine qui ne connaît pas son adresse IP.

Unspecified Address

10.1.5 Inclusion des adresses IPv4 dans IPv6



Slide 10.7
Inclusion des adresses IPv4 dans IPv6

Deux formats de codage des adresses IPv4 en adresses IPv6 ont été définis.

IPv4 Compatible Address

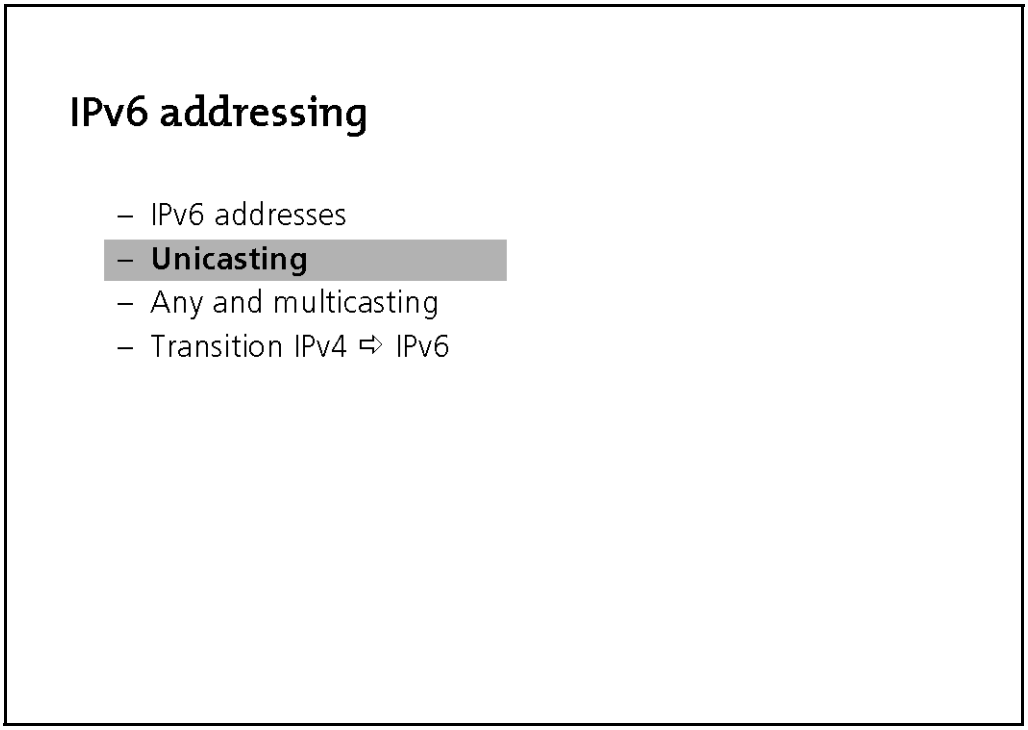
Le premier s'adresse aux machines devant établir des "tunnels" à travers un réseau IPv4. Ce format s'appelle "IPv4-compatible IPv6 address".

IPv4 Mapped Address

Le deuxième format sert à construire une adresse IPv6, afin de faire passer un paquet dans un réseau IPv6, de ou à destination d'une machine dans laquelle seul IPv4 est implanté. Il s'appelle "IPv4-mapped IPv6 address".

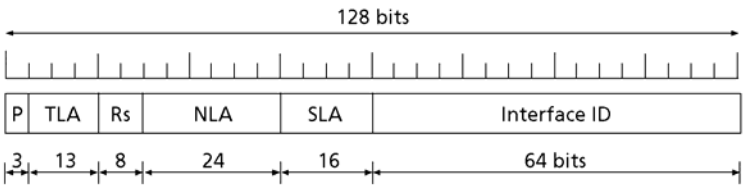
La représentation de ces adresses diffère un petit peu des autres adresses IPv6. On autorise la notation des 32 derniers bits au format IPv4 (4 octets décimaux, séparés par des points). Cela permet de reconnaître l'adresse IPv4 dans l'adresse IPv6.

10.2 Unicasting



Slide 10.8
Unicasting

10.2.1 IPv6 Unicasting global



P	Prefix = 001
TLA	Top-level Aggregation Identifier
Rs	Reserved for future use (extension of TLA and/or NLA)
NLA	Next-level Aggregation Identifier
SLA	Site-level Aggregation Identifier
Interface ID	Interface Identifier in EUI-64 format (Host address)

Slide 10.9
IPv6 Unicasting global

Aggregatable Global Unicast Address

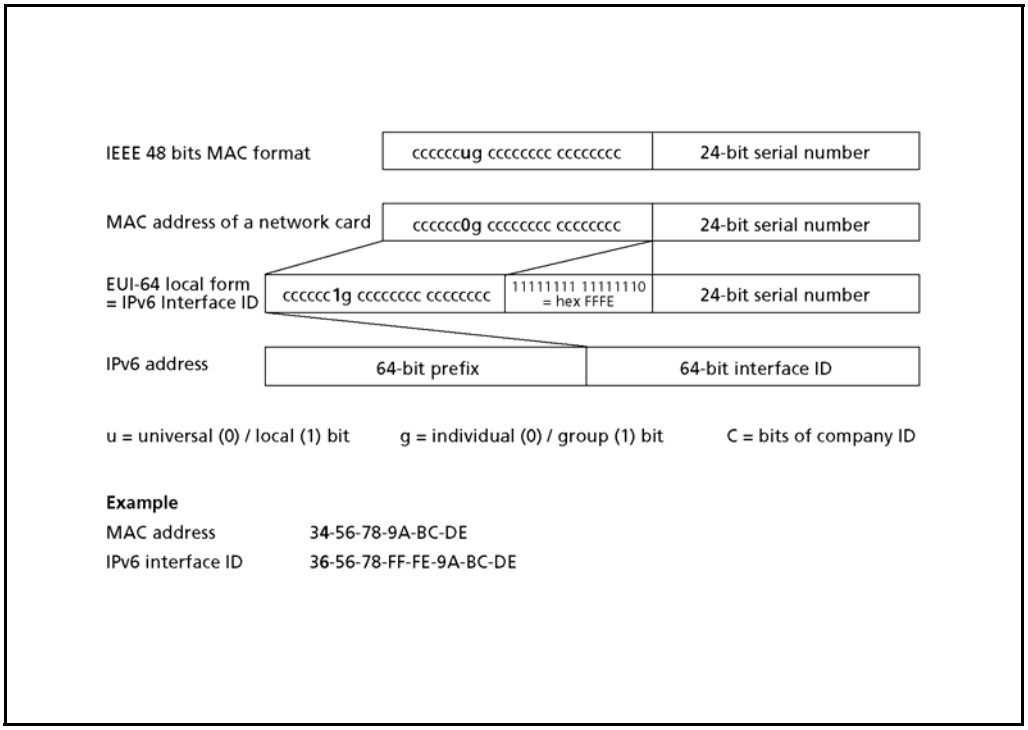
L'adresse agrégée globale IPv6 est décrite dans [RFC 2374]. Elle décomposée en deux groupes principaux.

TLA, NLA, SLA, Interface ID

La partie "Interface ID" permet de différencier de manière univoque un host sur son link. Le reste de l'adresse représente la partie réseau. Elle commence par 3 bits de préfixe, suivis de 3 parties TLA, NLA et SLA. Une partie réservée permettra d'étendre TLA et/ou NLA, selon les besoins futurs.

Les entreprises nécessitant un grand réseau se verront attribuer un TLA. Elle pourra profiter du champ NLA pour différencier ses différents sites et/ou ses différents services. Les sociétés plus petites recevront un couple TLA-NLA. Chacune d'elles pourra construire des sous-réseaux avec SLA.

10.2.2 Adresses IPv6, identificateur d'interface



Slide 10.10
Adresses IPv6, identificateur d'interface

Les formats IEEE-48 (MAC) et EUI-64 possèdent chacun 2 bits particuliers, définissant la portée (validité) de l'adresse (bit u) et sa fonction (bit g).

IEEE-48, EUI-64

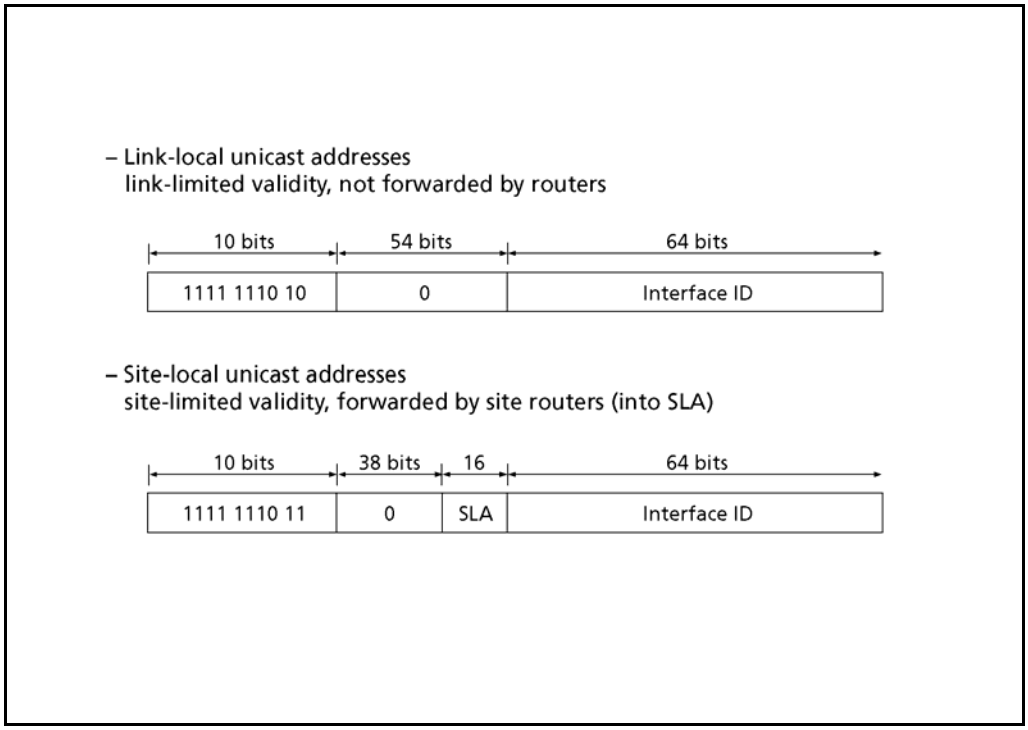
Pour écrire une adresse MAC au format EUI-64, il suffit d'ajouter 2 octets (FFFE) au milieu de l'adresse, entre la partie "code du fabricant" et le n° de série de la carte.

Dans le cas de IPv6, afin d'éviter des conflits avec d'autres technologies de réseau, on limitera la validité de cette adresse à notre link en activant le bit u.

validité locale

La validité globale de l'adresse IPv6 n'existe qu'avec le préfixe complet.

10.2.3 IPv6 Unicasting local



Slide 10.11
IPv6 Unicasting local

IPv6 offre deux formats d'adresses à validité locale.

Link Local

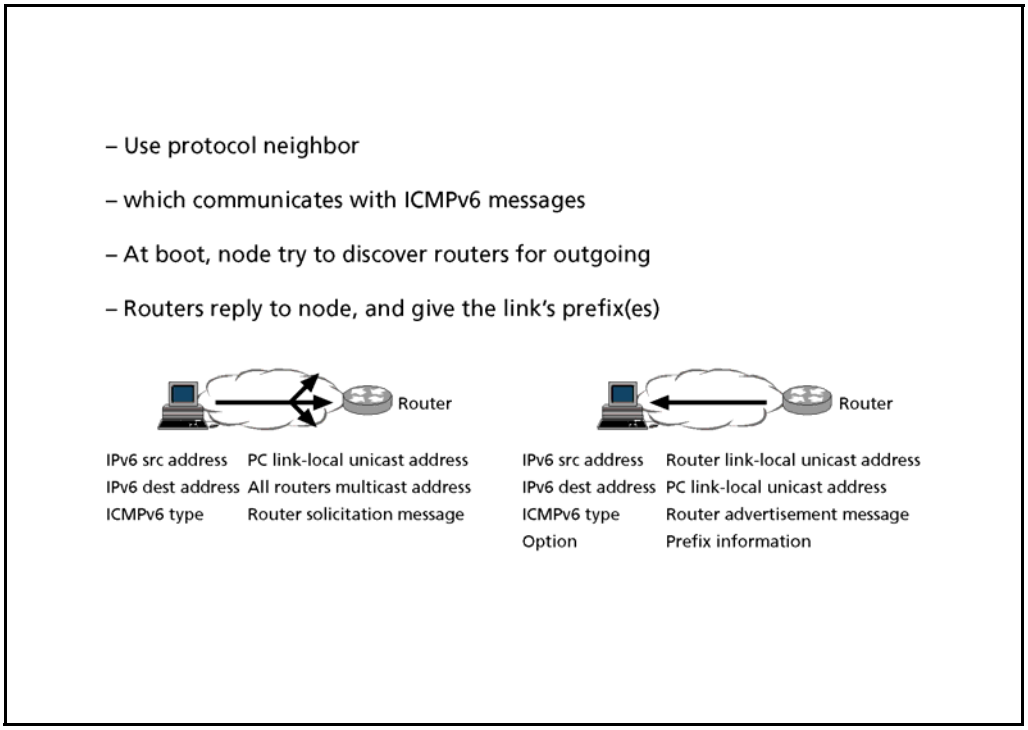
Link-local unicast addresses permet de faire voyager un paquet IP à l'intérieur d'un sous-réseau. Aucun routeur ne conduira ce paquet dans un autre sous-réseau. Ce format d'adresse est équivalent à une adresse IPv4 avec la partie réseau à 0.

Site Local

Site-local unicast addresses autorise le paquet à voyager plus loin dans le réseau. La validité est limitée à notre NLA, normalement utilisée pour différencier nos sites. Dans ce cas notre adresse de sous-réseau (SLA) doit être spécifiée.

Les routeurs IPv6 donnent les préfixes des SLA's, respectivement des NLA's. Ces adresses locales permettent donc la configuration automatique des adresses.

10.2.4 Configuration automatique des adresses



Slide 10.12
Configuration automatique des adresses

Toute machine IPv6 possède une adresse IP au boot. Il s'agit de son identificateur d'interface avec le préfixe "link-local".

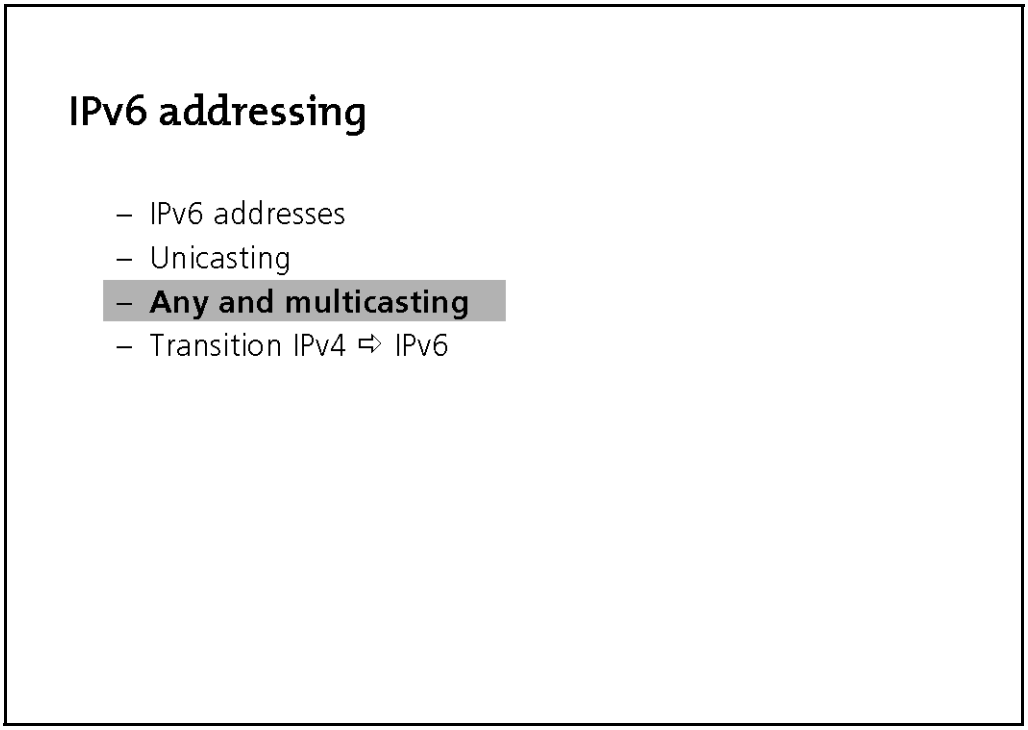
Cette adresse lui permet de se renseigner sur l'existence de routeur(s) permettant de sortir de son sous-réseau (link). Les routeurs concernés vont s'annoncer, et livrer le préfixe nécessaire pour rendre l'adresse de la machine globale.

Auto-Config

Ces échanges s'appuient sur un protocole appelé "Neighbor Discovery". Celui-ci gère tous les problèmes de résolution d'adresses dans un link. Il utilise des messages ICMPv6, accompagnés d'options.

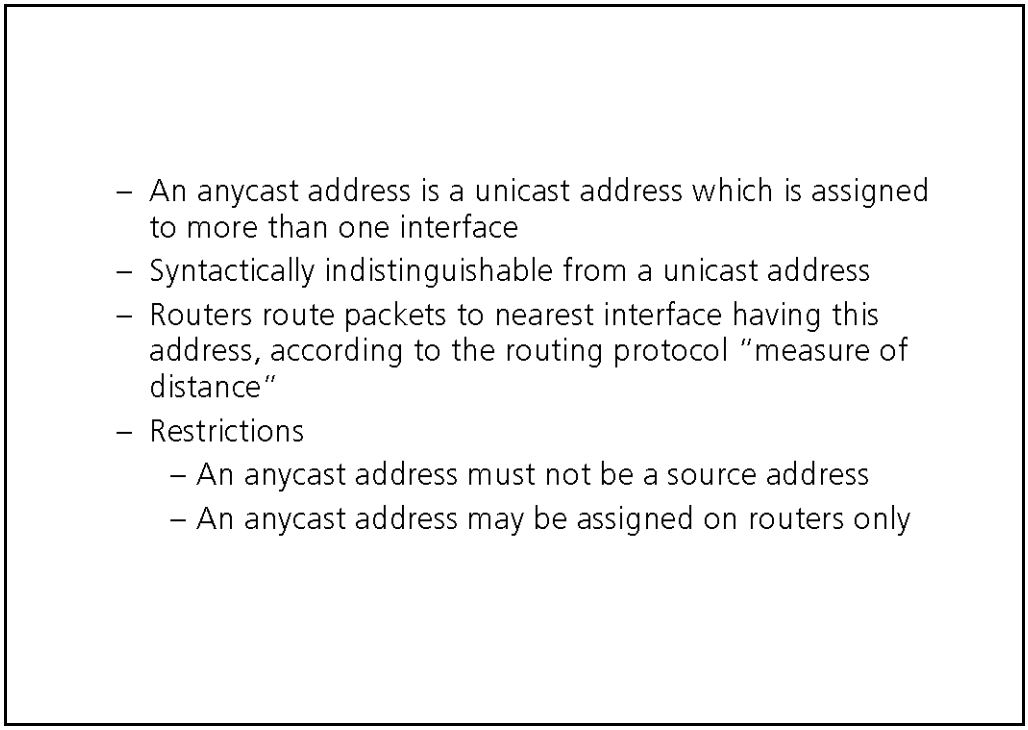
Neighbor Discovery

10.3 Any & Multicasting



Slide 10.13
Any & Multicasting

10.3.1 IPv6 Anycasting



Slide 10.14
IPv6 Anycasting

Anycasting

Les adresses anycast sont nouvelles par rapport à IPv4. Le principe est de donner la même adresse à plusieurs interfaces (plusieurs routeurs).

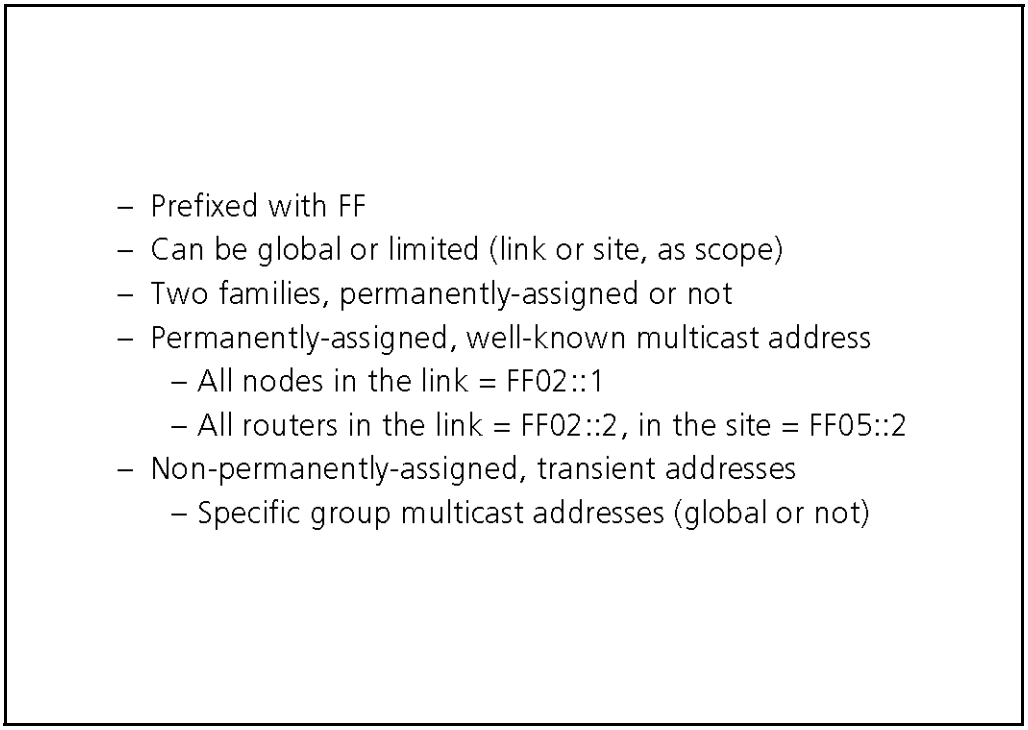
Ces adresses sont prises dans la zone d'adressage unicast. Une adresse unicast attribuée plus d'une fois devient automatiquement anycast. On ne peut pas différencier des adresses unicast et anycast à leur syntaxe.

Nearest Interface, Interface la plus proche

Un paquet à destination anycast atteindra l'interface la plus proche possédant cette adresse. On utilise pour cela les mesures de distance des protocoles de routage.

En attendant d'avoir plus d'expérience avec ces adresses, des restrictions ont été posées. Seuls les routeurs peuvent avoir des adresses anycast. Aucun paquet ne sera envoyé avec une adresse source anycast.

10.3.2 IPv6 Multicasting



Slide 10.15
IPv6 Multicasting

Les adresses multicast IPv6 sont toutes préfixées par "FF". Le deuxième octet de l'adresse permettra de définir la "portée" de cette adresse (limitée au link, au site, …). Cet octet séparera aussi les adresses multicast permanentes des adresses non-permanentes, spécifiques à des groupes particuliers.

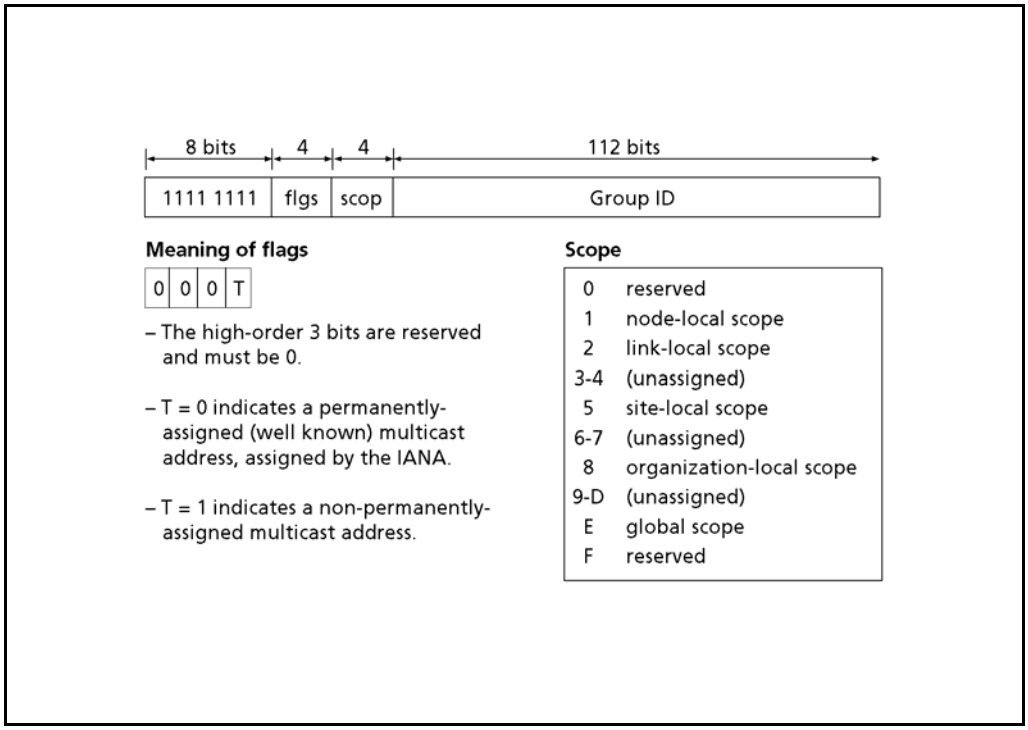
Broadcast

On notera l'adresse FF02::1, à destination de tous les nœuds sur notre link. Elle est équivalente à l'adresse de diffusion de sous-réseau IPv4 (255.255.255.255).

Les adresses FF0x::2 représentent tous les routeurs, "x" nous indiquera la "profondeur" de la distribution.

Plusieurs autres adresses permanentes ont été attribuées par l'IANA.

10.3.3 Format d'adresse multicast



Slide 10.16
Format d'adresse multi-cast

Après le préfixe "FF" on trouve un octet décomposé en deux champs.

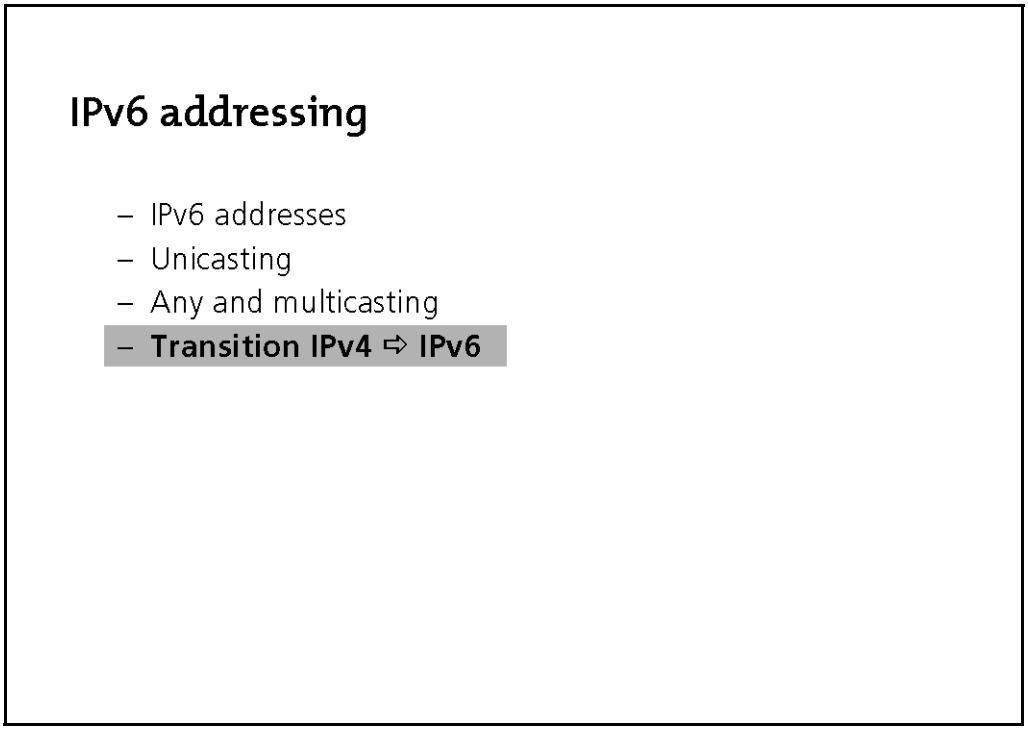
Le premier est composé de 4 indicateurs, dont les trois premiers n'ont actuellement pas d'utilisation. Le dernier indique s'il s'agit d'une adresse permanente ou non.

Scope

Les 4 bits suivants forme le "scope". Il s'agit d'un nombre indiquant la validité de cette adresse. Elle peut être limitée au nœud lui-même (interne à l'équipement), s'étendre au lien (sous-réseau), au site, à toute l'organisation ou encore à tout l'Internet.

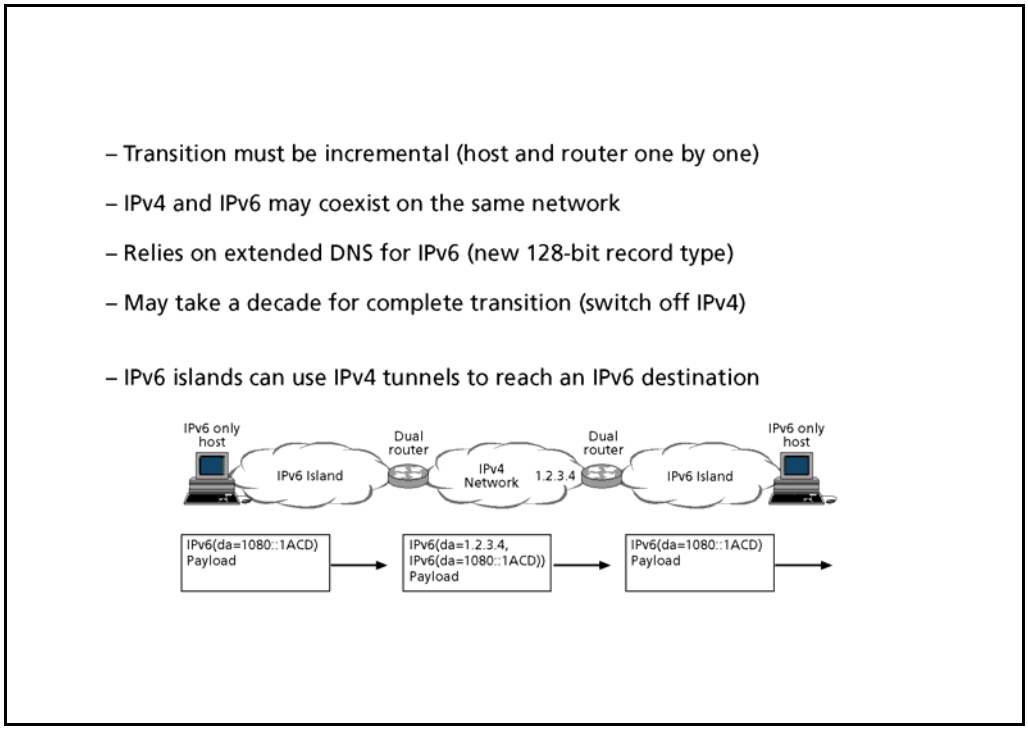
112 bits indiquent enfin quel groupe est visé par cette adresse multicast.

10.4 Transition IPv4 → IPv6



Slide 10.17
Transition IPv4 → IPv6

10.4.1 Principe de transition



Slide 10.18
Principe de transition

Tunnels

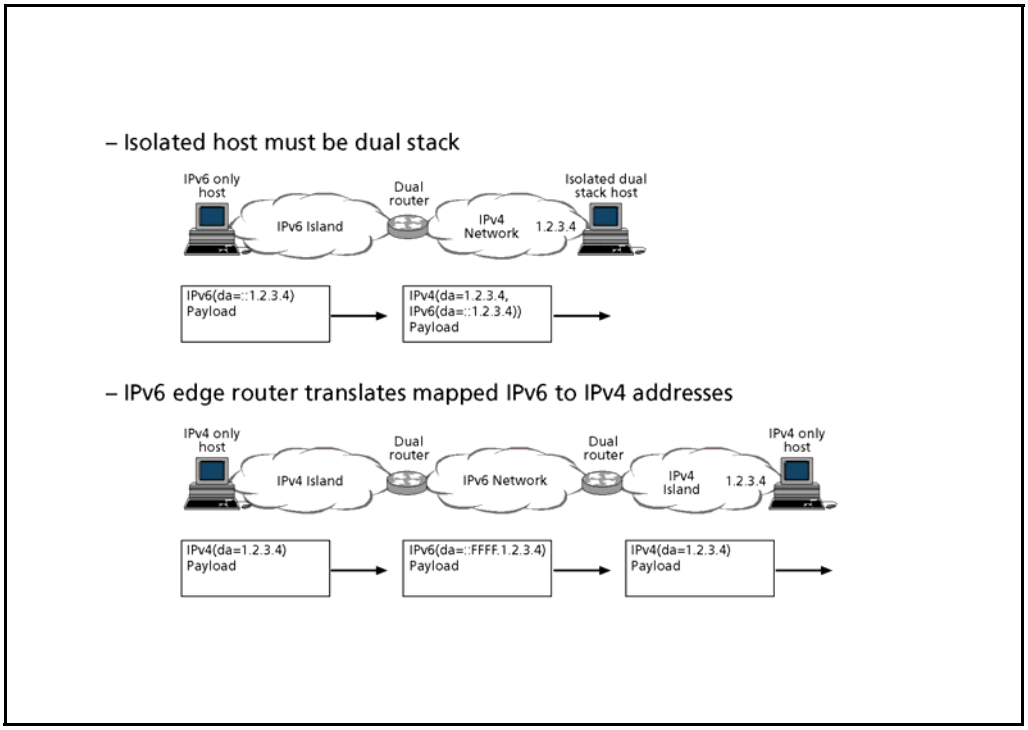
L'introduction d'IPv6 n'entraînera pas la disparition immédiate de IPv4. On prévoit une implémentation incrémentale de IPv6. La transition devrait prendre une dizaine d'année, jusqu'à la disparition totale d'IPv4.

Dual Routers

Pendant cette décade, ces deux protocoles devront coexister sur le réseau.

Des réseaux IPv6 pourront, à travers des tunnels IPv4, atteindre n'importe quel autre réseau IPv6 ou host IPv6 isolé.

10.4.2 Transition IPv4 → IPv6, exemples



Slide 10.19
Transition IPv4 → IPv6, exemples

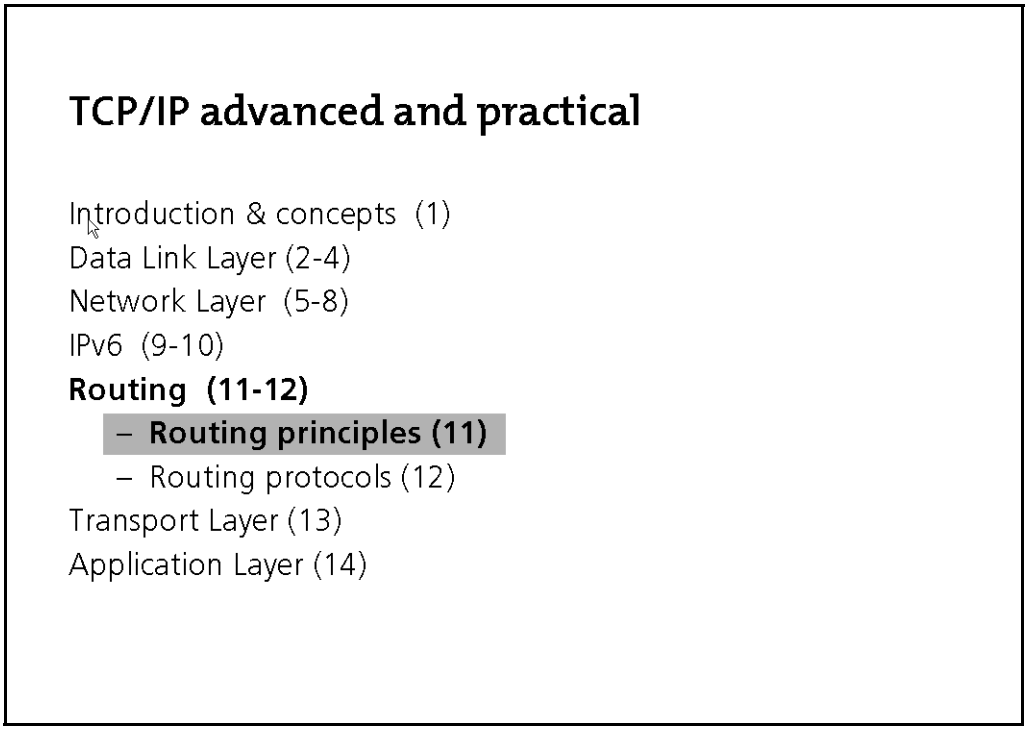
Les hosts IPv6 isolés dans un réseau IPv4 devront être "dual stack". Ils utiliseront IPv4 pour communiquer avec des partenaires IPv4 et IPv6 dans des tunnels IPv4 pour les partenaires IPv6.

Dual stack, Tunnel

Les routeurs périphériques à un réseau IPv6 transformeront les adresses IPv4 en adresses IPv6 mappées.

Mapped

11 Principes de routage



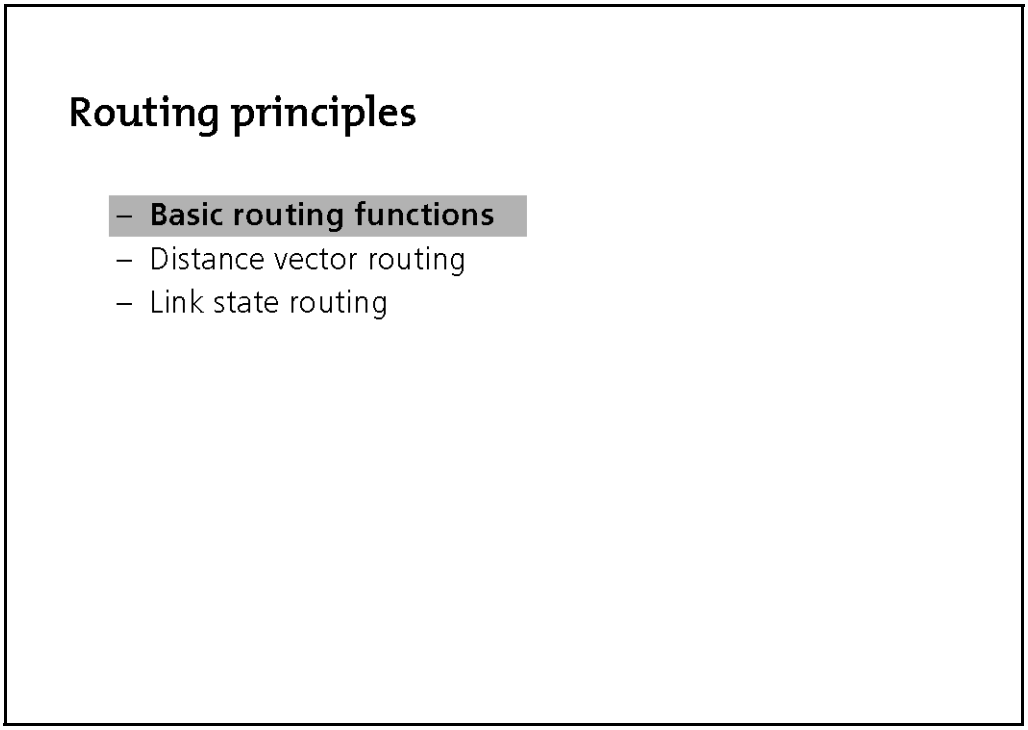
Slide 11.1
Principes de routage

Ce chapitre traite du routage. Il s'agit des protocoles mis en œuvre entre les éléments d'interconnexion des réseaux (les routeurs) pour établir dynamiquement le contenu des tables de routage (routing table). Après une présentations des principes généraux, sont présentées les deux grandes philosophies qui régissent le fonctionnement du routage : routage à vecteur de distance et routage à état des liasons.

Objectifs

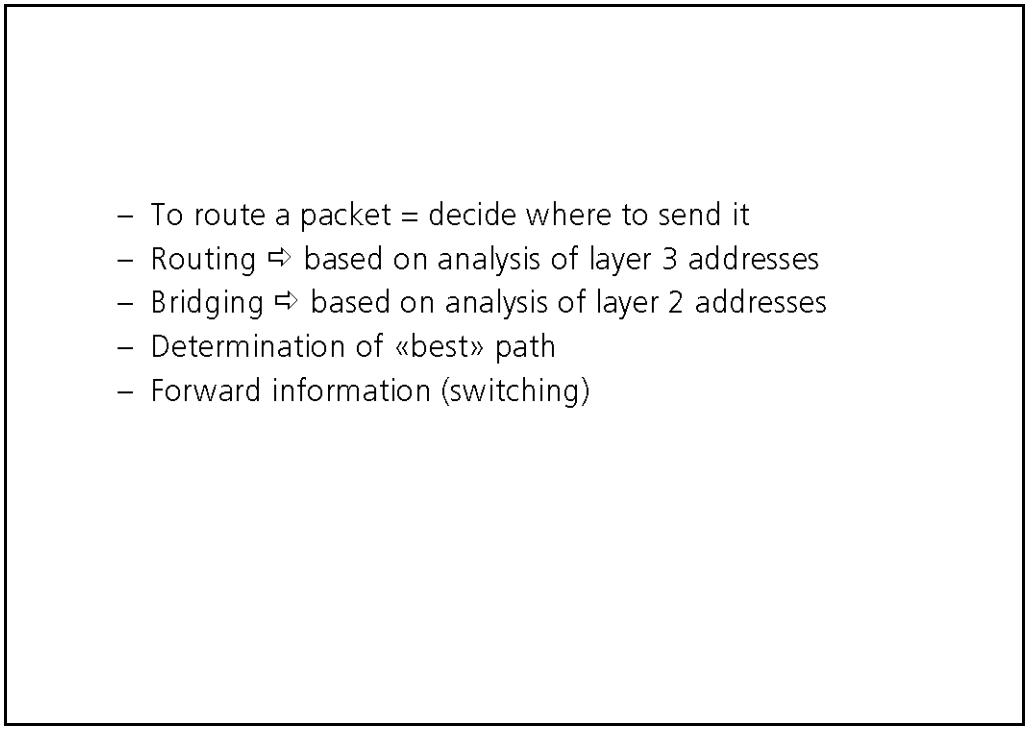
A l'issue de ce chapitre, les participants sont capables d'expliquer les différences entre le routage à vecteur de distance et celui à état des liaisons.

11.1 Fonctions de base du routage



Slide 11.2
Fonctions de base du routage

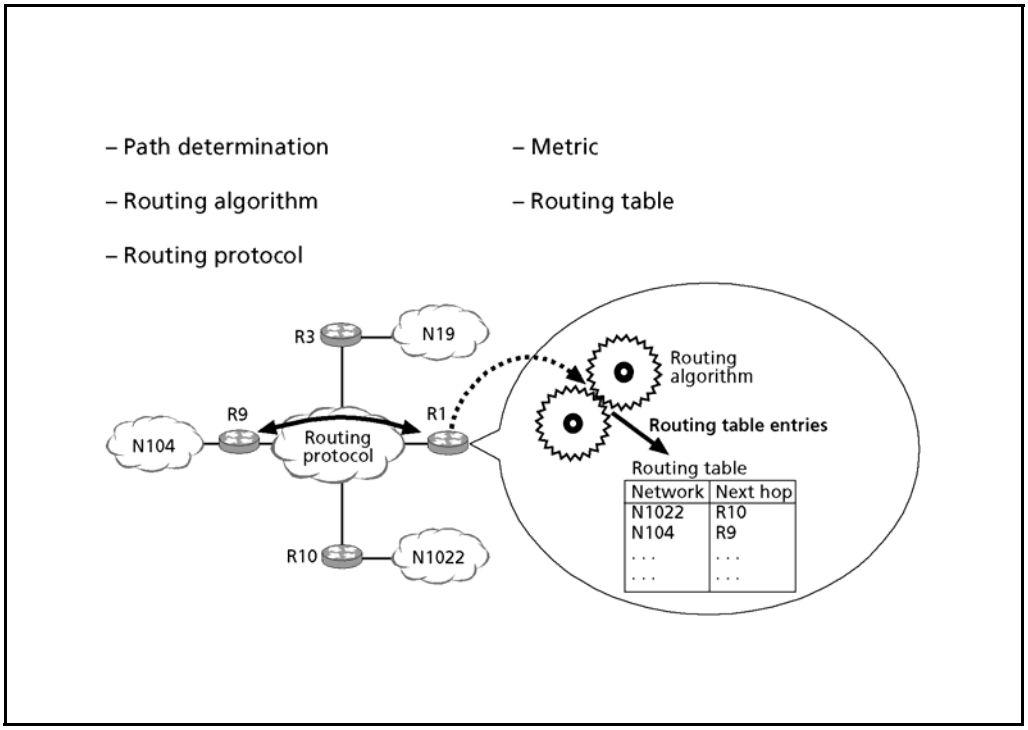
11.1.1 Principes du routage



Slide 11.3
Principes du routage

Le routage est l'action d'acheminer de l'information au travers d'un réseau, de la source vers la destination. Tout au long du chemin, au moins un nœud intermédiaire (un routeur) est rencontré. Bien qu'il puisse apparaître au premier abord, que le routage et le bridging réalisent les même fonctions, il convient de les différencier. Le routage est réalisé en utilisant des informations de niveau 3 (couche réseau du modèle OSI) alors que le bridging est opéré au niveau de la couche 2 (couche liaison de données). Le routage est constitué de deux activités principales : la détermination d'un chemin optimal et la commutation (switching) effective de l'information (des paquets).

11.1.2 Composants du routage



Slide 11.4
Composants du routage

Un "metric" est une unité de mesure, telle que la longueur d'un chemin, utilisée par les algorithmes de routage pour déterminer le chemin optimal vers une destination.

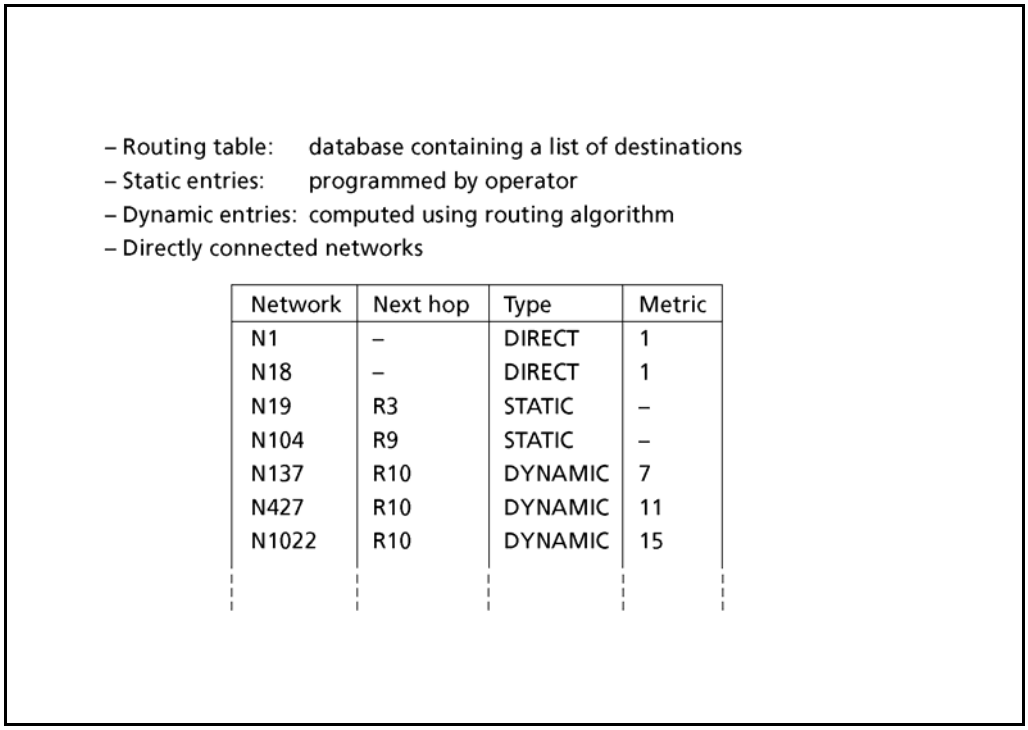
metric

Le processus de détermination d'un chemin optimal est réalisé grâce à une base de données appelée table de routage (routing table). Le type d'information contenu dans la table de routage dépend du type d'algorithme de routage. Le rôle principal d'un algorithme de routage est d'initialiser et de maintenir l'état de la table de routage.

