




Réseaux Informatiques

Filière: SMI – S5



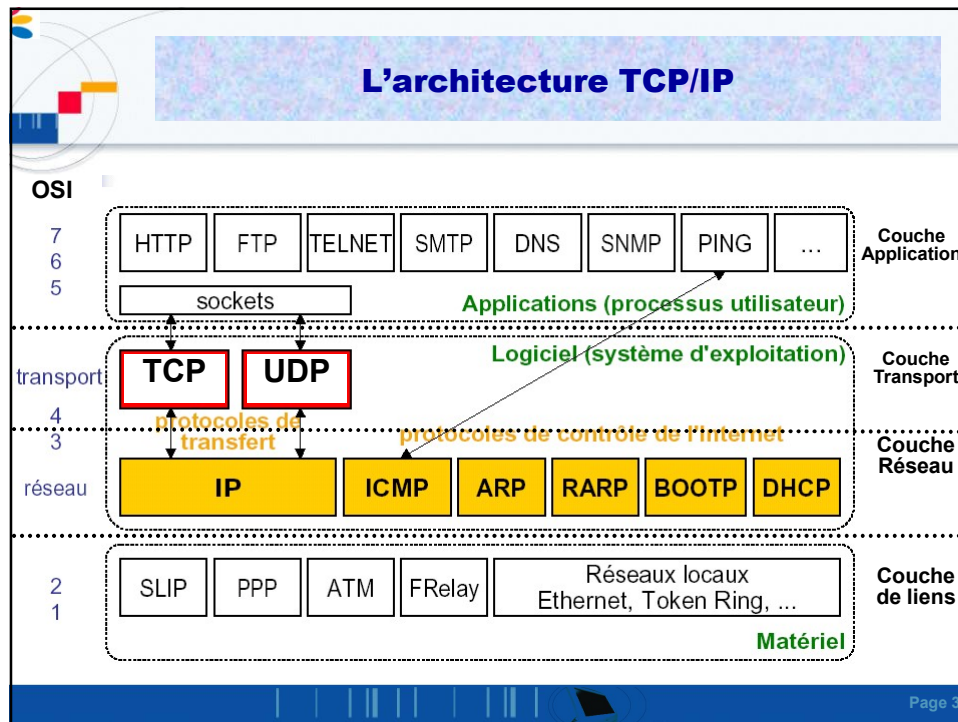
Pr. K. HOUSNI
Faculté des sciences
Université Ibn Tofail

Page 1



Chapitre VI


Architecture TCP/IP
Protocoles de base



TCP/IP Concepts de Base: L'interconnexion.

- C'est une architecture de **protocoles ouverts**, les sources (en langage C) en sont disponibles gratuitement et ont été **développées indépendamment**
 - ✓ d'une architecture particulière,
 - ✓ d'un système d'exploitation particulier,
 - ✓ d'une structure commerciale propriétaire.
- Ils sont donc théoriquement **transportables sur n'importe quel type de plate-forme**, ce qui est prouvé de nos jours.
- Les protocoles sont indépendants du support physique du réseau.
 - Cela permet à TCP/IP d'être véhiculé par des supports et des technologies aussi différents qu'une ligne série, un câble coaxial Ethernet, un réseau token-ring, une liaison radio (satellites, "wireless"), une liaison FDDI 600Mbits, une liaison par rayon laser, infrarouge, ADSL, ATM, fibre optique, ...
- Le mode d'adressage est commun à tous les utilisateurs de TCP/IP quelle que soit la plate-forme qui l'utilise.
- Les protocoles de hauts niveaux sont standardisés ce qui permet des développements largement répandus sur tous types de machines. La majeure partie des informations relatives à ces protocoles sont publiées dans les RFCs (Requests For Comments).

Page 4




Protocoles et applications

Niveau applicatif (La couche application)

La couche application est celle des programmes utilisateurs comme :

- **HTTP - HyperText Transport Protocol**
 - protocole du web
 - échange de requête/réponse entre un client et un serveur web
- **FTP - File Transfer Protocol**
 - protocole de manipulation de fichiers distants
 - transfert, suppression, création, ...
- **TELNET - TEletypewriter Network Protocol**
 - système de terminal virtuel
 - permet l'ouverture d'une session distante
- **SMTP - Simple Mail Transfer Protocol**
 - service d'envoi de courrier électronique
 - réception (POP, IMAP, IMAPS, ...)
- **DNS - Domain Name System**
 - assure la correspondance entre un nom symbolique et une adresse Internet (adresse IP)
 - bases de données réparties sur le globe
- **SNMP - Simple Network Management Protocol**
 - protocole d'administration de réseau (interrogation, configuration des équipements, ...)
- **Les sockets - interface de programmation permettant**
 - l'échange de données (via TCP ou UDP)

Page 5



Protocoles et applications

La couche transport : Protocoles de transport de données assure tout d'abord une communication de bout en bout en faisant abstraction des machines intermédiaires entre l'émetteur et le destinataire. Elle s'occupe de réguler le flux de données et assure un transport fiable (données transmises sans erreur et reçues dans l'ordre de leur émission). Dans cette couche on trouve deux protocoles :

- **TCP (Transmission Control Protocol)** : transfert fiable de données en mode connecté
- **UDP (User Datagram Protocol)** : transfert non garanti de données en mode non connecté

La couche Réseau : Protocole IP et Protocoles de contrôle de l'Internet

- **IP (Internet Protocol)** : gère la circulation des paquets à travers le réseau en assurant leur routage.
- **ICMP (Internet Control and error Message Protocol)** : assure un dialogue IP<-->IP (entre routeurs par ex.) pour signaler les congestions, synchroniser les horloges, estimer les temps de transit, ...- Utilisé par l'utilitaire **Ping** permettant de tester la présence d'une station sur le réseau
- **ARP (Address Resolution Protocol)** : protocole permettant d'associer une adresse MAC (adresse physique utilisée dans les réseaux locaux) à une adresse IP (adresse logique Internet)
- **RARP (Reverse ARP)** : permet à une station de connaître son adresse IP à partir de son adresse MAC (interrogation d'un serveur RARP)

Page 6

Protocoles et applications

- **BOOTP (Boot Protocol)** : permet à une station de connaître sa configuration réseau lors du démarrage par interrogation d'un serveur bootp ; au-dessus d'UDP (ports 67 et 68)
- **DHCP (Dynamic Host Configuration Protocol)** : extension du protocole BOOTP, meilleure gestion du plan d'adressage IP avec attribution dynamique des adresses IP pour une certaine durée (bail ou lease time) ; au-dessus d'UDP (ports 67 et 68)

La couche de liens : Interface avec le réseau
 La couche de liens est l'interface avec le réseau et est constituée d'un driver du système d'exploitation et d'une carte d'interface de l'ordinateur avec le réseau

Page 7

Protocoles et applications

- Communications sans routeur
 - Deux machines sur un même sous réseau

The diagram illustrates the TCP/IP stack for two machines, Ordinateur A and Ordinateur B, connected on the same network. The stack is shown as a series of layers connected by bidirectional arrows:

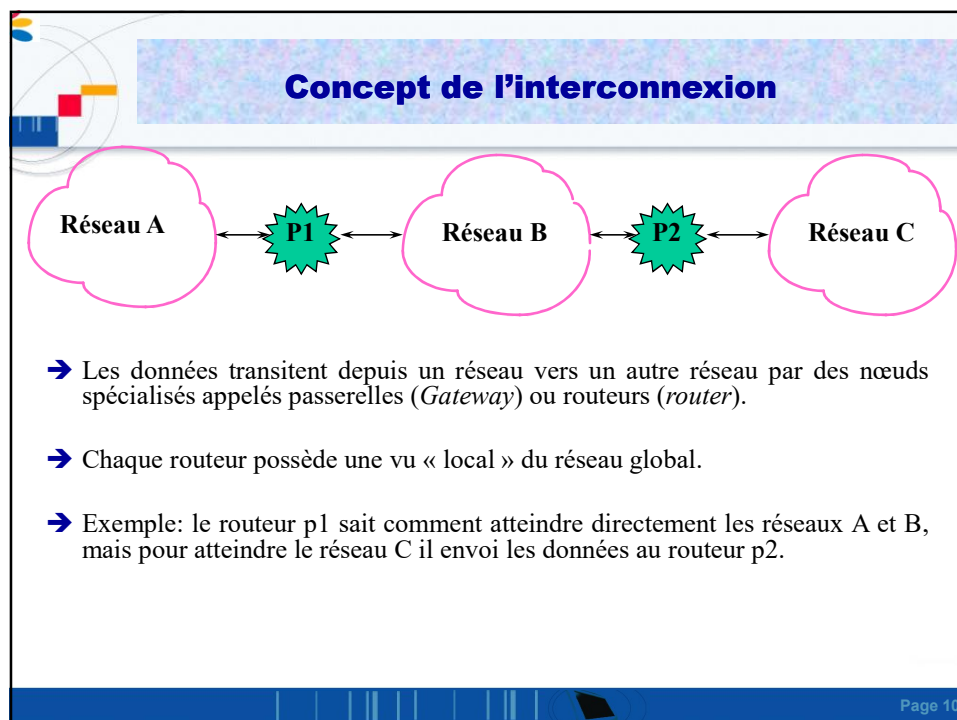
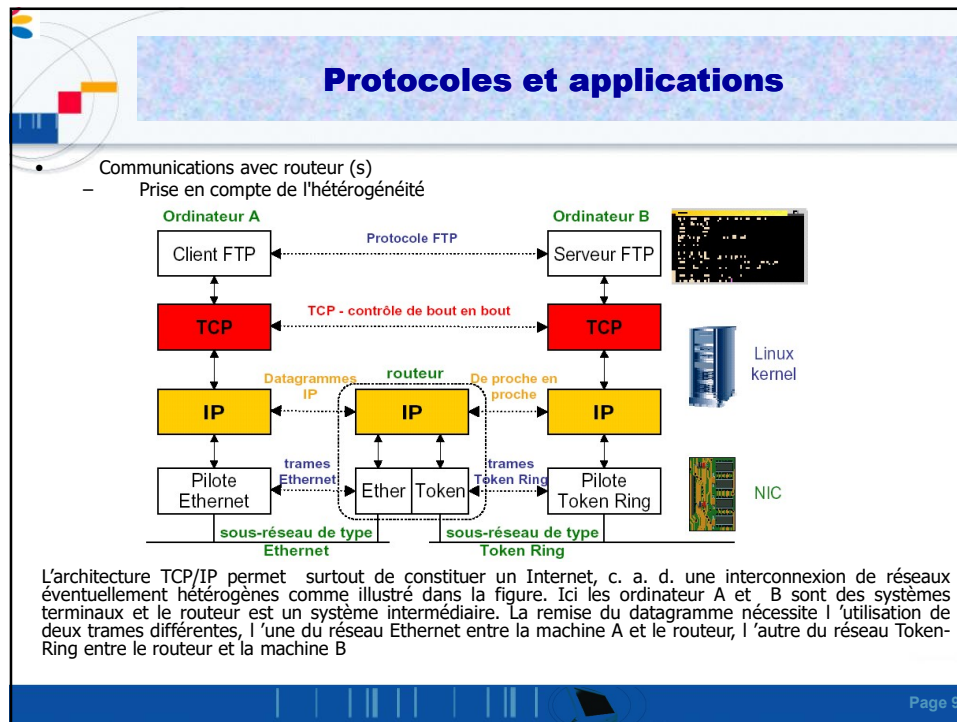
- Application Layer:** Client FTP (on Ordinateur A) and Serveur FTP (on Ordinateur B) are connected via the **Protocole FTP**.
- Transport Layer:** TCP (Transmission Control Protocol) is shown in red boxes on both machines, connected via the **Protocole TCP**.
- Network Layer:** IP (Internet Protocol) is shown in yellow boxes on both machines, connected via the **Protocole IP**.
- Link Layer:** Pilote Ethernet (Ethernet Driver) is shown in white boxes on both machines, connected via the **Protocole Ethernet**.