Table de routage

Les routeurs communiquent entre eux pour maintenir leur table de routage à l'aide d'un ou de plusieurs protocoles de routage (routing protocol). Différents protocoles de routage sont décrits plus loin dans ce chapitre.

11.1.3 Table de routage



Slide 11.5
Table de routage

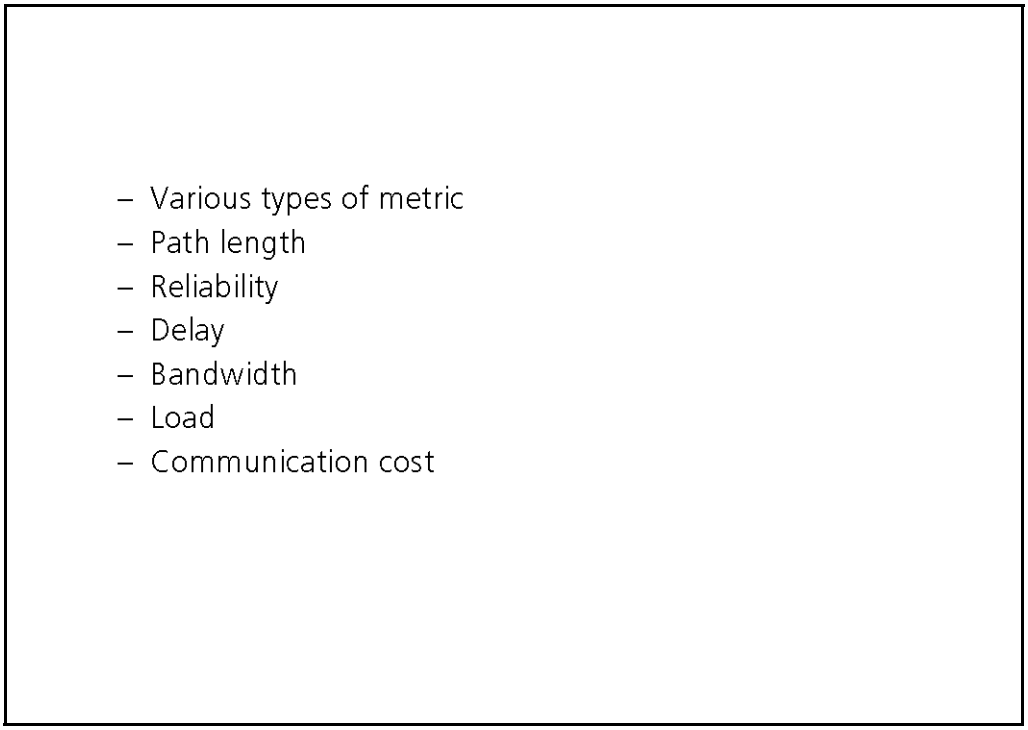
Next hop

L'algorithme de routage remplit la table de routage avec un certain nombre d'informations. Une association destination/prochain saut (next hop) indique au routeur qu'une destination particulière peut être atteinte optimalement en envoyant le paquet vers un routeur précis. Ce dernier représente le prochain saut (Next Hop) sur le chemin de la destination finale. Quand un routeur reçoit un paquet, il vérifie sont adresse de destination et tente d'associer cette adresse avec un saut suivant.

metric

Les tables de routage contiennent également d'autres types d'informations telle que le coût d'un chemin. Les routeurs comparent les "metrics" pour déterminer un chemin optimal. Le "metric" utilisé dépend de l'algorithme de routage. Différents type de "metrics" sont présentés plus loin.

11.1.4 Types de métriques



Slide 11.6
Types de métriques

Les algorithmes de routage peuvent utiliser de nombreux type de metrics.

Path length

Le plus commun des metrics est la "longueur de chemin" (Path length). Usuellement cette longueur correspond au nombre de relais qu'il faut traverser pour atteindre la destination. Certains algorithmes de routage permettent à l'administrateur de fixer des coûts arbitraires à chaque liaison. Dans ce cas la longueur de chemin correspond à la somme des coûts de chaque liaison traversée pour atteindre la destination.

Reliability

La fiabilité (Reliability) fait généralement référence au taux d'erreur bit (bit error rate) de chaque liaison. d'autres facteurs peuvent être pris en compte tel que la rapidité de réparation après un panne.

Delay

Le délai (Delay) désigne le temps qu'il faut à un paquet pour traverser un réseau. Le délai dépend de nombreux facteurs : débit des lignes, taille des paquets, taux de remplissage des files d'attente, distance physique, congestion et performance des nœuds intermédiaires.

Bandwidth

La bande passante (Bandwidth) peut également être prise en considération.

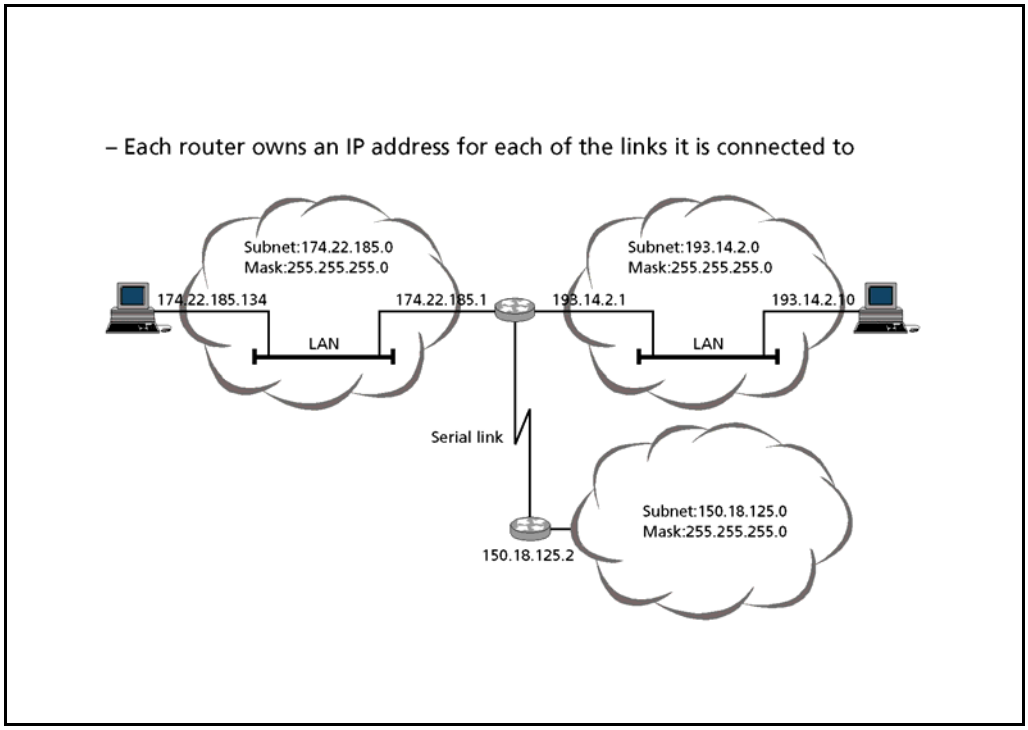
Load

La charge (Load) désigne le niveau d'occupation d'une ressource (par ex. routeur).

Cost

Les coûts de communication (Communication Cost) peuvent être utilisés pour faire des choix d'acheminement afin d'optimiser les charges financières.

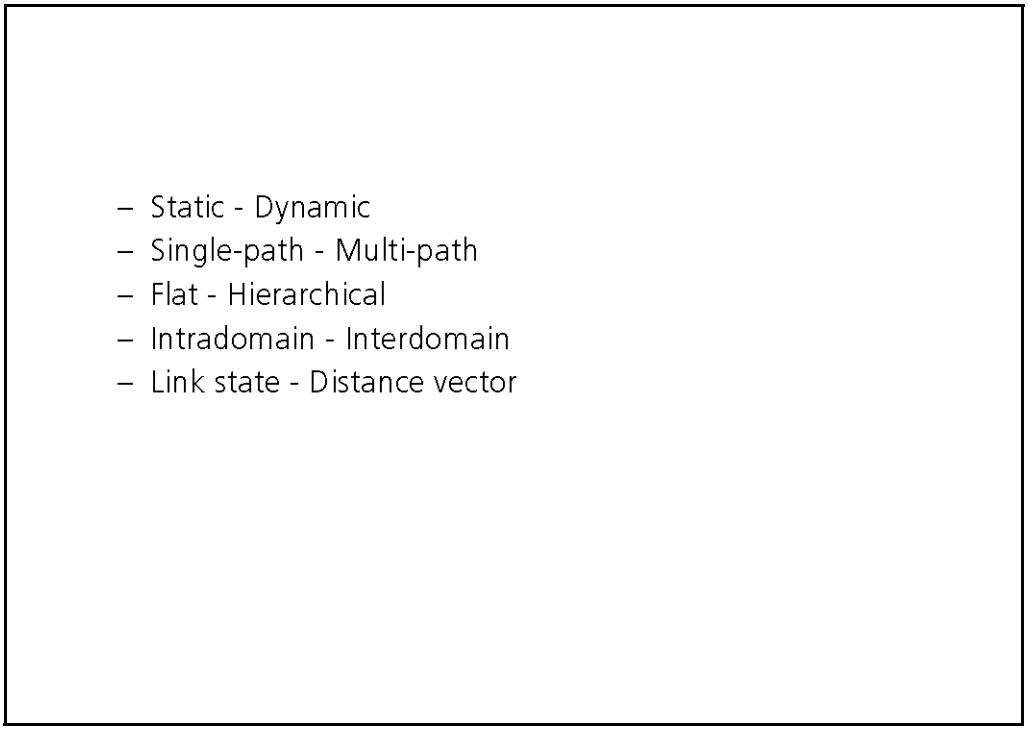
11.1.5 Routage et adresses IP



Slide 11.7
Routage et adresses IP

Chaque interface d'un possède une adresse IP qui appartient à l'espace d'adressage correspondant au sous-réseau relié. Ces adresses sont utilisées par les protocoles de routage pour identifier les routeurs voisins. Dans un environnement de diffusion (un LAN) l'adressage des interfaces des routeurs est nécessaire à la procédure de résolution d'adresse MAC (ARP).

11.1.6 Algorithmes de routage

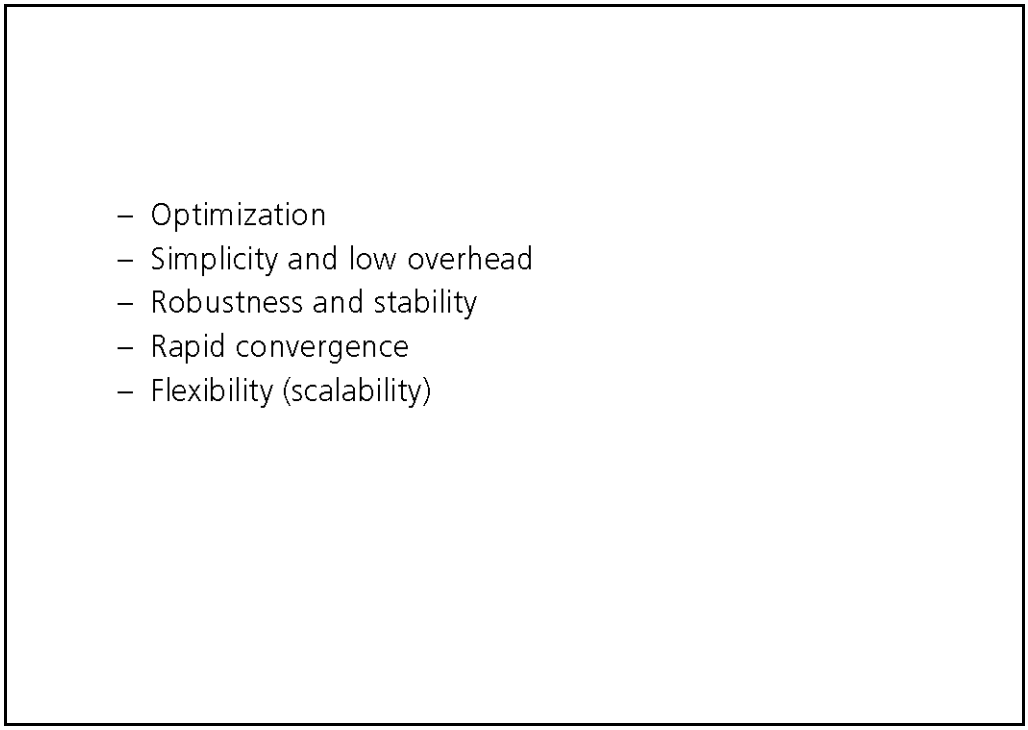


Slide 11.8
Algorithmes de routage

Les algorithmes de routage peuvent être différenciés sur la base de différentes caractéristiques fondamentales. Différents types d'algorithmes de routage existent chacun d'eux ayant des impacts différents sur le protocole de routage et sur les ressources nécessaires à leur mise en œuvre.

Le calcul des routes optimales peut être réalisé sur la base d'une ou de plusieurs metric mentionnée plus haut (algorithmes hybrides).

11.1.7 Objectifs des algorithmes de routage

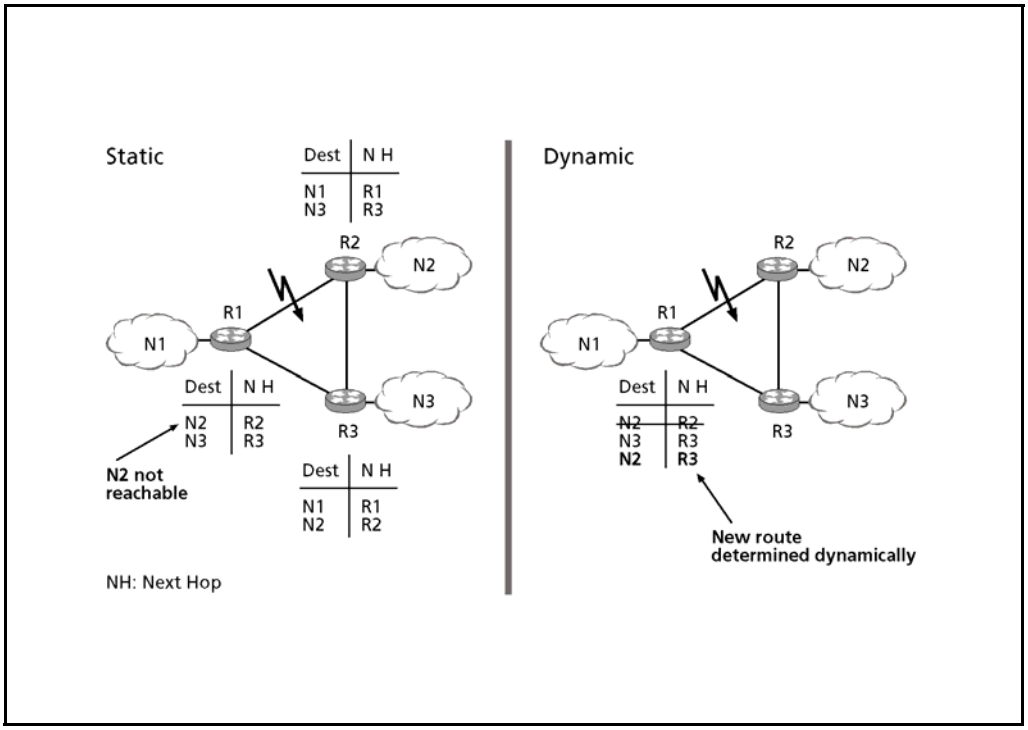


Slide 11.9
Objectifs des algorithmes de routage

Un algorithme de routage doit être en mesure de choisir la meilleure route en fonction des critères imposés (metric). On va en outre exiger de ces algorithmes qu'il soient :

- simples de façon à optimiser les ressources matérielles nécessaires à leur mise en œuvre.
- robustes, càd qu'ils soient capables de fonctionner correctement également dans des circontances imprévues telles que des pannes de lignes ou de matériel,
- à convergence rapide de façon à ce qu'un changement de topologie du réseau soit refleté dans les tables de routage dans un délai aussi court que possible,
- flexibles, donc capable de supporter des changements de topologie du réseau (scalability).

11.1.8 Routage statique et routage dynamique



Slide 11.10
Routage statique et routage dynamique

Static routing

Dans le routage statique, les correspondances destination-chemin sont établies manuellement par l'administrateur du réseau. Le routage statique est simple à mettre en œuvre et bien adapté aux environnements à topologie simple dans lesquels la nature du trafic est relativement prévisible.

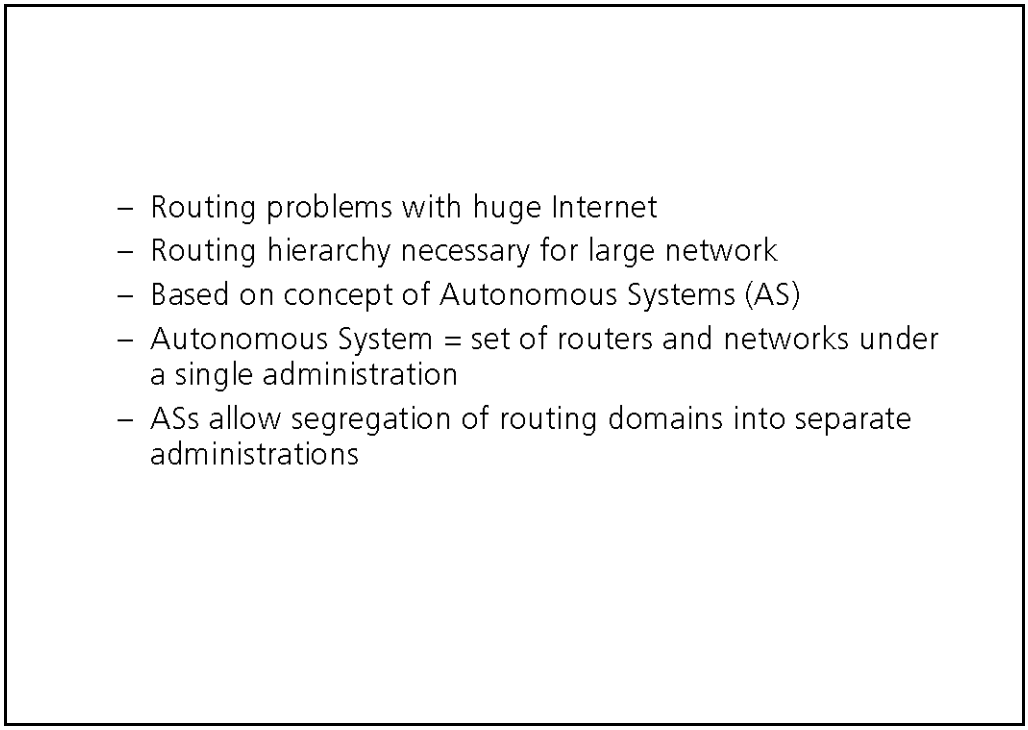
Dynamic routing

Dans le routage dynamique, l'algorithme de routage va détecter les changements de topologie, recalculer de nouveaux chemins et mettre à jour les tables de routage. Cette fonctionnalité est souhaitable dans un réseau complexe sujet à des changements de topologies

Default route

Les routages statique et dynamique peuvent cohabiter, par exemple, pour définir une route statique de "dernière instance" (default route) sur laquelle est acheminé le trafic vers tous les réseaux inconnus.

11.1.9 Réseaux et systèmes autonomes



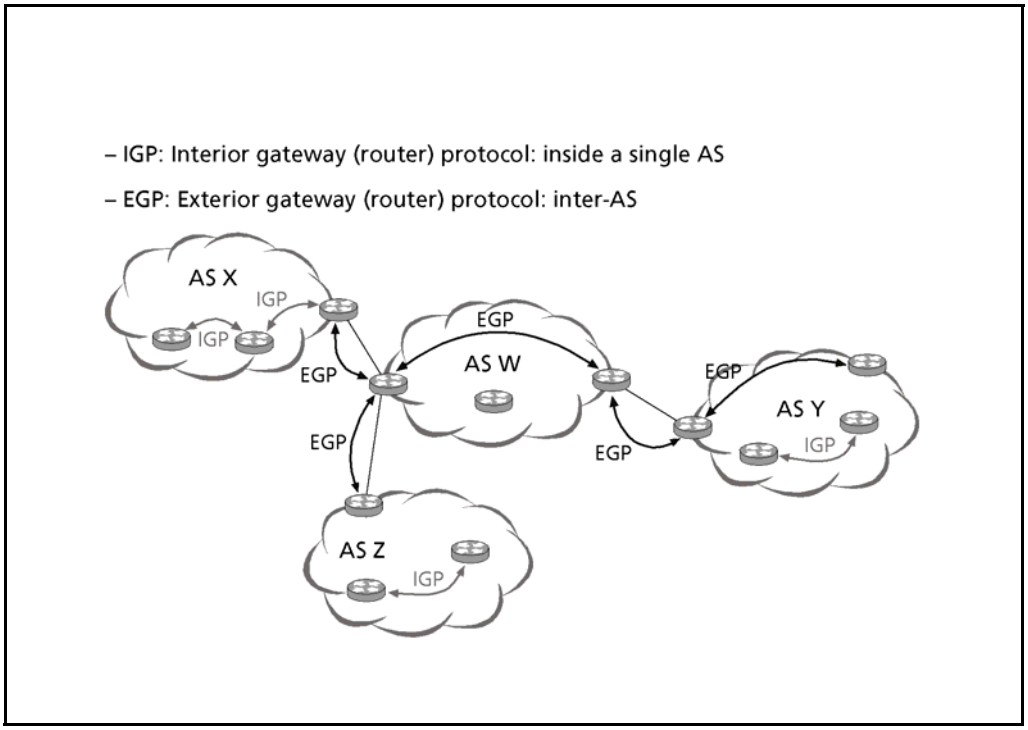
Slide 11.11
Réseaux et systèmes autonomes

Au delà d'une certaine taille de réseau, il devient très difficile d'exploiter un réseau sans une structure "administrative" permettant de délimiter des domaines de routage et de définir une structure hiérarchique.

AS (Autonomous System)

L'Internet a été divisée en "systèmes autonomes" (AS) comprenant chacun un ensemble de routeurs et de réseaux sous une administration commune. Un identificateur unique de 16 bits est attribué à chaque système autonome. Les adresses de systèmes autonomes sont gérées par l'IANA qui délègue des plages de numéros aux registres locaux. La [RFC 1930] propose des directives pour la sélection et l'enregistrement d'un système autonome.

11.1.10 Routage intérieur et extérieur



Slide 11.12
Routage intérieur et extérieur

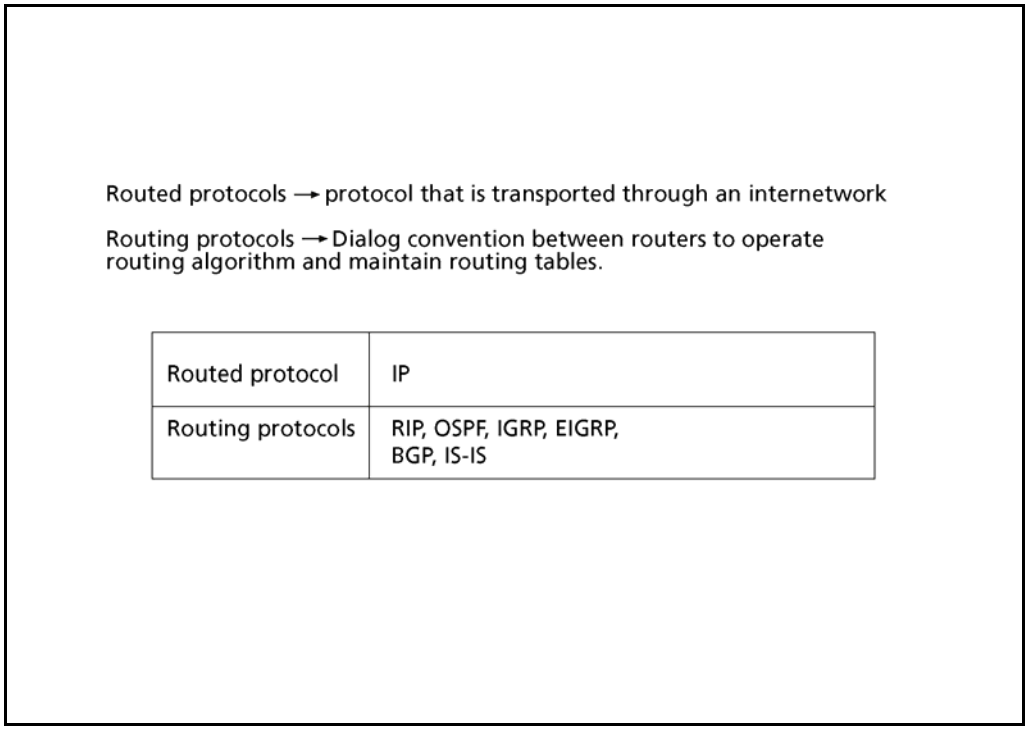
Au sein d'un système autonome, un ou plusieurs protocoles de routage "intérieur" (IGP) sont utilisés et prennent en charge l'acheminement vers des destinations à l'intérieur de l'AS. Les protocoles suivants : RIP, RIPv2, OSPF, IGRP, EIGRP sont des exemples de protocoles de routages de type IGP.

IGP (Interior Gateway Protocol)

Un protocole de routage "extérieur" prend en charge l'acheminement du trafic entre sytèmes autonomes distincts. la gestion de cet acheminement est effectuée par des protocoles tels que EGP, BGP-3, BGP-4.

EGP (Exterior Gateway Protocol)

11.1.11 Protocoles de routage et protocoles routés



Slide 11.13
Protocoles de routage et protocoles routés

Il convient de ne pas confondre les notions de protocole routé et de protocole de routage.

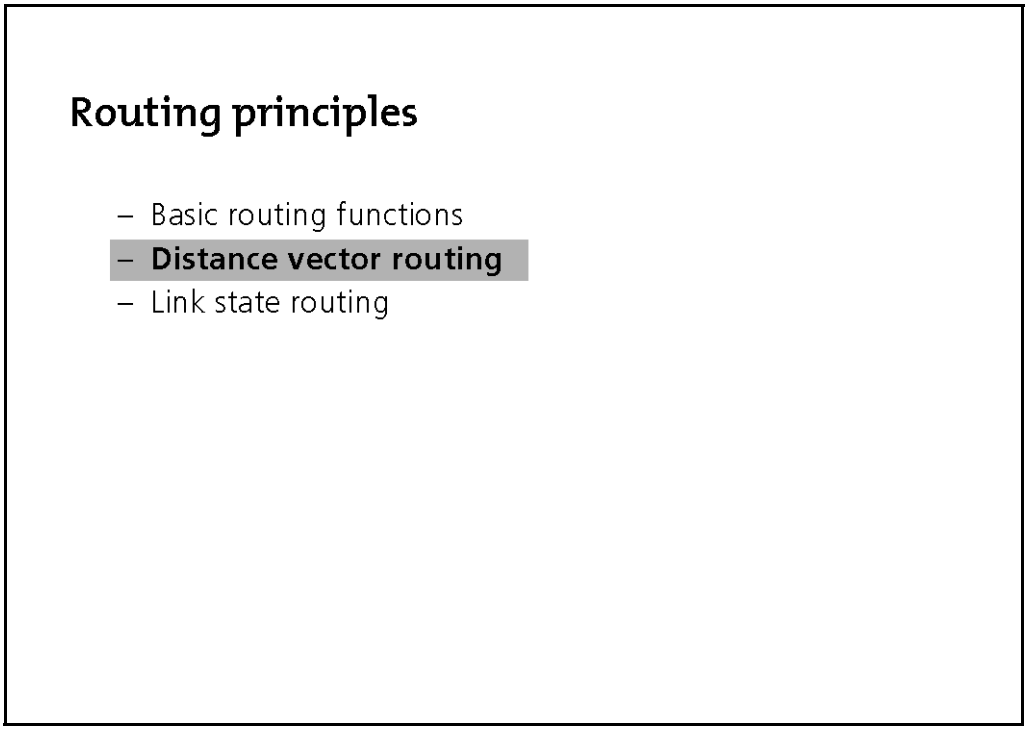
Protocole routé

Le protocole routé est transporté au travers d'un réseau. Il réalise un certain nombre de fonctions pour acheminer de l'information entre deux applications utilisateurs. On parle également de protocole "de couche réseau" pour désigner la couche 3 du modèle OSI.

Protocole de routage

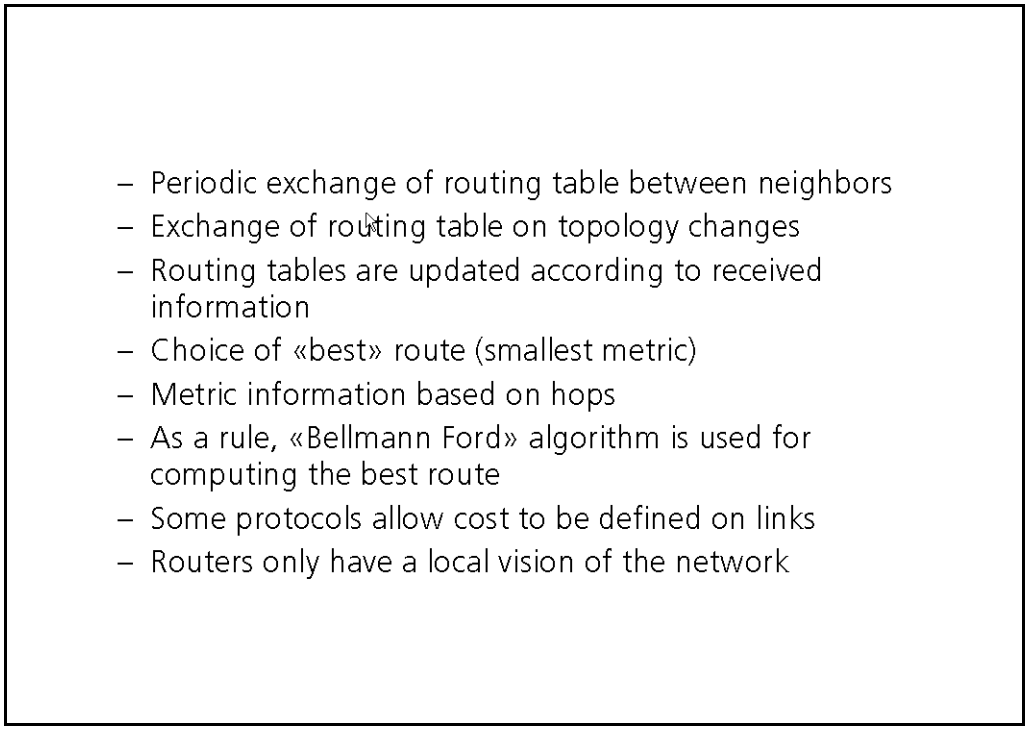
Le protocole de routage est une convention d'échange, entre routeurs, pour alimenter l'algorithme de routage et maintenir dynamiquement l'état des tables de routage.

11.2 Routage à vecteur de distance



Slide 11.14
Routage à vecteur de distance

11.2.1 Principes

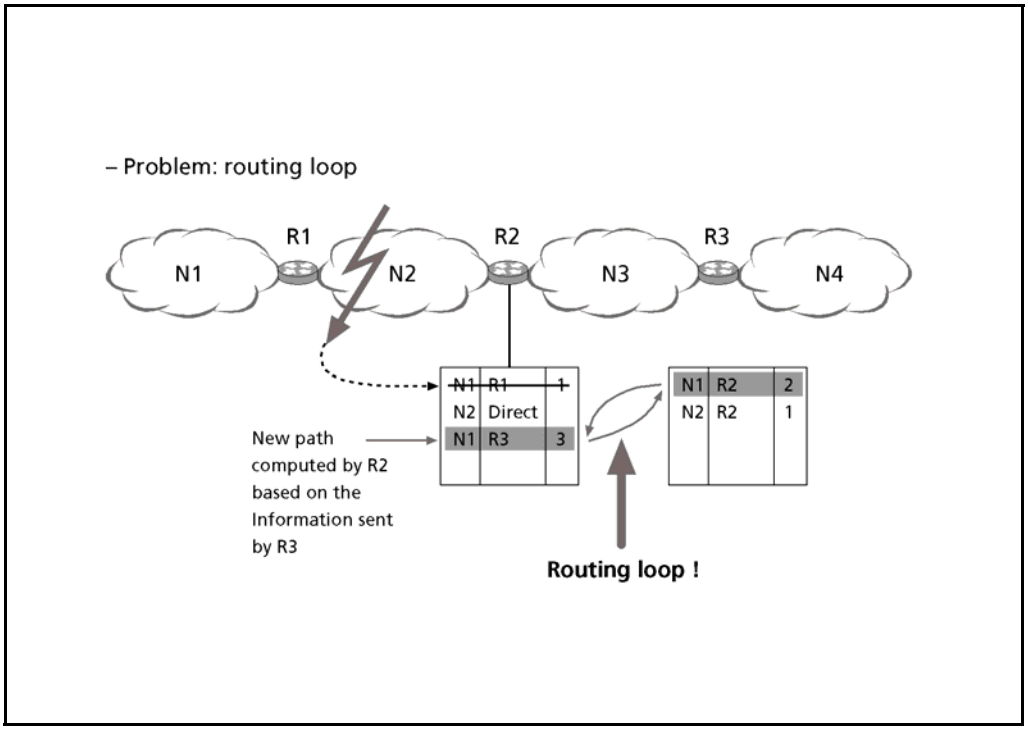


Slide 11.15
Principes

Distance vector routing, Bellmann Ford

Le routage à vecteur de distance (Distance Vector Routing) est basé sur l'échange périodique des tables de routage avec les routeurs voisins. A la mise sous-tension, seules les informations concernant les réseaux connectés localement sont connues. Les tables de routage reçues sont mises à jour selon un algorithme appelé "Bellman Ford". Ces mises à jour peuvent concerner la découverte d'un nouveau réseau, ou le changement d'une valeur de métric vers un réseau déjà connu. Dans ce type de routage, les nœuds n'ont qu'une vision locale du réseau.

11.2.2 Boucles de routage

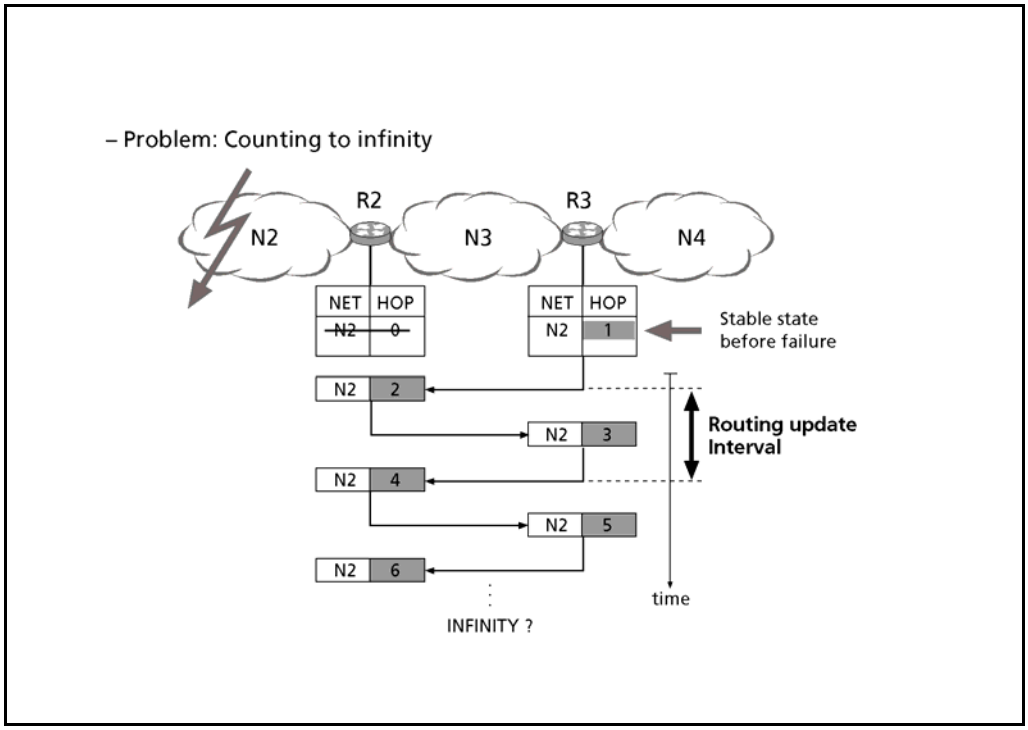


Slide 11.16
Boucles de routage

Routing Loops

Un problème fondamental du routage, en particulier du routage à vecteur de distance est la gestion des boucles de routage (Routing loops). Celles-ci peuvent survenir dans des états transitoires, par exemple lors de la défaillance d'une liaison, durant le temps qui sera nécessaire au protocole pour atteindre un nouvel état stable. Les paquets acheminés dans cette configuration vont "rebondir" dans la boucle jusqu'à expiration de leur temps de vie. La durée de cette situation sera d'autant plus courte que le protocole sera performant en terme de temps de convergence.

11.2.3 Compte à l'infini

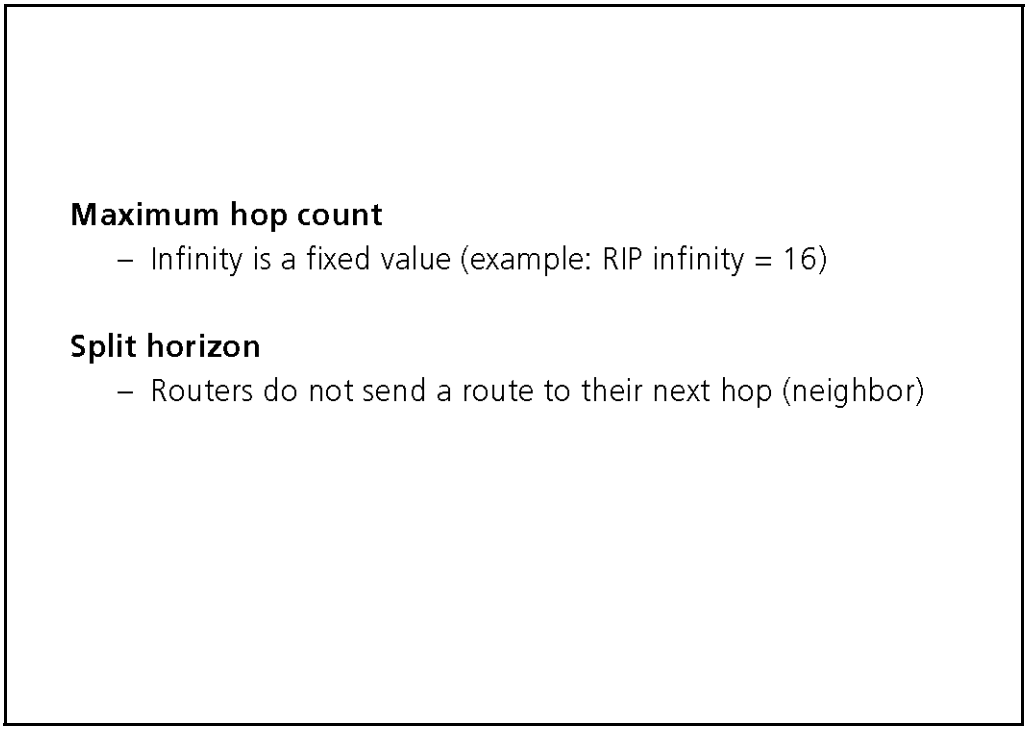


Slide 11.17
Compte à l'infini

Count to Infinity

Dans le cas de la défaillance d'une liaison ou d'un routeur, un routeur voisin va considérer la route comme inaccessible. Un deuxième routeur va diffuser sa table de routage en indiquant que le réseau considéré est encore accessible. Le premier routeur va remettre sa table de routage à jour avec le chemin le plus court que lui a livré le deuxième routeur. A son tour le premier routeur va diffuser sa table de routage avec une nouvelle information d'accessibilité du réseau défaillant. L'information va alterner entre les deux routeurs jusqu'à ce que la valeur "infinie" soit atteinte pour ce réseau.

11.2.4 Améliorations



Slide 11.18
Améliorations

Max Hop count

Une première mesure pour permettre la convergence consiste à définir une valeur de distance considérée comme infinie (Maximum Hop Count). Cette valeur sera attribuée à un chemin vers un réseau inatteignable. Le phénomène du comptage vers l'infini va alors se produire jusqu'à ce maximum. Ensuite le réseau sera considéré comme inatteignable par les routeurs.

Split Horizon

La seule définition d'un nombre maximum de saut ne suffit pas pour éviter les boucles de routage et pour garantir un temps de convergence court. L'horizon partagé (Split Horizon) est une autre mesure qui consiste à interdire à un routeur de transmettre de l'information de routage en direction de la provenance de cette information.

Améliorations (2)

Triggered update

- Network changes are directly retransmitted by the routers (independently of the timers)

Poison reverse

- Disappeared routes are directly announced by an infinite metric

Hold down

- Routes which are not regularly any more announced are regarded as no more valid

Slide 11.19
Améliorations (2)

Triggered update

Le principe des mises à jour déclenchées (Triggered update) consiste pour les routeurs à envoyer immédiatement les "mauvaises nouvelles" sans attendre l'expiration du délai de mise à jour.

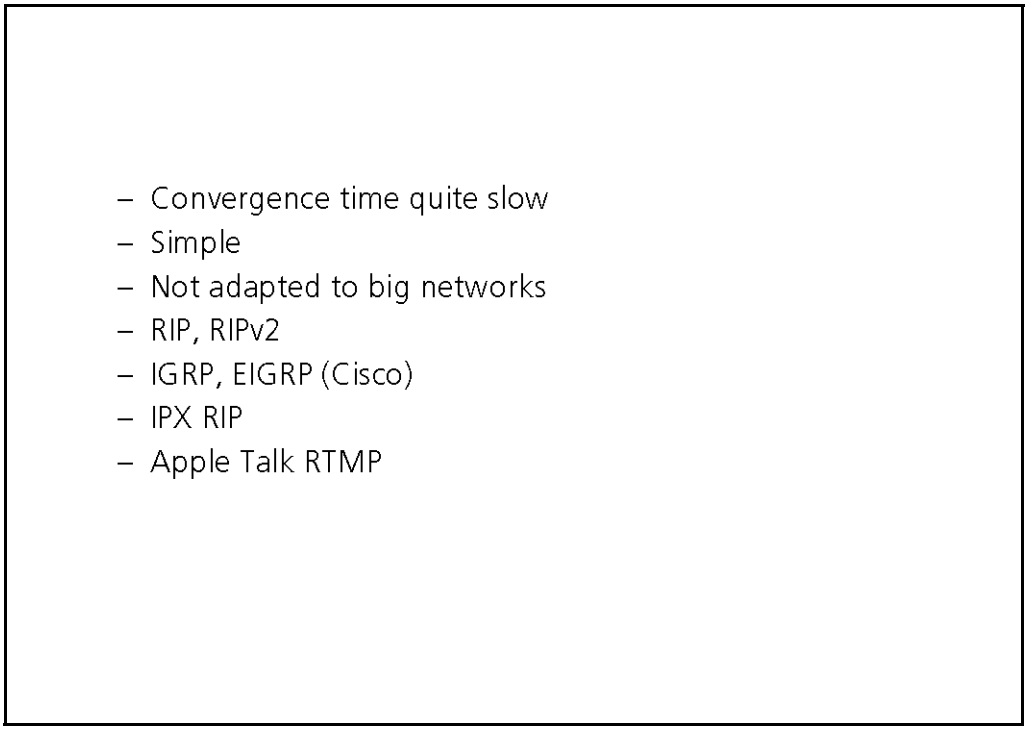
Poison Reverse

Un routeur qui exploite le "poison reverse" va envoyer dans un message de mise à jour habituel une indication d'indisponibilité d'un réseau en direction du réseau indisponible. Par ce mécanisme, le routeur indique explicitement qu'il n'y a pas de chemin alternatif passant par lui.

Hold Down

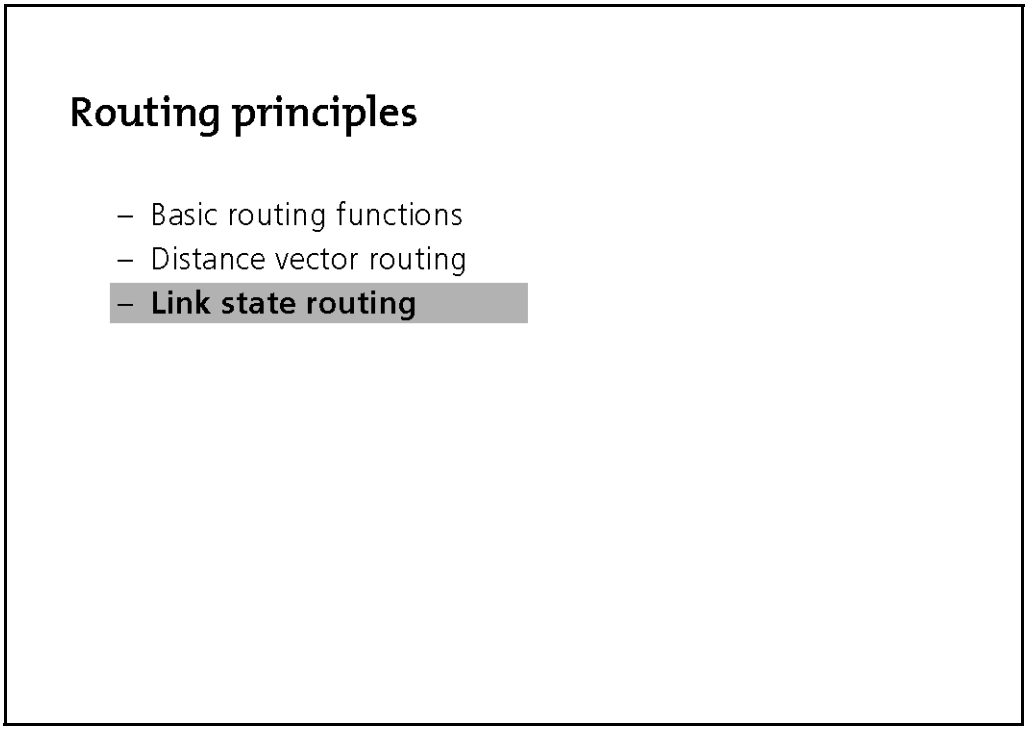
Lorqu'un routeur est informé de l'indisponibilité d'un réseau, il peut se mettre dans l'état "Hold down"pour cette destination. Pendant l'état "hold down", le routeur va ignorer toute remise à jour concernant ce réseau. Le laps de temps pendant lequel le routeur est maintenu dans cet état est généralement un multiple du délai de mise à jour.

11.2.5 Propriétés et exemples



Slide 11.20
Propriétés et exemples

11.3 Routage à état des liaisons



Slide 11.21
Routage à état des liaisons

11.3.1 Principe

- Router exchange link state information
- Link state update on topology change
- No periodic exchange of routing information
- Choice of «best» route
- Various metrics
- Dijkstra algorithm (shortest path first) is used for computing the shortest path (path graph)
- Routers have a global vision of the network
- In large networks: classification of routers hierarchy

Slide 11.22
Principes

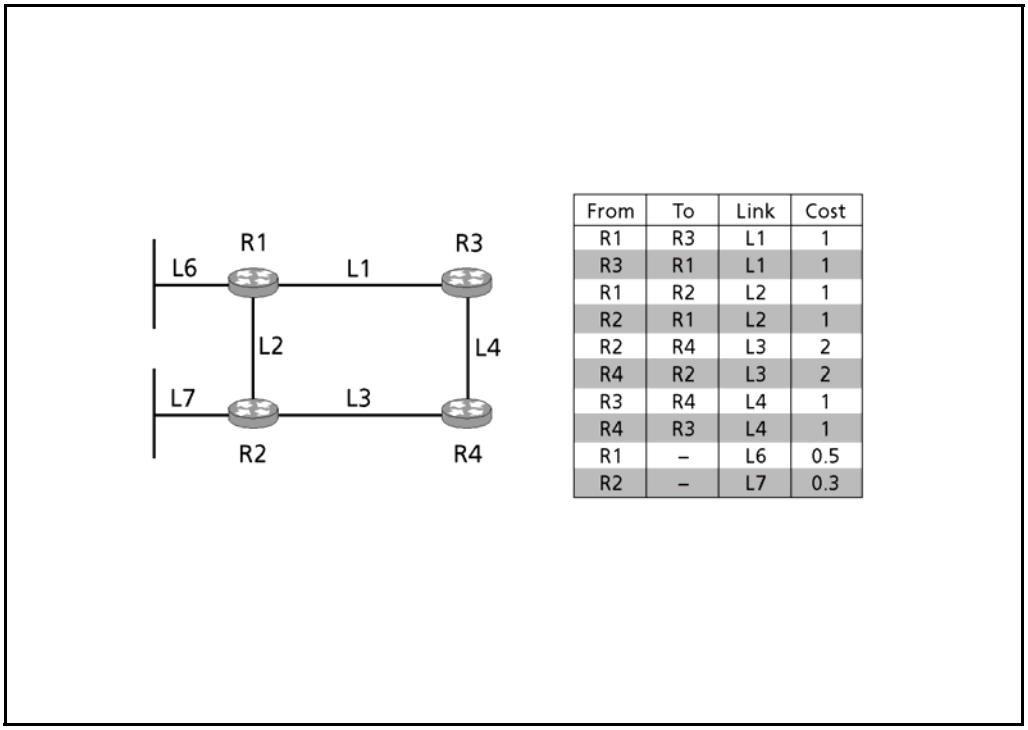
Link State routing

Le principe de base des protocoles à état des liaisons (Link-State Algorithm) est de maintenir dans tous les nœuds du réseau une copie synchronisée d'une base de données décrivant l'état des liaisons. Seule des mises à jour correspondant aux modifications de l'état des liaisons sont échangées.

Shortest Path First, Dijkstra

Les tables de routage sont créées à partir de la base d'état des liaisons à l'aide d'un algorithme appelé "Dijkstra"ou "Shortest Path First". L'ensemble des routeurs à une vision globale du réseau (ou de la partie du réseau à laquelle il appartient). Comme la base de données d'état des liaisons peut devenir très volumineuse dans les grands réseaux, on définit différents niveaux hiérarchiques pour les routeurs et la topologie peut être séparée en zones.

11.3.2 Base de données d'état des liaisons



From	To	Link	Cost
R1	R3	L1	1
R3	R1	L1	1
R1	R2	L2	1
R2	R1	L2	1
R2	R4	L3	2
R4	R2	L3	2
R3	R4	L4	1
R4	R3	L4	1
R1	–	L6	0.5
R2	–	L7	0.3

Slide 11.23
Base de données d'état des liaisons

LSDB (Link State Database)

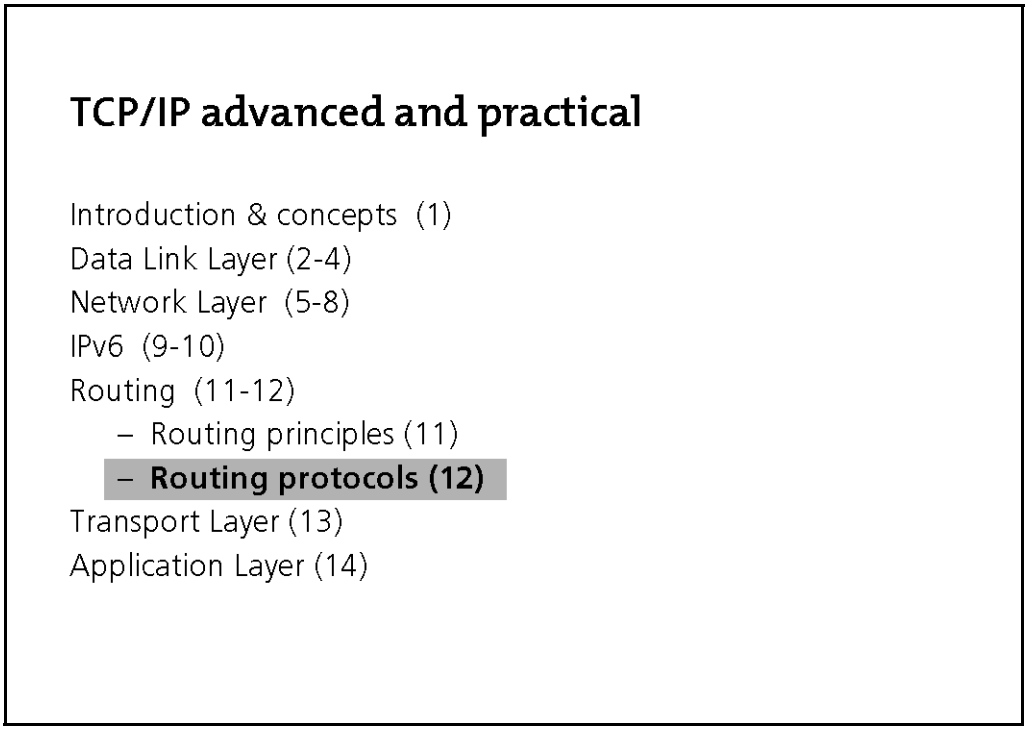
Les nœuds maintiennent une copie complète de la "carte" du réseau et exécutent le calcul des meilleures routes localement en utilisant cette carte. Cette carte appelée "base d'état des liaisons" LSDB (Link State Database) est une base de données où chaque enregistrement représente une liaison du réseau. Chaque enregistrement a été inséré dans la base par le nœud qui en est responsable. On y trouve un identificateur de l'interface, le numéro de liaison, et des informations décrivant l'état de la liaison. Chaque nœud peut facilement, à l'aide de ces informations, calculer le chemin le plus court vers chacun des autres nœuds.

11.3.3 Propriétés et exemples

- Fast convergence time
- Router requires more CPU
- Network load due to updates is low
- Well suited to big networks
- OSPF
- IS-IS (Integrated IS-IS)

Slide 11.24
Propriétés et exemples

12 Protocoles de routage



Slide 12.1
Protocoles de routage

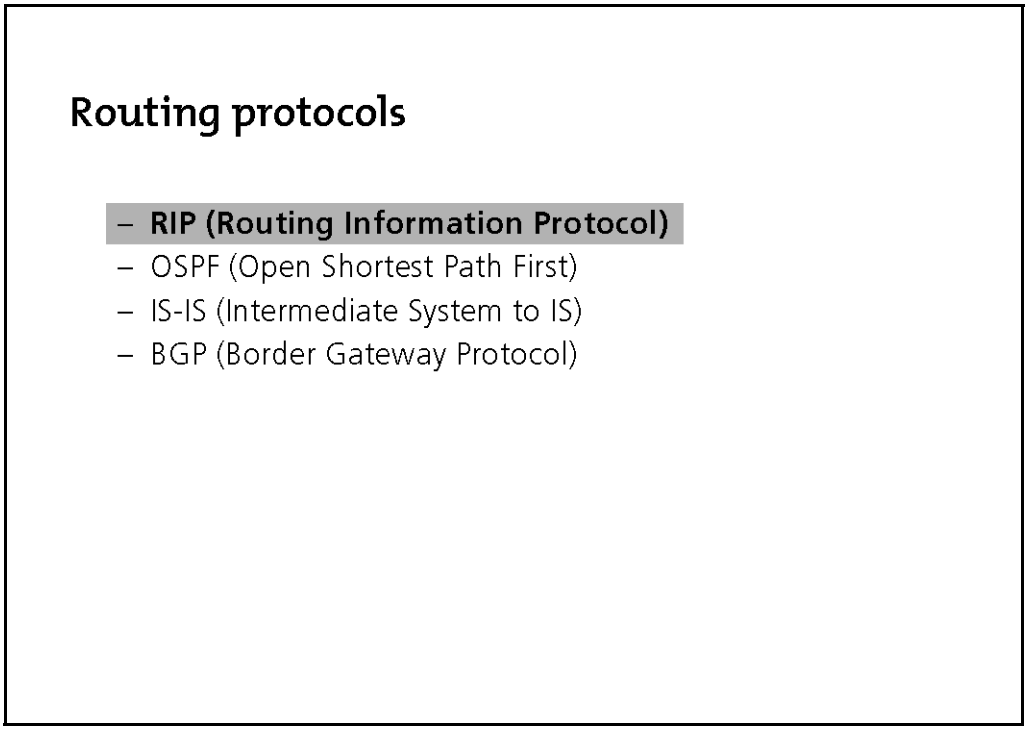
Ce chapitre présente quatre protocoles de routage utilisant les deux principes fondamentaux étudiés dans le chapitre précédant.

Objectifs

A l'issue de ce chapitre, les participants sont capables d'expliquer le fonctionnement du protocole de routage RIP, la manière dont ce crée la table de routage.

En outre, ils peuvent nommer les principes de routage utilisés par les protocoles OSPF, IS-IS et BGP, différencier leur domaine d'utilisation.

12.1 RIP (Routing Information Protocol)



Slide 12.2
RIP (Routing Information Protocol)

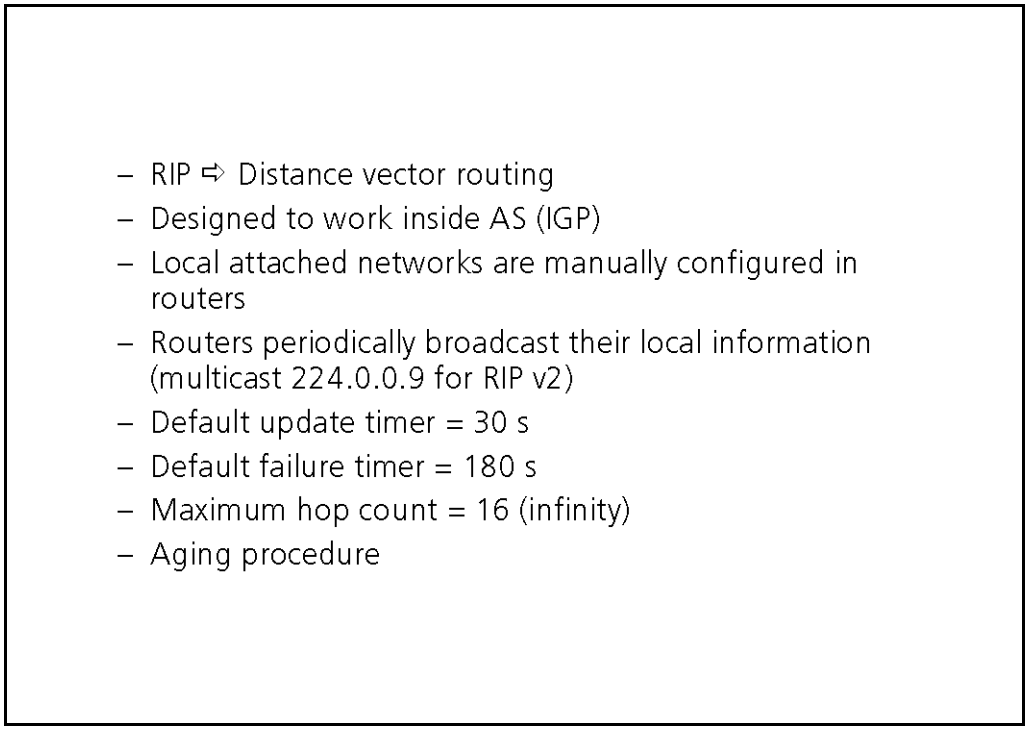
RIP

RIP est un protocole très répandu. Il doit sa popularité principalement à deux facteurs : il est simple et il fait partie de tous les sytèmes BSD UNIX à partir de la version 4.2. Il est basé sur l'échange d'information de routage entre nœuds de réseau au sein d'un système autonome.

RIPv1, RIPv2

RIP version 1 est décrit dans [RFC 1058], RIP version 2 est décrit dans la [RFC 2453]. La version 2 du protocole livre des fonctionnalités supplémentaires telles que l'authentification et la possibilité de définir des masques de sous-réseau de longueur variable.

12.1.1 Principe et caractéristiques de RIP



Slide 12.3
Principe et caractéristiques de RIP

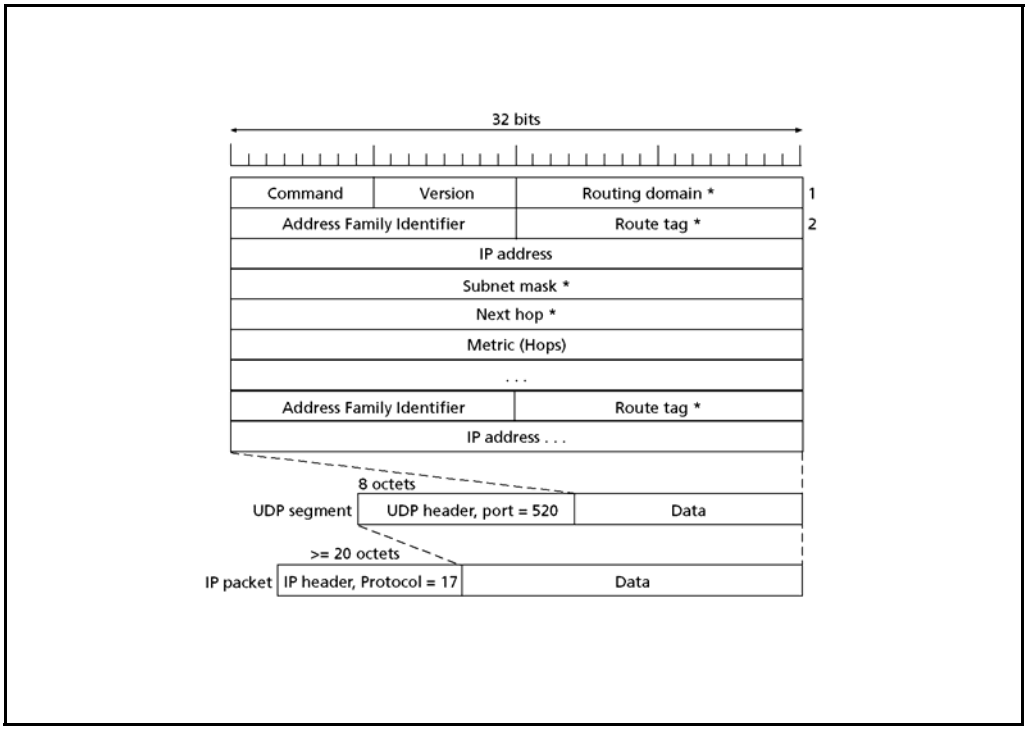
RIP est un protocole à vecteur de distance. Il est conçu pour opérer à l'intérieur d'un système autonome (IGP). A l'initialisation, les routeurs ont une entrée statique pour chaque sous-réseau directement attaché (distance = 1 hop). Chaque routeur diffuse périodiquement (par exemple toutes les 30 secondes) l'ensemble des enregistrements contenus dans la table de routage. A la réception de ces messages les routeurs voisins remettent à jour leurs tables de routage.

Après un certain nombre d'échange, le système atteint la stabilité et chaque routeur connaît l'ensemble des réseaux associé à la "meilleure" distance pour les atteindre.

RIP Aging

La procédure d'Aging est appliquée aux entrées des tables de routage : si un réseau n'est plus notifié pendant plus de 3x30s, la valeur 16 (= réseau inaccessible) lui est attribuée. L'entrée est supprimée 3x30 s plus tard.

12.1.2 Format de paquet RIPv2



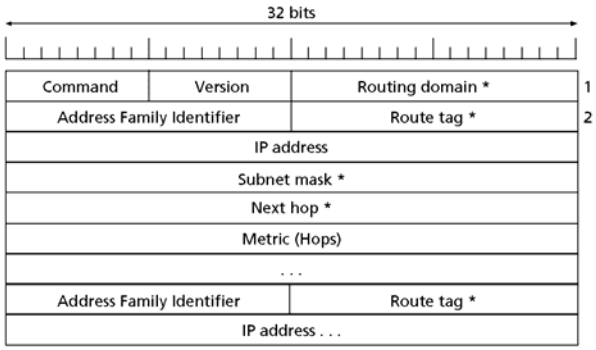
Slide 12.4
Format de paquet RIPv2

Un paquet RIP est constitué d'une entête de 8 octets associée aux enregistrements (de 1 à 25) de la table de routage constitués chacun de 20 octets.

Le champ Command indique s'il s'agit d'une requête (envoi de toute ou d'une partie de la table de routage) ou d'une réponse. Le champ version indique la version du protocole RIP.

Le champ Routing domain, valide uniquement dans la version 2 du protocole, permet d'identifier un domaine de routage RIP. Il est ainsi possible de définir des domaines de routage indépendants sur un même réseau physique. Les routeurs doivent ignorer les paquets RIP provenant d'un autre domaine de routage.

12.1.3 Données RIP



Slide 12.5
Données RIP

RIP data

Les données du paquet RIP (RIP data) sont constituées de 1 à 24 enregistrements contenant chacun les champs suivants :

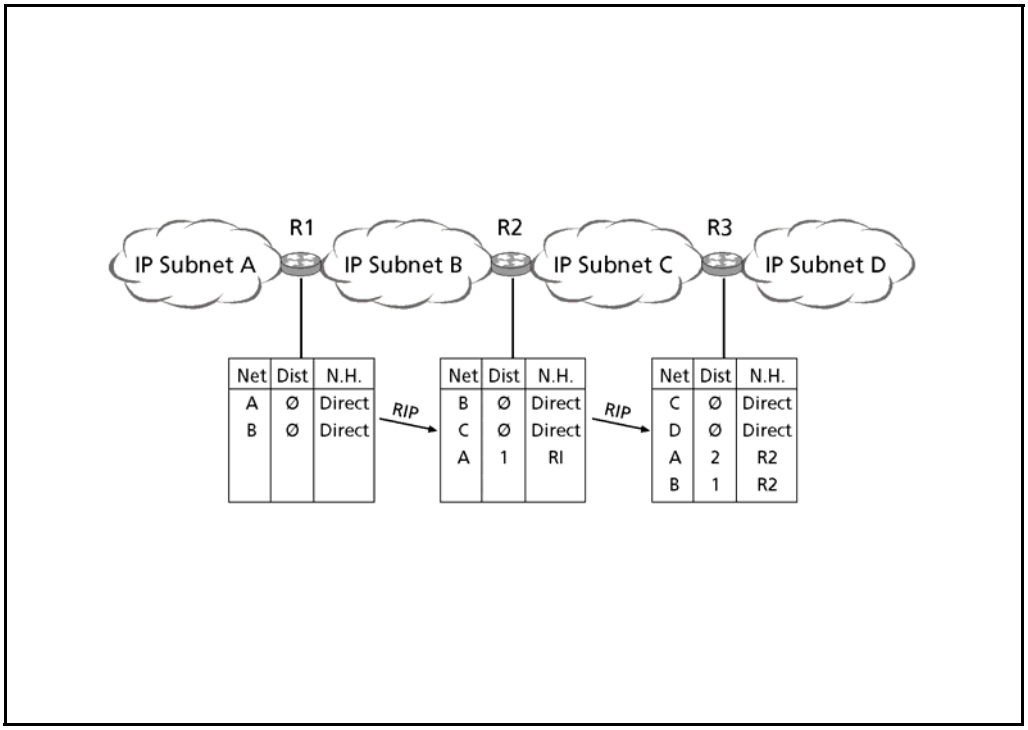
Address Family Identifier permet d'identifier le type d'adresse que contient cette entrée. la valeur 2 est définie pour IPv4. Si la valeur de ce champ est 0xFFFF, alors le reste de l'entrée contient des informations d'authententification (RIP v2).

Route Tag

Route Tag est prévu pour supporter des informations provenant d'un protocole de routage externe (EGP). Ce champ peut transporter, par exemple, un identificateur de système autonome.

IP address : adresse du réseau destination auquel il faut appliquer le Subnet Mask qui peut être atteint en passant par le routeur Next Hop à une distance spécifiée dans Metric.

12.1.4 Exemple RIP



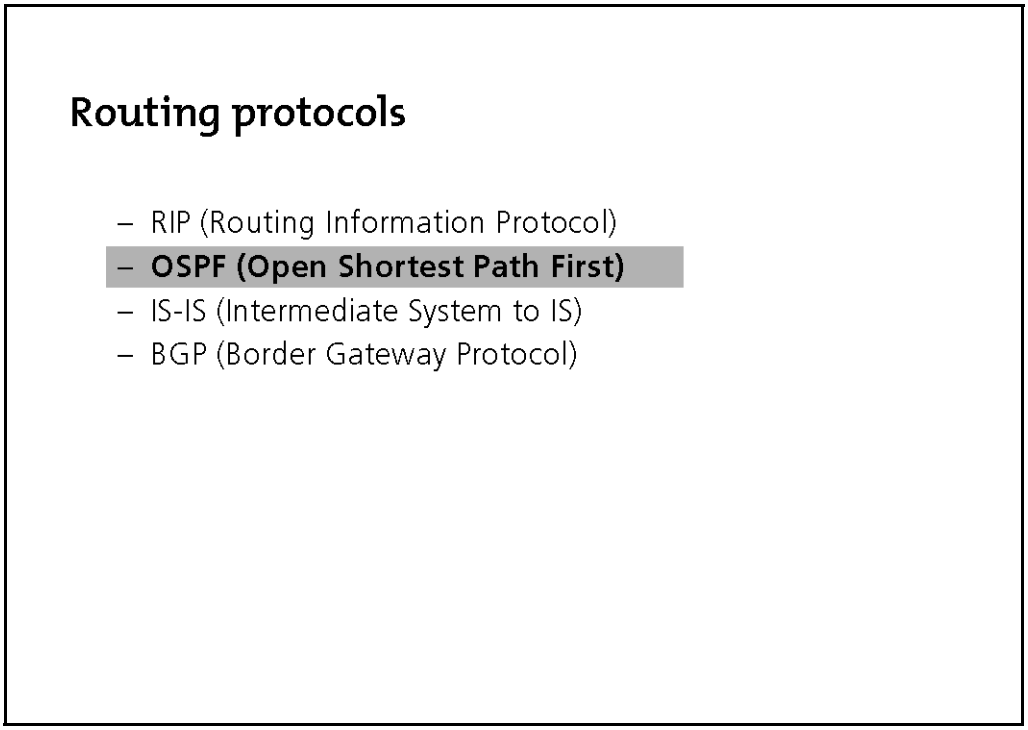
Slide 12.6
Exemple RIP

12.1.5 Propriétés de RIP

- Simple
- Convergence time slow
- Suitable for small network
- Needs few CPU resources
- Routing update contains the whole routing table ⇨ High traffic overhead if routing tables are big
- Doesn't allow load balancing over redundant path
- Authentication and multiple routing domains foreseen in RIPv2

Slide 12.7
Propriétés de RIP

12.2 OSPF (Open Shortest Path First)

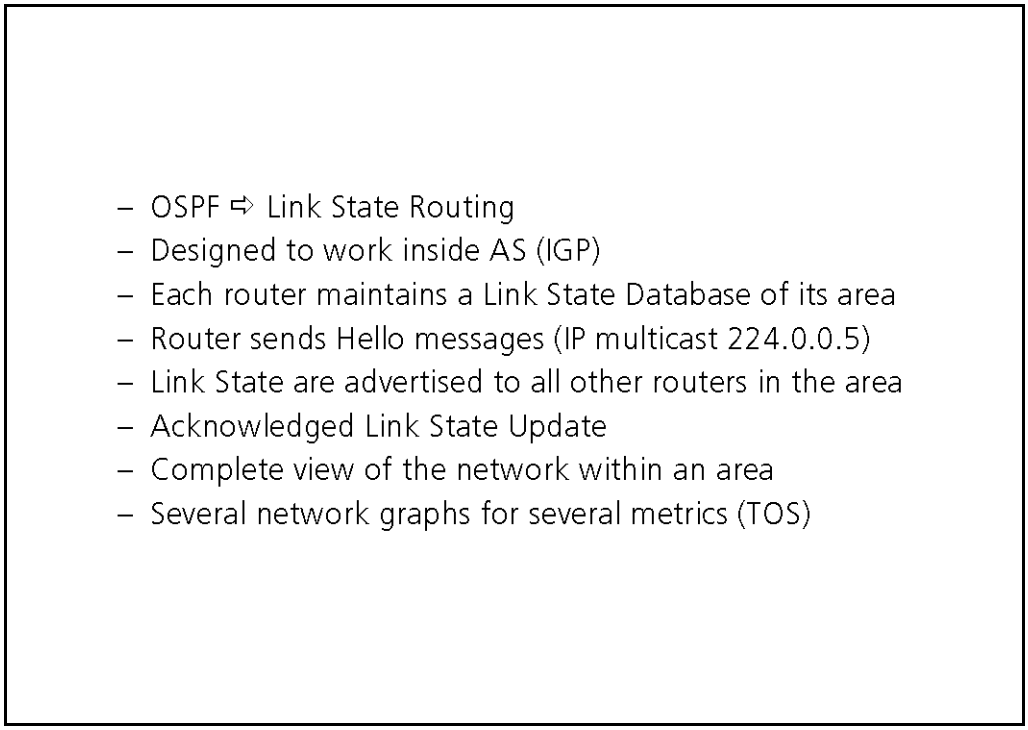


Slide 12.8
OSPF (Open Shortest Path First)

OSPF a été développé depuis le début des années 90 pour résoudre les problèmes de RIP : temps d'adaptation lent et taille des remises à jour proportionnelles à la taille du réseau. Le terme "Open" indique qu'il s'agit d'un standard du domaine public. "Shortest Path First" fait référence au chemin le plus court que l'algorithme de Dijkstra détermine.

OSPF version 2 est décrit dans [RFC 2328].

12.2.1 Principe et caractéristiques de OSPF



Slide 12.9
Principe et caractéristiques de OSPF

OSPF est un protocole à état des liaisons. Il est conçu pour opérer à l'intérieur d'un système autonome (IGP).

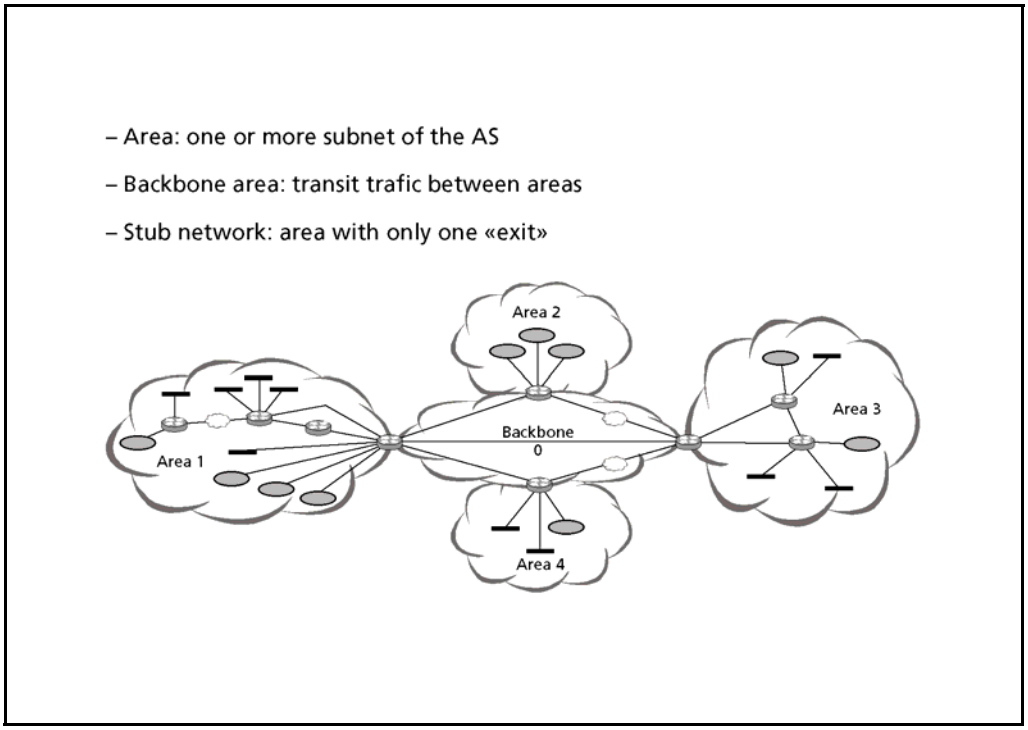
A l'initialisation, un routeur OSPF envoie des messages "Hello" sur toutes ses interfaces. Ces messages permettent de déterminer la présence des routeurs voisins.

LSDB, Link State Database

La LSDB est constituée de l'ensemble des LSA (Link State Advertisment) reçu de tout les autres routeurs de la zone.

Toutes les 30 minutes, il s'opère une synchronisation générale de la LSDB.

12.2.2 Notion de zone (Area)

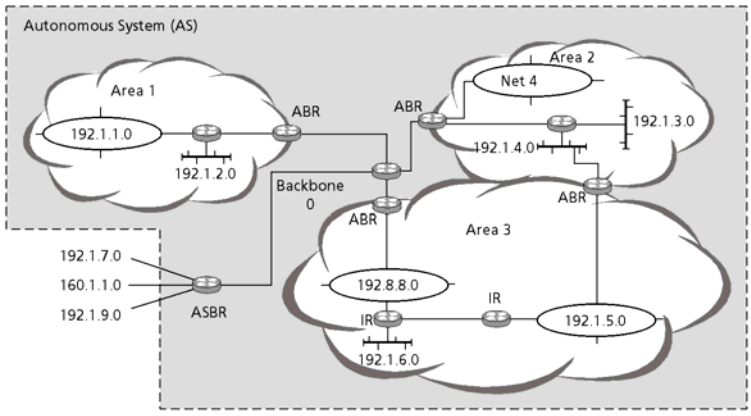


Slide 12.10
Notion de zone (Area)

Area

Pour simplifier le processus de calcul des routes dans les grands réseaux ainsi que pour diminuer la taille de la base d'état des liaisons, le concept de "zone" (Area) a été introduit. Une zone est un sous ensemble de système autonome qui peut comprendre un ou plusieurs sous-réseaux IP. On distingue la zone Backbone sur laquel aucun utilisateur n'est généralement raccordé et qui fait office d'épine dorsale du système autonome et assure l'acheminement du trafic entre les différentes zones.

12.2.3 OSPF Areas : exemple



Slide 12.11
OSPF Areas :Exemple

Il existe quatre types de nœuds OSPF :

IR (Intenal Router) — IR (Internal Router) qui est situé entièrement au sein d'une zone.

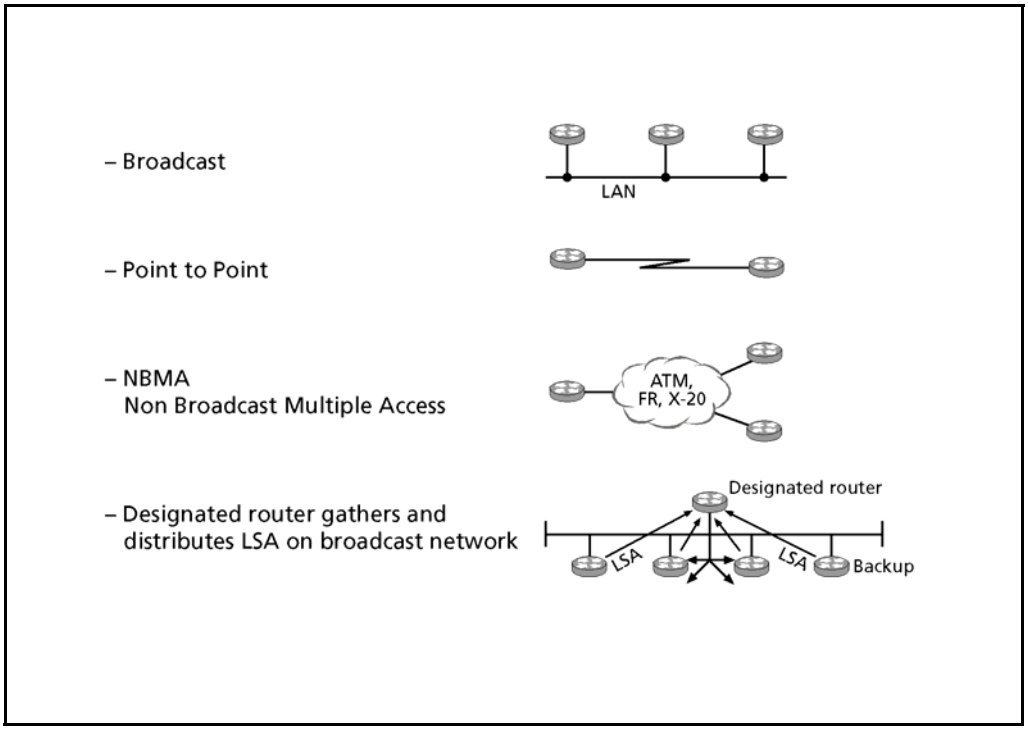
ABR (Area Border Router) — ABR (Area Border Router) qui est un élément de liaison entre une zone et le backbone

BR (Backbone Router) — BR (Backbone Router) qui est situé entièrement dans la zone backbone

ASBR (Autonomous System Border Router) — ASBR (Autonomous Sytem Boundary Router) qui assure la communication vers l'extérieur du système autonome à l'aide de route statique ou d'un EGP.

Les modifications de topologie au sein d'une zone sont uniquement transmises au sein de cette zone. Les routeurs à la frontière de deux zones maintiennent des bases de données séparées pour chacune des zones

12.2.4 Type de raccordements OSPF et routeur désigné



Slide 12.12
Type de raccordements OSPF, routeur désigné

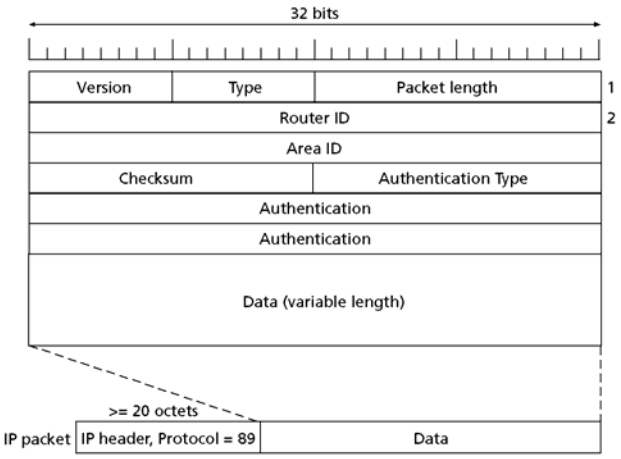
NBMA

OSPF doit connaître le type de liaison le séparant de son voisin. On distingue entre les réseaux de diffusion (par ex. Ethernet), les lignes point à point (par ex.PPP) et les réseaux à accès multiples sans diffusion NBMA (Non Broadcast Multiple Access).

Designated router

Afin de diminuer le volume d'information à échanger sur un réseau de type diffusion (LAN), le protocole OSPF élit un routeur désigné (Designated Router). Son rôle est de rassembler les informations de remise à jour (LSA = Link State Advertisment) est de les distribuer à tous les routeurs voisins. Le routeur Backup prend le relais en cas de défaillance du routeur désigné.

12.2.5 Format général des paquets OSPF



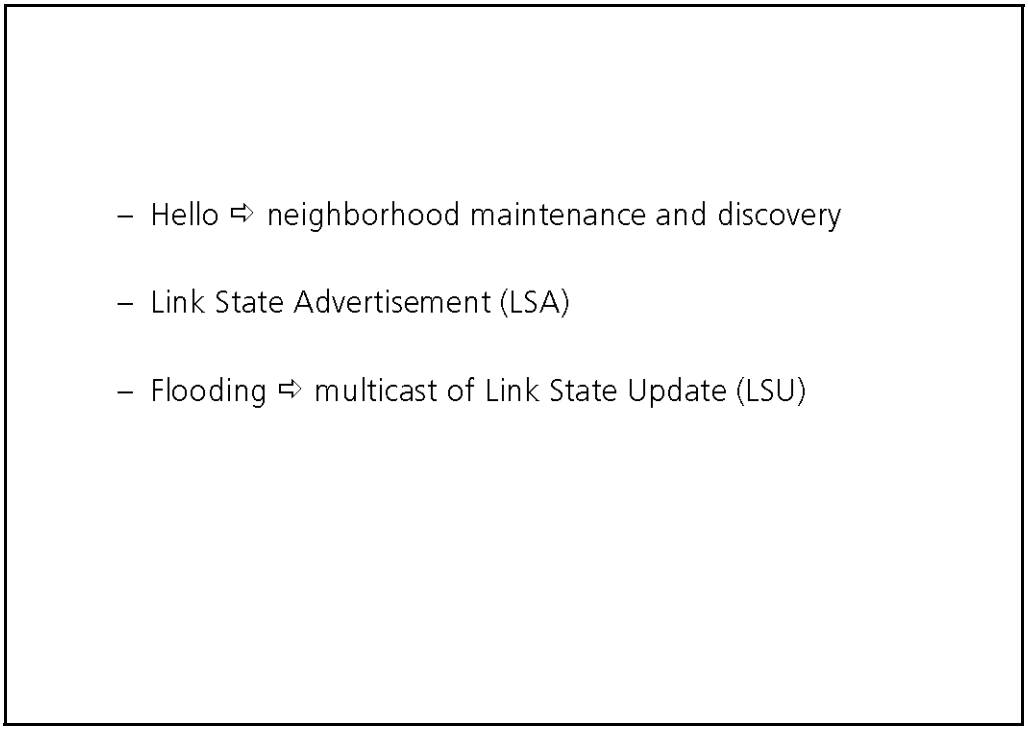
Slide 12.13
Format général des paquets OSPF

Paquet OSPF

L'entête d'un paquet OSPF est constituée de neuf champs :

- Le champ Version identifie la version du protocole OSPF.
- Type identifie le type de paquet OSPF (Hello, Database Description, Link-state Request, Link-State Update, Link-State Acknowledgment)
- Packet Lengh spécifie la longueur du paquet en byte, y compris l'entête.
- Router ID Indique la source du paquet.
- Area ID Identifie la zone à laquelle le paquet appartient. Tout les paquets OSPF doivent être associés à une zone.
- Checksum permet le contrôle de l'intégrité du paquet.
- Authentication type spécifie le type d'authentification mise en œuvre. Tous les échanges de protocole OSPF sont authentifiés. Le type d'authentification peut être spécifié par zone. Les données d'authentification sont contenues dans Authentication.
- Data contient les données spécifiques aux messages

12.2.6 Opérations OSPF



Slide 12.14
Opérations OSPF

Hello

La partie "Hello" du protocole OSPF est utilisée pour établir et maintenir les relations de voisinage entre routeurs. Sur les réseaux à diffusions, le protocole Hello peut également découvrir dynamiquement les voisins et élire le routeur désigné.

LSA

les "Link state advertisement (LSA)" sont des unités de données qui décrivent l'état d'un routeur ou d'un réseau. Ceci comprend l'état des interfaces et des ses routeurs adjacents. Chaque LSA est diffusée dans le domaine de routage (Area). L'ensemble des LSA reçu par un routeur constitue la base de données d'état des liaisons (LSDB).

Flooding

"Flooding" est la partie du protocole OSPF qui distribue et synchronise la base d'état des liaisons (LSDB) entre routeurs OSPF.

12.2.7 Propriétés d'OSPF

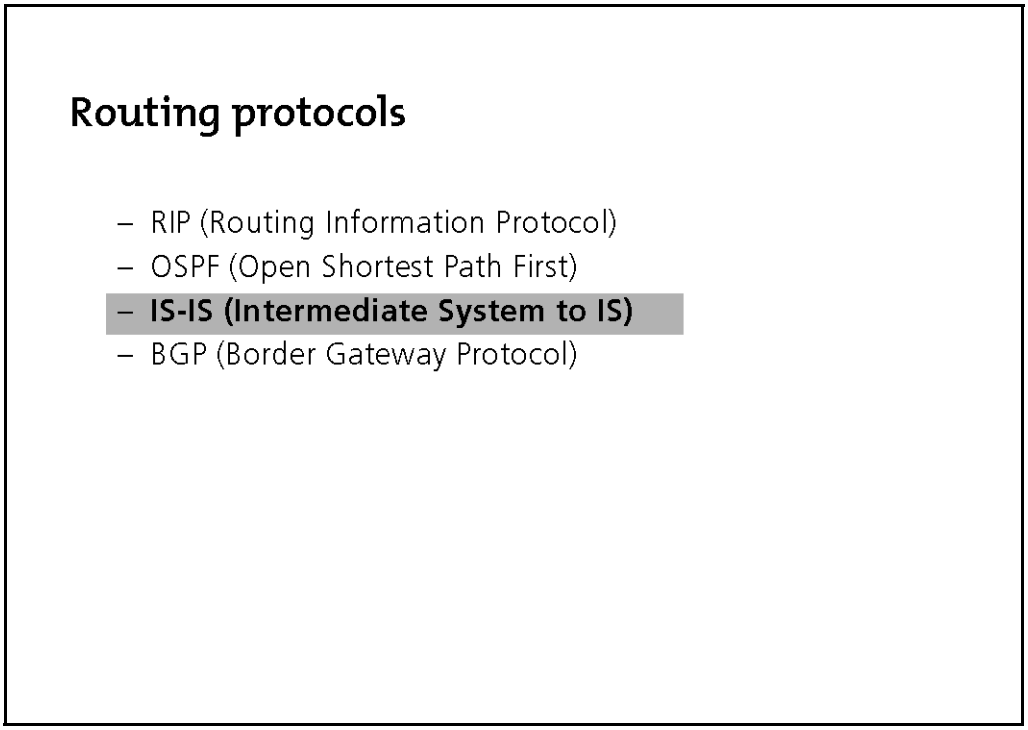
- Allows variable length subnet mask
- Suitable for big network
- Quick convergence time
- Needs high CPU resources
- Only Link State Update ⇨ low traffic for network
- Allows multipath routing
- Allows Type of Service based on various metrics

Slide 12.15
Propriétés d'OSPF

OSPF présente des avantages significatifs par rapport à RIP. Il est notamment possible d'effectuer un routage différencié en fonction de la qualité de service requise par le champ "Type of service" des paquets IP. Cette fonctionalité est optionellement rendue possible par l'utilisation de plusieurs metrics et donc de plusieurs tables de routage. On peut par exemple optimiser le débit, le délai ou la fiabilité du chemin.

La définition de masque de sous-réseau de longueur variable permet de diviser un réseau IP en de nombreux sous-réseaux de taille variable.

12.3 IS-IS (Intermediate System to Intermediate System)



Slide 12.16
IS-IS

IS-IS est un protocole de routage développé par l'ISO. Il était originellement conçu pour supporter le routage du protocole CLNP (Connectionless Network Protocol) de l'ISO.

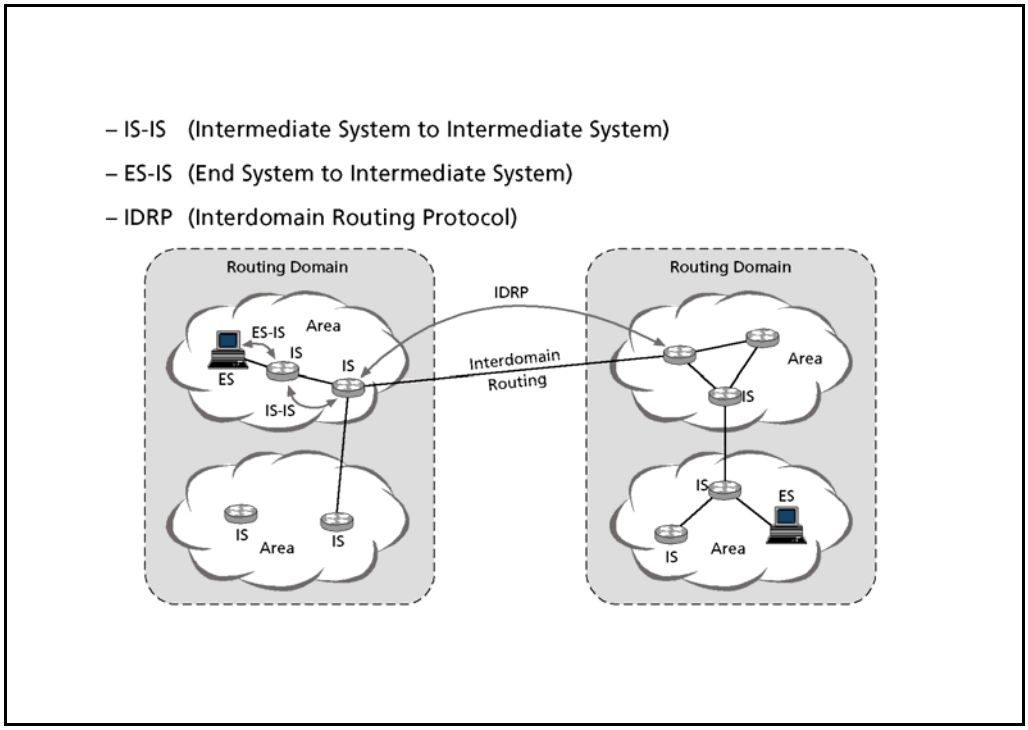
CLNP, Connectionless Network Protocol

Un système intermédiaire (Intermediate System) est la terminologie utilisée par l'ISO pour désigner un routeur. IS-IS est donc le protocole de routage mis en œuvre dans OSI, l'abréviation IS-IS désigne le protocole mis en œuvre entre systèmes intermédiaires.

IS, Intermediate System

IS-IS est décrit dans le document [ISO 10589] et ANSI X3S3.3.

12.3.1 Protocoles de routage et terminologie OSI



Slide 12.17
Protocoles de routage et terminologie OSI

IS-IS

IS-IS : Protocole de routage mis en œuvre entre routeurs (IS : intermediate System)

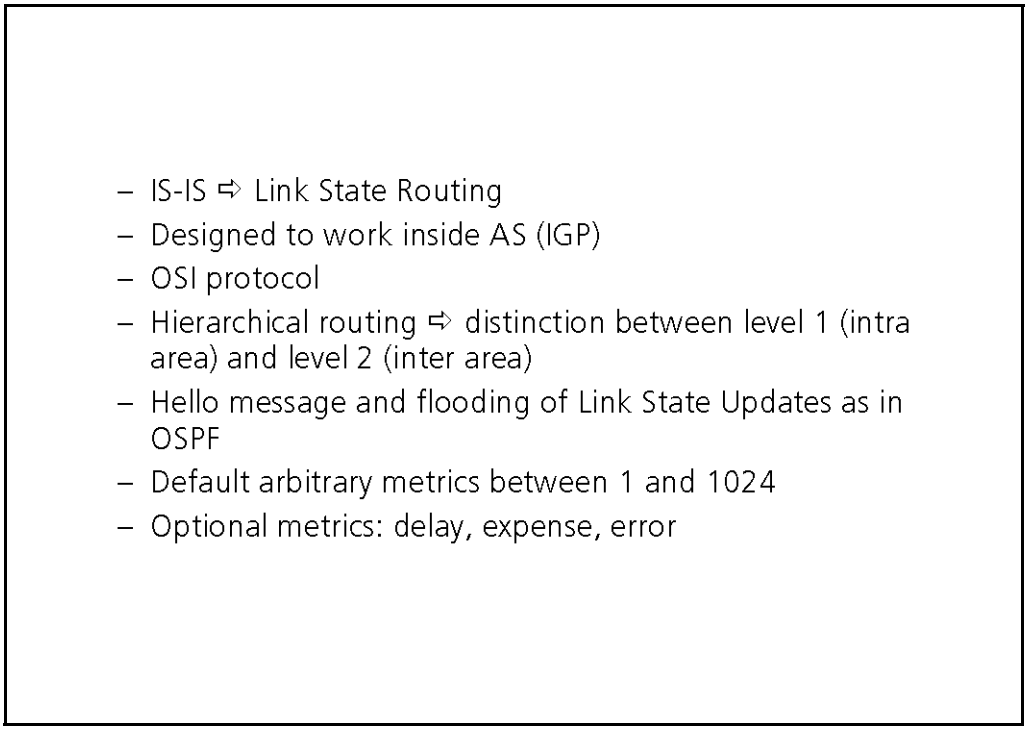
ES-IS, ES, End System

ES-IS est le protocole qui définit le dialogue entre terminaux (ES : End system) et le système intermédiaire (le routeur). Il s'agit d'un protocole de découverte (discovery) qui permet à une station de s'annoncer au routeur.