Additional labels and components include:

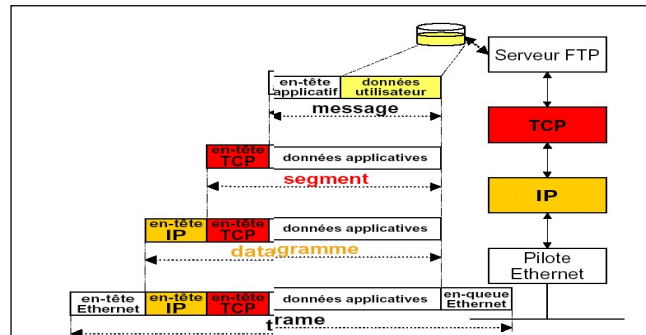
- Réseau logique IP:** A green label indicating the logical network layer.
- Sous-réseau de type Ethernet:** A green label indicating the physical network type.
- Linux kernel:** A blue server icon representing the operating system.
- NIC:** A green circuit board icon representing the Network Interface Card.

L'architecture TCP/IP permet de faire fonctionner un réseau local ; par exemple sur un réseau Ethernet reliant un ordinateur client A qui interroge un serveur FTP B

Page 8

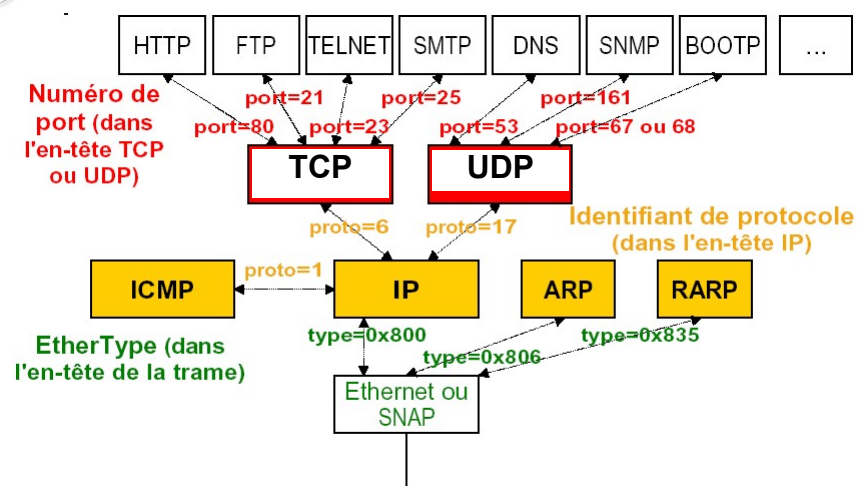



Encapsulation



Comme nous l'avons décrit avec le modèle des couches OSI, les couches TCP/IP fonctionnent par encapsulations progressives : lorsqu'une application envoie des données à l'aide de TCP/IP les données traversent de haut en bas chaque couche jusqu'à aboutir au support physique où elles sont alors émises sous forme de suite de bits. L'encapsulation consiste pour chaque couche à ajouter de l'information aux données en commençant par des en-têtes, voire en ajoutant des informations de remorque dans certains cas.