IDRP

IDRP (Interdomain Routing Protocol) définit la manière dont les routeurs communiquent entre eux dans des domaines différents. IDRP est une évolution de BGP.

12.3.2 Principe et caractéristiques de IS-IS

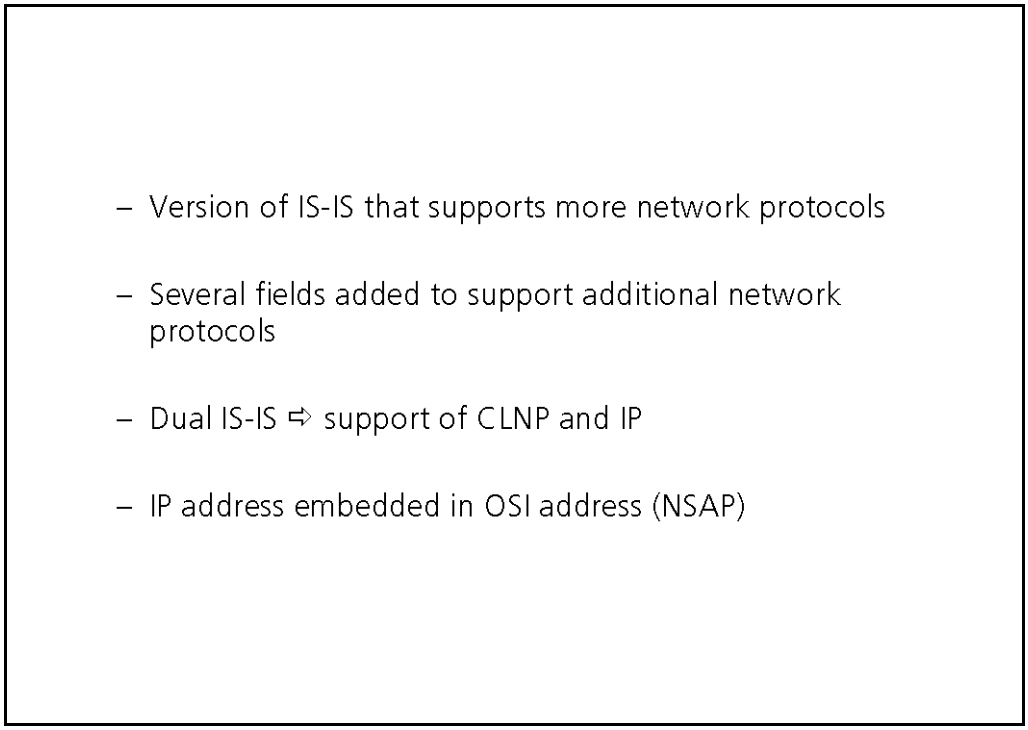


Slide 12.18
Principe et caractéristiques de IS-IS

IS-IS est un protocole à état des liaisons. Il est conçu pour opérer à l'intérieur d'un système autonome (IGP). Pour simplifier les opérations de routage, un distinction est faite entre les IS (routeurs) de niveau 1 qui communiquent entre eux au sein d'une zone et les IS de niveau 2 qui assure le routage entre zones de niveau 1 (Backbone).

Le metric IS-IS par défaut est une valeur arbitraire définie par l'administrateur du réseau. cette valeur est comprise entre 1 et 1 024. Optionellement des metrics basés sur le délai, les coûts de communication ou sur le taux d'erreurs de la liaison peuvent être définies.

12.3.3 IS-IS intégré

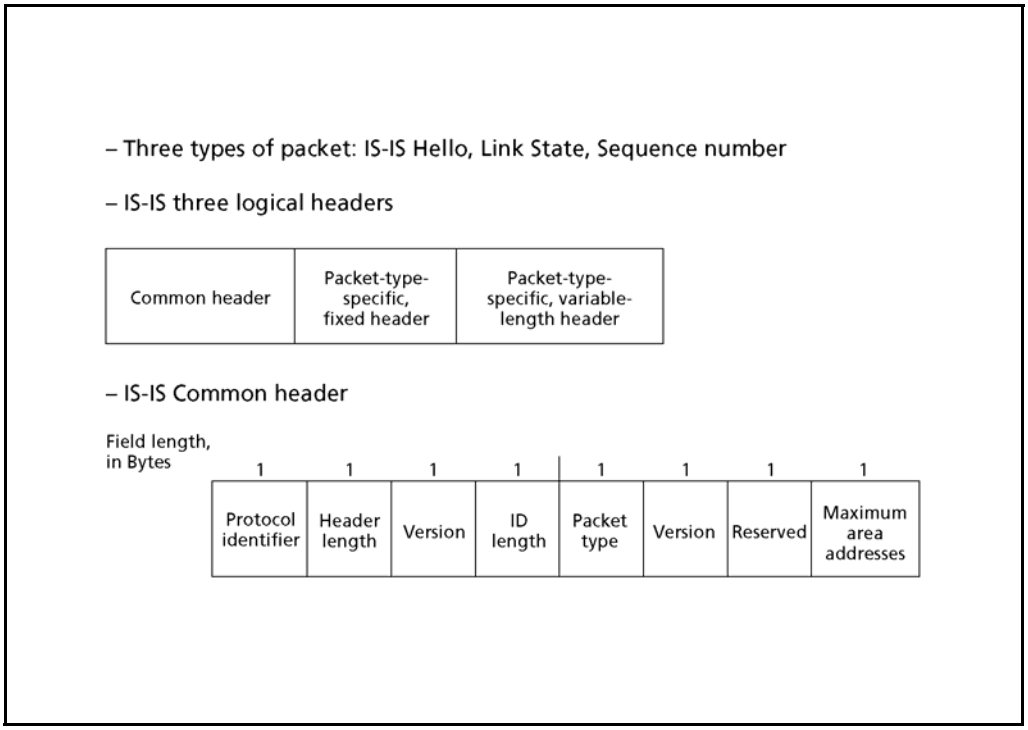


Slide 12.19
IS-IS Intégré

Dual IS-IS

IS-IS intégré est une version du protocole OSI IS-IS qui utilise un seul algorithme de routage pour supporter plusieurs protocoles routés. IS-IS intégré est parfois appelé "Dual IS-IS" pour désigner la version qui intègre les protocoles IP et CLNP.

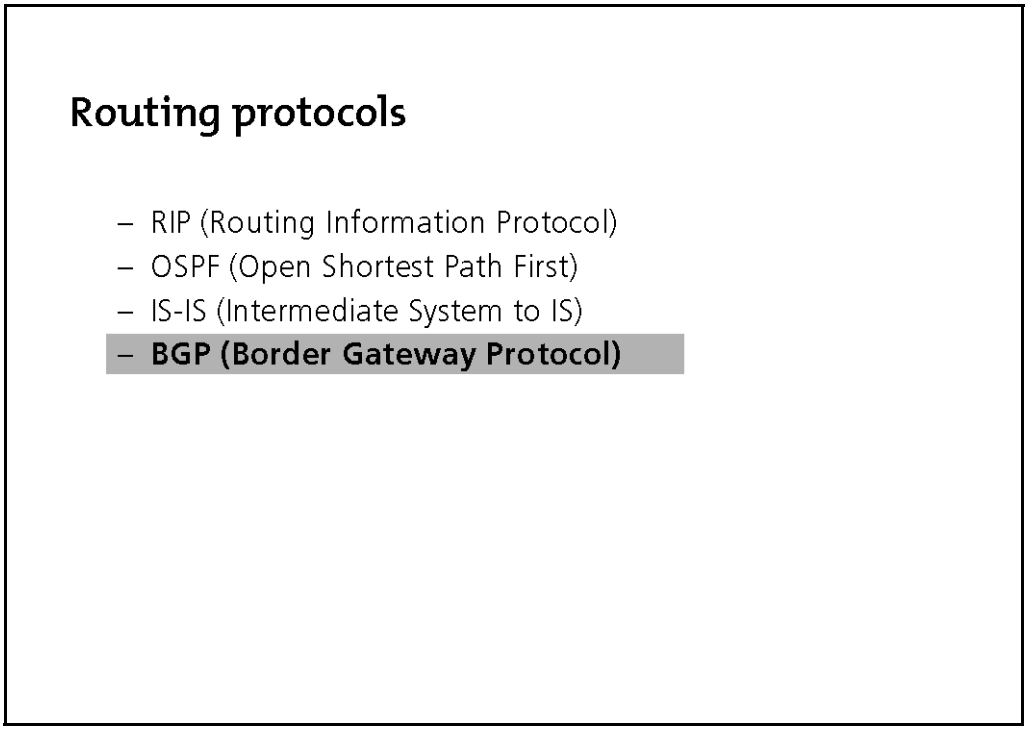
12.3.4 Format général de paquets IS-IS



Slide 12.20
Format général de paquets IS-IS

Chaque type de message (Hello, Link State, Sequence number) est composé d'une strucure complexe, articulée autour de trois parties logiques (Common header, Packet specific fix length Header, Packet specific variable length Header) L'entête commune des paquets IS-IS est constituée de huit champs : (Protocol Identifier, Header Length, Version, ID length, Packet Type, Version, Reserved, Maximum Area Address)

12.4 BGP (Border Gateway Protocol)

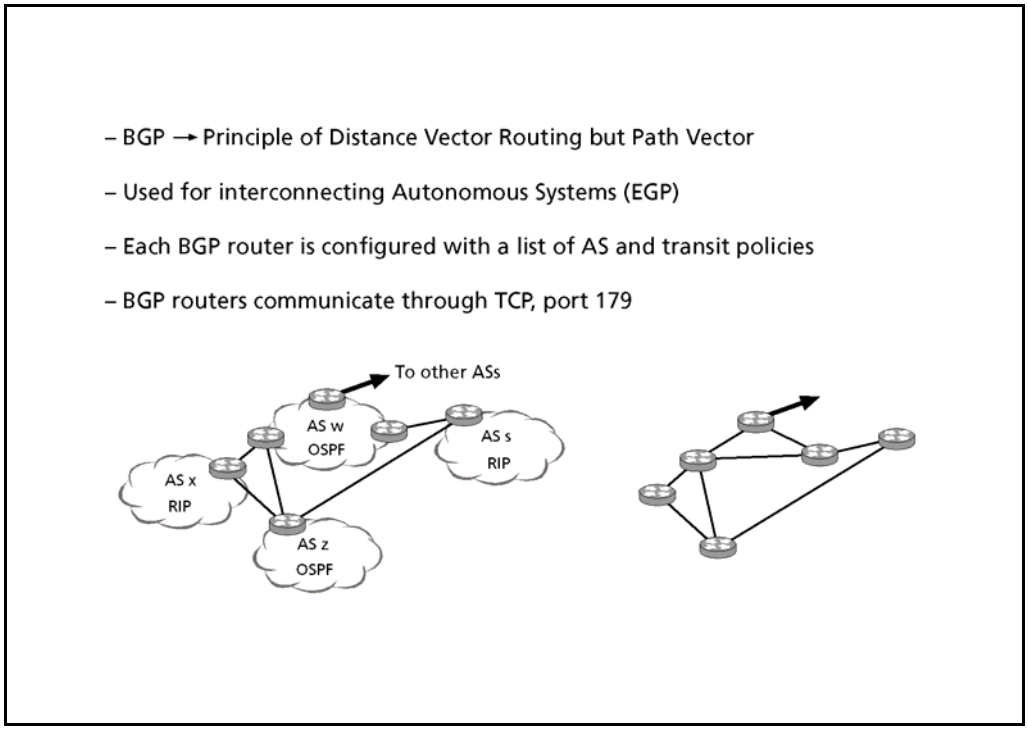


Slide 12.21
BGP (Border Gateway Protocol)

BGP version 4 est décrit dans [RFC 1654]

BGP-4

12.4.1 Principe et caractéristiques de BGP



Slide 12.22
Principe et caractéristiques de BGP

vecteur de chemin, path vector routing

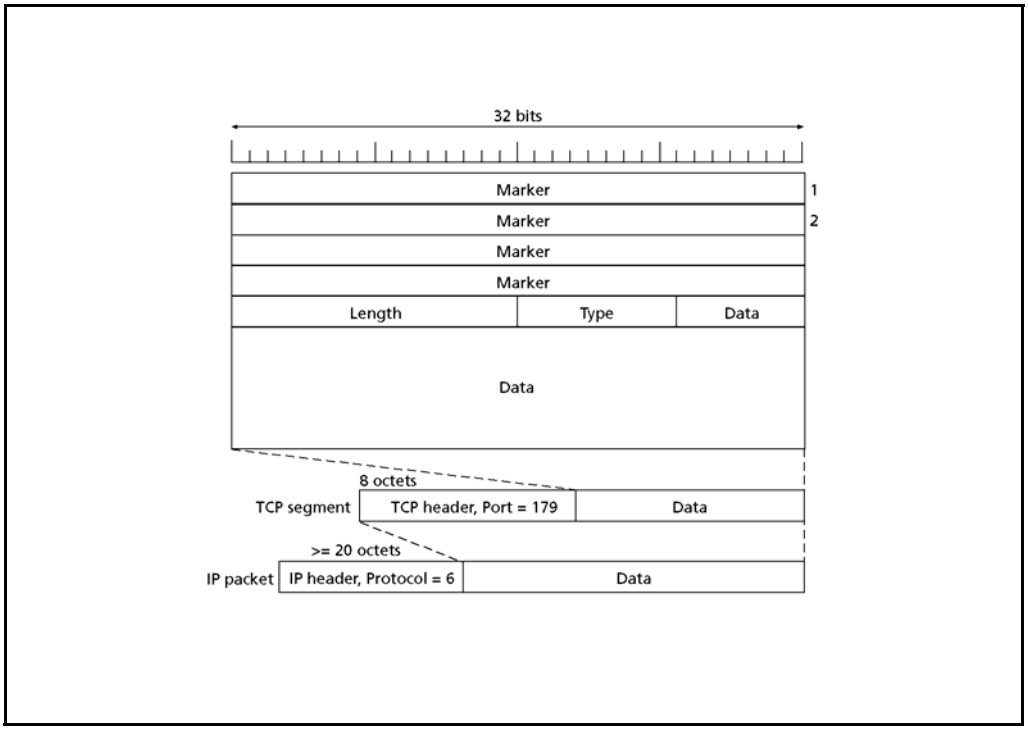
BGP est un protocole basé sur le principe du vecteur de distance. On parle également de "vecteur de chemin" car le metric utilisé n'est pas basé sur un nombre de sauts mais sur nombre de sytèmes autonomes traversés. Il est donc un protocole de routage extérieur (EGP).

Les routeurs BGP communiquent entre eux en établissant des connexions TCP sur le port 179. ils sont considérés comme voisins s'il partage un AS commun.

AS, Autonomous System

Au lieu de maintenir un coût vers chaque destination, un routeur BGP enregistre la route exacte (AS traversés) vers chaque destination. Il échange périodiquement sa table des routes avec ses voisins. Les entrées de la table qui ne sont pas compatibles avec les politiques d'acheminement sont détruites. Ensuite, la route la plus courte est choisie pour l'acheminement des paquets.

12.4.2 Format de paquets BGP



Slide 12.23
Format de paquets BGP

Paquet BGP

Chaque paquet BGP est constitué d'un entête dont le rôle principal est d'identifier la fonction du paquet en question. Il est constitué de quatres champs :

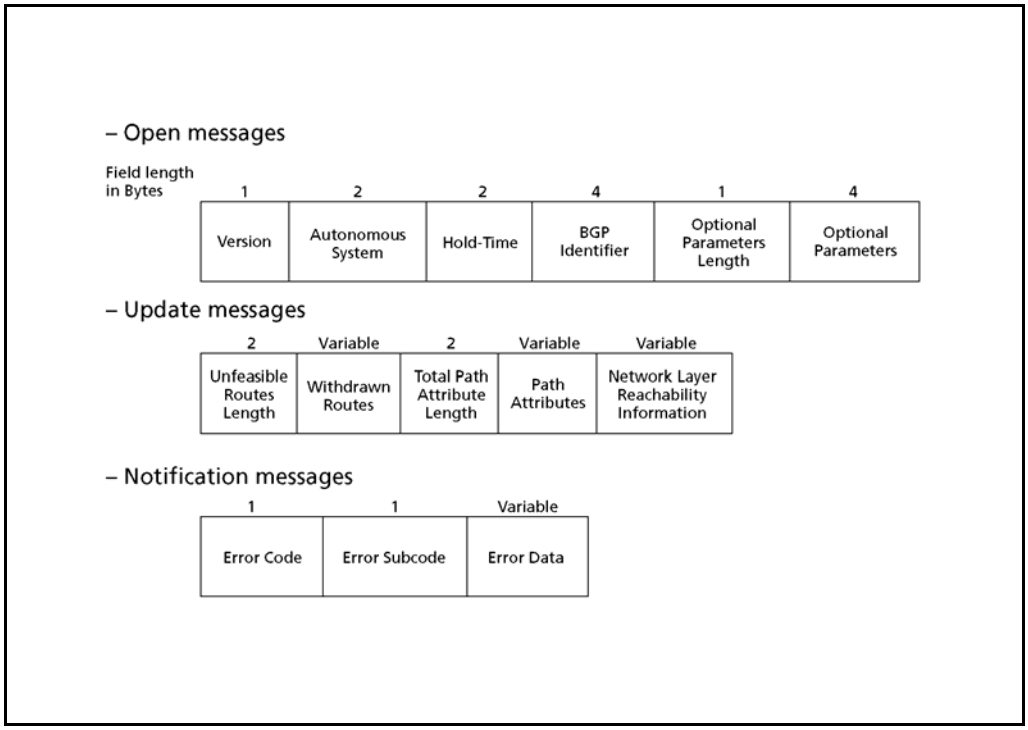
Marker contient des données d'authentification.

Length spécifie la longueur totale du paquet en bytes.

Type spécifie le type de message contenu dans les données (Open, Update, Notification, Keep-alive)

Data contient les informations des couches supérieures

12.4.3 Principaux messages BGP



Slide 12.24
Principaux messages BGP

Open message

Un message Open ouvre une communication BGP entre routeurs. Il s'agit du premier message envoyé après l'ouverture de la connexion TCP. Les messages Open sont confirmés avec des messages Keep-Alive.

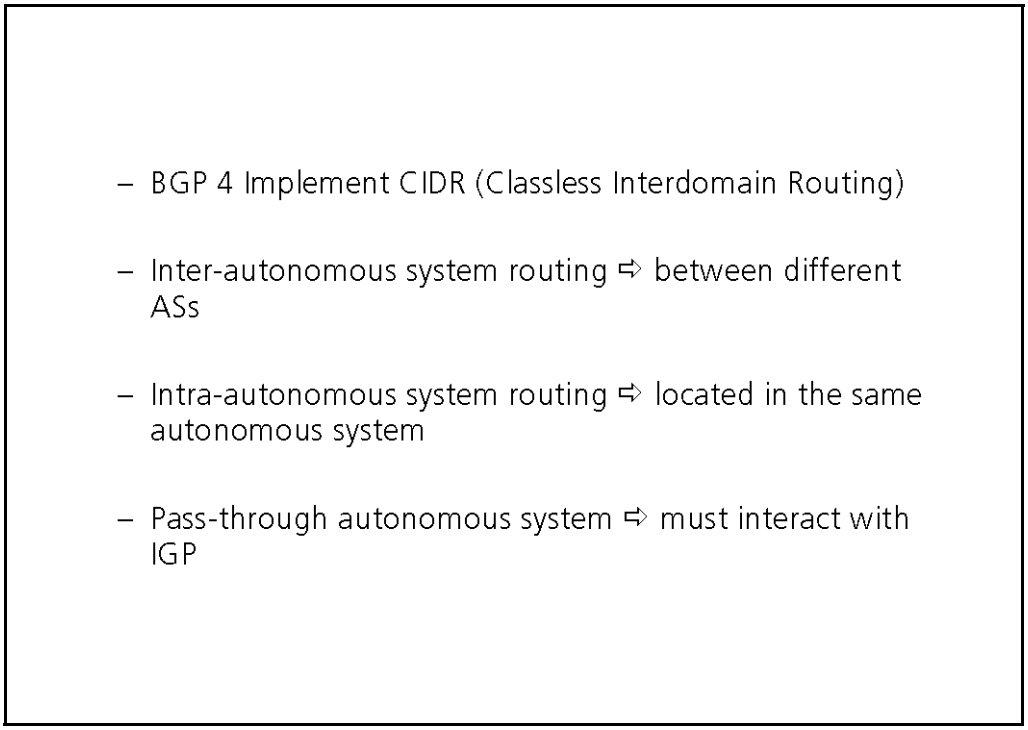
Update message

Le message Update est utilisé pour fournir des mises à jour de routage aux autres sytèmes BGP. Ainsi une vision cohérente de la topologie du réseau est garantie. Un message Update peut retirer (Withdraw) une route (adresse IP) devenue indisponible et simultanément annoncer de nouveaux chemins (Path attributes)

Notification message

Le message Notification est envoyé lorsqu'une condition d'erreur est détectée. Les notifications sont également utilisées pour fermer les sessions actives et pour communiquer la cause de la fermeture d'une session.

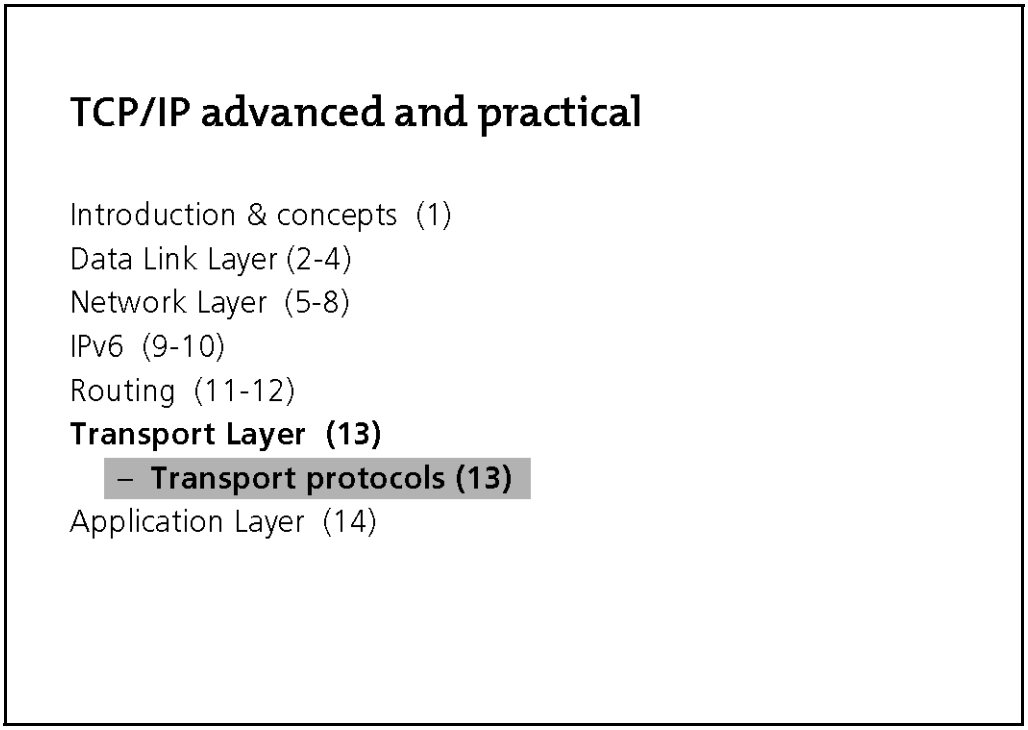
12.4.4 Propriétés de BGP-4



Slide 12.25
Propriétés de BGP-4

BGP 4 implémente le CIDR. Il s'agit d'un procédé d'aggrégation de route (super-netting) destiné à rendre les tables de routage moins volumineuses.

13 Protocoles de transport



Slide 13.1
Protocoles de transport

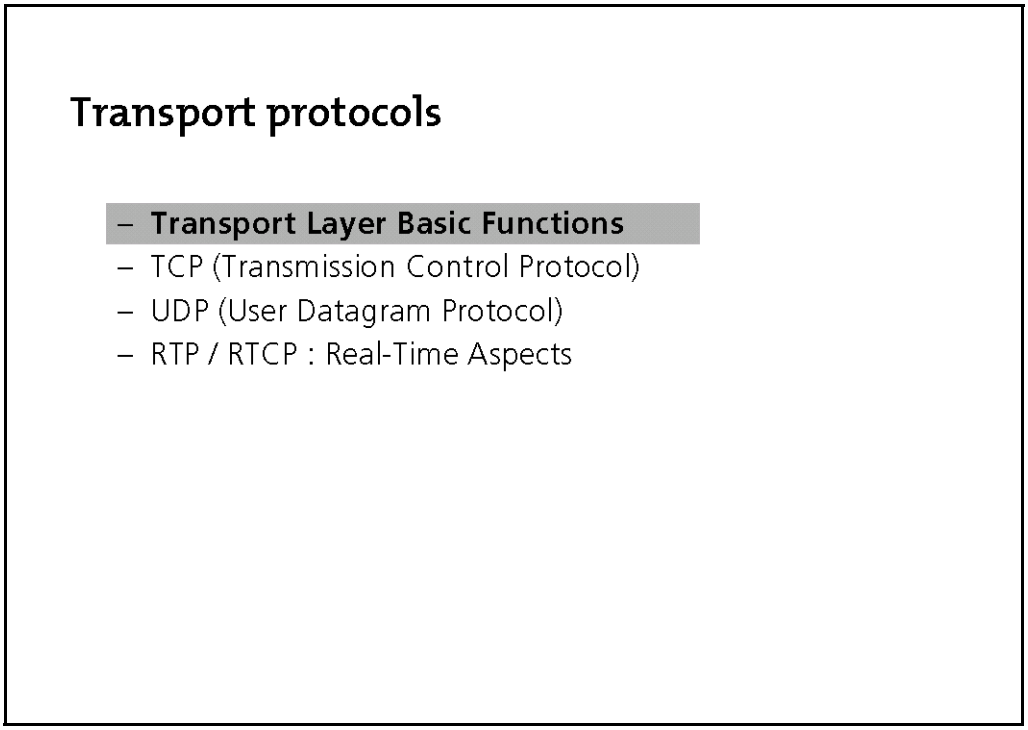
Après un aperçu des fonctions de base de la couche transport, ce chapitre traite des protocoles s'y trouvant.

Objectifs

A l'issue de ce chapitre, les participants sont capables de différencier les rôles de TCP et de UDP. Ils peuvent reconnaître les entêtes de ces protocoles et leur manière de fonctionner.

En outre, ils savent nommer les protocoles de transports complémentaires utilisés pour les applications "temps réel" et différencier leurs fonctions.

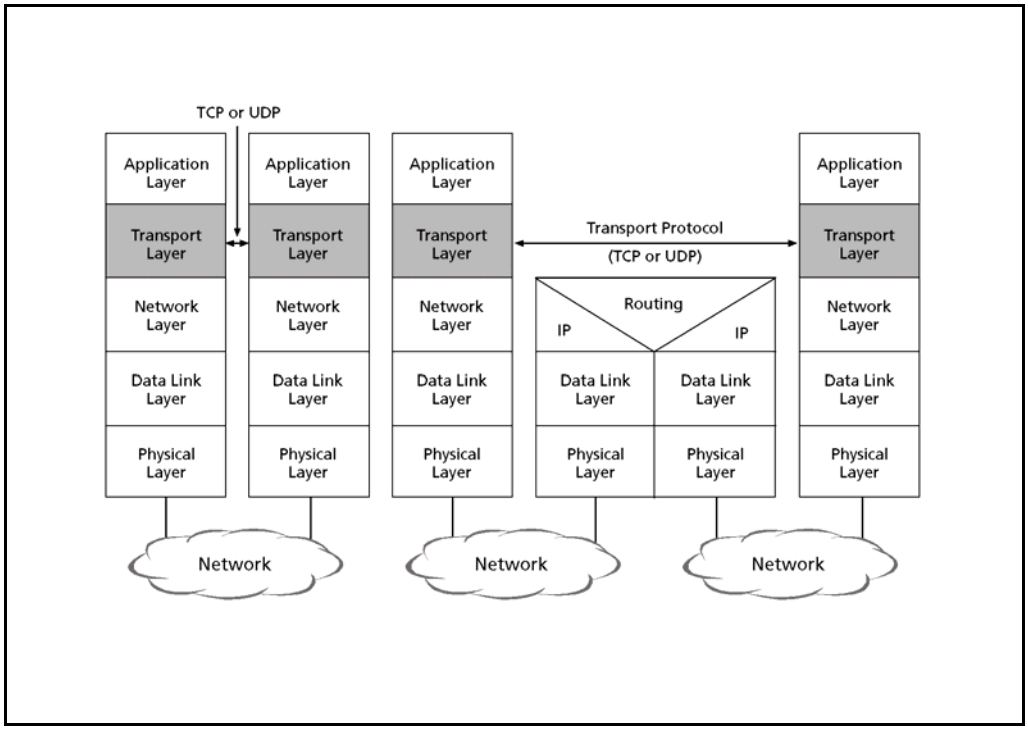
13.1 Fonctions de base de la couche transport



Slide 13.2
Fonctions de base de la couche transport

La couche transport a pour fonction principale de transférer les flux de données par multiplexage entre les différentes applications et la couche IP.

13.1.1 Architecture de la couche transport



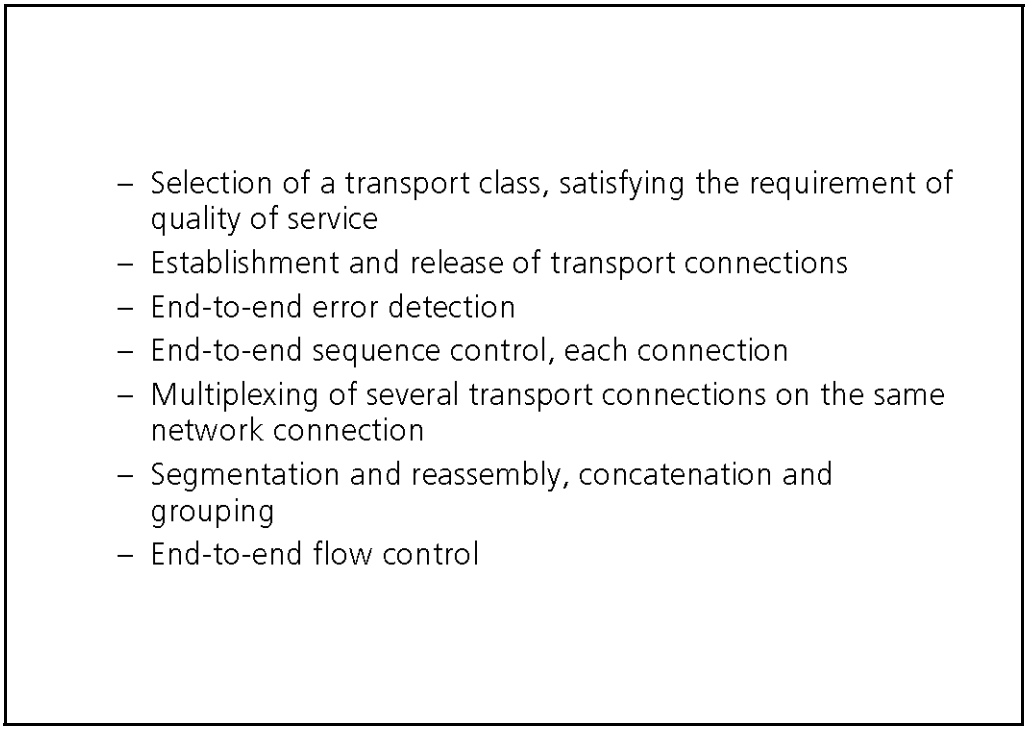
Slide 13.3
Architecture de la couche transport

La couche transport travaille de manière indépendante par rapport à la structure du réseau sur laquelle elle se fonde.

Elle est la première couche qui permet une communication de bout en bout, même au travers d'un nombre quelconque de réseaux et de routeurs.

La couche application accède aux fonctions de la couche de transport pour procéder à l'échange des données.

13.1.2 Fonctions de base



Slide 13.4
Fonctions de base

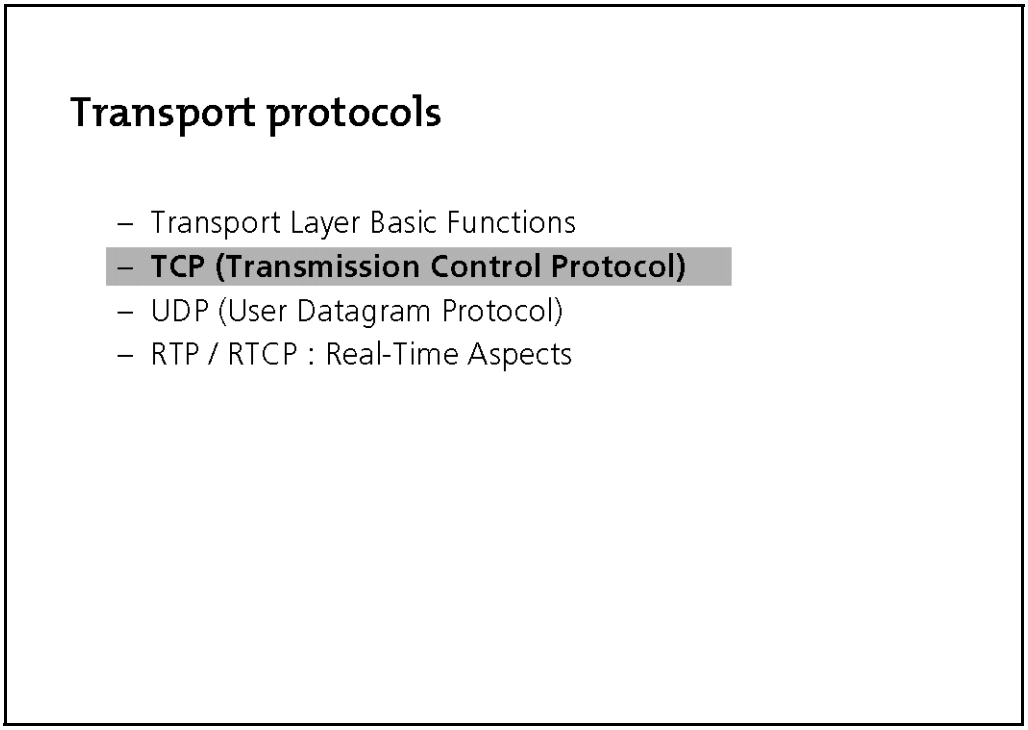
Dans les réseaux TCP/IP, la fonction de la couche transport est assurée par deux protocoles : TCP (Transmission Control Protocol) et UDP (User Datagram Protocol). TCP, UDP

C'est l'application de l'utilisateur qui détermine, parmi ces deux protocoles, lequel est appliqué.

Tous deux ont pour objectif de remettre les données aux services concernés de la couche d'application. Pour identifier ces différents processus d'application, on fait appel à des adresses de transport désignées par numéros de port (port number). Port

TCP fournit un service de transport fiable et utilise un mode de transport orienté connexion. En revanche, UDP offre un service en mode sans connexion et ne peut garantir la remise des données.

13.2 TCP (Transmission Control Protocol)



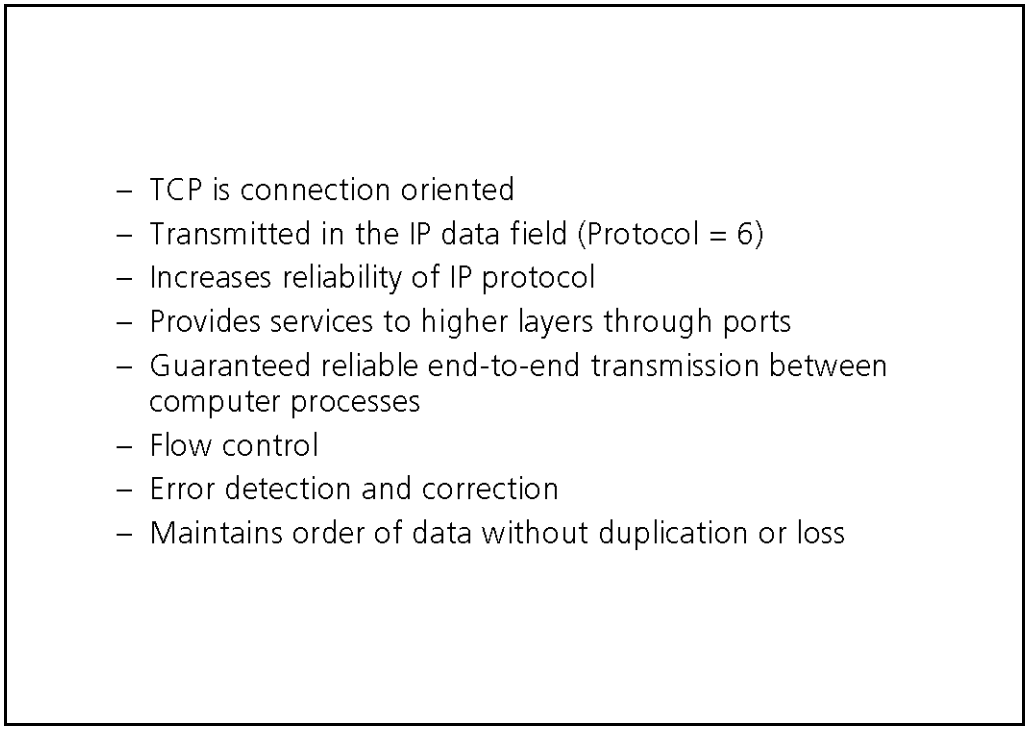
Slide 13.5
TCP (Transmission Control Protocol)

TCP

TCP (Transmission Control Protocol) offre un service de transfert de données fiable, orienté connnexion, en utilisant le service datagramme de IP.

TCP est décrit dans [RFC 793].

13.2.1 Principes et caractéristiques de TCP



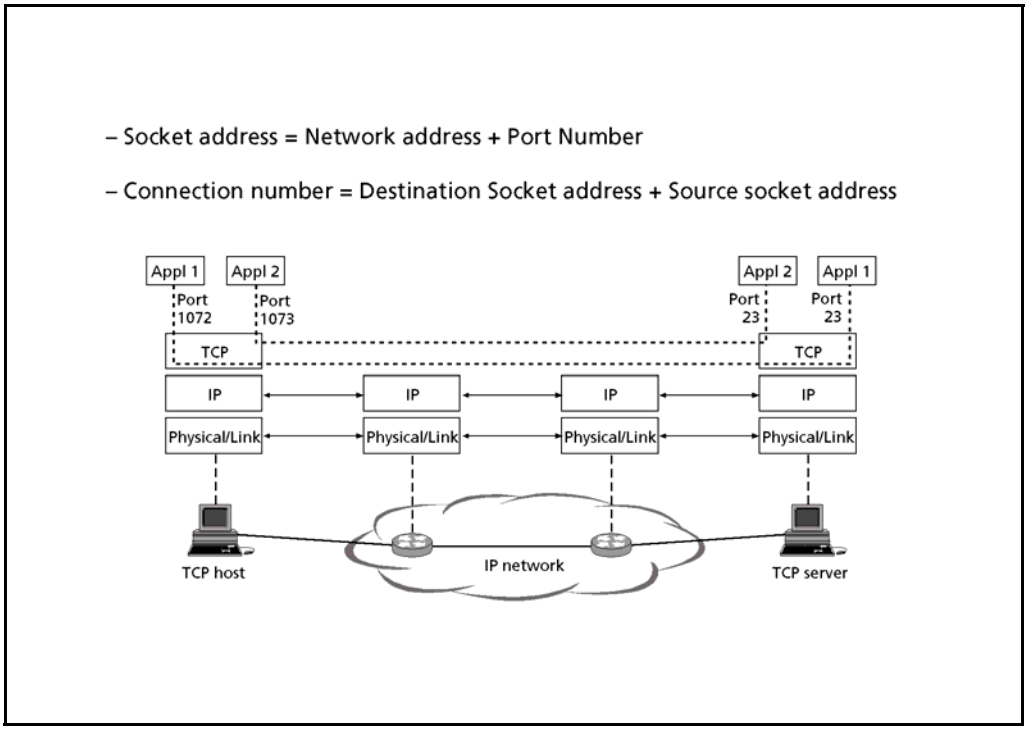
Slide 13.6
Principes et caractéristiques de TCP

TCP offre des services fiables point à point entre processus d'application s'exécutant sur des machines distantes. Cette fiabilité est renforcée notament par un adressage des services de la couche application au moyen de numéros de port (port number).

Les données remises par le service TCP au protocole IP sont regroupées en segments qui se composent d'un entête TCP et des données de la couche application.

Les processus d'application transmettent leurs données dans la taille la plus appropriée. Chaque octet transmis par TCP est numéroté assurant ainsi une chronologie des données envoyées au processus d'application.

13.2.2 Architecture TCP



Slide 13.7
Architecture TCP

Dans un environnement client-serveur, plusieurs applications peuvent simultanément communiquer par la même interface réseau et ainsi partager la même adresse IP.

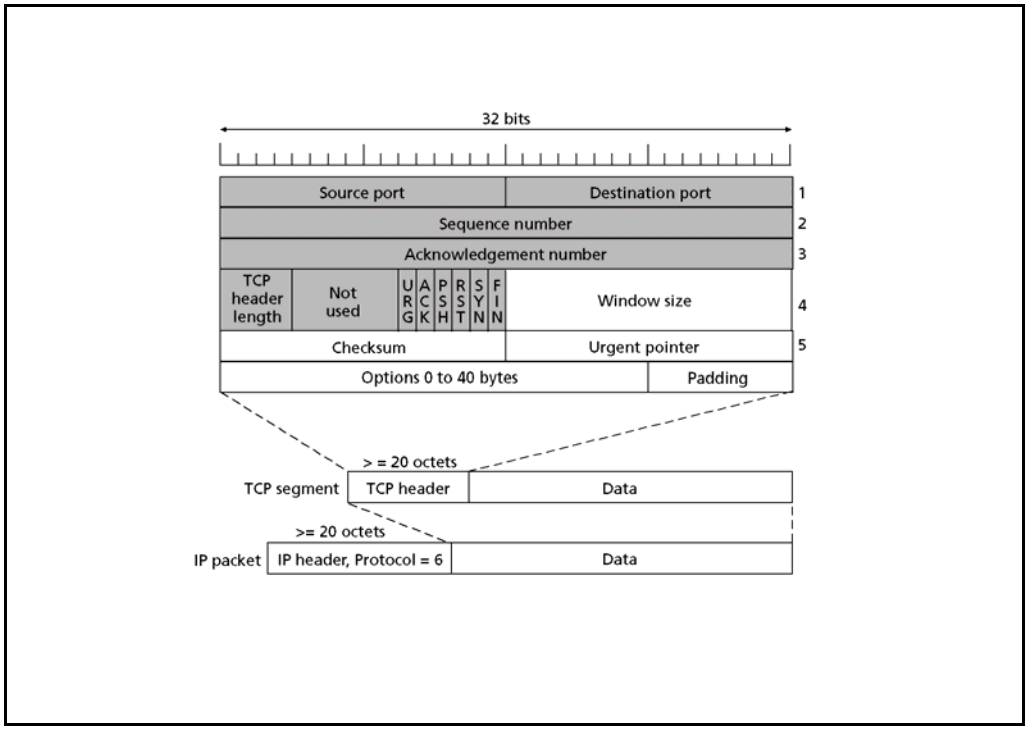
Port

L'adresse IP ne permettant pas d'identifier une application d'une autre, TCP associe un numéro de port (port number) à chaque protocole d'application. Ce numéro est compris entre 0 et 1 023 (20, 21 = FTP, 23 = Telnet, 25 = SMTP, 80 = HTTP) pour le port destination (coté client). alors qu'une une valeur supérieure à 1 024 est choisie arbitrairement pour identifier le port source.

Socket

L'association d'une adresse IP et d'un numéro de port est appelée "socket". Le socket source et le socket destination forment ensemble un numéro de connexion unique.

13.2.3 Format de paquet TCP



Slide 13.8
Format de paquet TCP

Port

Source port et Destination port identifient les différent flux de données générés par les applications.

Sequence Number

Sequence Number numérote les octets envoyés et vérifie si tous les segments envoyés ont été reçus. A l'établissement d'une connexion, les deux nœuds terminaux conviennent de l'utilisation d'un numéro de séquence initial.

Acknowledgment Number

Acknowledgment Number contient le numéro de séquence du prochain octet attendu par le récepteur.

Header Length

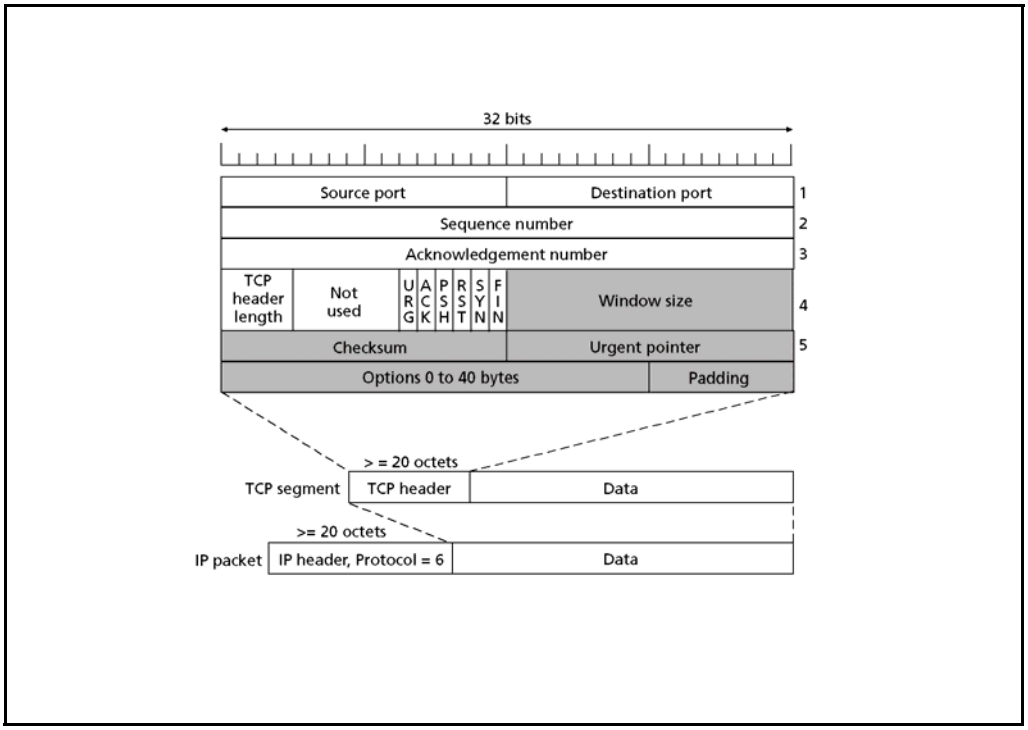
Header Length indique le nombre de mots de 32 bits contenus dans l'en-tête. Cette valeur pointe ainsi sur le début des données. (Valeur minimum = 5).

Flags

Les Flags ont des fonctions de contrôle de la connexion :

Flag	Indication
URG	le champ Urgent Pointer est actif et indique la position des données prioritaires
ACK	le champ Acknowledgment Number est significatif
PSH	provoque la remise immédiate des données à la couche application, sans " bufferisation "
RST	réinitialise la connexion suite à des erreurs irrécupérables
SYN	demande d'établissement d'une connexion et synchronisation des numéros de séquence
FIN	déclenche la libération de la connexion

Format de paquet TCP



Slide 13.9
Format de paquet TCP

Window Size définit le nombre d'octets qui peuvent être envoyés au delà du dernier octet quittancé. Il est possible d'agrandir la taille de la fenêtre au delà de la valeur 65 536 en négociant un facteur multiplicatif dans le champs option. Cette mesure peut être nécessaire dans les réseaux à haut débit et/ou à haut délai.

Window Size

Checksum sert à la protection de l'intégralité du segment TCP.

Checksum

Pour le calcul de ce champ, un pseudo en-tête est conceptuellement ajouté à l'en-tête TCP pour protéger la couche transport des éventuelles erreurs de routage.

Pseudo-Header

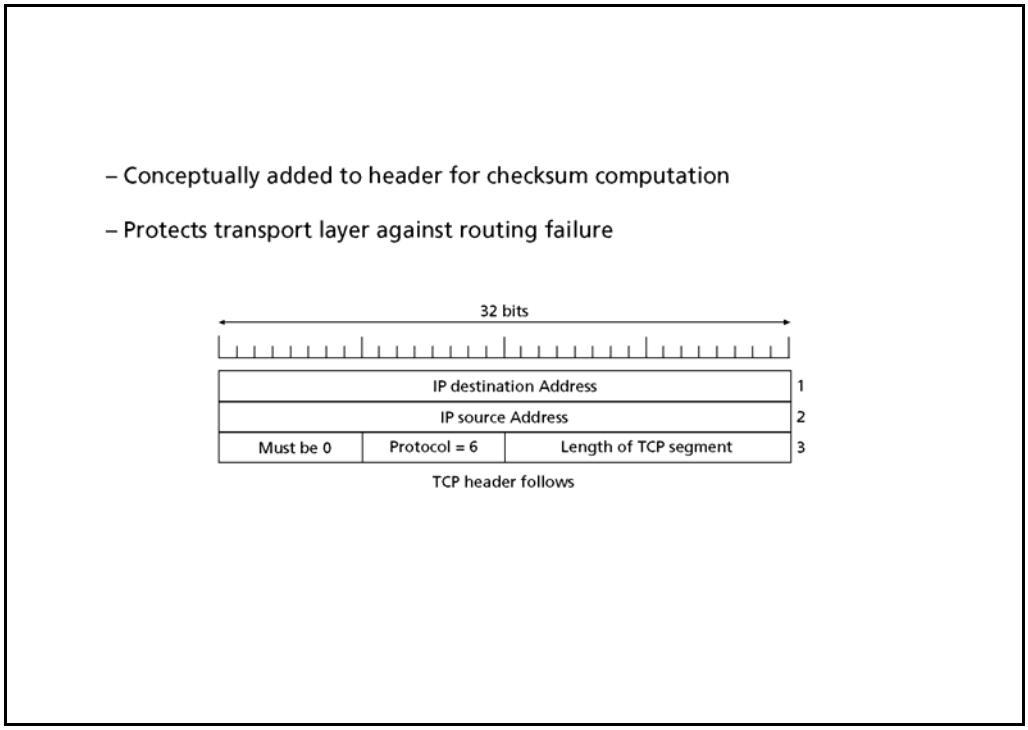
Urgent Pointer pointe vers le numéro de séquence du dernier octet des données à traiter en priorité. Ce champ n'est actif que si URG Flag = 1

Urgent Pointer

Le champ Options est utilisé pour transporter différentes informations optionelles, par exemple la taille maximale du segment TCP ou un facteur d'échelle pour le champ Windows.

Padding complète le champ Option pour obtenir un mot de 32 bits.

13.2.4 Le pseudo en-tête TCP



Slide 13.10
Pseudo en-tête TCP

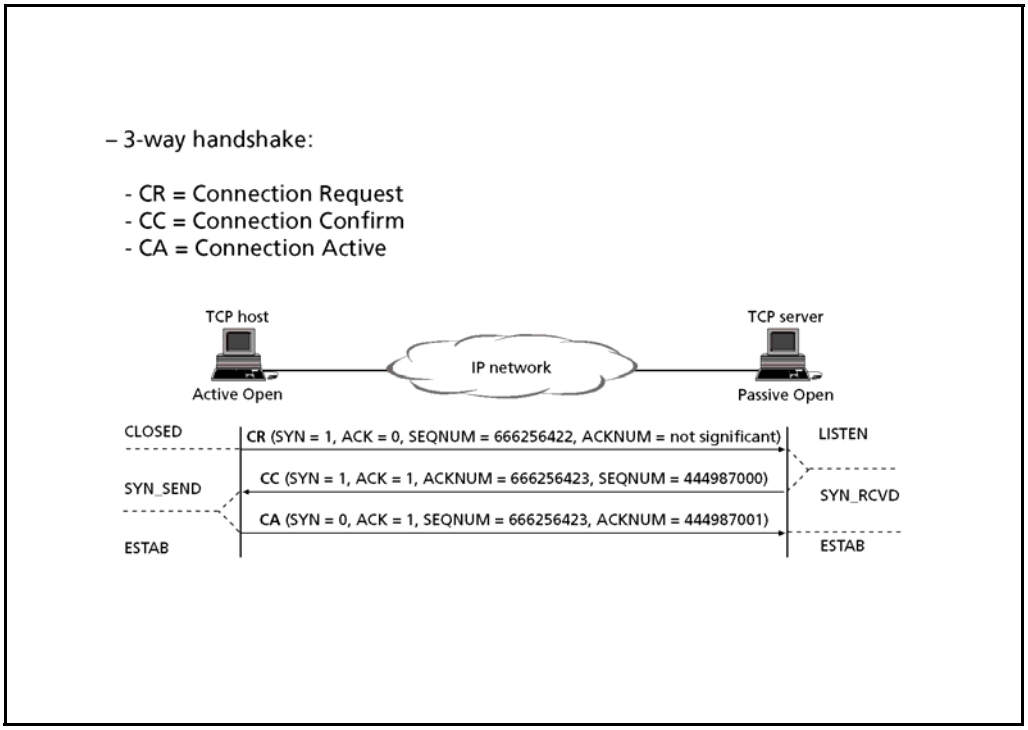
Afin de protéger TCP des erreurs de routage, un pseudo en-tête est utilisé dans le calcul du cheksum TCP.

Ce pseudo en-tête est constitué des grandeurs de l'entête IP qui ne vont pas varier durant le cheminement du paquet.

On y trouve donc les adresses IP source et destination, le champ protocol dont la valeur doit être 6 (= TCP), ainsi qu'une information de longueur des données IP, correspondant à la longueur du segment TCP transporté.

Ce pseudo en-tête n'est pas ajouté au paquet transmis, il est simplement utilisé pour le calcul de la somme de contrôle au départ et à l'arrivée du segment TCP.

13.2.5 Etablissement de connexion TCP



Slide 13.11
Etablissement de connexion TCP

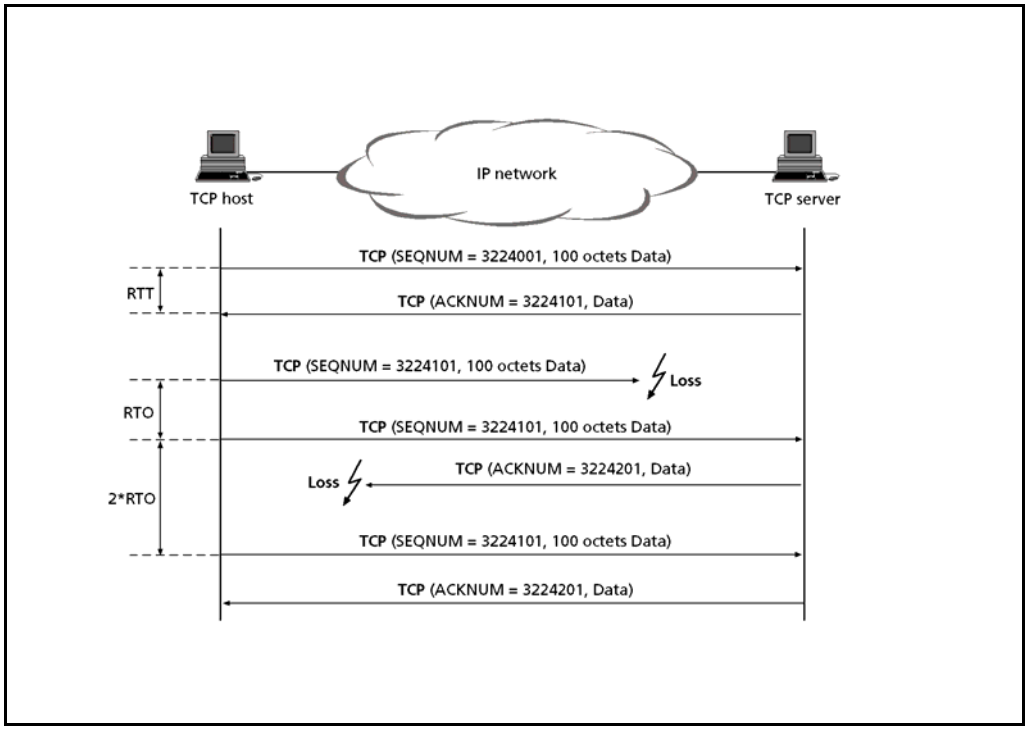
Avant d'envoyer des données avec TCP, les processus concernés doivent d'abord établir une connexion qui s'opère en trois étape (3-way handshake) :

Connection Request, Connection Confirm et Connection Active.

Ces différents messages sont identifé par les valeurs des fanions (Flag) "SYN" et "ACK"

Les numéros de séquence (Seqnum), dont la valeur initiale est généralement choisie de manière aléatoire, sont codés sur 32 bits.

13.2.6 Quittancement et retransmission TCP



Slide 13.12
Quittancement et retransmission TCP

Pour assurer la fiabilité du transfert, c'est à dire la retransmission des données erronées ou perdues, TCP met en œuvre une technique de numérotation et d'acquittement positif (Positive Acknowledgment). Chaque segment (paquet TCP) contient un numéro de séquence qui désigne le 1er octet du segment. Le numéro d'acquittement est envoyé par le récepteur des données et désigne le numéro du prochain octet attendu.

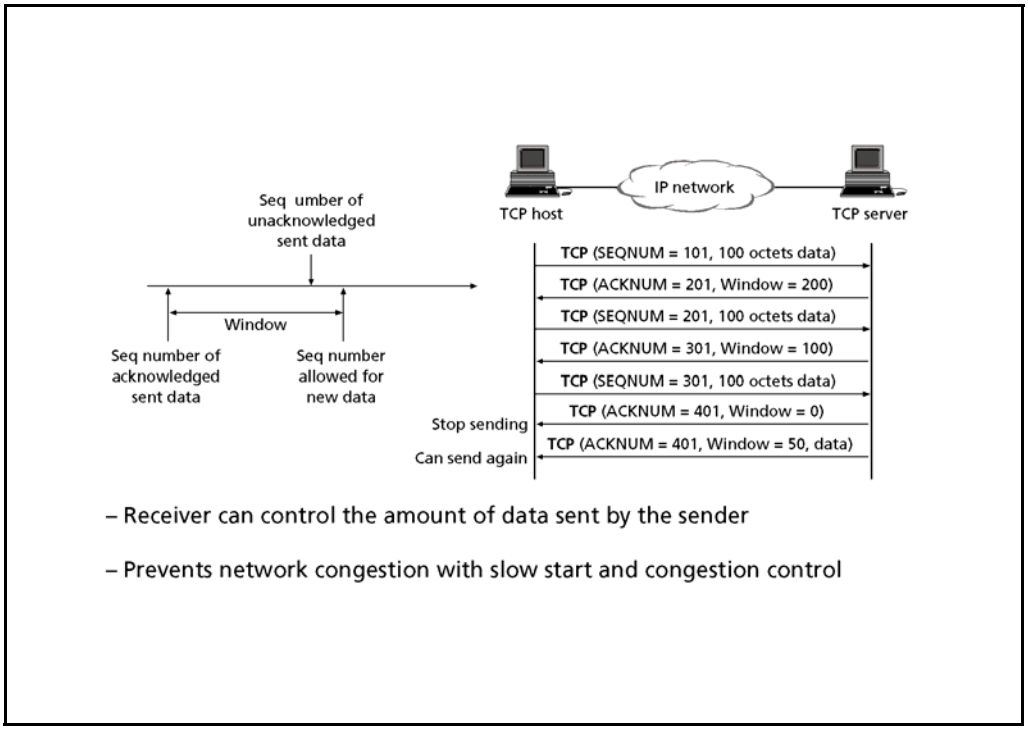
RTT, Round Trip Time

RTT (Round Trip Time) correspond au temps écoulé entre l'envoi d'un octet avec un numéro de séquence particulier et la réception de son acquittement. RTT est constamment adapté aux conditions de transmission.

RTO, Retransmission Time Out

RTT est utilisé pour calculer RTO (Retransmission Time Out) qui fixe le temps après lequel un segment est considéré comme perdu si aucun acquittement n'a été reçu. Une seconde retransmission est réalisée après 2 x RTO, une troisième après 3 x RTO.

13.2.7 Contrôle de flux TCP



Slide 13.13
Contrôle de flux TCP

Le contrôle de flux utilise la technique de la fenêtre coulissante (sliding window) qui fixe le nombre d'octets que l'émetteur peut transmettre. La taille de cette fenêtre dépend de la capacité mémoire du buffer du récepteur. Lorsque ce dernier est trop sollicité, il transmet par l'intermédiaire du champs "Windows" une taille de fenêtre réduite ou nulle.

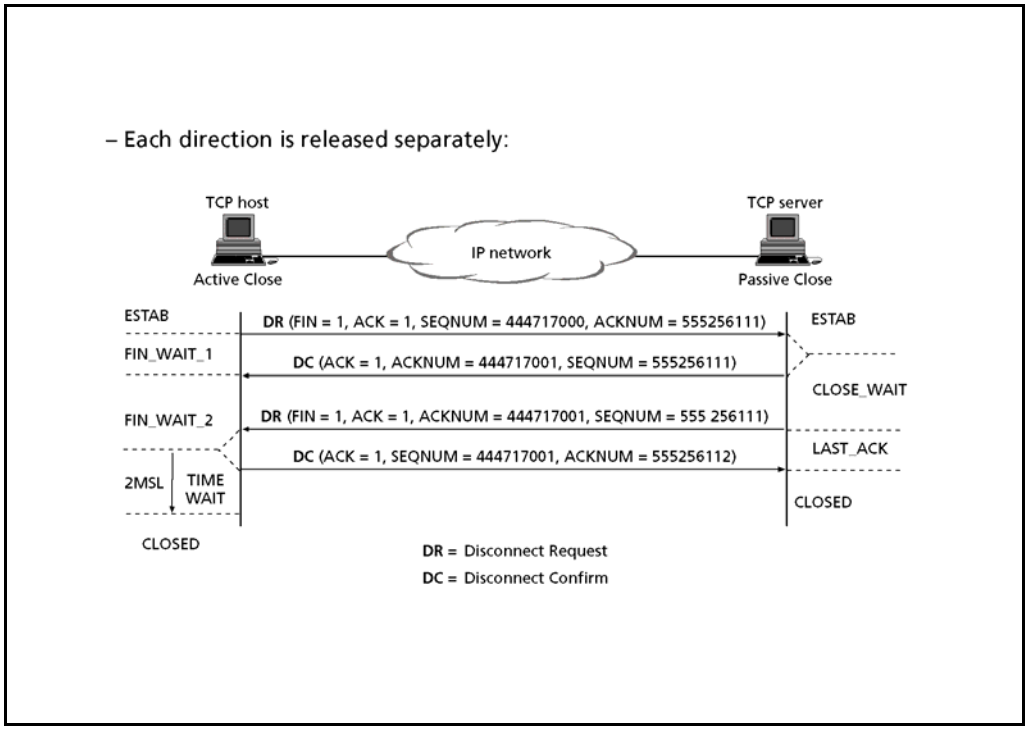
Slow start

Slow start : Permet d'augmenter progressivement le nombre de données émises jusqu'à ce que la taille de la fenêtre émise par le récepteur soit atteinte.

Congestion control

Congestion control : Technique de prévention de congestion utilisée par la source qui réduit volontairement la taille de la fenêtre en cas de congestion du réseau.

13.2.8 Déconnexion TCP



Slide 13.14
Déconnexion TCP

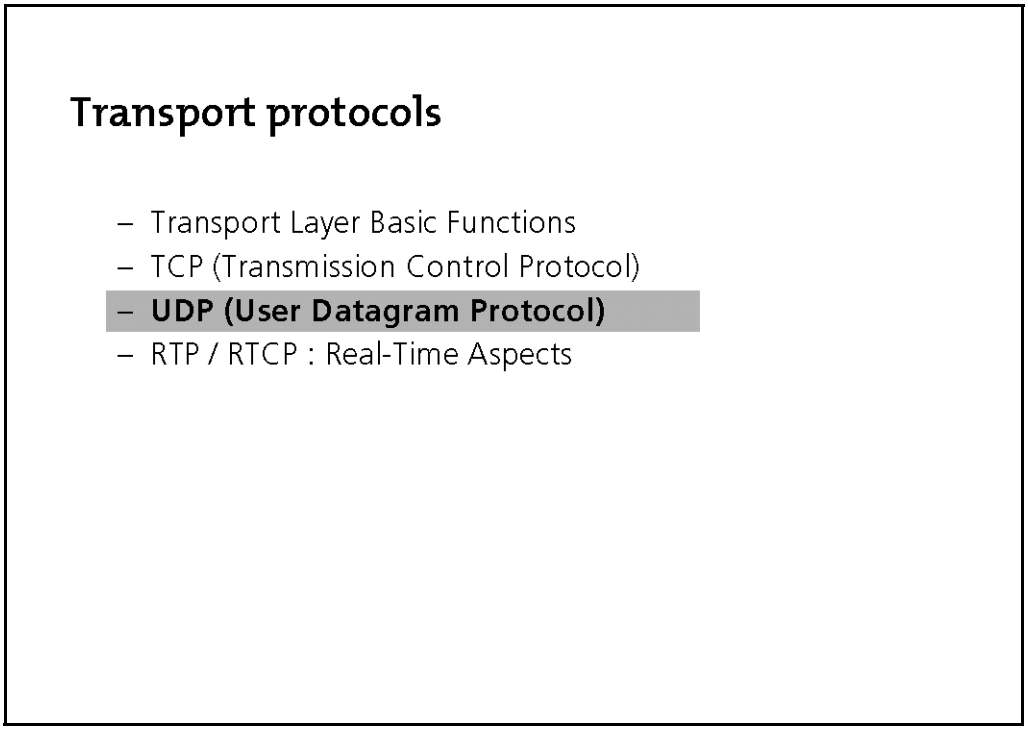
Quand la communication entre deux processus d'application est terminée, la connexion TCP est libérée, de même que les ressources.

Pour éviter la perte de données lors de la fermeture d'une session, la libération de la communication se déroule en deux phases; c'est-à-dire que chaque terminal libère sa propre "demi-connexion".

Time wait

Un temps d'attente (time wait) est nécessaire pour s'assurer que des segments retardés ne soient pas interprétés comme faisant partie d'une nouvelle connexion. Ce temps est équivalent à 2 x MSL (MSL = Maximum Segment Live = 2 min).

13.3 UDP (User Datagram Protocol)

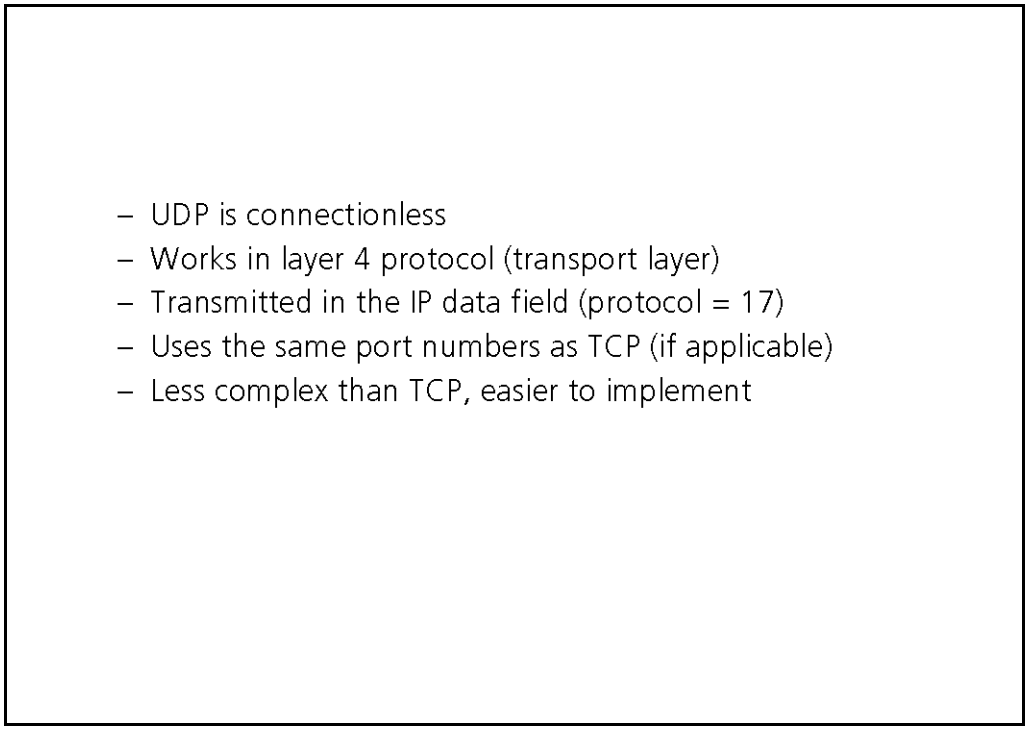


Slide 13.15
UDP (User Datagram Protocol)

UDP (User Datagram Protocol) offre un service de transport de type datagramme. UDP est décrit dans [RFC 768].

UDP

13.3.1 Principes et caractéritiques de UDP



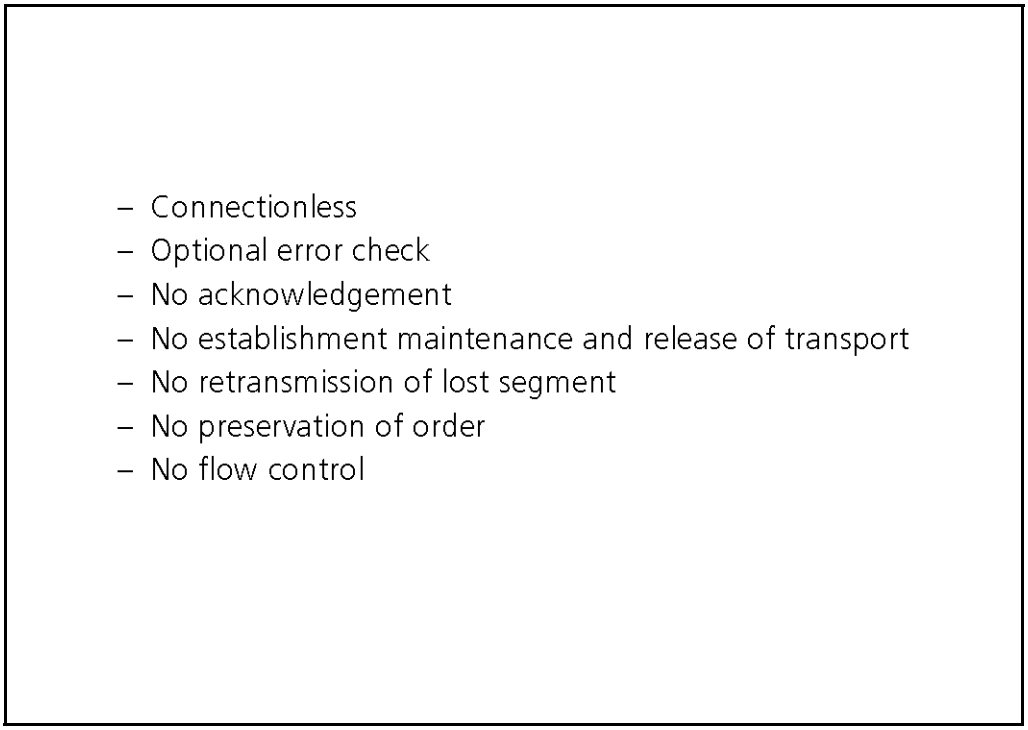
Slide 13.16
Principes et caractéristiques de UDP

UDP est un protocole de transport particulièrement simple qui offre un service de type datagramme. Il est bien adapté aux applications nécessitant de courtes sessions interactives dans des environnements réseau de bonne qualité.

UDP, associé à un protocole de transport temps réel (RTP), est utilisé pour le transport de flux de données nécessitant de la transparence temporelle. Il est également le protocole de transport mis en œuvre dans les environnements à diffusion (multicasting).

Les segments UDP sont encapsulés dans des paquets IP (protocol = 17).

13.3.2 Propriétés de UDP



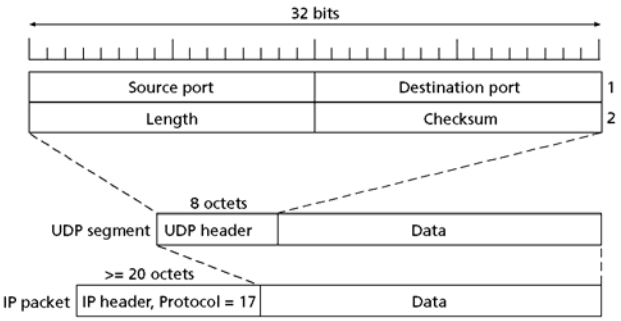
Slide 13.17
Propriétés de UDP

Les propriétés de UDP sont similaires à celles de IP. Il permet à des applications de communiquer avec un minimum d'"overhead" protocolaire. Il offre un service datagramme et en hérite de ce fait les propriétés.

Parmi les applications qui utilisent UDP, on peut citer :

- DNS (Domain Name System)
- SNMP (Simple Network Management Protocol)
- RIP (Routing Information Protocol).

13.3.3 Fomat de paquet UDP



Slide 13.18
Format de paquet UDP

L'en-tête UDP a une taille fixe de 8 octets.

Port

Source Port identifie l'application à partir de laquelle le datagramme a été émis. Il est optionnel et sa valeur vaut 0 s'il n'est pas utilisé.

Destination Port identifie l'application à laquelle le datagramme est destiné.

Length

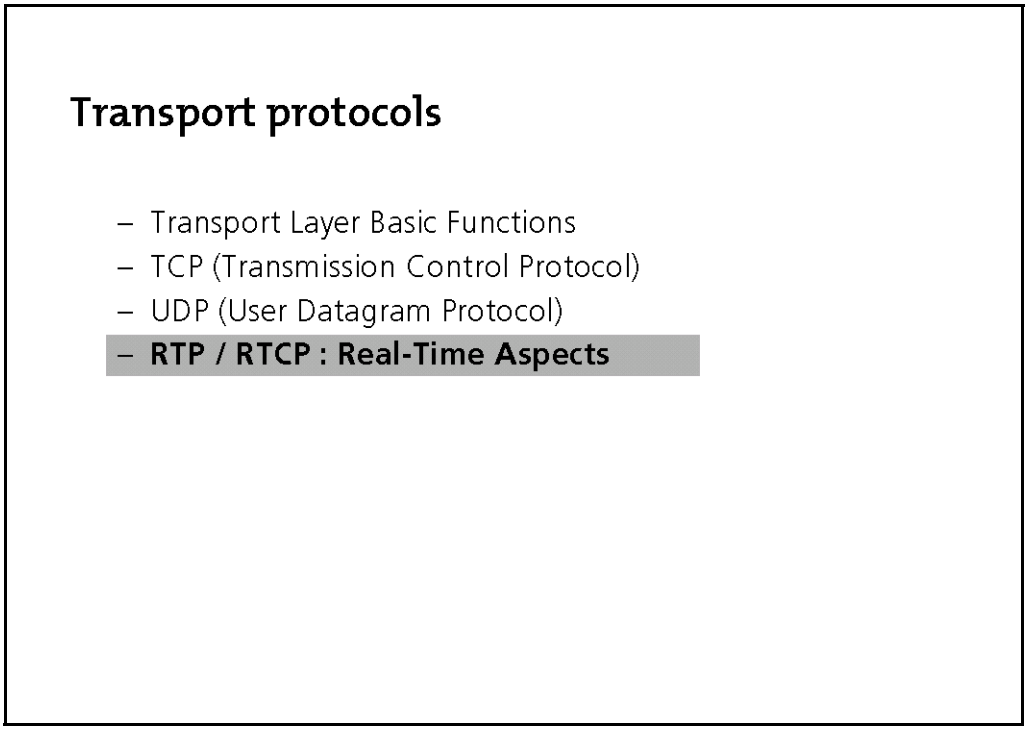
Length contient la longueur du datagramme UDP en octets (en-tête et données compris).

Checksum

Checksum assure l'intégrité de l'en-tête et des données. Comme pour TCP, le calcul du checksum se base sur un pseudo en-tête (pseudo header) de 12 octets.

Checksum est optionnel et sera inactif lorsque sa valeur vaut 0.

13.4 Transport “Temps réel” : RTP / RTCP



Slide 13.19
RTP / RTCP

Les nouveaux services qui apparaissent sur l’Internet nécessitent des efforts particuliers dans le “temps réel”.

Les délais de transmission doivent non seulement être relativement courts, mais il faudrait qu’ils soient constants. Cette réalité n’est malheureusement pas le point fort des réseaux de transmission de données.

Il nous faut surveiller ces données, de manière à ce que leur séquencement soit garanti, tout comme leur “identité temporelle”.

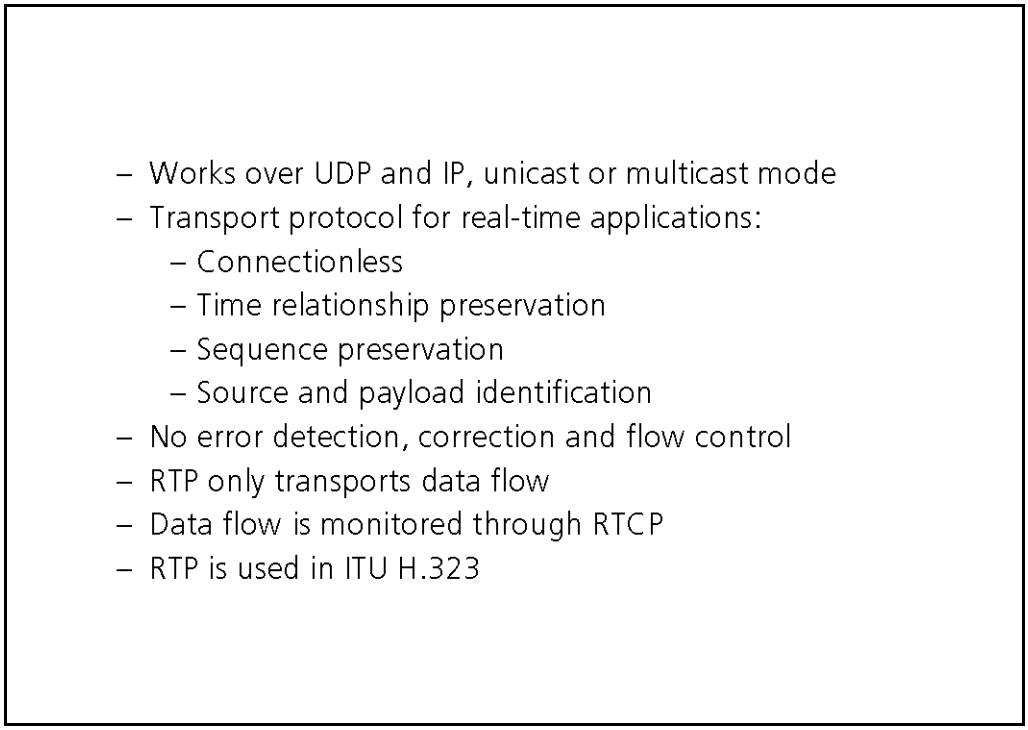
Dans notre stack TCP/IP, un couple de protocole offrent conjointement ce service.

RTP

RTP (Real-time Transport Protocol) offre un service de transfert qui permet de restituer les propriétés temporelles du flux de donnée. Il utilise les services de UDP pour l'adressage de l'application.

Les paramètres de contrôle qui y sont liés passent au travers d’un second protocole, RTCP (Real-Time Control Protocol)

13.4.1 Principes et caractéristiques de RTP / RTCP



Slide 13.20
Principes et caractéristiques de RTP / RTCP

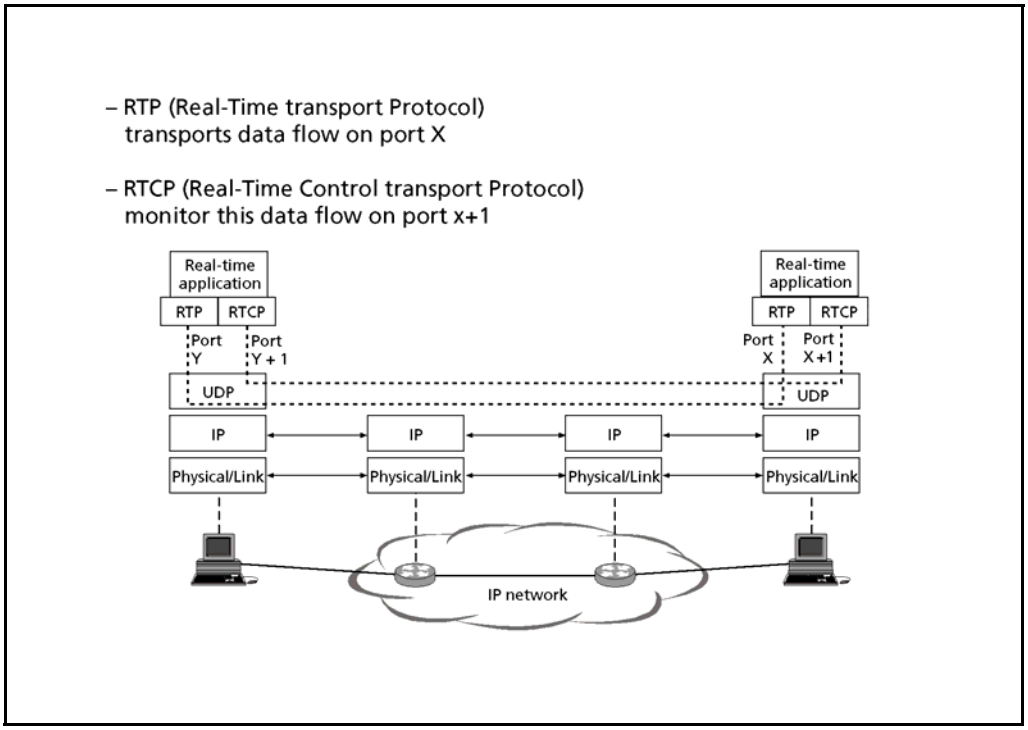
Le protocole RTP a été développé pour assurer un service bout-en-bout de remise de données en restituant leurs propriétés temporelles. Bien qu'il utilise généralement les services de UDP, il peut fonctionnner sur d'autres protocoles, orientés connexion ou sans connexion.

RTP met en œuvre un mécanisme d'horodatage et de numérotation qui permettent, de restituer le synchronisme, de remettre les paquets en séquence et d'identifier leur perte.

RTCP (Real Time Control Protocol)

RTP est associé au protocole RTCP (Real Time Control Protocol) qui prend en charge la surveillance de la qualité de service et transporte périodiquement des informations complémentaires liées aux participants d'une session en cours.

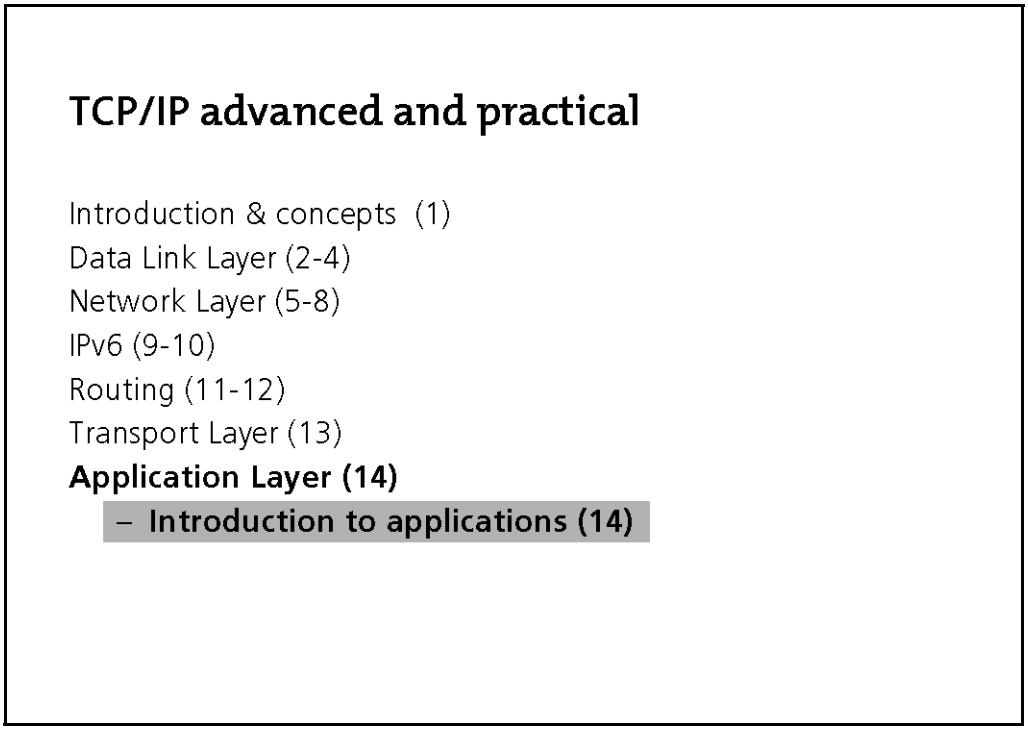
13.4.2 Architecture RTP / RTCP



Slide 13.21
Architecture RTP / RTCP

Lors du transport de données RTP dans des datagrammes UDP, les données liées à une application et les données de contrôle RTCP utilisent deux ports consécutifs (X et X+1); le premier (X) étant toujours attribué à RTP et le second à RTCP.

14 Introduction dans les applications



Slide 14.1
Introduction dans les applications

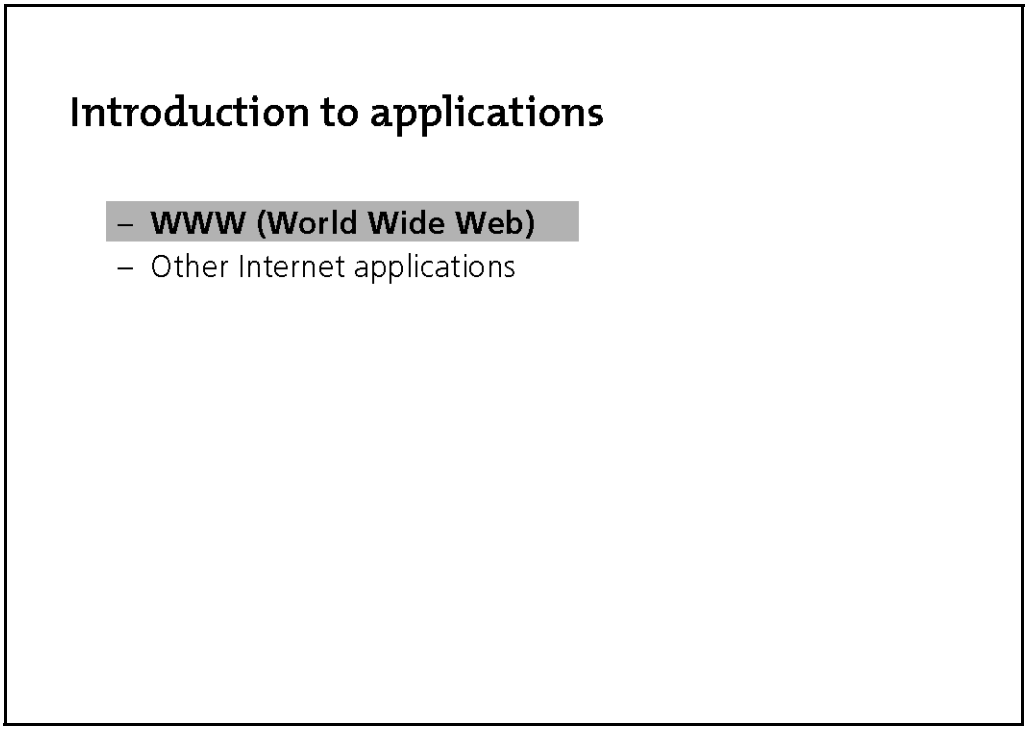
En premier lieu, ce chapitre présente succintement les trois piliers sur lesquels repose le "Web", le protocole HTTP, le langage de description de page HTML, ainsi que le principe d'adressage URL.

Dans un deuxième temps, un aperçu des protocoles d'application "historiques" de l'Internet est effectué.

Objectifs

A l'issue de ce chapitre, les participants sont capables de nommer les différents protocoles d'application disponibles dans l'Internet, de différencier leurs fonctions et leur domaine d'utilisation.

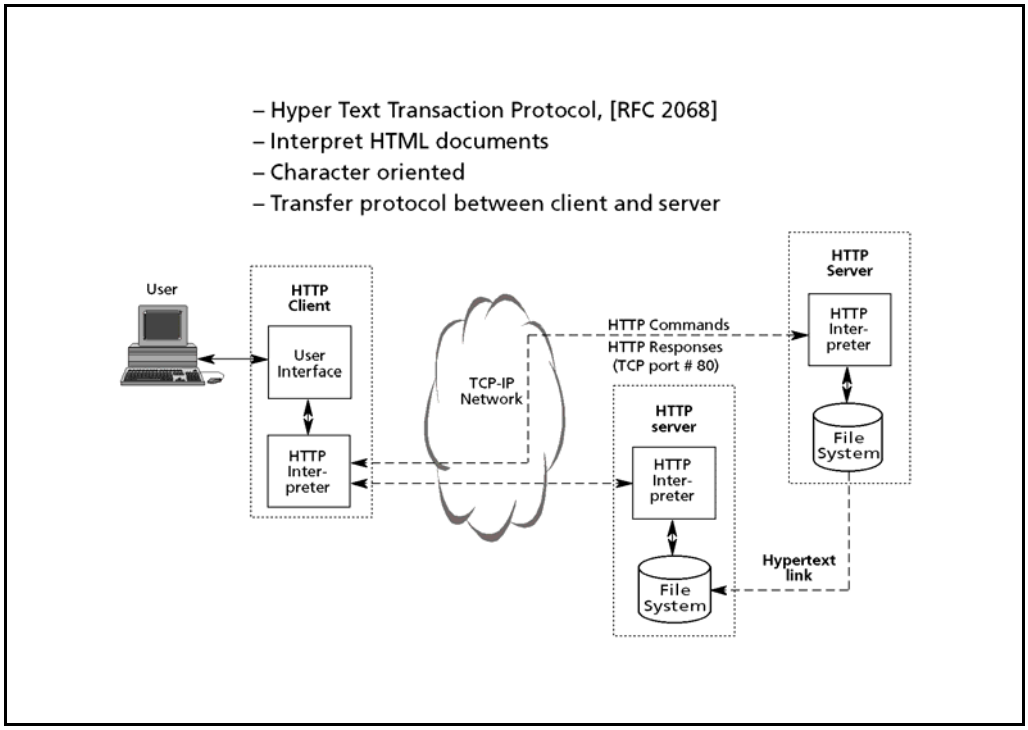
14.1 World Wide Web



Slide 14.2
World Wide Web

Le World Wide Web (WWW) n'est pas un nom équivalent à Internet. Internet est le nom donné au réseau global, WWW n'est qu'un de ses services.

14.1.1 HTTP (HyperText Transaction Protocol)



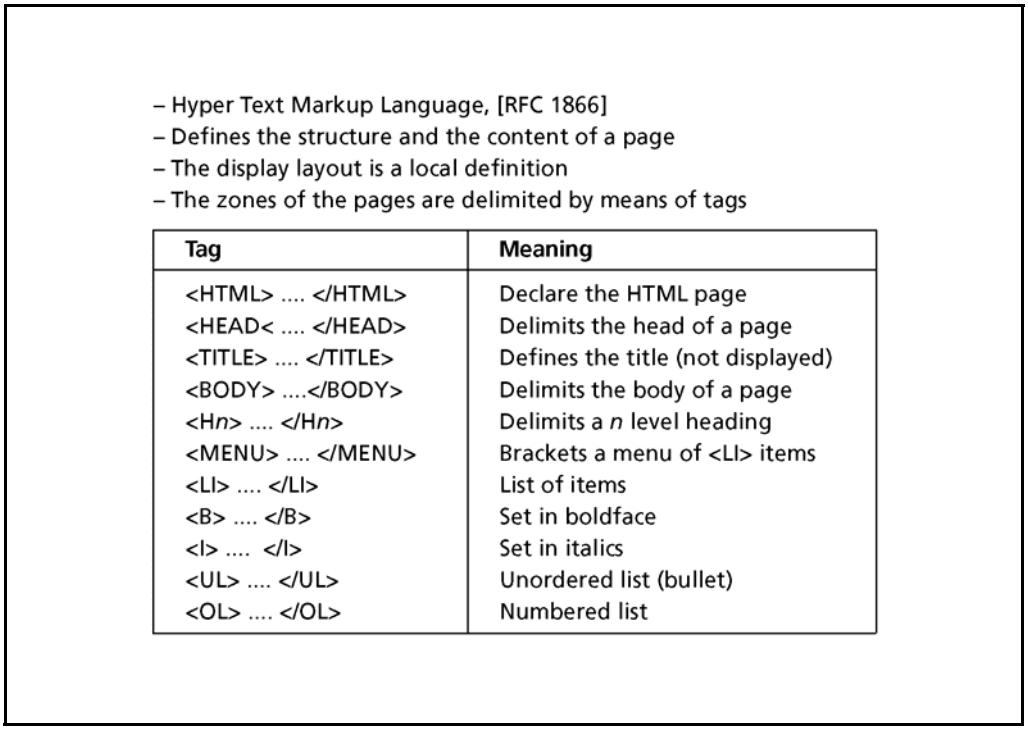
Slide 14.3
HTTP (HyperText Transaction Protocol)

HTTP est le premier des trois piliers du WWW. Ce protocole d'application permet l'échange de fichiers spécifiques, tels que les fichiers HTML.

Il fonctionne au-dessus de TCP, où il utilise le port 80. Une connection est ouverte du client vers le serveur, elle permet de passer les commandes ainsi que la page web désirée.

Cette page web peut contenir des éléments qui seront téléchargés, à l'aide de HTTP, dans des connections TCP séparées. Ces éléments peuvent d'ailleurs se trouver sur un autre serveur, ailleurs dans le monde.

14.1.2 HTML (HyperText Markup Language)



Slide 14.4
HTML (HyperText Markup Language)

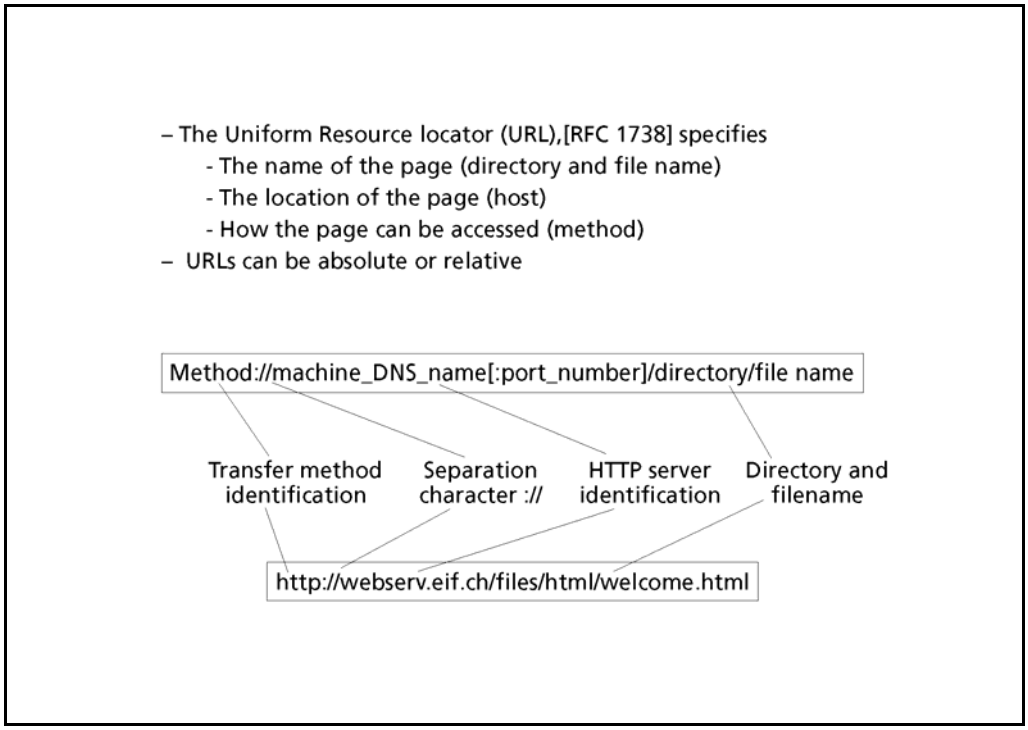
HTML signifie Hyper Text Markup Language. Il s'agit d'un langage de description de page.