Identification des protocoles






Le protocole IP

Internet Protocol

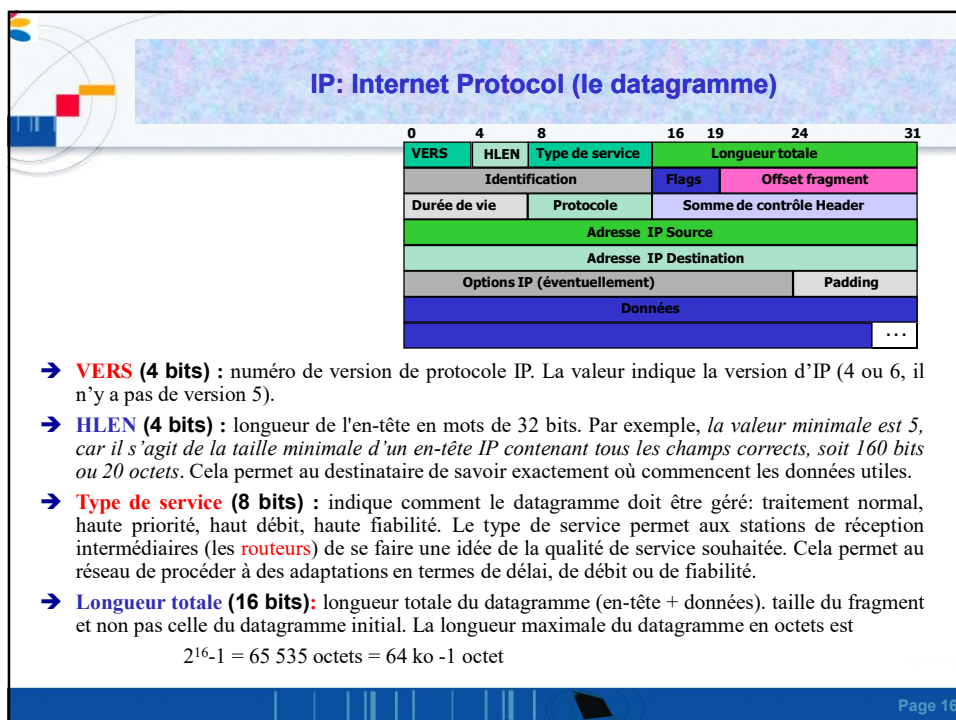
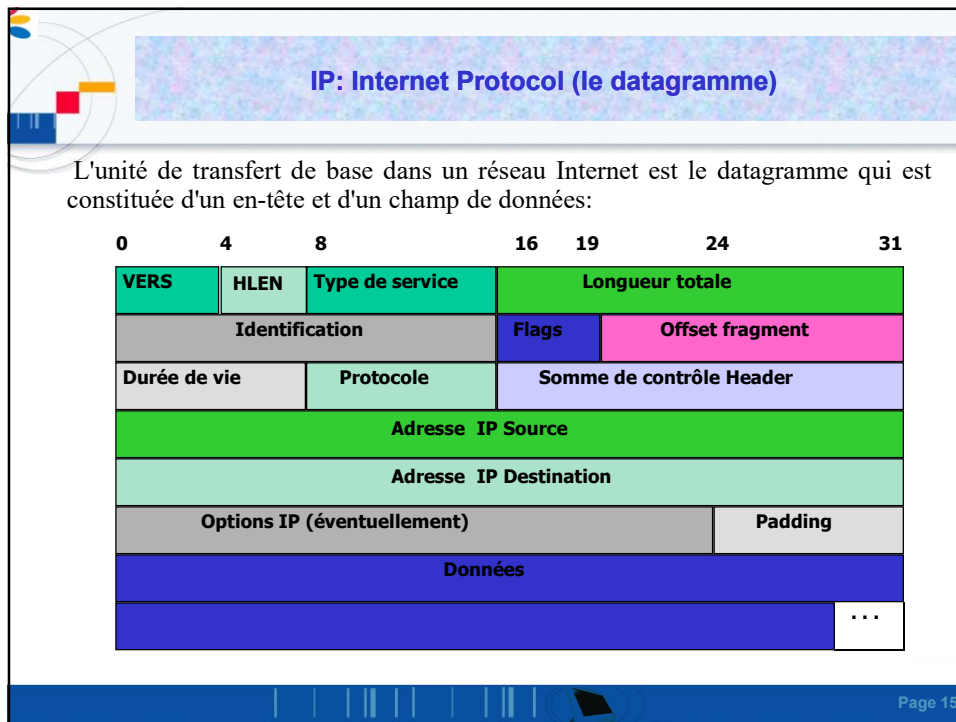
Page 13



Caractéristiques d'IP

- **Implémente la couche réseaux** par rapport au modèle OSI.
- **Définit l'adressage logique** des machines ainsi que **le routage des données** entre les nœuds.
- **C'est un protocole non fiable** car il **ne garanti pas la remise des données à la destination final.**
- **C'est un protocole sans connexion** car il n'y a pas de circuit établi au préalable et les paquets sont acheminés indépendamment les uns des autres.
- Le protocole IP définit :
 - **L'unité de donnée transférée dans les interconnexions (le Datagramme).**
 - **La fonction de routage.**

Page 14



IP: Internet Protocol (le datagramme)

0		4		8		16		19		24		31	
VERS		HLEN		Type de service		Longueur totale							
Identification						Flags		Offset fragment					
Durée de vie				Protocole		Somme de contrôle Header							
Adresse IP Source													
Adresse IP Destination													
Options IP (éventuellement)										Padding			
Données													
...													

- **Offset fragment, Flags, Identification:** informations utilisées par IP pour la reconstitution d'un paquet IP fragmenté.
- **IDENTIFICATION (16 bits):** entier qui identifie le datagramme initial (utilisé pour la reconstitution à partir des fragments qui ont tous la même valeur).
- **FLAGS (3 bits):**
 - le premier bit est inutilisé
 - le deuxième bit DF (don't fragment) permet d'interdire ou d'autoriser la fragmentation. positionné à 1, il est interdit de fragmenter ce datagramme IP.
 - le troisième bit MF (more fragment) est utilisé lors de la fragmentation : il indique si le fragment est le dernier fragment du datagramme (MF=0) ou non (MF=1).
- **Offset fragment (13 bits):** Lorsqu'un datagramme est fragmenté, il est nécessaire de réassembler les fragments dans le bon ordre. Le nombre d'offset numérote les fragments de manière à pouvoir être réassemblés correctement.

Page 17

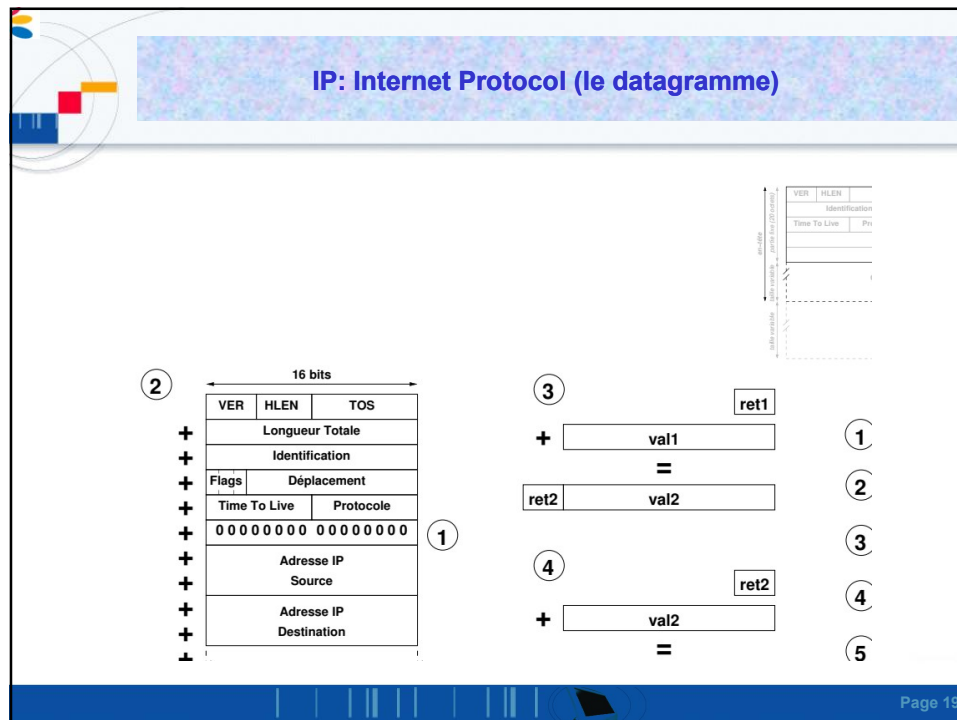
IP: Internet Protocol (le datagramme)

0		4		8		16		19		24		31	
VERS		HLEN		Type de service		Longueur totale							
Identification						Flags		Offset fragment					
Durée de vie				Protocole		Somme de contrôle Header							
Adresse IP Source													
Adresse IP Destination													
Options IP (éventuellement)										Padding			
Données													
...													

- **Durée de vie (8 bits) :** Ce champ indique en **second**, la durée maximale de transit du datagramme sur Internet. Chaque passerelle diminue la valeur du TTL d'au moins 1 avant de le router.
- **Protocole (8 bits):** Cela indique quel type de protocole est encapsulé dans le datagramme IP. Certaines des valeurs communes incluent:

6 : TCP
17 : UDP
1 : ICMP
...
- **Somme de contrôle de l'en-tête (16 bits):** Ce champ permet de détecter les erreurs survenant dans l'en-tête du datagramme, et par conséquent l'intégrité du datagramme. Le total de contrôle d'IP porte sur l'en-tête du datagramme et non sur les données véhiculées.
- **OPTIONS :** Le champ OPTIONS est facultatif et de longueur variable. Les options concernent essentiellement des fonctionnalités de mise au point. Une option est définie par un champ octet.