Le texte est transmis en mode caractère, sans spécifications particulières. Les principales grandeurs y relatives sont alors passées comme paramètres, à l'aide de "tag".

Notre "browser" Internet affiche alors ces caractères en tenant compte de la police, couleur, taille, aspect, etc. Il faut toutefois remarquer que les paramètres d'affichage peuvent être différent d'un PC à l'autre, modifiant alors l'aspect de la page une fois affichée.

Cette méthode de travail, qui minimise la taille du fichier à transmettre, nécessitera toutefois quelques ressources processeur pour son affichage.

14.1.3 URL (Uniform Ressource Locator)



Slide 14.5
URL (Uniform Ressource Locator)

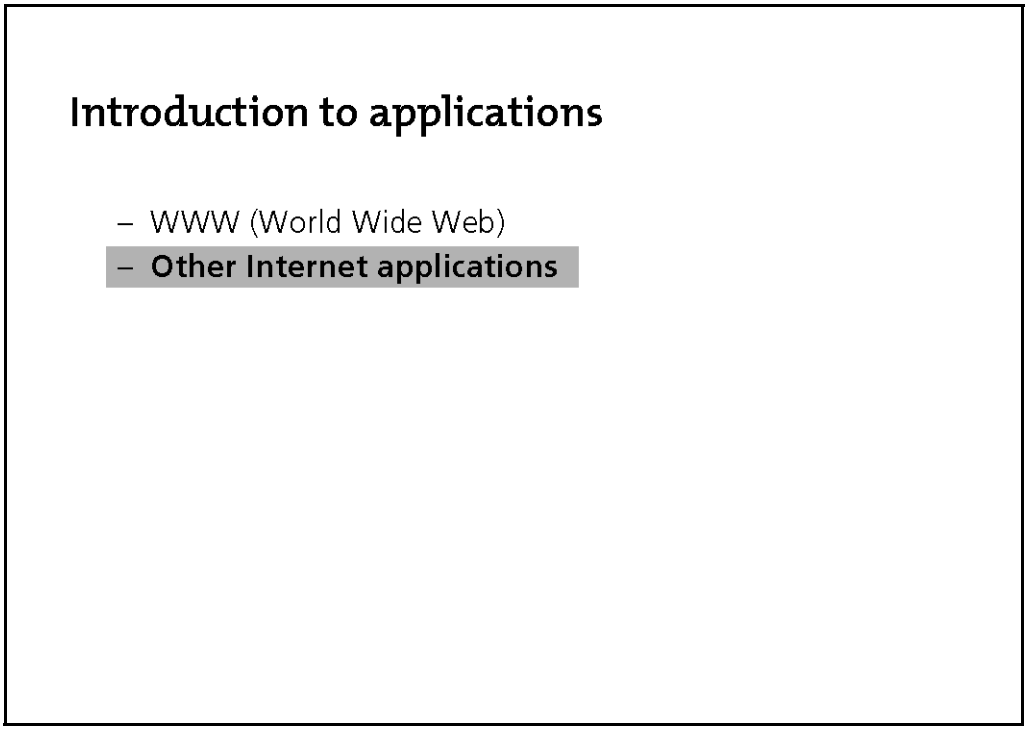
Uniform Ressource Locator (URL) est la méthode d'adressage d'un fichier dans l'Internet.

On commence par donner le type de méthode utilisée, la plupart du temps HTTP (http://), ensuite vient le nom DNS complet de la machine (nom + domaines : www.swisscom.com) et, enfin, le nom du fichier avec son chemin d'accès complet (/combox/login.htm).

Le nom du fichier peut être omis, on chargera alors une page par défaut paramétrée dans le serveur. C'est le cas des pages d'acceuil de tous les sites web.

Ces URL's ne sont pas seulement utilisés dans la barre d'adresse de notre browser, mais également dans les descriptions de page HTML, derrière chaque lien hypertexte.

14.2 Autres applications Internet

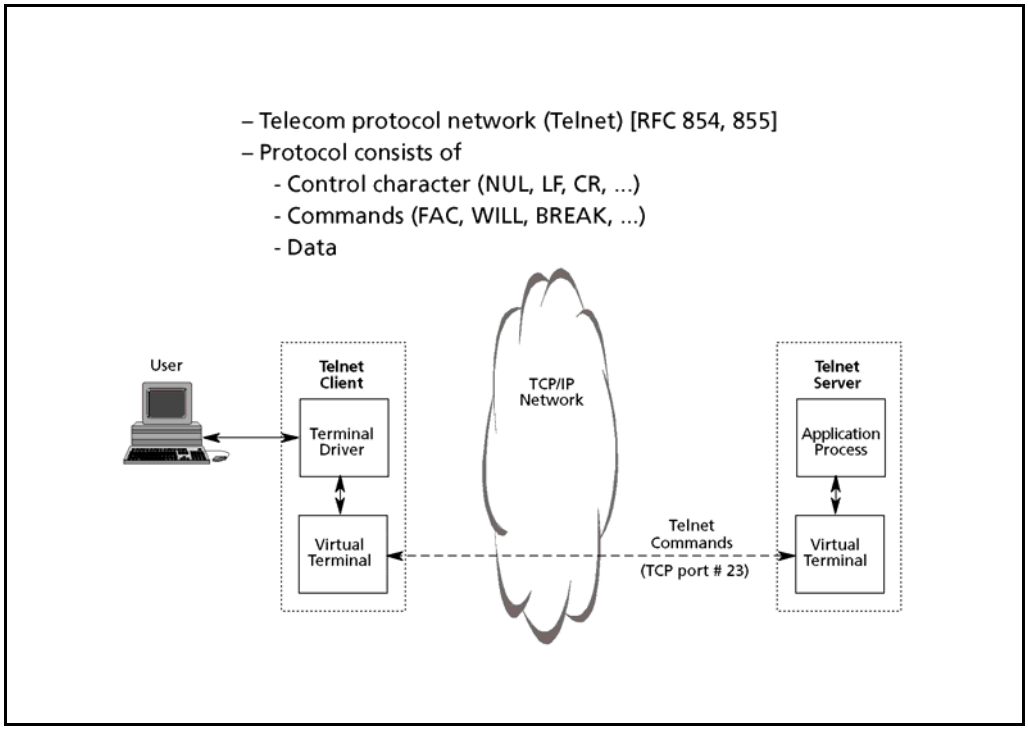


Slide 14.6
Autres applications Internet

Si le World Wide Web est une application Internet récente, Ce réseau existe depuis bien plus longtemps.

On utilisait alors diverses applications qui sont toujours utilisées aujourd'hui.

14.2.1 Telnet : Terminal virtuel



Slide 14.7
Telnet : Terminal virtuel

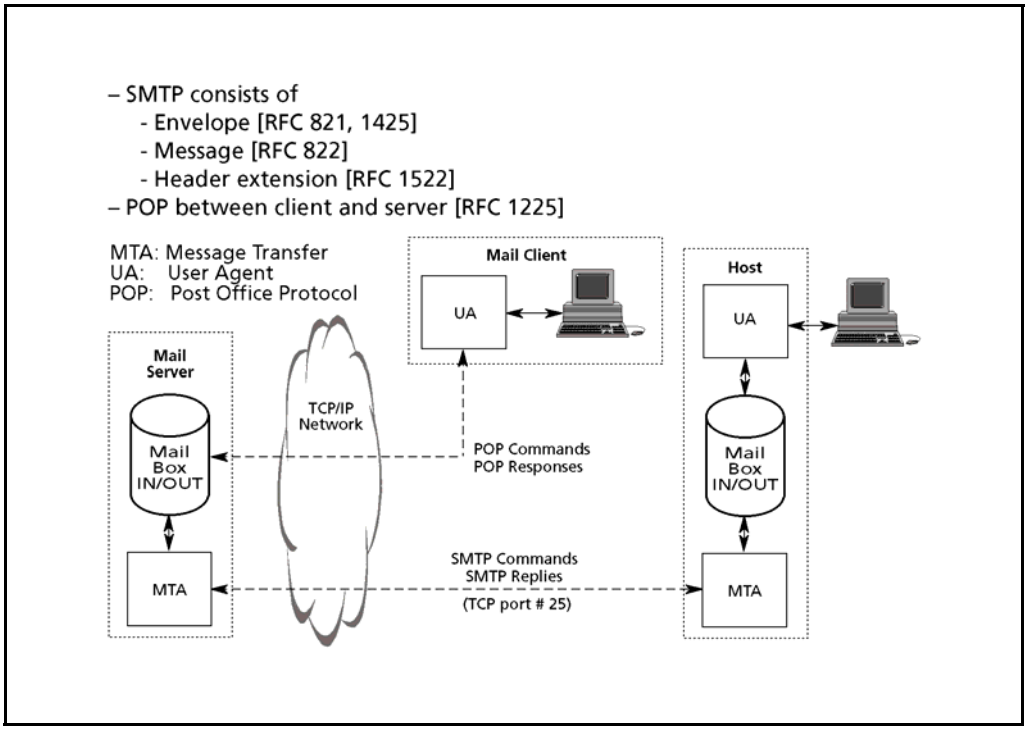
Telnet est typiquement une application utilisée dans l'Internet par les personnes qui entretiennent les éléments de ce réseau, mais qui paraît incompréhensible pour les utilisateurs du web.

Nous avons ici une application de terminal virtuel, cela signifie que nous utilisons le réseau Internet pour relier une machine distante (processeur, mémoires) sur un terminal local. On peut imager en disant que le réseau nous sert de câble écran et de câble clavier. Toutes les opérations saisies au clavier sont envoyées à l'équipement distant, traitées là-bas est nous sont renvoyées pour affichage.

Les environnements Unix utilisent un terminal virtuel appelé "rlogin", qui est une utilisation propre de Telnet.

l'équipement distant fait office de "serveur" Telnet, notre PC est le client. Nous sommes reliés au dessus d'une connexion TCP, établie sur le port 23.

14.2.2 SMTP (Simple Mail Transfer Protocol)



Slide 14.8
SMTP (Simple Mail Transfer Protocol)

SMTP est le protocole de messagerie électronique utilisé dans l'Internet. Ce n'est pas une composante du WWW, mais bien une application séparée.

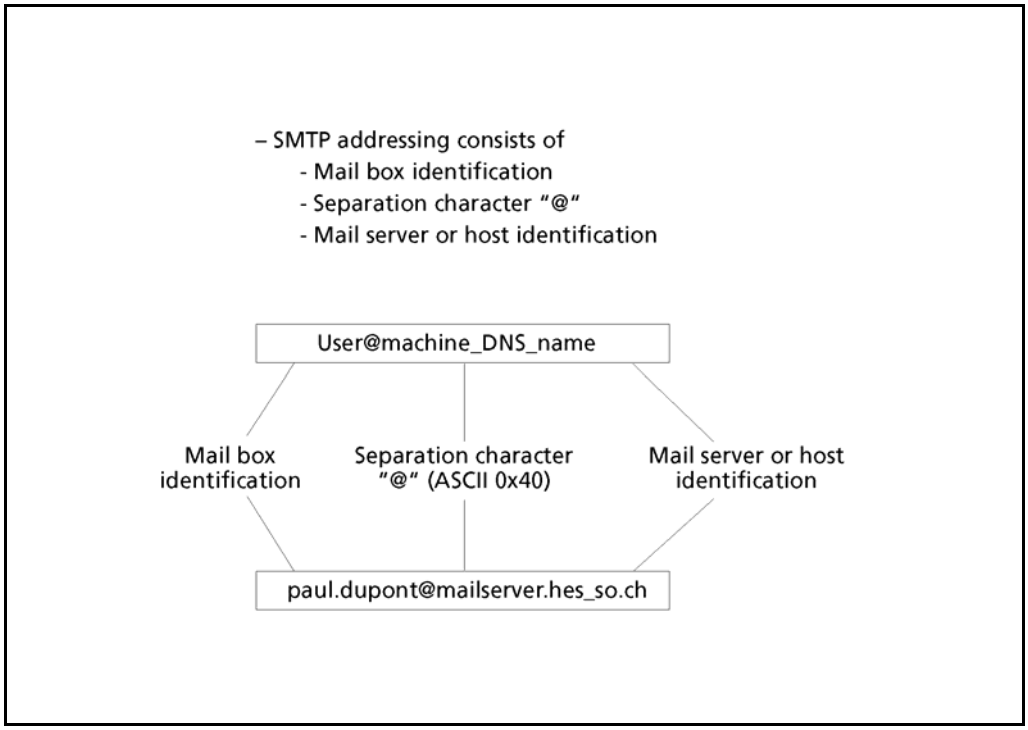
Lorsque nous envoyons un message électronique, nous envoyons des commandes d'édition de message à notre serveur mail local à l'aide d'un protocole de messagerie particulier, le protocole de bureau de poste (POP : Post Office Protocol).

Notre serveur de messagerie va alors transférer notre courrier au serveur de destination, à travers l'Internet, à l'aide du protocole de messagerie SMTP. Il devrait conserver ce protocole pour transmettre ce message au destinataire final.

A noter que plusieurs protocoles de messagerie "propriétaires" peuvent être utilisés entre le client est son serveur (Exchange, par ex.).

SMTP utilise une connexion TCP sur le port 25.

14.2.3 Adressage SMTP



Slide 14.9
Adressage SMTP

Lorsque nous tapons une adresse e-mail, nous donnons deux informations essentielles:

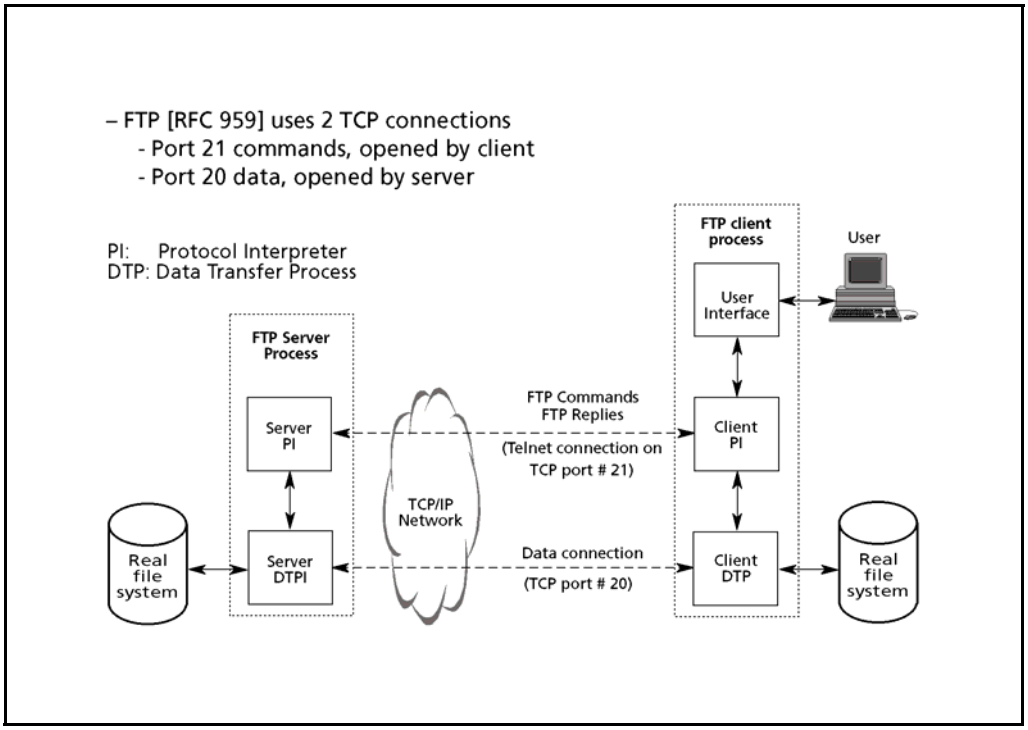
- Le nom de la boîte aux lettres du serveur de destination
- le nom du serveur de destination

Ces deux informations sont séparées par le caractère "@".

La deuxième partie de l'adresse n'est en fait que le nom DNS d'une machine. Notons toutefois que, la plupart du temps, il s'agit d'une machine sans nom, qui répond directement au nom de domaine.

La première partie de l'adresse n'est qu'une chaîne de caractère, qui identifie l'utilisateur final de cette adresse de messagerie. La présence de points de séparation, utilisés par "habitude" dans les syntaxes Internet, n'a ici aucune importance du point de vue hiérarchique.

14.2.4 FTP (File Transfer Protocol)



Slide 14.10
FTP (File Transfer Protocol)

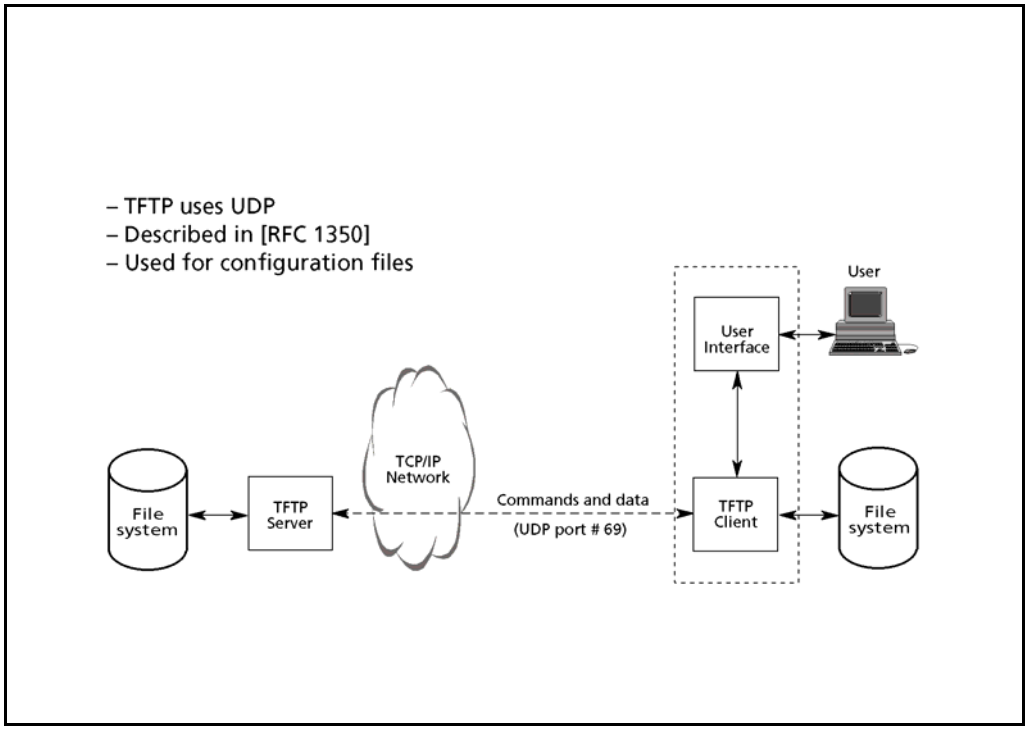
L'application de transfert de fichier FTP repose sur une structuer client / serveur.

Elle possède toutefois une particularité importante. Le client ouvre une connection TCP sur le port 21 en direction du serveur. Une fois cette connection établie, le client peut envoyer des commandes au serveur, comme l'affichage du répertoire, le changement de répertoire, etc...

Au moment de l'envoi d'une commande de "download", le serveur ouvre lui-même une seconde connection TCP en direction du client, sur le port 20. Le transfert effectif des données est réalisé sur cette deuxième connexion.

La première connection est toujours disponible pour passer d'autres commandes. En cas de nouvelle demande de download, notre serveur va à nouveau ouvrir une connection TCP, et ceci pour chaque fichier séparément.

14.2.5 TFTP (Trivial File Transfer Protocol)



Slide 14.11
TFTP (Trivial File Transfer Protocol)

TFTP est une application qui repose sur le protocole UDP.

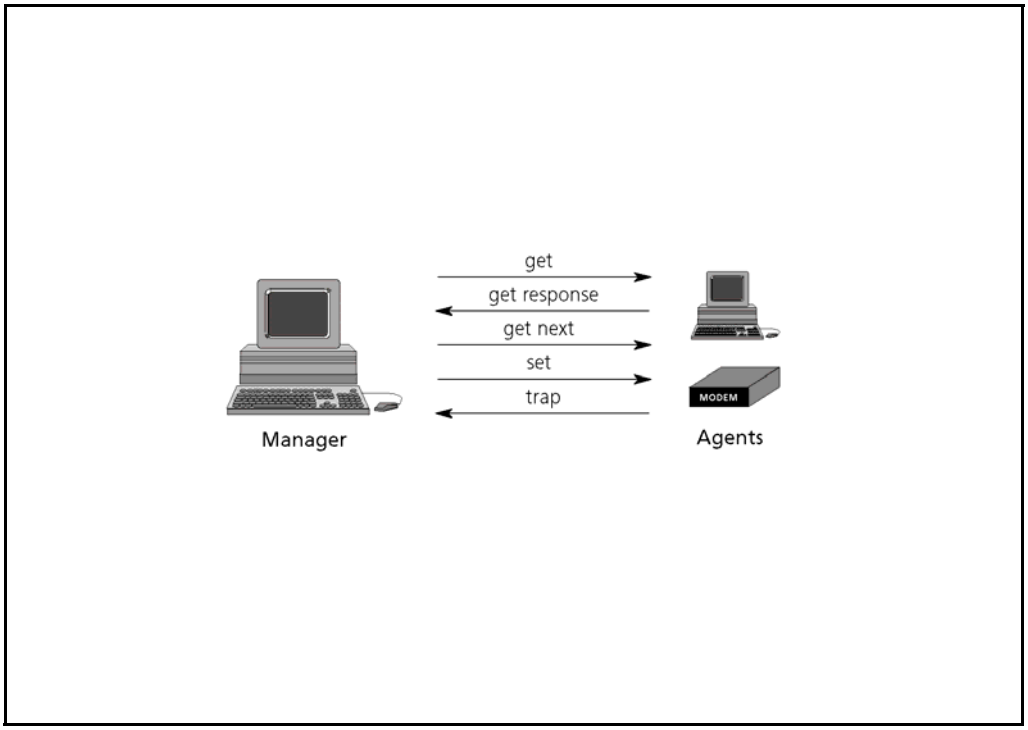
La couche transport n'offrant pas la qualité de service recquise pour un transfert des données fiable, c'est notre application qui va se charger du contrôle de qualité.

TFTP est utilisé généralement pour la descente de fichiers de configuration entre les équipements du réseau est un serveur de sauvegarde.

Ces fichiers sont généralement de taille modeste et les machines les utilisant n'ont pas forcément les ressources pour mettre en place une surveIllance de machine TCP.

Chez nous TFTP est principalement utilisé pour les sauvegardes de configuration des routeurs du réseau.

14.2.6 SNMP (Simple Network Management Protocol)



Slide 14.12
SNMP (Simple Network Mgmt Protocol)

Le protocolle SNMP sert, comme son nom l'indique, de système de management. Il doit permettre de lire et de paramétrer les plus importants paramétres clients depuis le manager.

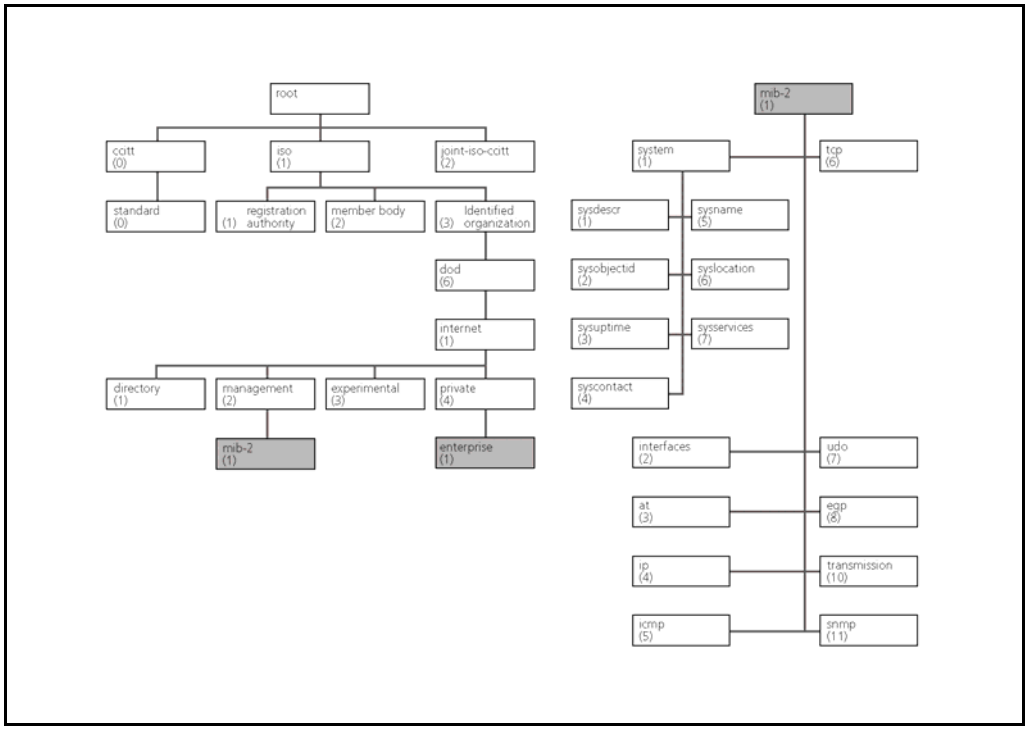
Il est construit de manière simple

SNMP est utilisé principalement dans la gestion de réseaux.

Les prétendus systèmes "Enterprise Management - Tools" comme par ex. Tivoli, Unicenter TNG ou Netview peuvent lire et gérer les paramètres réseaux (IP Pakkets in / IP-Packets out, Sytsem-name, System-Responsible, etc.). En outre, ils peuvent également modifier les paramètres systèmes tels que les capacités de disques, la charge du CPU, etc.

SNMP est défini dans les RFC's indiquées ci-dessus. Nous pouvons dire que les versions 1 et 2 sont, en ce moment, toujours utilisées. Celles-ci ne sont pas bien protégées contre les manipulations des hackers. Dans la prochaine version (v3), il sera possible de crypter les données et de véritablement protéger ses accès. En ce moment est utilisé seulement une identification IP, associée à un "Community-word" pour la vérification de l'utilisateur.

SNMP (Simple Network Management Protocol) (2)



Slide 14.13
SNMP (Simple Network Mgmt Protocol) (2)

Le "Simple" Network Management Protocol est une application normale qui utilise les ports 161 et 162 de UDP.

Des messages courts et simples seront transmis, avec les paramètres correspondants. Ceux-ci seront ensuite introduits, sous forme texte (par ex. Oid's = Object ID's), dans la structure de la "Management Information Base Version 2" (MIB II) ou dans une structure propriétaire (Private - MIB). La requête ou le paramètrage se fera de manière numérique.

Exemple :

snmp > SET -ipaddress 172.16.191.21 -community admin -oid 1.3.6.1.2.1.1.5 text=Mysystem

Une telle commande serait, par exemple, le paramètrage du nom du système sur la machine correspondante.

15 Pratique PC

Objectif

Les principaux protocoles utilisés dans l'Internet seront étudiés dans le cadre du réseau installé dans notre salle de cours.

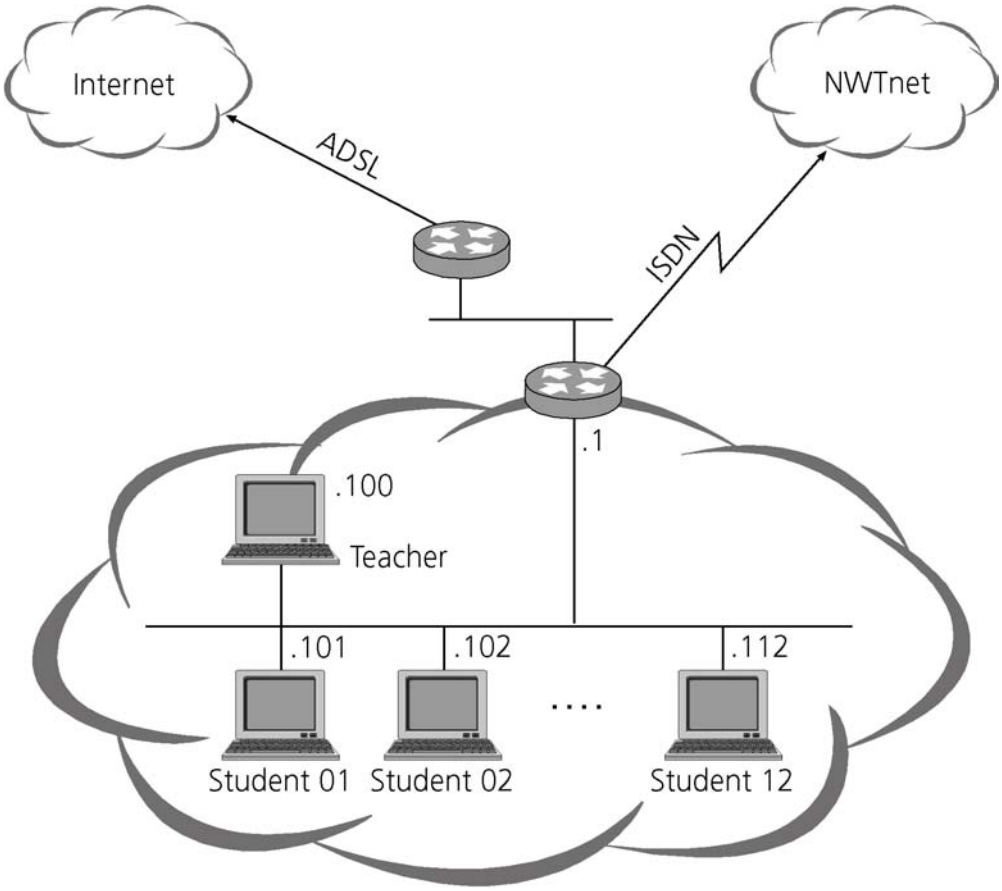
Le trafic de notre réseau sera capturé à l'aide d'un logiciel d'analyse de protocole et, ensuite, analysé par les participants.

15.0.1 Structure du réseau

Stack de protocole ARPA

L'objectif de ce travail pratique est l'analyse des dialogues entre client du réseau, ainsi que des contenus des principaux protocoles utilisés dans le stack ARPA (Ethernet, ARP, IP, ICMP, DNS).

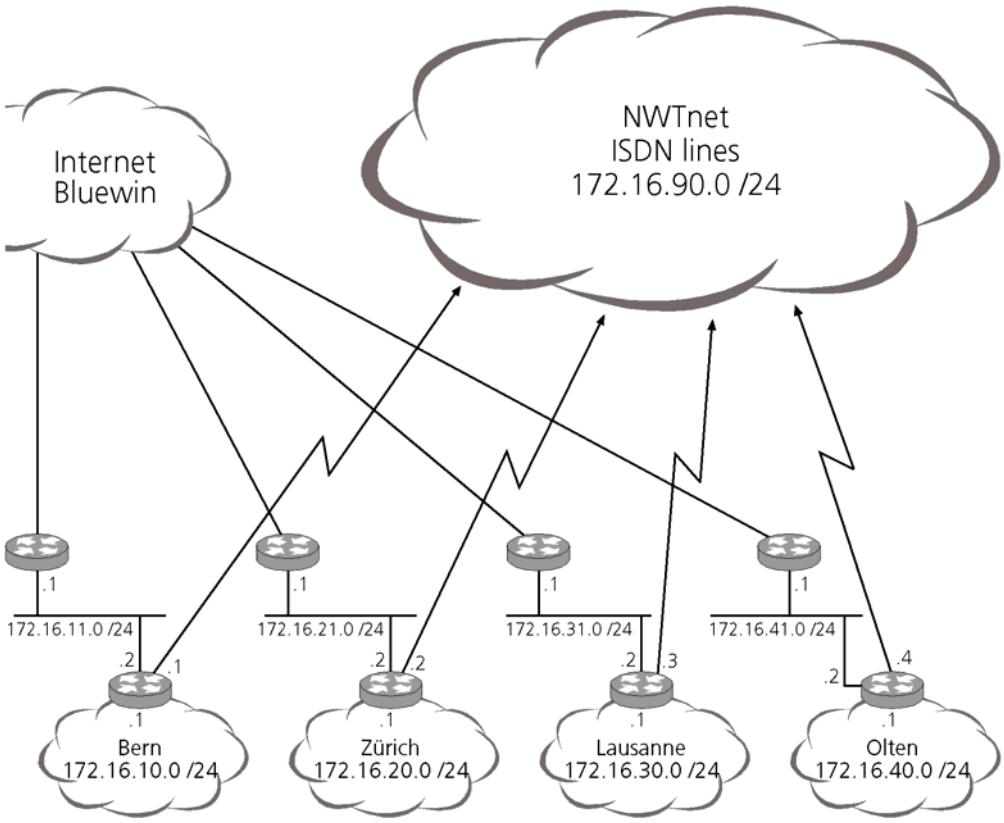
Figure 15.1
Réseau pour l'analyse TCP/IP



15.0.2 Structure générale du réseau

La figure suivante montre le plan d'adressage complet du NWTnet.

Figure 15.2
Structure générale du réseau



15.1 Analyse de l'environnement

Chaque PC du laboratoire est connecté au même segment logique que les autres. Chaque place de travail possède sa propre configuration IP, ainsi qu'un certain nombre d'outils réseaux. Certains permettent de visualiser de données réseau, d'autres effectuent des petits tests liés à son fonctionnement. Dans cette partie, nous essayerons les outils proposés et étudierons l'environnement dans lequel nous nous trouvons.

15.1.1 Configuration du PC

Les différents paramètres de configuration du PC seront livrés, en fonction du système d'exploitation, par une des commandes suivantes :

- Winipcfg (Start → Run. . . → 'winipcfg')
- IPconfig (Start → Run. . . → 'ipconfig')
- ou, sous DOS " ipconfig /all "

Relever les paramètres de configuration suivants, relatifs à la carte réseau Ethernet.

1. Quelle est l'adresse IP de notre PC ?

   . . . . . .

2. Quelle est l'adresse IP du routeur par défaut (default Gateway) ?

   . . . . . .

3. Quel est le masque de notre sous-réseau ?

   . . . . . .

4. Quel est l'adresse MAC (hardware) de notre PC ?

   . . . . . .

5. Quel nom logique possède le PC (Host Name) ?

   . . . . . .

6. Quelles sont les adresses des serveurs DNS ?

   . . . . . .

   . . . . . .

7. Y-a-t'il d'autres paramètres de configuration liés à cette carte réseau ?

   . . . . . .

   . . . . . .

   . . . . . .

15.1.2 Analyse du Réseau

1. Dans quelle classe d'adresse se trouve notre réseau ?

   . . . . . .
   . . . . . .

2. Quelle est l'adresse du sous-réseau sur lequel notre PC est raccordé ?

   . . . . . .
   . . . . . .

3. Quelle est la plage d'adresses de ce sous-réseau ?

   . . . . . .
   . . . . . .

4. Quelle est la valeur de notre adresse de diffusion ?

   . . . . . .
   . . . . . .

5. Combien d'adresses sont disponibles pour adresser des PC ?

   . . . . . .
   . . . . . .

15.1.3 Applications DOS

1. Ouvrir une fenêtre DOS (Start → Run. . . → "Command"→ OK).
   Introduire la commande «**ping** (IP-Adresse Gateway)»
   Quel est la fonction de cette commande ?

   . . . . . .
   . . . . . .

2. Le paramètre -a indique que le nom logique de la machine doit être résolu. Introduisez la commande «**ping –a** 130.59.10.30». Quel est le nom de cette machine ?

   . . . . . .
   . . . . . .

3. Faites un «ping» sur la même machine, en donnant son nom logique en paramètre.
   Le résultat est-il différent ?

   . . . . . .
   . . . . . .

4. Faites un «ping» sur l'adresse 130.59.10.30 en fixant le TTL à 3 . Que se passe t'il ?

   . . . . . .
   . . . . . .

5. Introduire la commande «**tracert** 130.59.10.30».
   Quelle est la fonction de cette commande ?

   . . . . . .
   . . . . . .

15.2 Analyse de protocole

15.2.1 ARP et DNS

1. Avant de démarrer la mesure, effacer la table de correspondance arp à l'aide de la commande « arp -d ».
2. Démarrer le FLUKE Protokoll Inspector sur le premier PC
3. Paramétrer-le comme décrit dans l'annexe 19.1.
4. Ouvrez une fenêtre DOS sur l'autre PC (Start → Run. . .→"Command"→OK).
5. Démarrer la capture comme décrit dans l'annexe 19.2.
6. Donner cette commande DOS : "ping www.experteach.ch"
7. Arrêter la capture et étudier les trames émises et reçues par notre PC.

Consignes

1. Comment le protocole ARP est-il identifié (Type), comment est-il transporté ?

   . . . . . .

   . . . . . .

2. Quelle est l'adresse MAC que le PC essaie de résoudre en premier ?

   . . . . . .

   . . . . . .

3. Qui lui donne la réponse ?

   . . . . . .

   . . . . . .

4. Quel est l'enjeu de la requête DNS ? Qui répond ?

   . . . . . .

   . . . . . .

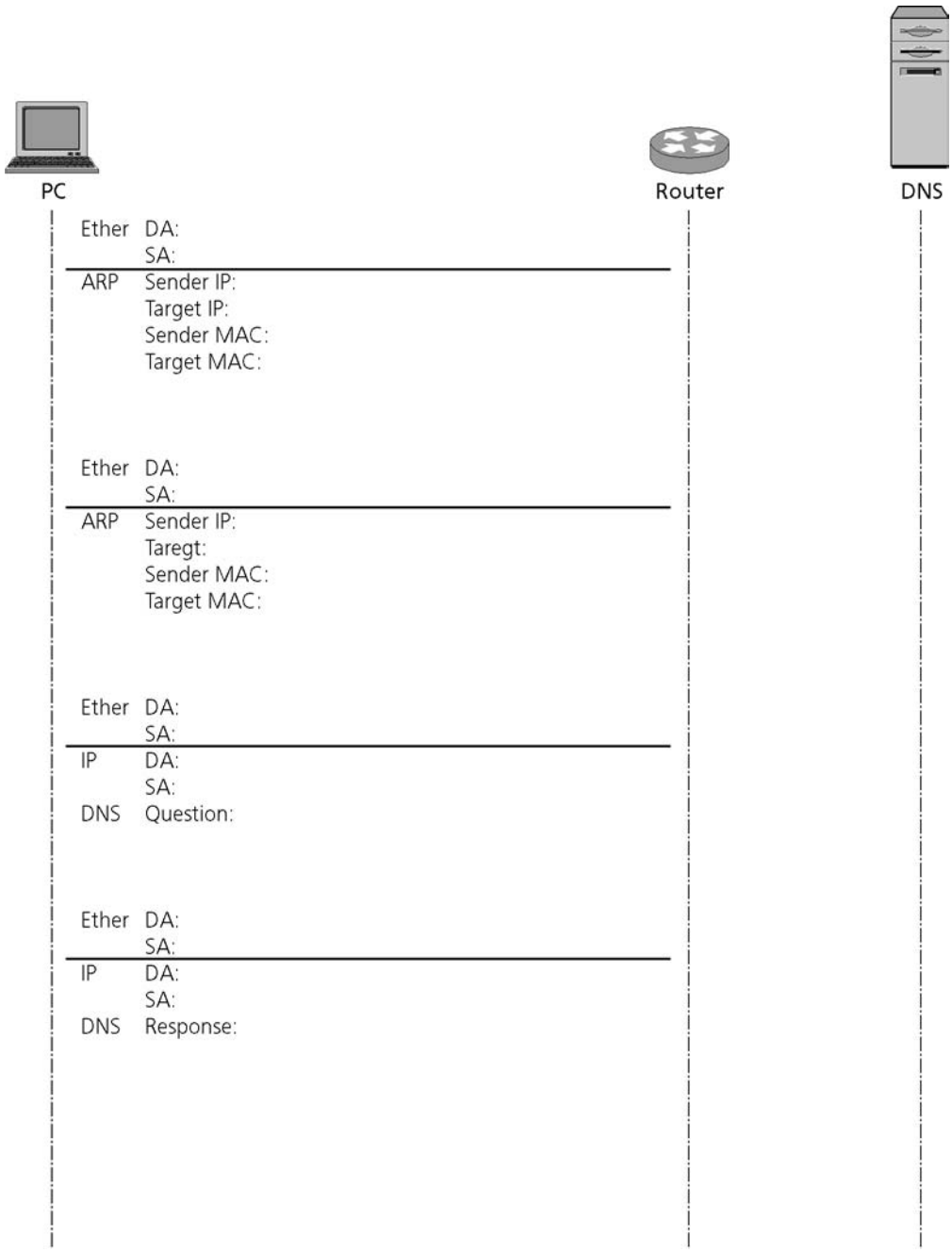
5. Donner la commande DOS "arp -a". Commentaires ?

   . . . . . .

   . . . . . .

6. Dessiner, dans le diagramme suivant, l'échange des informations, en dessinant les pointes de flèches indiquant les directions des trames. Notez ensuite les paramètres intéressants générés par notre commande ping. On trouve 3 sessions distinctes : ARP, DNS, (ICMP).

Figure 15.3
Diagramme en flèche pour ARP et DNS



15.2.2 ICMP : Ping

1. Démarrer une capture.
2. Donner la commande "ping <Adresse IP du Routeur>".
3. Arrêter la capture.

Questions

1. Quel protocolle est nécessaire pour la réalisation des demandes d'echos ?

   . . . . . .

   . . . . . .

2. Comment ce protocole est-il identifié ?

   . . . . . .

   . . . . . .

3. Que peut-on dire de la couche transport ?

   . . . . . .

   . . . . . .

4. Analysez les adresses MAC et IP de notre échange ICMP et complétez le diagramme ci-dessous.

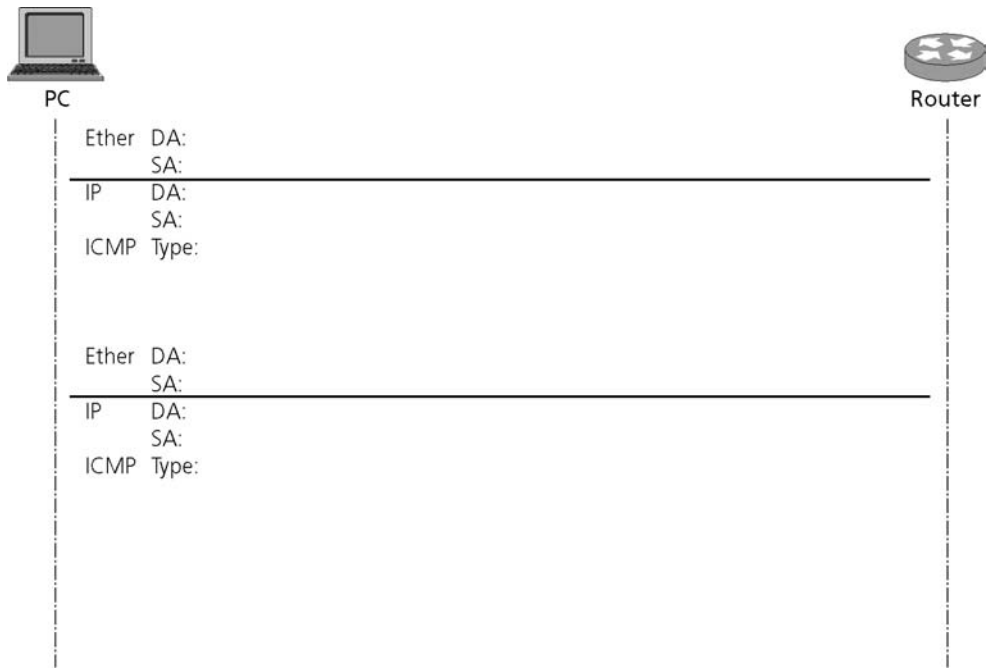


Figure 15.4 Diagramme pour ICMP

15.2.3 ICMP : Traceroute

1. Ouvrir une fenêtre DOS (Start → Run. . →"Command"→OK)
2. Démarrer une capture.
3. Donner la commande "tracert 130.59.10.30".
4. Arrêter la capture.

Questions

1. Quels sont les protocolles utilisés pour effectuer cette fonction ?

   . . . . . .

   . . . . . .

2. Quel champ de l'entête IP est-il important pour réaliser cette fonction ? Pourquoi ?

   . . . . . .

   . . . . . .

   . . . . . .

   . . . . . .

3. Comment est résolu le nom logique de chaque routeur traversé ?

   . . . . . .

   . . . . . .

   . . . . . .

15.2.4 Fragmentation IP

1. Chercher, à l'aide de la documentation disponible dans l'annexe 19.6, le paramètre de la fonction "ping" qui permet de fixer la longueur des données transmises.
2. Démarrer la capture.
3. Envoyer au routeur un ping contenant 3 000 octets.
4. Arrêter la capture.

Questions

1. Combien de paquets IP ont été nécessaires pour la transmission de ce message ?

   . . . . . .

   . . . . . .

2. Quelle est la taille maximale de données que peut transporter une trame Ethernet ?

   . . . . . .

   . . . . . .

3. Analysez la fragmentation du paquet IP.

   . . . . . .

   . . . . . .

   . . . . . .

15.2.5 Connexion et déconnexion TCP

1. Démarrer la capture.
2. Donner la commande "telnet <adresse IP du routeur>"
3. Frapper plusieurs fois (3-4) "Enter" en guise de mot de passe, jusqu'à ce que la liaison soit interrompue.
4. Arrêter la capture

Questions

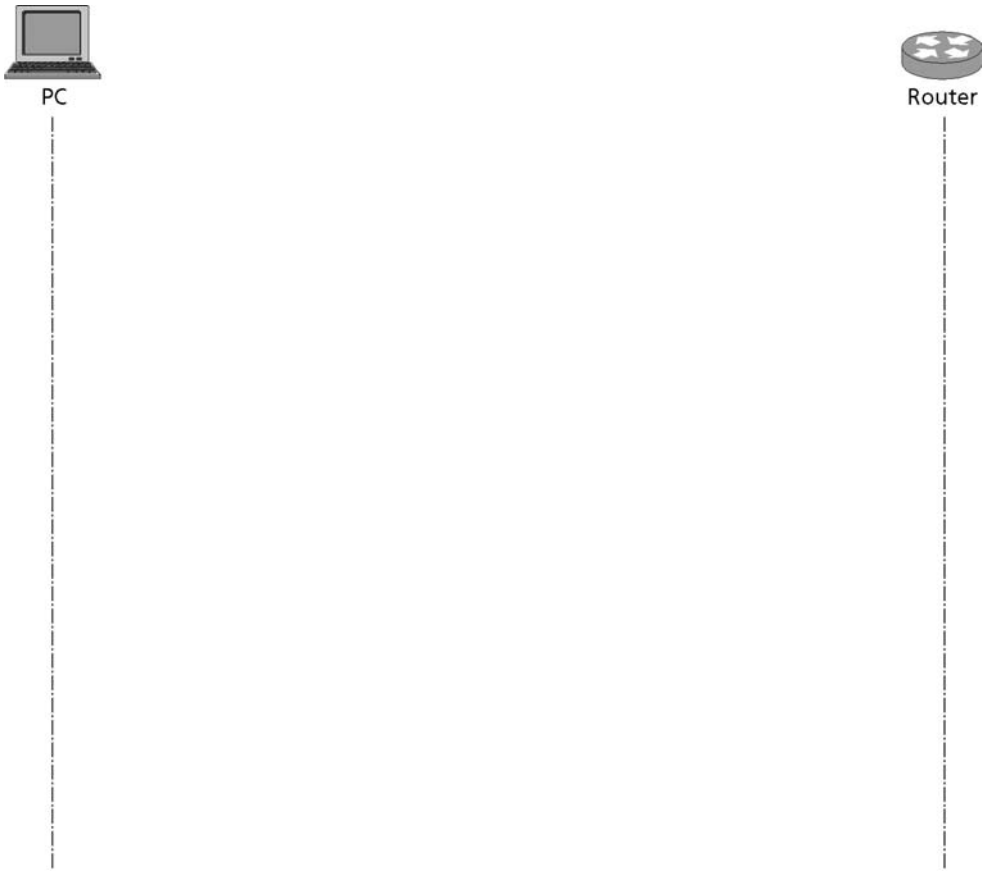
1. Comment le protocole TCP est-il identifié ?