Page 18



L'adressage IP

- **But** : Fournir un service de communication universel permettant à toute machine de communiquer avec toute autre machine de l'interconnexion.
- Une machine doit être accessible aussi bien par des humains que par d'autres machines
- Une machine doit être identifiée par :
 - Un nom (mnémotechnique pour les utilisateurs),
 - Une adresse qui doit être un identificateur universel de la machine,
 - Une route précisant comment la machine peut être atteinte.
- **Solution** : Un adressage binaire compact assurant un routage efficace
- Utilisation de noms pour identifier des machines (réalisée à un autre niveau que les protocoles de base)
- **Les classes d'adressage**
 - Une adresse = 32 bits dite « Internet Address" ou "IP Address" constituée d'une paire (netid, hostid) où netid identifie un réseau et hostid identifie une machine sur ce réseau.
 - Cette paire est structurée de manière à définir cinq classes d'adresse.

Page 20

L'adressage IP

Structure d'une adresse IP:

0
32

Identifiant Réseau	Identifiant Machine
---------------------------	----------------------------

- La partie réseau: est un identifiant commun pour un groupe de machines connectées sur le même réseau physique et/ou logique.
- La partie host: identifie une machine donnée dans le réseau physique et/ou logique, identifié par l'identifiant réseau.

Cette paire est structure d'une manière à définir 5 classes d'adresses IP.

L'adressage IP

	0	8	16	24	31
<u>Classe A</u>	0	Net-id		Host-id	
<u>Classe B</u>	1	0	Net-id		Host-id
<u>Classe C</u>	1	1	0	Net-id	
<u>Classe D</u>	1	1	1	0	Multicast
<u>Classe E</u>	1	1	1	1	0
	Réservé				

Page 22

L'adressage IP

→ Notation décimale:

L'interface utilisateur concernant les adresses IP consiste en la notation de quatre entiers décimaux séparés par un point, chaque entier représentant un octet de l'adresse IP :

10000000 00001010 00000010 00011110 est écrite :

128.10.2.30

Les adresses réseaux sont distribuées par un organisme international à but non lucratif : **ICANN** (Internet Corporation for Assigned Names and Numbers) puis décentralisé au niveau de chaque pays.

Page 23

L'adressage IP

L'originalité de ce format d'adressage réside dans l'association de l'identification du réseau avec l'identification de l'hôte.

- La partie réseau est commune à l'ensemble des hôtes d'un même réseau,
- La partie hôte est unique et désigne une seule interface physique.

Le masque de réseau:

Le masque de réseau sert à séparer les parties réseau et hôte d'une adresse. On retrouve l'adresse du réseau en effectuant un **ET logique** bit à bit entre une adresse complète et le masque de réseau.

L'adresse de diffusion:

Chaque réseau possède une adresse particulière dite de **diffusion**. Tous les hôtes du réseau « écoutent » cette adresse en plus de la leur. Certaines informations telles que le routage ou les messages d'alerte sont utiles à l'ensemble des hôtes du réseau. Il existe deux définitions d'adresses de diffusion : la plus petite (192.168.100.0 dans notre exemple) ou la plus grande (192.168.100.255). La convention sur l'Internet veut que l'on utilise l'adresse la plus grande comme adresse de diffusion.

Page 24

L'adressage IP

Adresses particulières: ip=192.20.1.2 /255.255.255.0

- **Adresse réseau:** adresse IP dont la partie hostid ne comprend que des zéros : 192.20.1.0 désigne le réseau de classe C
- **Adresse machine locale:** adresse IP dont le champ réseau (netid) ne contient que des zéros: 0.0.0.2
 - ▶ **hostid**= 0 (=> tout à zéro), l'adresse est utilisée au démarrage du système afin de connaître son adresse IP (Cf RARP/DHCP).
- **Adresse de diffusion limitée:** netid ne contient que des 1 : l'adresse constituée concerne uniquement le réseau physique associé. (255.255.255.255).
- **L'adresse de diffusion dirigée:** netid est une adresse réseau spécifique => la diffusion concerne toutes les machines situées sur le réseau spécifié : 192.20.1.255 désigne toutes les machines du réseau 192.20.1.0
- **Adresse de boucle locale:** l'adresse réseau 127.0.0.1 (localhost) est réservée pour la désignation de la machine locale, c'est à dire la communication intra-machine. Elle permet de tester la pile TCP/IP locale sans passer par une interface matérielle.