   . . . . . .

   . . . . . .

2. Analyser le rôle des indicateurs (Flags) SYN, FIN et ACK, ainsi que des champs Sequence et Acknowledgment number. Visualiser ces grandeurs en dessinant la connexion TCP, dans le diagramme en flèche ci-dessous.

Figure 15.5
Diagramme pour connexion TCP



3. A quoi sert le champ "Window" de l'entête TCP ? Quelle est son unité ?

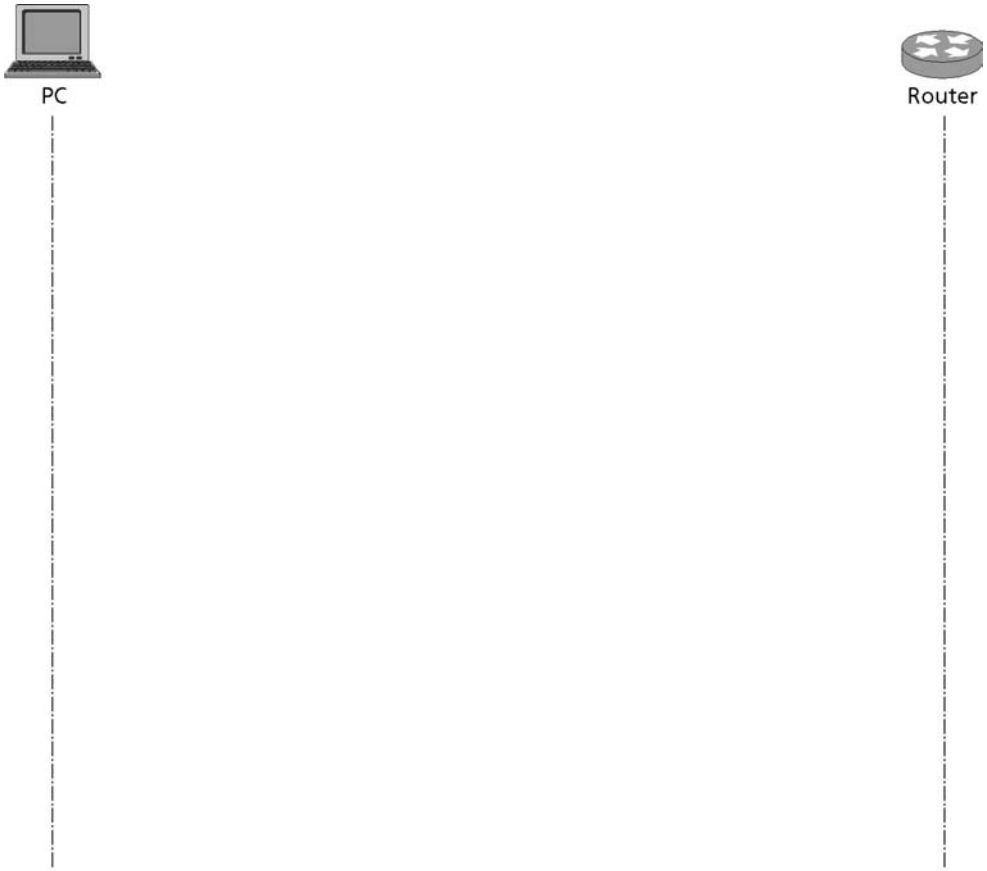
. . . . . .
. . . . . .
. . . . . .

4. Qui est à l'origine de la déconnexion TCP ?

. . . . . .
. . . . . .
. . . . . .

5. Analyser le rôle des indicateurs (Flags) SYN, FIN et ACK, dans le cas de la déconnexion TCP. Représenter cette déconnexion dans le diagramme en flèche ci-dessous.

Figure 15.6
Diagramme pour TCP



16 Pratique Réseau

Objectif

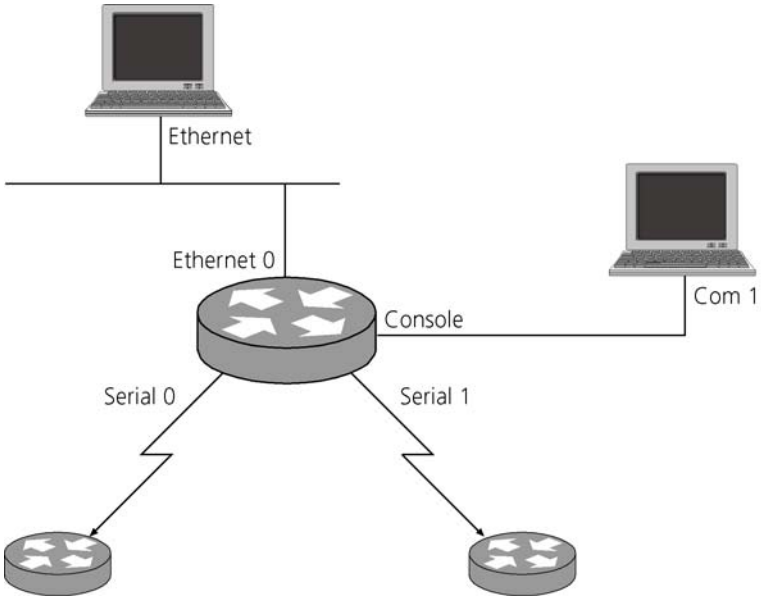
Un réseau simple avec trois routeurs sera tout d'abord construit. A l'aide de ce réseau, les participants pourront tester et comparer les diverses technologies du "Routing".

En outre, nous essayerons, au travers d'une translation d'adresse, de connecter notre réseau à l'Internet.

16.0.1 Structure du réseau par table

Sur chacune de ces tables on trouve deux PC, dont le premier sera relié au réseau Ethernet. Le second ne servira qu'au paramétrage de notre routeur, au travers de son port série.

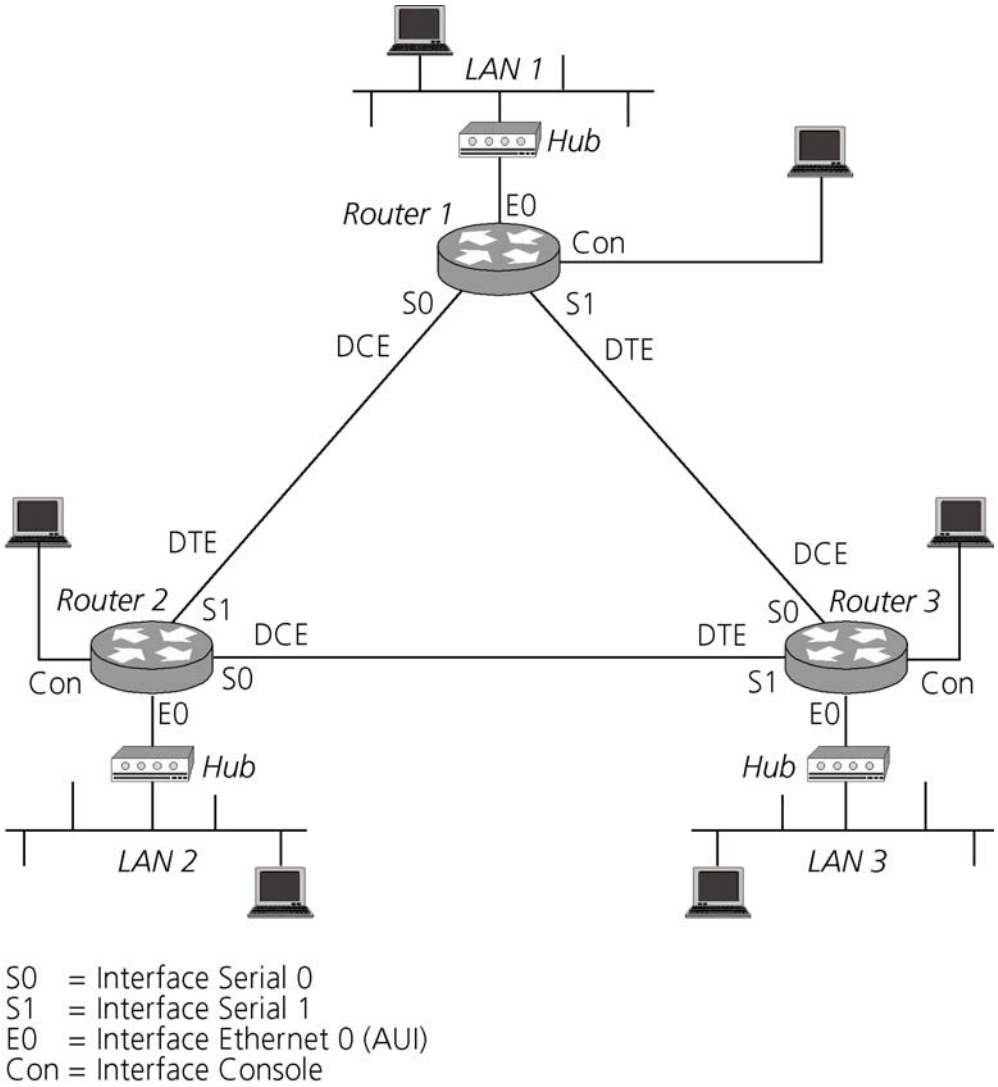
Figure 16.1
Structure de réseau d'une table



16.0.2 Structure du réseau sur trois tables

Cablez le réseau selon le schéma ci-dessous. Il est primordial que les groupes (3 tables sur une ligne) travaillent de manière synchrone pendant tout le long de cette pratique.

Figure 16.2
Structure du réseau sur 3 tables



16.0.3 Adressage IP du réseau

1. L'adressage des sous-réseaux est représenté dans la figure 16.3

2. Le masque de sous-réseau des segments Ethernet sera 255.255.255.0, Les lignes séries possèderont le masque standard des lignes point-à-point, soit 255.255.255.252

3. Dans chaque sous-réseau Ethernet, le PC possèdera l'adresse 10.10.xx.10

4. Le routeur par défaut (default gateway) du sous-réseau aura l'adresse 10.10.xx.1

5. L'interface serial0, connectée à un câble DCE, aura l'adresse 10.10.xx.1

6. L'interface serial1, connectée à un câble DTE, aura l'adresse 10.10.xx.2

7. Compléter le tableau ci-dessous pour les routeurs avec les adresses IP et les masques de sous-réseaux associés.

Tableau 16.1 Configuration IP des routeurs

		Router1	Router2	Router3
int S0	IP Address			
	Subnet mask			
int S1	IP Address			
	Subnet mask			
int E0	IP Address			
	Subnet mask			

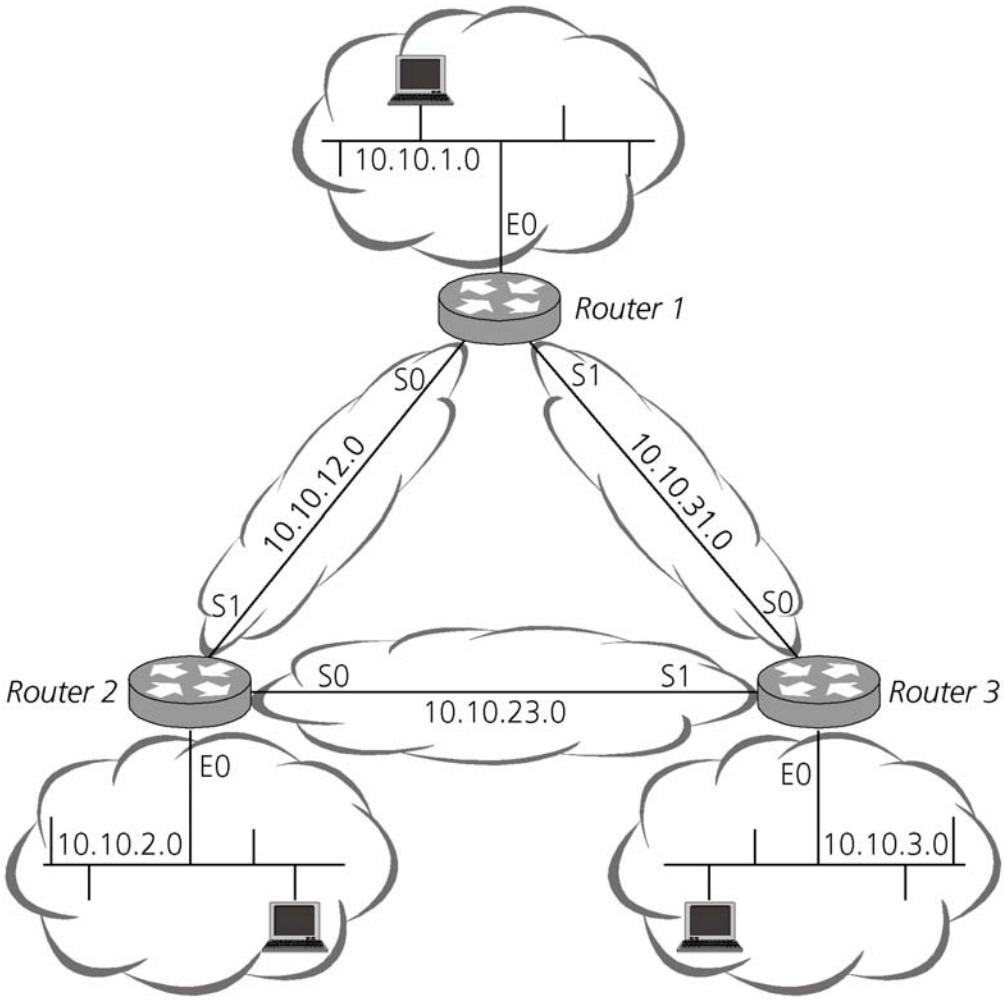
8. Compléter le tableau ci-dessous pour les PC présents dans les LAN

Tableau 16.2 Configuration IP des PC

	PC in LAN1	PC in LAN2	PC in LAN3
IP address			
Subnet mask			
Default Gateway			
DNS server	Disable DNS	Disable DNS	Disable DNS

9. Compléter le graphique ci-dessous avec les adresses IP des différents équipements

Figure 16.3
Plan d'adressage du réseau



16.1 Préparation du routeur

1. Allumez le routeur et attendez qu'il soit prêt.

2. Passez en mode privilégié

```
router>enable
router#
```

3. Renommer le routeur hostname

```
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Cisco_<Routernumber>
Cisco_1(config)#^Z    (ctrl+z)
Cisco_1#
%SYS-5-CONFIG_I: Configured from console by console
```

4. Pour un routeur Cisco 2500, les interfaces seront configurées à l'aide des commandes ci-dessous : Cisco 2500

   Remarque : Dans le cas des routeurs 2600, les interfaces seront numérotées 0/0 ou 0/1. Le premier chiffre indique le slot d'interfaces, le deuxième le n° de l'interface. Cette remarque est valable pour l'ensemble de la manipulation pratique. En cas de doute, se renseigner auprès du formateur. Cisco 2600

```
Cisco_1#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
Cisco_1(config)#interface serial 0
Cisco_1(config-if)#ip address (adresse IP) (subnet mask)
Cisco_1(config-if)#clock rate 64000
Cisco_1(config-if)#no shutdown
Cisco_1(config-if)#exit
Cisco_1(config)#interface serial 1
Cisco_1(config-if)#ip address (adresse IP) (subnet mask)
Cisco_1(config-if)#no shutdown
Cisco_1(config-if)#exit
Cisco_1(config)#interface ethernet 0
Cisco_1(config-if)#ip address (adresse IP) (subnet mask)
Cisco_1(config-if)#no shutdown
Cisco_1(config-if)#exit
Cisco_1(config)# ^Z(Ctrl+z)
Cisco_1#
%SYS-5-CONFIG_I: Configured from console by console
```

5. Les interfaces pouront ensuite être contrôlées individuellement grâce aux commandes ci-dessous :

```
Cisco_1#sh interface serial 0
```

show interface

ou

```
Cisco_1#sh interface ethernet 0
Ethernet0 is administratively down, line protocol is down
  Hardware is QUICC Ethernet, address is 0010.7bdf.32f1 (via
0010.7bdf.32f1)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load
1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 pakets/sec
  5 minute output rate 0 bits/sec, 0 pakets/sec
     0 pakets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input pakets with dribble condition detected
     0 pakets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Show interface

6. Contrôler la configuration IP de toutes les interfaces avec la commande
   `Cisco_1#show ip interface brief`

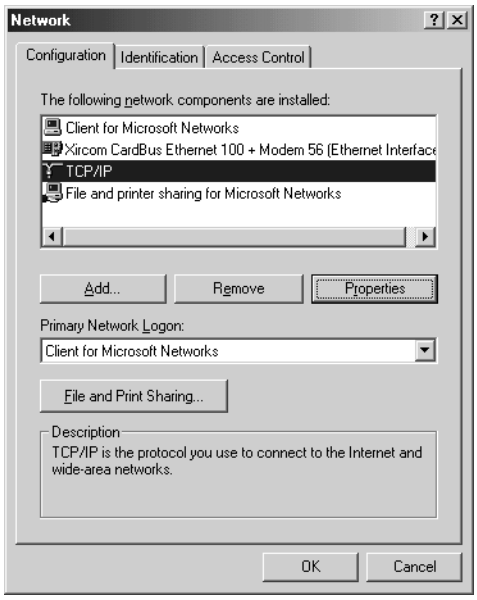
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .

16.2 Configuration du PC

Configuration du PC

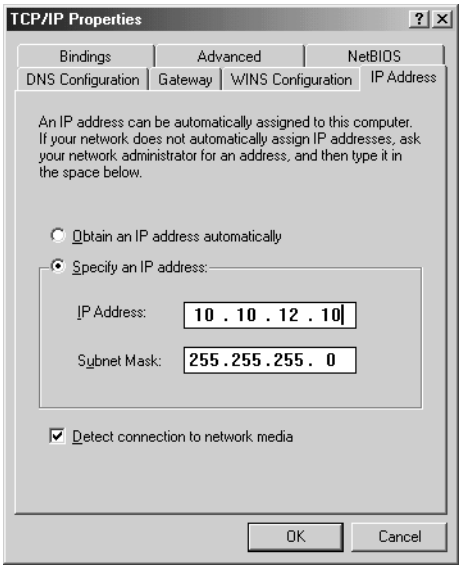
- Configurer le PC pour le nouveau sous-réseau:
- Start → settings → control panel
- Double-cliquer sur «Network»
- Choisir la configuration TCP/IP de la carte Ethernet
- Cliquer sur [properties]

Figure 16.4
Choix du stack TCP/IP



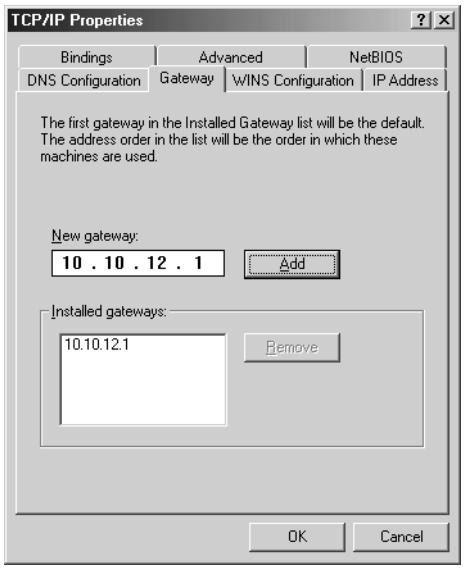
- Donner la nouvelle adresse IP
- Donner le nouveau masque

Figure 16.5
Introduction de l'adresse IP



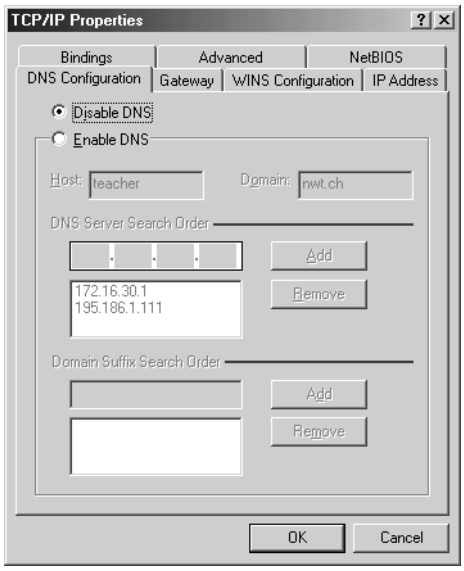
- Effacer le “default gateway“ actuel
- Introduire le nouveau “default gateway“
- Cliquer sur [ADD]

Figure 16.6
Introduction du routeur (default gateway)



- Onglet «DNS Configuration» :
  Disable DNS

Figure 16.7
désactiver le DNS



- Cliquer sur [OK]
- Puis cliquer OK dans la fenêtre de configuration générale des paramètres réseaux. Il faudra ensuite redémarrer le PC.

16.3 Routage statique

Afin de rendre le routage statique plus simple, nous allons programmer une route par défaut (default Route : 0.0.0.0). Avec cette route nous construisons une boucle (1 à 2, 2 à 3, 3 à 1)

1. Donner la route par défaut

```
Cisco_1#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
Cisco_1(config)#ip route (ip net) (subnet mask) (address next hop)
```

Exemple : ip route 0.0.0.0 0.0.0.0 10.10.23.2

Sans indication particulière, les routeurs Cisco essaient d'envoyer les paquets IP ne correspondant à aucun sous-réseau de la table de routage dans le sous-réseau le plus " proche ". On parle de " best match ".

La route par défaut est, d'une manière mathématique, la route la moins proche de nos sous-réseaux. Cette solution permet d'éviter d'envoyer dans l'Internet des paquets qui, manifestement, sont destinés à un client interne du réseau.

Dans notre cas, nous allons devoir obliger le routeur à travailler de manière rigoureuse avec sa table de routage.

2. La commande ci-dessous, va obliger le routeur à travailler rigoureusement avec sa table de routage.

```
Cisco_1(config)#ip classless
Cisco_1(config)# ^Z(Ctrl+z)
Cisco_1#
%SYS-5-CONFIG_I: Configured from console by console
```

3. Visualiser la table de routage avec la commande « show ip route ». Analyser son contenu

```
Cisco_1#show ip route
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
```

Questions

- Ouvrir une fenêtre DOS : Start → run → "Command" → OK
- Envoyer un ping à un PC dans un autre sous-réseau.

1. Le PC est-il atteignable ? Quel chemin la demande d'echo a-t'elle suivi ?

   . . . . . .
   . . . . . .
   . . . . . .

2. Déconnecter un câble de la boucle principale (liaisons sérielles). Pouvez-vous toujours atteindre l'autre station ? Le troisième PC est il atteignable ?

   . . . . . .
   . . . . . .
   . . . . . .

3. Quels sont les chemins suivis par ces demandes d'echos ?

   . . . . . .
   . . . . . .
   . . . . . .
   . . . . . .

4. Essayer d'établir une liaison de et vers chaque PC (6 ping).
   Combien de liaisons ne sont maintenant plus possibles ?

   . . . . . .
   . . . . . .

   Pourquoi ?

   . . . . . .
   . . . . . .
   . . . . . .

16.4 Routage dynamique avec RIP

RIP (Routing Information Protocol) est un protocole de routage à vecteur de distance. Les routeurs l'utilisent afin de créer et maintenir leur table de routage.

Routing Information Protocol

Après avoir activé le protocole, il faut encore indiquer au routeur dans quel réseau il doit échanger ses informations de routage.

1. Désactiver le routage statique

```
Cisco_1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Cisco_1(config)#no ip route (ip net)(subnet mask)(address next hop)
Cisco_1(config)# ^Z(Ctrl+z)
Cisco_1#
%SYS-5-CONFIG_I: Configured from console by console
```

2. Activer RIP

router rip

```
Cisco_1#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
Cisco_1(config)#router rip
Cisco_1(config-router)#version 2
Cisco_1(config-router)#network 10.0.0.0
Cisco_1(config-router)# ^Z(Ctrl+z)
Cisco_1#
%SYS-5-CONFIG_I: Configured from console by console
```

3. Regarder les protocoles de routage IP actifs

show ip protocol

```
Cisco_1#show ip protocol
```

4. Analyser le contenu des tables de routage

show ip route

```
Cisco_1#show ip route
```

5. Analyser le contenu des paquets RIP

debug ip rip

- Démarrer une analyse avec la commande

  ```
  Cisco_1#debug ip rip
  ```

- Attendre environ deux minutes que des paquets RIP soient échangés
- Déconnecter un câble de la boucle principale
- Attendre à nouveau environ deux minutes que le réseau se soit stabilisé
- Arrêter l'analyse avec la commande

  ```
  Cisco_1#undebug all
  ```

6. Essayer les liaisons entre les PC avec des Ping.

Questions

1. Quelles sont les informations contenues dans un paquet RIP ?

   . . . . . .
   . . . . . .
   . . . . . .

2. Quel est le metric utilisé ?

   . . . . . .
   . . . . . .
   . . . . . .

3. Quelle est la fréquence d'envoi des paquets RIP ?

   . . . . . .
   . . . . . .
   . . . . . .

4. Combien de temps faut-il aux routeurs pour réaliser qu'un sous-réseau n'est plus accessible ?

   . . . . . .
   . . . . . .

5. Pourquoi ce délai ?

   . . . . . .
   . . . . . .
   . . . . . .

6. Quels sont les avantages par rapport au routage statique ?

   . . . . . .
   . . . . . .
   . . . . . .
   . . . . . .

Vous pouvez maintenant reconnecter le câble de la boucle principale.

16.5 Routage dynamique avec OSPF

OSPF est un protocole de routage à état des liaisons (link state). Le fonctionnement de ce protocole est plus complexe que celui de RIP.

Open Shortest Path First

On doit également lui donner une information de "portée" des échanges de données OSPF.

1. Désactiver le routage RIP

```
Cisco_1#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
Cisco_1(config)#no router rip
Cisco_1(config)#^Z(Ctrl+z)
Cisco_1#
02:24:35: %SYS-5-CONFIG_I: Configured from console by console
```

2. Activer le routage OSPF

router ospf

```
Cisco_1#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
Cisco_1(config)#router ospf 100
Cisco_1(config-router)#auto-cost
Cisco_1(config-router)#network 10.10.0.0 0.0.255.255 area 0
Cisco_1(config-router)# ^Z(Ctrl+z)
Cisco_1#
```

3. Observer la table de routage avec « show ip route »

4. Analyser le contenu des paquets OSPF

debug ip ospf

- Démarrer une analyse avec la commande

```
Cisco_1#debug ip ospf packet
```

- Attendre environ une minute que des paquets OSPF soient échangés
- Déconnecter un câble de la boucle principale
- Attendre à nouveau environ une minute que le réseau se soit stabilisé
- Arrêter l'analyse avec la commande

```
Cisco_1#undebug all
```

5. Essayer les liaisons entre les PC avec des Ping.

Questions

1. Quelles sont les informations contenues dans un paquet OSPF lorsque le réseau est stable ?

   . . . . . .
   . . . . . .
   . . . . . .

2. Quelle est la fréquence d'envoi de ces paquets ?

   . . . . . .
   . . . . . .

3. Quelles sont les informations contenues dans un paquet OSPF lorsque les routeurs mettent à jour leur table d'état des liaisons ?

   . . . . . .
   . . . . . .
   . . . . . .

4. Quel est le metric utilisé par OSPF ?

   . . . . . .
   . . . . . .

5. Combien de temps faut-il aux routeurs pour réaliser qu'un sous-réseau n'est plus accessible ?

   . . . . . .
   . . . . . .

6. Quels sont les avantages par rapport au routage RIP ?

   . . . . . .
   . . . . . .
   . . . . . .

7. Quels en sont les inconvénients ?

   . . . . . .
   . . . . . .
   . . . . . .
   . . . . . .

Vous pouvez maintenant reconnecter le câble de la boucle principale.

16.6 Interconnexion à l'Internet avec NAT

Afin de nous connecter à l'Internet, nous avons besoin de différentes choses:

Fournisseur d'accès

Notre fournisseur d'accès (ISP : Internet Service Provider) sera le réseau local de notre salle de cours.

Connexion physique

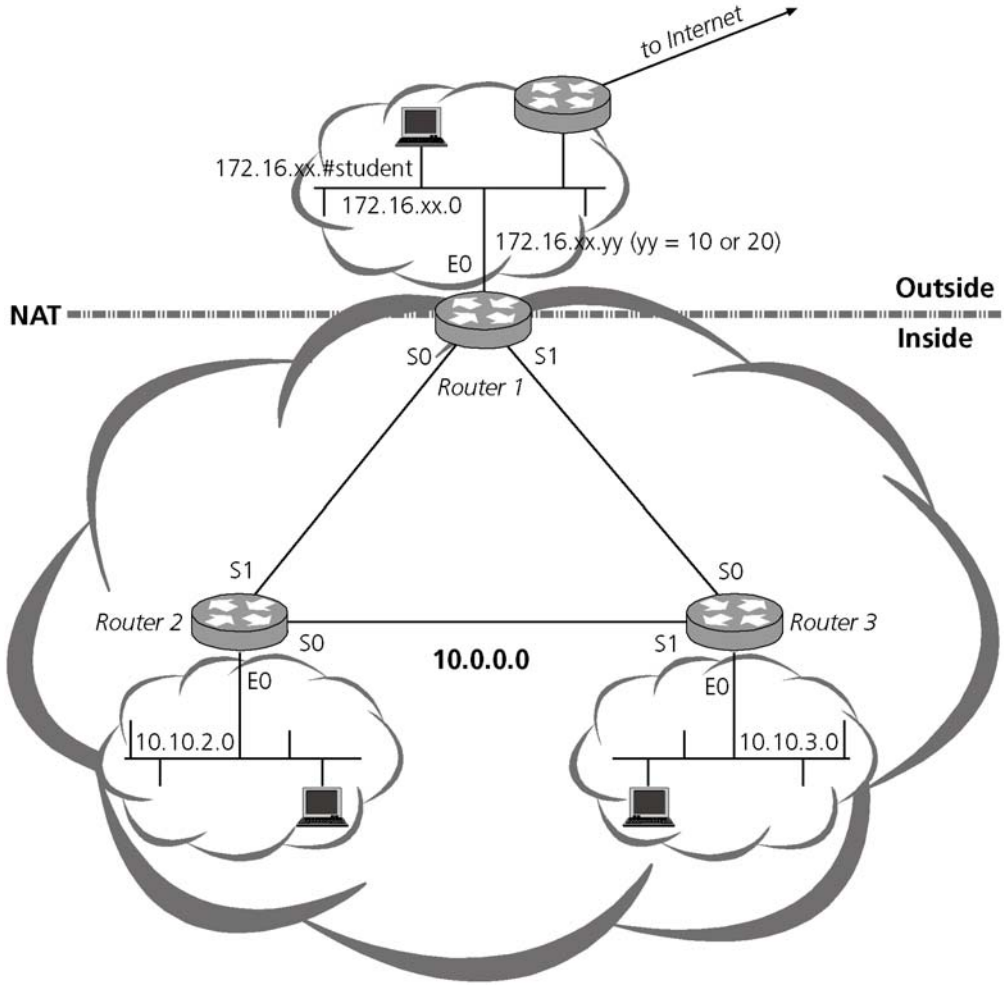
Nous allons utiliser l'interface Ethernet0 de notre routeur1 comme interface de liaison. Son adresse devra faire partie du domaine d'adressage de notre Provider.

Translation d'adresse (NAT)

Les adresses que nous utilisons en interne dans notre réseau sont des adresses privées. Elles ne peuvent pas circuler dans l'Internet. Nous devrons donc "emprunter" des adresses à notre fournisseur d'accès pour notre trafic Internet.

Cette opération de translation sera faite automatiquement par notre routeur d'accès, après que nous lui ayons donné les paramètres nécessaires.

Figure 16.8
Interconnexion à l'Internet



16.6.1 Configuration du NAT

Provider

Nous allons maintenant utiliser le routeur 1 comme routeur d'accès à l'Internet. Son interface Ethernet nous servira de lien vers le réseau de notre "Provider", le LAN de notre salle de cours. Pour cela, nous allons directement brancher le câble du LAN dans l'interface de notre routeur, sans passer par le hub.

"PC outside" et "PC inside"

Le PC qui était connecté sur le LAN1 sera connecté au réseau de la salle de cours, nous l'utiliserons, pour effectuer certains tests "depuis l'Internet". Nous l'appelerons "PC outside". Les PC des LAN2 et LAN3 porteront le nom de "PC inside". Les termes inside et outside proviennent directement de la norme du NAT.

Configuration du "PC outside"

1. Pour rendre à ce PC sa configuration d'origine, il faut répéter à l'inverse les opérations du chapitre 16.2.
   On peut lancer l'Internet Explorer pour tester la configuration. Si la configuration est bonne, on doit pouvoir surfer.

Nous pouvons maintenant configurer notre routeur de liaison, le routeur 1. Les deux autres routeurs ne subiront aucune modification, seule la "porte de sortie" doit être créée.

Configuration IP de l'interface

2. La première chose consiste à donner à cette interface une configuration qui correspond au réseau du Provider:
   groupe1: 172.16.[lieu].10
   groupe2: 172.16.[lieu].20

```
Cisco_1#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
Cisco_1(config)#interface ethernet 0
Cisco_1(config-if)#ip address 172.16.[lieu].[10/20] 255.255.255.0
Cisco_1(config-if)#exit
Cisco_1(config)# ^Z(Ctrl+z)
```

Configuration NAT des interfaces

3. Nous devons maintenant indiquer à notre routeur le positionnement des interfaces à l'intérieur (inside) ou à l'extérieur (outside) de notre réseau

```
Cisco_1#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
Cisco_1(config)#interface serial 0
Cisco_1(config-if)#ip nat inside
Cisco_1(config-if)#exit
Cisco_1(config)#interface serial 1
Cisco_1(config-if)#ip nat inside
Cisco_1(config-if)#exit
Cisco_1(config)#interface ethernet 0
Cisco_1(config-if)#ip nat outside
Cisco_1(config-if)#exit
Cisco_1(config)# ^Z(Ctrl+z)
```


4. Notre routeur doit connaître quelle est la "direction" de l'Internet. Pour cela nous lui donnons une route par défaut vers le routeur de sortie de notre LAN de liaison.

Configuration de la route par défaut

```
Cisco_1#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
Cisco_1(config)#ip route 0.0.0.0 0.0.0.0 172.16.[lieu].1
```

5. Cette route par défaut devra être enseignée aux autres routeur par notre protocole de routage. Nous permettons à notre routeur OSPF de le faire en lui demandant de propager la route par défaut

Routage de la route par défaut

```
Cisco_1(config)#router ospf 100
Cisco_1(config-router)#default-information originate
Cisco_1(config-router)# ^Z(Ctrl+z)
Cisco_1#
```

6. Il ne nous reste plus qu'à configurer l'outil de translation d'adresse, le NAT. Cette opération nécessite un certain nombre d'opérations. Nous allons les traiter point par point

Configuration NAT

```
Cisco_1#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
```

- Le routeur devra oublier la translation après 20 secondes sans trafic

Timeout

```
Cisco_1(config)#ip nat translation timeout 20
```

- On définit un pool d'adresse, appelé NWTNET:
  groupe1: de 172.16.[lieu].210 à 172.16.[lieu].219
  groupe2: de 172.16.[lieu].220 à 172.16.[lieu].229

Address pool

```
Cisco_1(config)#ip nat pool NWTNET [start end] netmask 255.255.255.0
```

- On lie le pool d'adresse à une liste d'accès gérant l'autorisation d'utilisation du pool

Access list

```
Cisco_1(config)#ip nat inside source list 1 pool NWTNET
```

- et on définit cette liste d'accès

```
Cisco_1(config)#access-list 1 permit any

Cisco_1(config)# ^Z(Ctrl+z)
Cisco_1#
```

Questions

visualisation de la table de translation NAT

La commande suivante permet d'afficher la table de translation active.

```
Cisco_1#show ip nat trans
```

1. Nous allons maintenant analyser les translations.
   - Faites un Ping du "PC inside" vers le "PC outside".
   - Entrez la commande ci-dessus dans les 20 secondes
   - Analyser le contenu de la table de translation

   Quelle adresse IP a été "prêtée" à nos paquets pour sortir vers l'Internet ?

   . . . . . .
   . . . . . .

2. On devrait donc pouvoir surfer sur l'Internet. Démarrer un browser Internet et donner l'adresse suivante: *http://138.190.1.60.*
   Quel est le résultat ?

   . . . . . .
   . . . . . .

   Pourquoi avoir utilisé directement l'adresse IP ?

   . . . . . .
   . . . . . .

3. Après contrôle de la disparition de notre translation, essayons maintenant depuis le " PC outside " de faire un ping en direction de notre "PC inside". Pour cela, nous devrons bien sûr utiliser une adresse globale, c'est-à-dire l'adresse "prêtée".
   Quel est le résultat ?

   . . . . . .
   . . . . . .
   . . . . . .

4. Nous allons maintenant essayer d'atteindre le "PC inside" depuis le "PC outside", pendant la validité de la translation.
   - Faites un Ping ininterrompu "PC inside" vers le "PC outside".
   - Chercher l'adresse prêtée dans la table de translation.
   - Faites un Ping du "PC outside" vers le "PC inside".

   Quel est le résultat ?

   . . . . . .
   . . . . . .
   . . . . . .

   Nous pouvons maintenant interrompre le fonctionnement du ping ininterrompu.

16.6.2 Configuration statique NAT

Configuration NAT statique

La commande ci-dessous permet de fixer de manière statique la translation entre l'adresse 10.10.2.10 est 172.16.[lieu].251 (.252 pour le groupe2).

```
Cisco_1(config)#ip nat ins sour static 10.10.2.10 172.16.[lieu].251
```

Cette translation fixe est généralement utilisée pour les serveurs présents dans les réseaux isolés par un translateur d'adresse. A l'aide de son adresse globale, 172.16.[lieu].251, on peut maintenant atteindre notre "serveur" 10.10.2.10 depuis l'Internet.

Questions

1. Maintenant que nous avons parametré cette translation, essayons d'atteindre notre nouveau serveur. Faites un Ping depuis le "PC outside" vers le serveur. Quel est le résultat ?

   . . . . . .

   . . . . . .

2. Le serveur est-il atteignable avec son adresse 10.10.2.10 ? Pourquoi ?

   . . . . . .

   . . . . . .

   . . . . . .

Dans des cas particuliers, la translation d'adresse fixe peut aussi être utilisée pour atteindre un serveur placé à l'extérieur de notre réseau, depuis notre réseau et avec une adresse locale.

La configuration ci-dessous permettrait cette spécialité pour le PC maître :

```
Cisco_1(config)#ip nat out sour static 172.16.[lieu].100 10.10.1.10
```

3. Avec cette commande, le "PC outside", c'est-à-dire le PC maître, devrait être atteignable depuis l'intérieur de notre réseau grâce à l'adresse 10.10.1.10. Quel est le résultat ?

   . . . . . .

   . . . . . .

   . . . . . .

16.6.3 Terminologie du NAT

Dans la terminologie du NAT, on distingue deux notions importantes :

- **Inside / outside** indiquent la position d'un équipement à l'intérieur d'un réseau isolé (généralement privé) ou à l'extérieur de celui-ci (généralement le réseau du Provider).
- **Local / global** donnent une vision locale ou globale d'une machine, en se référant au genre d'adresse utilisée.

inside local

Notre "serveur" possède l'adresse IP 10.10.2.10. Cette adresse n'est valable que localement, à l'intérieur de notre réseau. On parle d'une signification **inside local.**

outside global

A l'inverse, l'adresse de notre "PC outside", 172.16.[lieu].[student], a une signification **outside global.** Il est visible d'une manière globale avec cette adresse et est bien placé à l'extérieur de notre réseau.

inside global

La première translation statique que nous avons configuré offre maintenant à notre "serveur" interne une adresse globale. Or cette machine est bien à l'intérieur de notre réseau. L'adresse 172.16.[lieu].251 a donc une signification **inside global**.

outside local

Finalement, les adresses à signification **outside local** permettent d'atteindre, de notre réseau, une machine qui serait placée à l'extérieur, et ceci à l'aide d'une adresse locale. C'est la configuration proposée avec l'attribution de l'adresse 10.10.1.10 à notre "PC outside".

16.6.4 Configuration de la translation d'adresse de port (PAT)

Nous avons effectué jusqu'ici des translations d'adresses IP. Cette solution limite le nombre de PC qui "surfent" simultanément aux pool d'adresses disponibles.

A l'aide de la translation d'adresse de port, PAT, nous allons nous contenter d'utiliser une adresse IP. Dans notre cas, il s'agit de l'adresse IP de l'interface de sortie de notre routeur 1.

Socket

Toutes les machines présentes à l'intérieur de notre réseau ne seront vue de l'Internet qu'avec une seule et unique adresse. Les différents flux de données seront reconnus et séparés par les N° de port TCP ou UDP. Cette combinaison d'adresse IP et de port de transport s'appelle un socket.

NAT overload

La commande ci-dessous remplace l'utilisation du pool d'adresse par l'utilisation unique de l'adresse IP de l'interface ethernet de notre routeur.

```
Cisco_1(config)#ip nat inside source list 1 interface Eth0 overload
```

- La partie "Eth0" indique l'adresse IP utilisée. On pourrait stipuler une autre adresse.
- Le paramètre "overload" active la translation de port PAT.

Afin d'établir une translation PAT réaliste, il nous faut créer un trafic utilisant TCP ou UDP. Nous allons tenter d'établir une connexion telnet sur le routeur de sortie du LAN de la salle de cours. Il s'agit du routeur 172.16.[lieu].1.

Questions

1. Dans un premier temps, nous allons établir une liaison Telnet depuis le "PC inside" du LAN3, en direction du routeur 172.16.[lieu].1
   - Executer telnet vers le routeur
   - Analyser le contenu de la table de translation
   - Fermer la fenêtre telnet

   Quels sockets ont été utilisés par nos paquets pour sortir vers le routeur ?

   . . . . . .
   . . . . . .

   Quels sockets utilisaient nos paquets à l'intérieur de notre réseau ?

   . . . . . .
   . . . . . .

2. Nous allons maintenant essayer cette même connexion, mais depuis notre "PC inside" du LAN2.
   - Executer telnet vers le routeur
   - Analyser le contenu de la table de translation
   - Fermer la fenêtre telnet

   Quels sockets ont été utilisés par nos paquets pour sortir vers le routeur ?

   . . . . . .
   . . . . . .

3. L'adresse IP mise à disposition par le translateur était-elle la même ?

   . . . . . .
   . . . . . .

   Pourquoi ?

   . . . . . .
   . . . . . .
   . . . . . .

18 Compléments

18.1 Glossaire

0-9

2M	2 Mbit/s
34M	34 MBit/s

A

AAA-Server	Authentication Authorisation Accounting
AAL	ATM Adaption Layer
ABR	Available Bit Rate
ABR	Area Border Router
ACP	Access Control Panel
ADSL	Asymetric Digital Subscriber Line
ANSI	American National Standardization Institute
AoD	Audio on Demand
AP	Access Point
ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
AS	Autonomous System
ASAM	ATM Subscriber Access Multiplexer (Alcatel Designation for their DSLAM)
ASBR	Autonomous System Boundary Router
ASCII	American Standard Code for Information Interchange
ASW	ATM Switch
ATM	Asynchronous Transfer Mode
ATMF-25	ATM Forum 25,6 Mbit/s → interface
ATU-C	ADSL Transceiver Unit - Central Office
ATU-R	ADSL Transceiver Unit - Remote Office
AUI	Attachement Unit Interface

B

BA	ISDN Basis Access
BB	Broad Band
BBA	Broad Band Access
BBA-VAS	Broad Band Access - Value Added Services
BBCS	Broad Band Connectivity Services
BGP	Border Gateway Protocol
BNN	Betriebs Netze Netz
BOOTP	Bootstrap Protocol
BPX	Broad Band Packet eXchange
BR	Backbone Router
BW	Bluewin

C

CAR	Comitted Access Rate
CARIP	Comitted Access Rate over IP
CATV	Cable TV (Community Antenna Television)
CBR	Constant Bit Rate
CD	Collision Detection
CE	Customer Edge
CER	Customer Edge Router
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Interdomain Routing

CLNS	Connectionless Network Services
CO	Central Office
CONS	Connection Oriented Network Service
CoS	Class of Service
CPE	Customer Premises Equipment
CPR	Customer Premises Router
CRC	Cyclic Redundancy Check
CSMA	Carrier Sense Multiple Access
CSMA/CD	Camier Sense Multiple Acces with Collision Detection

D

dB	Decibel
DF	Dark Fiber
DF	Don‘t fragment
DHCP	Dynamic Host Configuration Protocol
DIX	Dec, Intel und Xerox; Company Forum
DLCI	Data Link Connection Identifier
DMT	Discrete Multi Tone
DNS	Domain Name Server, Domain Name Service
DoD	Department of Defense
DOS	Disc Operating System
DPT	Dynamic Packet Transport
DQDB	Distributed Queue Dual Bus
DR	Designated Router
DSL	Digital Subscriber Line
DSLAM	DSL Access Multiplexer
DTE	Data Terminal Equipment
DTMF	Dual Tone Multiple Frequency
DVD	Digital Versatil Disk or Digital Video Disk

E

E1	2 048 kbit/s, primary ITU-PDH-Bitrate
E3	34 368 kbit/s, third Hierarchy of ITU-PDH-Technique
E-BGP	External BGP
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
ESR	Errored Second Ratio
ETSI	European Telecommunications Standards Institute

F

FCS	Frame Check Sequence
FDDI	Fibre Distributed Data Interface
FIB	Forwarding Information Base
FR	Frame Relay
FTP	File Transfer Protocol
FTTB	Fiber To The Building
FTTC	Fiber To The Curb
FTTCab	Fiber To The Cabinet
FTTH	Fiber To The Home
FTTLex	Fiber To The Local Exchange
FTTO	Fiber To The Office

G

G.Lite	Splitterless ADSL Transceiver
GAN	Global Area Network
Gbps	Gigabit per second

GOSIP	Government OSI Profile
GSR	Gigabit Switch Router

H

HDLC	High Level Data Link Control
HDSL	High bit-rate Digital Subscriber Line
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transport Protocol

I

I/O	Input / Output
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
I-BGP	Internal BGP
ICMP	Internet Control Message Protocol
IEEE	Institute of Electronic and Electrical Engineering
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IN	Intelligent Network
INOC	Internet Network Operation Center
IP	Internet Protocol
IPCP	IP Control Protocol
IPng	IP new generation
IPSEC	IP Security Protocol
IPSO	IP Security Option
IPSS	Internet Protocol for Standard Services
IPX	Internet Packet eXchange
IR	Internal Router
IRTF	Internet Research Task Force
ISDN	Integrated Services Digital Network
ISDN-BA	ISDN Basic Access
IS-IS	Intermediate System – Intermediate System
ISOC	Internet Society
ISP	Internet Service Provider
ITU	International Telecommunications Union
ITU-T	International Telecommunication Union – Telecommunication

J

JPEG	joint picture (Photographics) expert group

K

Kbps	Kilobit per second

L

L2TP	Layer 2 Tunnelling Protocol
LAC	Local Access Concentrator, L2TP Access Concentrator
LAN	Local Area Network
LAN-E	LAN-Emulation
LAN-I	LAN-Interconnection
LAN-I over IPSS	LAN-Interconnection over IPSS
LCN	Logical Channel Number
LCP	Link Control Protocol
LDP	Label Distribution Protocol
LLC	Logical Link Control
LNS	Local Network Server, L2TP Network Server
LR	Long Reach
LSA	Link State Advertisements

LSB	Least Significant Bit
LSDB	Link State Data Base
LSP	Link State Protocol
LT	Line Termination

M

MAC	Media Access Control
MAN	Metropolitan Area Network
MASS	Marktführerschaft für Standard Services / market leadership for standard services
MAU	Media Access Unit
MCU	Multipoint Control Unit
MED	Multi Exit Discriminator
MF	More Fragments
MGCP	Merged Gateway Control Protocol
MGX	Multiservice Gigabit eXchange
MIME	Multipurpose Internet Mail Extension
MIPA	Marktgetriebene Investitionsplanung im Anschlussnetz
MIPS	Mega Instruction Per Second
MM	Multi Mode
MPEG	Motion Picture Expert Group
MPLS	Multi Protocol Label Switching
MSB	Most Significant Bit
MTS	Message Transfert System
MTU	Message Transfer Unit
MUX	Multiplexer

N

NAT	Network Address Translation
NET	Network Emtity Titles
NBMA	None Broadcast Multi Access Network
NCP	Network Control Protocol
NIC	Network Information Center
NLRI	Network Layer Reachability Information
NMS	Network Management System
NNI	Network Node Interface
NOC	Network Operation Center
NSAP	Network Service Access Point
NT	Network Termination
NTP	Network Timing Protocol

O

OC-12	STM-4
OC-192	STM-64
OC-3	STM-1
OC-48	STM-16
OF	Optical Fibre
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First

P

PA	ISDN Primary Access
PABX, PBX	Private Branche eXchange
PAP	Password Authentication Protocol
PCM	Pulse Code Modulation
PCR	Peak Cell Rate
PDH	Plesiochrone Digital Hierarchy
PDU	Protocol Data Unit

PE	Provider Edge
PER	Provider Edge Router
PoP	Point of Presence
POP	Post Office Protocol
POS	Packet over Sonet/SDH
POTS	Plain Old Telephony Services
PP	Point-Point
PPP	Point-to-Point-Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPTP	Point-to-Point-Tunnelling-Protocol
PS	Print Server
PSDN	Packet Switched Data Network
PSPDN	Public Switched Packet Data Network
PSTN	Public Switched Telephone Network
PT	Payload Type
PVC	Permanent Virtual Connection, Permanent Virtual Channel

Q

QCIF	Quarter Common Intermediate Format
QoS	Quality of Service

R

RARP	Reverse Address Resolution Protocol
RD	Route Distinguisher
RFC	Request For Comments
RIB	Routing Information Base
RIP	Routing Information Protocol
RR	Route Reflector
RSVP	Ressource Reservation Protocol
RTCP	Real Time Control Protocol
RTP	Real Time Transport Protocol

S

S/MIME	Secure/Multipurpose Internet Mail Extensions
SAP	Service Access Point
SAPI	Sercvice Access Point Identifier
SDH	Synchronous Digital Hierarchy
SDLC	Synchronous Data Link Control
SDSL	Symmetric Digital Subscriber Line
SDU	Service Data Unit
SGCP	Simple Gateway Control Protocol
S-HTTP	Secure Hyper Text Transaction Protocol
SLIP	Serial Line Internet Protocol
SLT	SDH Line Termination
SM	Single Mode
SMS	Short Message Service
SMTP	Single Mail Transport Protocol
SNA	Systems Networks Architecture (IBM)
SNAP	Sub Network Access Point
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SP	Service Provider
SPF	Shortest Path First
SR	Short Reach

SS7	Signalling System Nr 7
SSD	Service Selection Dashboard
SSG	Service Selection Gateway (Cisco)
STM	Synchronous Transfer Mode
STM-1	155 Mbit/s
STM-16	2,5 Gbit/s
STM-4	622 Mbit/s
STM-64	10 Gbit/s
STP	Shielded Twisted Pair
S-UTP	Shielded- Unshielded Twisted Pair; screened
SVC	Switched Virtual Connection, Switched Virtual Channel
SWANET	Swisscom ATM Network
SYDINET	Swisscom SDH Network

T

T1	1,544 Mbit/s, Primary US-Data rate
T3	44,736 Mbit/s, US-Data rate
TA	Terminal Adapter
TAG	Switching info from Cisco TAG-Switching
TCP	Transmission Control Protocol
TDM	Time Division Multiplex
TDP	Tag Distribution Protocol
TFIB	Tag Forwarding Information Base
TFTP	Trivial File Transfer Protocol
TIB	Tag Information Base
TMN	Telecommunication Managment Network
ToS	Type of Service
TP	Twisted Pair
TS	Terminal Server
TTL	Time to Live

U

UBR	Unspecified Bit Rate
UDP	User Datagramm Protocol
ULL	Unboundling Local Loop
UMTS	Univeral Mobile Telecommunication System
UNI	User Network Interface
URL	Universal Resource Locator
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
UUS	User to User Signaling

V

VC	Virtual Channel
VPC	Virtual Path Connection
VoIP	Voice over IP
VXR	Very eXtended Ratio
VBR	Variable Bit Rate
VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VDSL	Very High Speed Digital Subscriber Line
VLAN	Virtual LAN
VoD	Video on Demand
VP	Virtual Path
VPI	Virtual Path Identifier
VPN	Virtual Private Networks

W

WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WWW	World Wide Web

X

xDSL	different flavour (actual and future) of Digital Subscriber Lines technologies
XNS	Xerox Network System

Y

Z

18.2 Liste des figures

19 Annexes

19.1 Paramétrage du Fluke Protocol Inspector

Avant de pouvoir utiliser le Fluke Protocol Inspector, il convient de le paramétrer pour notre utilisation.

Pour avoir les résultats les plus cohérents, nous allons analyser les données relatives à un autre PC du sous-réseau. Dans notre cas, nous allons procéder au filtrage des trames ethernet, sur la base de l'adresse MAC du PC qui nous intéresse.

1. Lancer l'application Fluke Protocol Inspector

2. Ouvrir la fenêtre d'analyse détaillée

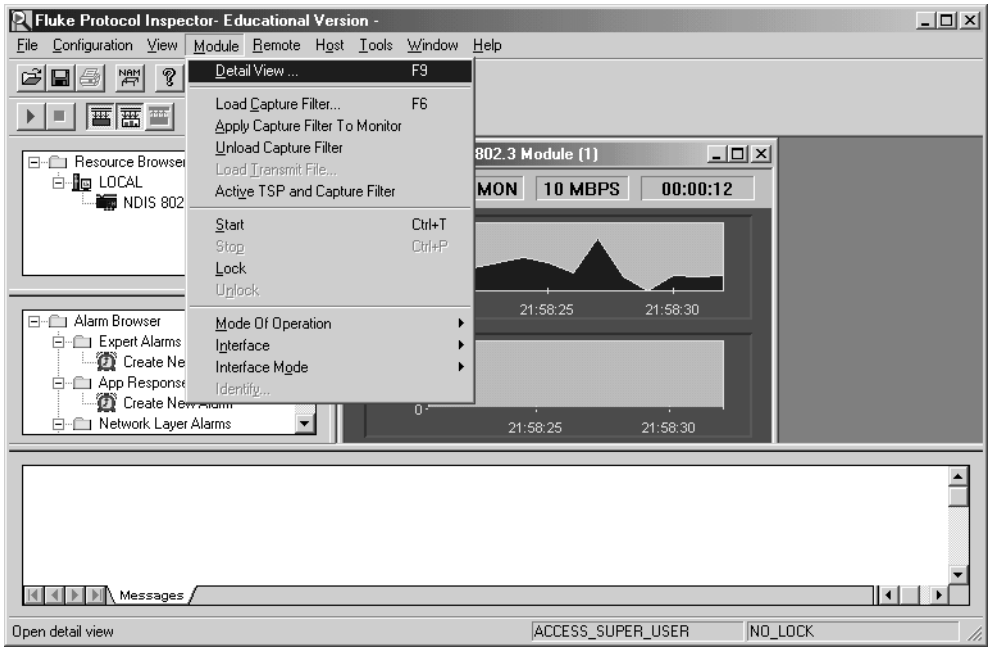
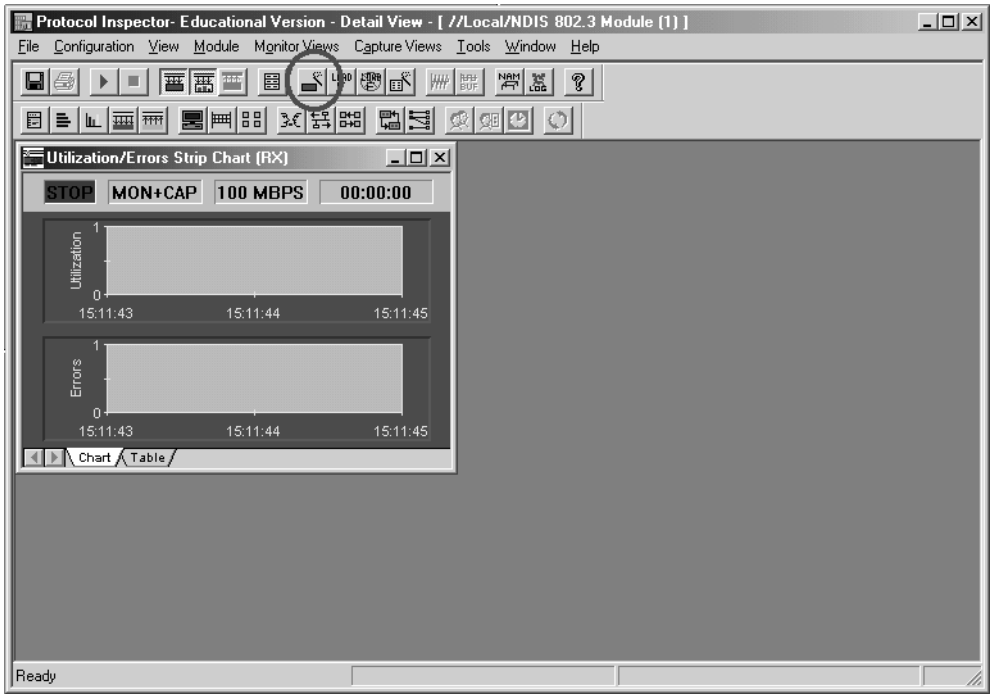


Figure 19.1
Ouverture de la fenêtre d'analyse détaillée

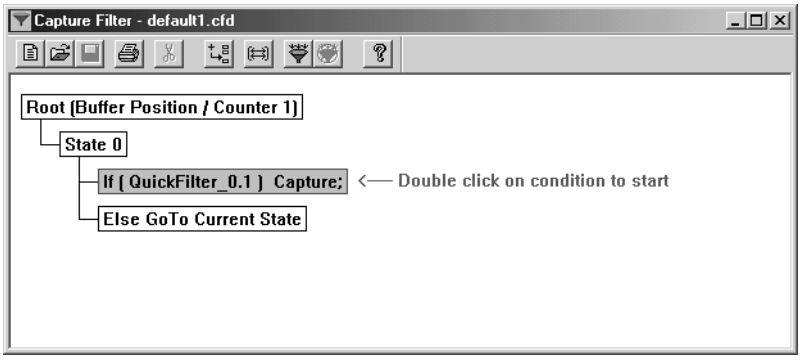
3. Ouvrir le filtre de capture

Figure 19.2
Ouverture du filtre de capture



4. Ouvrir la fenêtre de condition

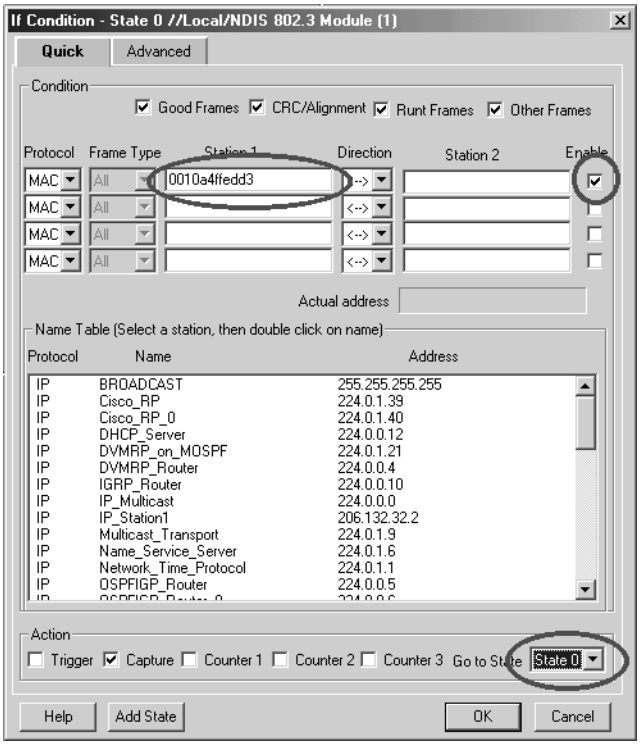
Figure 19.3
Ouverture de la fenêtre de condition



5. Donner les différentes conditions de capture

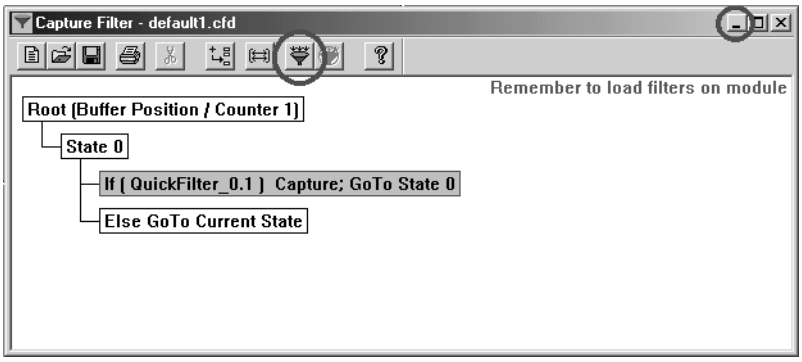
- Adresse MAC du PC à analyser
- Activer cette adresse (enable)
- Retour à l'état initial (State 0)

Figure 19.4
Introduction des conditions de capture



6. Charger le filtre dans le module d'analyse

Figure 19.5
Chargement du filtre



7. Puis réduire la fenêtre du filtre (ne pas fermer !)

19.2 Analyse avec le Fluke Protocol Inspector

Une fois notre analyseur de protocole paramétré, nous pouvons procéder à une ou plusieurs captures, puis analyses de protocole.

1. Lancer la capture

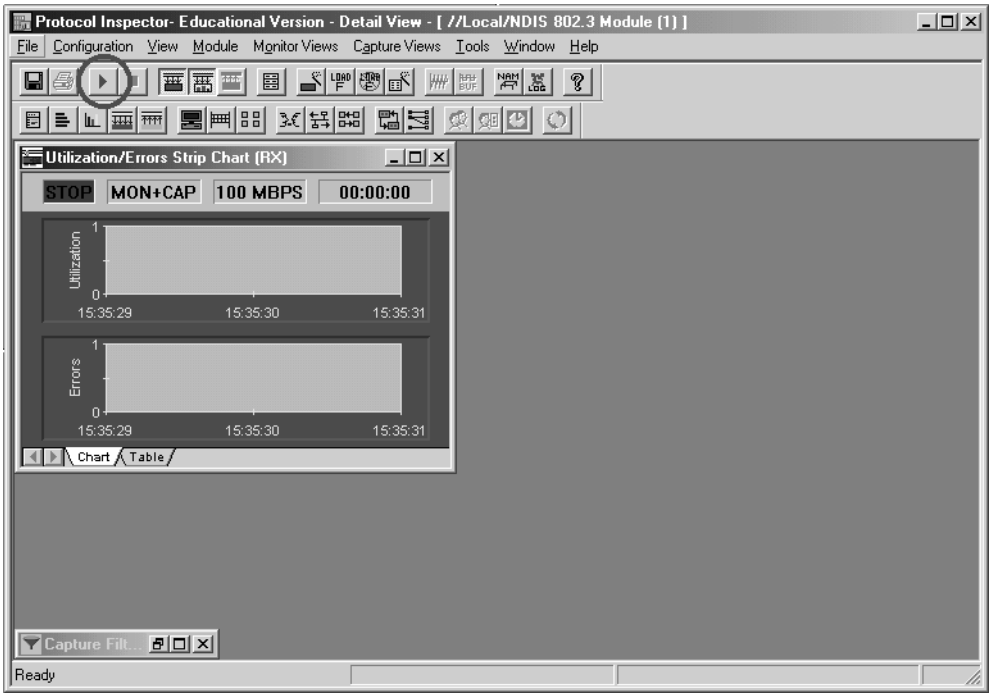


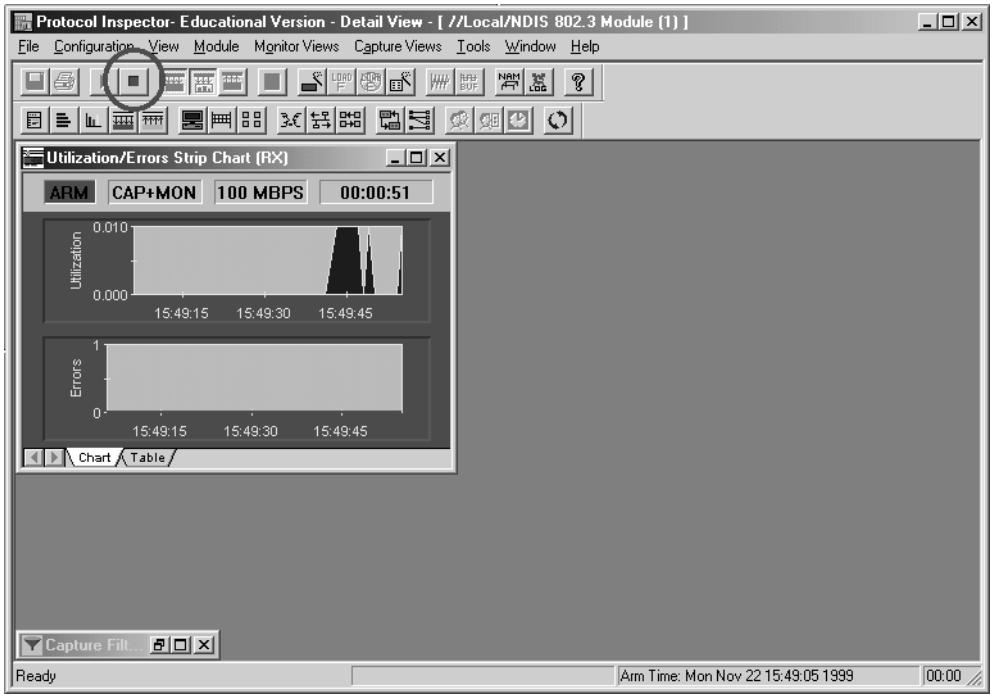
Figure 19.6
Lancement de la capture

2. Générer le trafic à analyser sur le PC désiré.

Ceci peut se faire à l'aide d'une fenêtre DOS, de telnet ou encore d'un browser Internet par exemple.

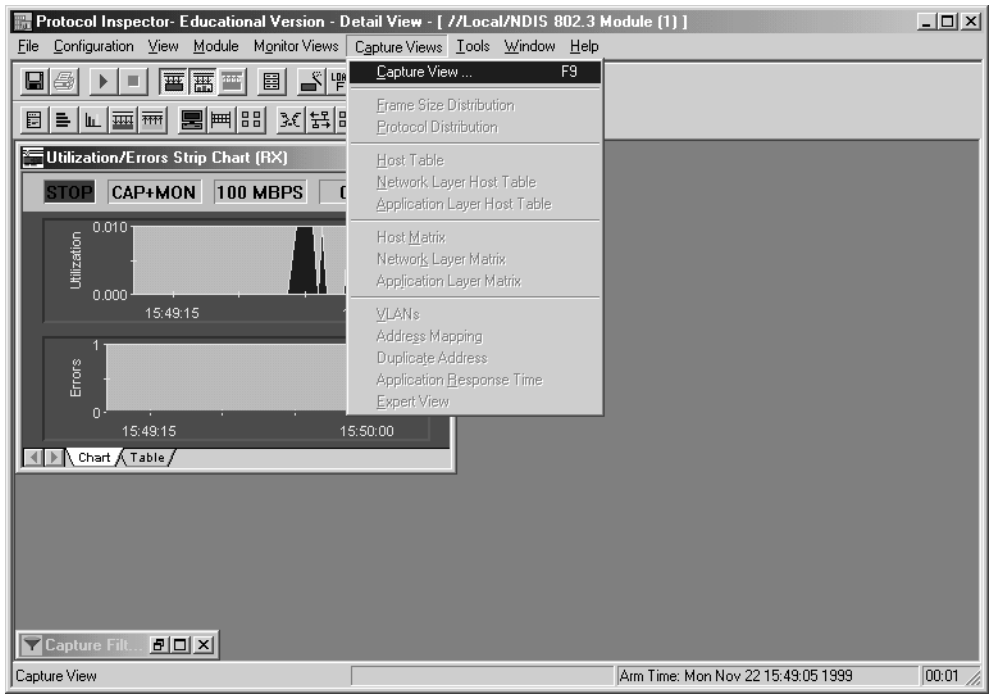
3. Stopper la capture

Figure 19.7
Arrêt de la capture



4. Ouvrir la fenêtre de visualisation des trames capturées

Figure 19.8
Ouverture de la fenêtre de visualisation



5. Analyser le trafic capturé

Pour l'analyse, on voit trois fenêtres :

- une fenêtre d'analyse sommaire, comprenant toutes les trames capturées
- une fenêtre d'analyse de détail, comprenant le contenu de chacune des trames
- une fenêtre représentant la trame complète en mode héxadécimal

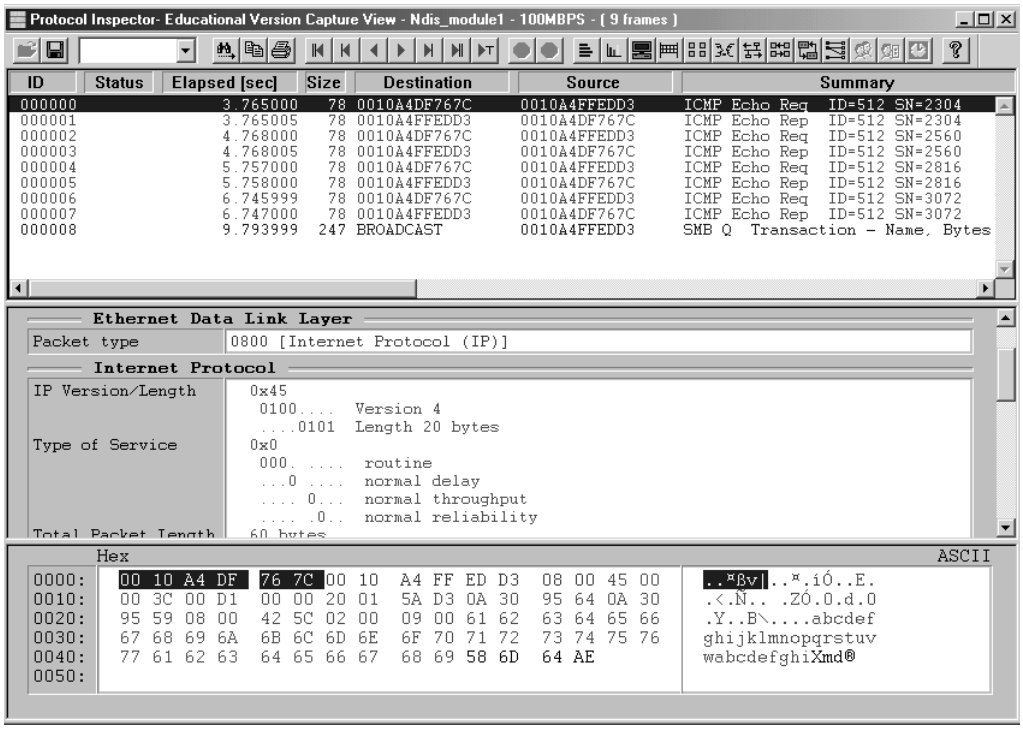


Figure 19.9
Fenêtre de visualisation

6. Fermer la fenêtre de visualisation

Après l'analyse, il faut fermer la fenêtre de visualisation avant de relancer une nouvelle capture, sinon les nouvelles trames ne seront pas capturées

19.3 Modes du Routeur

Indépendamment du mode d'accès à un routeur (via la console, un liaison par modem ou une interface routeur), on peut accéder à divers modes. A côté du mode d'utilisateur et du mode de privilégié, il existe divers autres modes de fonctionnement du routeur. Chaque mode de fonctionnement permet la réalisation de certaines fonctions. Parmi les divers modes on compte le mode utilisateur, le mode privilégié, le mode d'installation, le mode RXBOOT et le mode de configuration.

Mode utilisateur

Mode utilisateur

Le mode utilisateur (Usermod) fournit un environnement d'affichage exclusif. Il permet de consulter des informations via le routeur mais il est impossible de modifier la configuration.

Mode privilégié

Mode privilégié

Le mode privilégié (Privilegmod) permet de réaliser un contrôle exhaustif du routeur. Ce mode supporte les commandes de contrôle, de débugage ainsi que les commandes de gestion pour la configuration du routeur.

Mode installation

Mode installation

Le mode installation est activé lors de l'initialisation du routeur,

lorsqu'il n'y a pas de fichier de configuration dans la mémoire virtuelle non volatile (NVRAM = RAM non volatile). A l'aide des ordres d'entrée interactifs, ce mode réalise un dialogue en vue de la génération d'une configuration routeur de base.

RXBOOT

RXBOOT

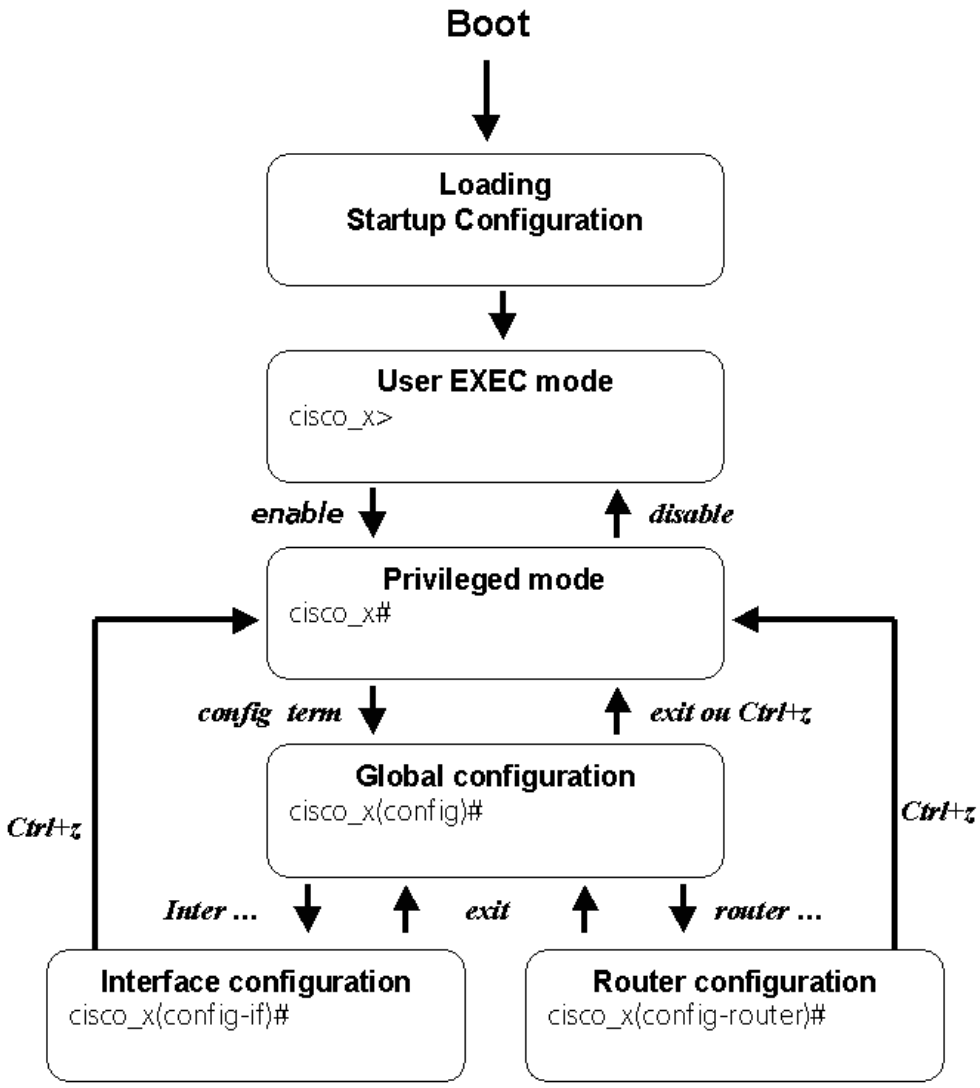
Le mode de maintenance d'un routeur est désigné comme mode RXBOOT ou mode de contrôle ROM (moniteur ROM). Il assure les fonctions de rétablissement lorsque l'utilisateur a perdu le mot de passe du routeur ou lorsque le fichier IOS mémorisé dans la mémoire FLASH a été supprimée ou endommagée. En pressant la touche PAUSE sur un terminal connecté au routeur dans les 60 s. qui suivent l'initialisation permettent de mettre le routeur en mode maintenance.

Mode de configuration général

Mode de configuration général

Le mode de configuration général est prévu pour les tâches de configuration simples. Ainsi, l'utilisateur peut configurer le nom du routeur, les mots de passe y relatifs et la bannière de routeur dans ce mode.

Figure 19.10
Modes du routeur



19.4 Composants du routeur

Chaque routeur est configuré à l'aide de plusieurs composants : RAM, ROM, NVRAM, mémoire FLASH et interfaces.

RAM

Random Access Memory

La mémoire intermédiaire (RAM = Random Access Memory) sert de mémoire de travail pour le routeur.

Elle contient des fichiers divers tels que les tables de routage, des caches divers ainsi qu'une mémoire tampon et des files d'attente pour l'entrée et la sortie des données. En plus de cela, la RAM fournit une mémoire temporaire pour l'IOS et le fichier de configuration (running-config) du routeur. Le contenu de la RAM est toutefois perdu lorsqu'on réinitialise ou redémarre le routeur.

NVRAM

Non-Volatile RAM

Contrairement à ce qui se passe avec la RAM, le contenu de la RAM non volatile (NVRAM) n'est pas perdu en cas de désactivation ou de redémarrage du routeur. Ainsi, les informations permanentes comme la copie de sauvegarde du fichier de configuration du routeur sont mémorisées en permanence. La configuration de démarrage (startup-config) est chargée à partir de la NVRAM dans la RAM durant l'initialisation.

Flash

Mémoire Flash

La mémoire FLASH abrite le fichier d'images du IOS Cisco ainsi que le microcode y relatif. La mémoire FLASH est en fait une ROM réinscriptible et reprogrammable qui sauvegarde son contenu lors de la désactivation et du redémarrage du routeur. La mémoire FLASH peut contenir une ou plusieurs versions / configurations de l'image IOS. La mémoire FLASH permet d'actualiser les logiciels sans devoir ajouter, retirer ou remplaces des puces.

ROM

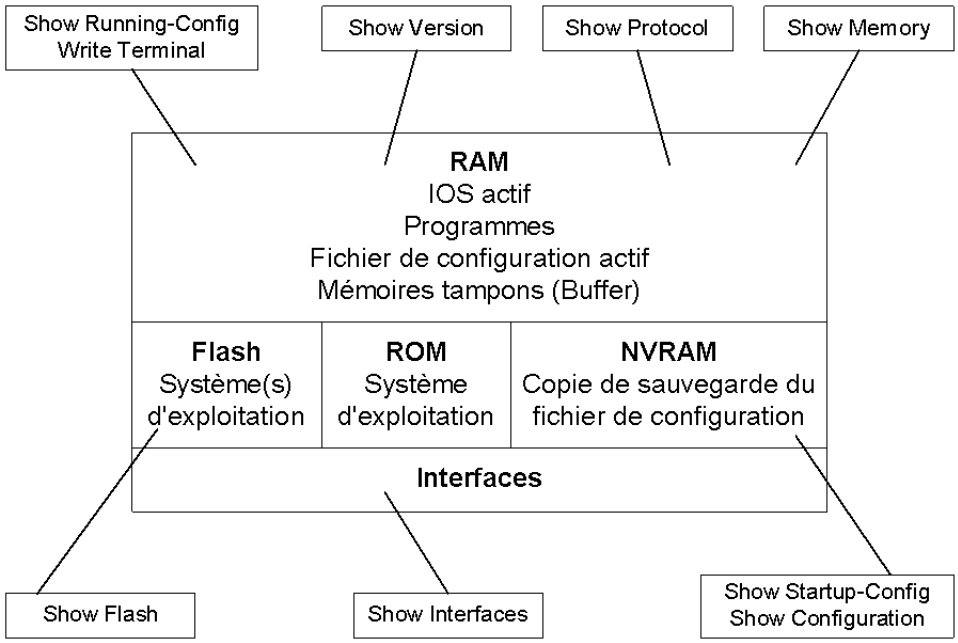
Read Only Memory

Comme cela est le cas pour la mémoire FLASH, la ROM contient également une version IOS. Normalement, cette version est plus ancienne et contient les fonctions de base minimales, c'est-à-dire le programme d'initialisation et les programmes de diagnostic POWER ON pour assurer le bon déroulement des opérations après le démarrage. Toutefois, l'actualisation des logiciels n'est possible que par un remplacement des puces.

Interfaces

Les interfaces assurent les connexions réseau du routeur lors de l'entrée et de la sortie des paquets. Suivant le modèle de routeur, les interfaces sont situées soit directement sur la platine principale ou sur des cartes d'interface faisant partie de l'interface. L'illustration ci-après représente les divers composants d'un routeur.

Figure 19.11
Mots clés de la commande **show**



19.5 Commandes du Routeur

Router # configure terminal

Permet d'ajouter, de modifier ou de supprimer des ordres faisant partie de la configuration courant pendant l'exploitation.

Router # configure memory

Permet d'ajouter des ordres à la configuration de démarrage.

Router # show running-config (ancien ordre: Router # write terminal)

Affiche la configuration avec laquelle le routeur travaille en ce moment.

Router # show startup-config (ancien ordre: Router #show configuration)

Affiche la configuration qui est chargée lors du démarrage du routeur.

Router # show interface

Affiche les valeurs statistiques pour toutes ou pour une partie des interfaces du routeur.

Router # show flash

Affiche des informations sur la mémoire Flash.

Router # show cdp neighbors

Fournit un résumé de toutes les informations cdp (cisco discovery program) sur les voisins directs.

Router # show cdp entry<< ID équipement >>

Fournit des informations sur un appareil voisin précis.

Router # show protocol

Affiche le protocole activé sur le routeur (par ex. IP) et les adresses réseau des interfaces concernées.

Router # show ip protocol

Affiche les protocoles de routage utilisés et leur configuration.

Router # show ip interface

Affiche les informations sur une interface utilisant le protocole IP.

Router # show ip route

Affiche le table de routage et la manière dont le routeur a obtenu les informations.

Router # show ip interface

Affiche les informations IP d'une interface.

Router # show version

Affiche la version de l'IOS (Internet Operating System Software) qui est chargé.

Router # show memory

Affiche les valeurs de mémoire du routeur.

Router # copy running-config TFTP

Proceed? (confirm) <Return>

Cet ordre permet de charger la configuration actuelle sur un serveur TFTP.

Router # copy TFTP running-config

Proceed? (confirm) <Return>

Cet ordre permet de charger un fichier de configuration du serveur TFTP direc-tement dans la configuration active du routeur.

Router # copy running-config startup-config

Proceed? (confirm) <Return>

Cet ordre permet de copier la configuration actuelle dans la configuration de démarrage du routeur.

Router # copy startup-config running-config

Proceed? (confirm) <Return>

Cet ordre permet de copier la configuration de démarrage dans la configuration active du routeur.

Router # copy flash TFTP

Proceed? (confirm) <Return>

Cet ordre permet de copier l'IOS sur le serveur TFTP.

Router # copy TFTP flash

Proceed? (confirm) <Return>

Cet ordre permet de charger une version IOS d'un serveur TFTP sur le routeur.

Router # reload

Cet ordre permet de redémarrer le routeur.

Router # erase startup-config

Cet ordre permet de supprimer la configuration chargée au démarrage du routeur.

Router (config)# enable << Mot de passe >>

Cet ordre permet de protéger l'accès à un routeur à l'aide d'un mot de passe.

Router (config)# line vty 0 4

Router (config line)# login

Router (config line)# password << Mot de passe >>

Ces ordres permettent d'attribuer un mot de passe pour l'accès à distance Telnet (indispensable pour activer Telnet).

Router (config)# enable secret << Mot de passe >>

Cet ordre permet de protéger l'accès à un mot de passe routeur supplémentaire.

Router (config)# hostname <<Router Name>>

Cet ordre permet de renommer un routeur.

Router (config)# service password encryptio

Permet le cryptage des mots de passe 'enable' et 'vty'.

Router (config)# Interface s0

Router (config-if)# description << description de l'interface >>

Cet ordre permet de donner certaines descriptions relatives à l'interface. Exemples: débit binaire et désignation de la liaison (64 k between Phoenix and San Diego).

Router (config)#banner motd

Cet ordre permet d'entrer des informations relatives à la sécurité, affichées lors de l'initialisation du routeur.

Router (config)#interface ethernet 0

Router (config-if)# no shutdown

Monte l'interface et ne lui permet pas de retomber

Router (config-if)# IP address 172.16.24.12 255.255.255.0

Permet de configurer une adresse IP à l'interface Ethernet0.

Router (config)#router rip

Router (config-router)# network 172.16.0.0

Configuration du réseau afin qu'il soit connu.

Router # write erase

Suppression du fichier startup-config dans NVRAM.

Router # tracerout 172.16.24.12

Permet d'afficher la route parcourue jusqu'à destination.

Router> ping 172.16.24.12

Envoi d'un " ping " (demande d'echo).

19.6 Commandes TCP/IP

19.6.1 ping

On peut tester avec Ping si une station distante est disponible. Ping travaille avec le protocole ICMP. Il envoie des „echo request" et affiche les "echo reply", pour autant que la station de destination réponde.

Attention : Pour des raisons de sécurité, l'envoi de paquet echo a pu être désactivé sur la machine de destination. Dans ce cas un message de dépassement de temps est affiché.

```
Syntaxe:        PING [-t] [-a] [-n compte] [-l taille] [-f] [-i TTL]
                [-v TOS] [-r compte] [-s compte] [[-j liste-hôte] |
                [-k liste-hôte]] [-w délai] liste_destination

Options:
-t              Ping l'hôte spécifié jusqu'à interruption.
-a              Résoud les adresses en noms d'hôtes.
-n compte       Nombre de demande d'echo à envoyer.
-l taille       Envoie la taille de la zone de mémoire tampon.
-f              ne fragmente pas les paquets.
-i TTL          Durée de vie.
-v TOS          Type Of Service.
-r compte       Enregistre l'itinéraire pour comptage de tronçons.
-s compte       Timestamp pour comptage de tronçons.
-j liste-hôte   Itinéraire source libre le long de la liste d'hôtes.
-k liste-hôte   Itinéraire source strict le long de la liste d'hôtes
-w délai        délai (millisecondes) d'attente pour chaque réponse.
```

Exemples:

ping 194.87.125.56	Ping une adresse IP
ping www.novell.com	Ping sur un nom DNS
ping –l 4000 198.251.123.5	Un paquet de 4000 octets sera transmis

19.6.2 Traceroute

Tracert

Tracert trace le chemin entre la source et la destination. Cela veut dire que chaque routeur traversé sera affiché. En fonction des paramètres on affichera le nom de chaque routeur, ou alors seulement son adresse IP.

```
Syntaxe:          TRACERT [-d] [-h max_tronçons] [-j liste_hôte] [-w
                  délai] nom_cible

Options:
-d                ne résoud pas les adresses vers les noms d'hôtes.
-h max_tronçons   Nombre maximal de tronçons pour la recherche de la
                  cible.
-j liste_hôte     Itinéraire source libre le long de la liste
                  d'hôtes.
-w délai          Délai d'attente (millisecondes) pour chaque
                  réponse.
```

Exemples :

tracert 68.23.58.1	Trace le chemin jusqu'à l'adresse IP
tracert www.autsch.de	Trace le chemin jusqu'au nom DNS

19.6.3 netstat

Affiche les statistiques de protocole et de connexions réseau TCP/IP en cours.

Statistique des protocoles

```
NETSTAT [-a] [-e] [-n] [-s] [-p Proto] [-r] [intervalle]

-a            Affiche toutes les connexions et ports d'écoute. (Les
              connexions côté serveur sont normallement inhibées).
-e            Affiche les statistiques Ethernet. Peut être
              combinée avec l'option –s.
-n            affiche les adresses et les numéros de ports sous
              forme numérique.
-p Proto      Montre les connexions pour le protocole spécifié par
              proto; proto peut être TCP ou UDP. Utilisé avec
              l'option –s pour afficher des statistiques par
              protocole, proto peut être TCP, UDP ou IP.
-r            Affiche le contenu de la table de routage.
-s            Affiche les statistiques par protocole. Par défaut,
              des statistiques sur TCP, UDP et IP sont visualisées;
              l'option –p peut être utilisée pour spécifier un
              sous-ensemble par défaut.
intervalle    Réaffiche les statistiques sélectionnées, avec une
              pause de „intervalle“ secondes entre chaque
              affichage. Appuyez sur Ctrl+C pour arrêter
              l'affichage des statistiques. En cas d'omission,
              netstat imprimera une fois les informations.
```

Exemples:

netstat –r	Affiche la table de routage du PC

19.6.4 arp

Adresse IP / adresse MAC

Modifie et affiche la table de correspondance entre adresses physiques et logiques, qui ont été résolues par le protocole ARP.

```
ARP -s adr_inet adr_eth [adr_if]
ARP -d adr_inet [adr_if]
ARP -a [adr_inet] [-N adr_if]
```

-a	Affiche les entrées ARP actives en interrogeant le protocole de données actif. Si adr_inet est spécifié, seules les adresses IP et Physique de l'ordinateur spécifié sont affichées. Si plus d'une interface réseau utilise ARP, les entrées de chaque table ARP sont affichées.
-g	Identique à -a.
adr_inet	Spécifie une adresse Internet.
-N adr_if	Affiche les entrées ARP pour l'interface réseau spécifiée par adr_if.
-d	Efface l'hôte spécifié par adr_inet.
-s	Ajoute l'hôte et associe l'adresse Internet adr_inet à celle physique adr_eth. L'adresse physique est donnée sous la forme de 6 octets en héxadécimal séparés par des traits d'union. L'entrée est permanente.
adr_eth	Spécifie une adresse physique.
adr_if	Précisée, elle spécifie l'adresse Internet de l'interface dont la table de traduction des adresses devrait être modifiée. Non-précisée, la première interface applicable sera utilisée.

Exemple :

arp –a	Montre la table ARP actuelle

19.6.5 ipconfig (Windows98, WindowsNT, Windows2000)

Configuration IP

Par défaut, sont uniquement affichées : l'adresse IP, le masque de sous-réseau et la passerelle par défaut pour chaque carte liée à TCP/IP.

Pour Release et Renew, si aucun nom de carte n'est spécifié, alors l'adresse IP attachée à toute carte liée à TCP/IP sera libérée ou renouvellée.

```
Syntaxe:        IPCONFIG [/? | /ALL | /RELEASE [carte] | /RENEW
                [carte]]

/?              Affiche ce message d'aide.
/ALL            Affiche l'ensemble des informations de
                configuration.
/RELEASE        Libère l'adresse IP de la carte spécifiée.
/RENEW          Renouvelle l'adresse IP de la carte spécifiée.
```

Attention: avec Windows 95 et Windows NT ces programmes se lancent à l'aide des commandes ci-dessous :

Windows 95 **winipcfg**

Windows 95

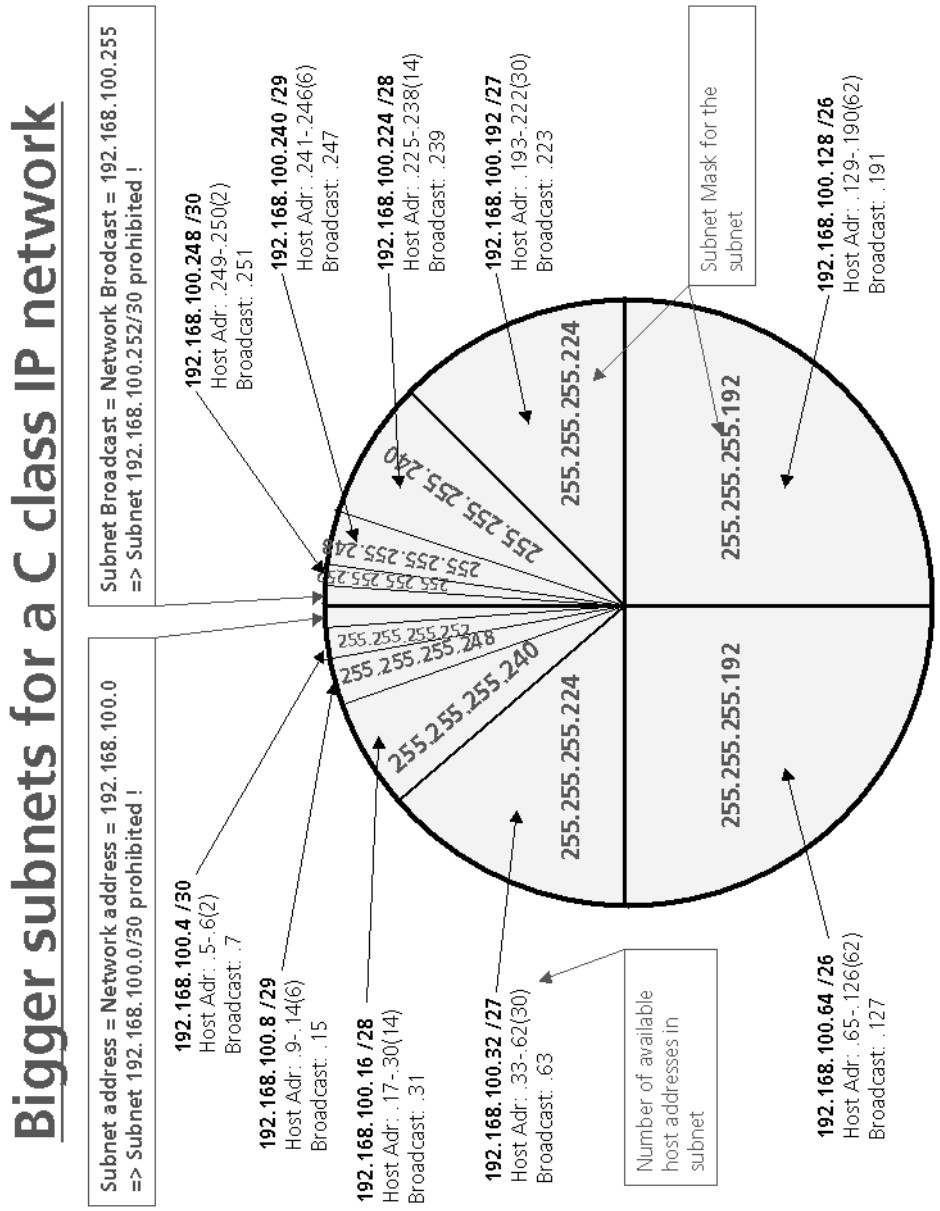
Windows NT **wntipcfg**

Windows NT

19.7 Grands sous-réseaux pour un réseau de classe C

Dans les réseaux de classe C, seul le dernier octet permet de faire du subnetting. La plage d'adresse à disposition n'étant pas grande, on doit créer les sous-réseaux au mieux. l'exemple ci-dessous montre la manière dont il faut procéder pour créer les plus grands sous-réseaux. Chacun des sous-réseaux présentés pourraient être divisés en sous-réseaux plus petits, à l'exception des deux sous-réseaux possédant déjà le masque minimum, soit 255.255.255.252.

Figure 19.12
Sous-réseaux dans un réseau de classe C



Une telle représentation dans le cas d'un réseau de classe A ou B n'a généralement pas de sens. L'espace d'adressage à disposition est suffisament grand pour qu'on sépare les sous-réseaux des clients entre les deux derniers octets.

20 Exercices