Page 25

L'adressage IP

0	8	16	24	31	
Tout à zéro					désigne la machine courante
Tout à zéro			Host-id		machine Host-id sur le réseau courant
Tout à un					diffusion limitée sur le réseau courant
Net-id			Tout à un		diffusion dirigée sur le réseau Net-id
127	N'importe quoi (souvent 1)				boucle locale

Page 26

L'adressage IP

→ **Notion d'Interface :**

Une adresse IP => une interface physique => une connexion réseau.
 A une machine, est associé un certain nombre N d'adresses IP.
 Si $N > 1$ la machine (ou passerelle) est multi-domiciliée.

La passerelle est multi-domiciliée:
 interface 1 : Ethernet 193.49.60.1
 interface 2 : Token Ring 192.100.1.1

Page 27

L'adressage IP: Notion du Masque

→ **Le masque réseau** est un entier sur 32 bits, constitué d'une suite de 1 suivi par une suite de 0 :

11111111 11111111 11111111 00000000

→ **Le masque** sert à identifier l'adresse Réseau qui correspond à une adresse IP donnée.

→ En appliquant un and logique entre une adresse IP quelconque et le masque associé on obtient la partie réseau de l'adresse (l'adresse réseau).

@ip-machine AND Masque = @network

▶ Par exemple le masque associé à une adresse de classe A est:

1111 1111 0000 0000 0000 0000 0000 0000

→ Ce qui correspond en notation décimale : 255.0.0.0

→ **Notation CIDR** (Classless Inter-Domain Routing) : l'adresse est suivie d'un chiffre indiquant le nombre de bits à "1" du masque de sous réseau. L'adresse et le masque sont séparés par « / ».

▶ Exemple : 147.128.25.58/24

Page 28

L'adressage IP: Notion du Masque

→ **Autre Notation pour le Masque:** Puisque les masques ne représentent qu'un certain nombre de 1 complétés par des 0 (pour obtenir 32 bits), la seule information intéressante est ce nombre de 1.

- Une autre notation consiste à faire suivre une adresse donnée par le nombre de bits égal 1 dans le masque.

192.168.6.0

24 bits

255.255.255.0

- Dans l'exemple, on parle du réseau 192.168.6.0 avec le masque de sous réseau 255.255.255.0. Il est noté plus simplement 192.168.6.0/24
- Les masques associés aux 3 classes d'adresses IP sont respectivement:
 - Pour la classe A: 255.0.0.0 ou bien /8
 - Pour la classe B: 255.255.0.0 ou bien /16
 - Pour la classe C: 255.255.255.0 ou bien /24

Page 29

L'adressage IP: Notion du Masque

- Résumé:


Classe d'adresse	Nombre d'octets pour la partie réseau	Nombre d'octets pour la partie host	Nombre d'adresses valides par réseau
Classe A	1 octet (8 bits)	3 octets (24 bits)	$2^{24} - 2$
Classe B	2 octets (16 bits)	2 octets (16 bits)	$2^{16} - 2$
Classe C	3 octets (24 bits)	1 octet (8 bits)	$2^8 - 2$

Classe	Adresses réseaux valides	Nombre d'adresses réseau pour cette classe
Classe A	1.0.0.0 à 126.0.0.0	2^7
Classe B	128.0.0.0 à 191.254.0.0	2^{14}
Classe C	192.0.0.0 à 223.255.254.0	2^{21}

Page 30

L'adressage IP: Limites de l'adressage IP classique

Problèmes (fin des années 80):

- ▶ Problèmes d'allocation des adresses:
 - 1- épuisement de la classe B : 
 - 2- utilisation rapide des classes C
 - 3- accroissement des tables de routages

Solution =>

- *Allouer exactement la quantité nécessaire*
 - sous adressage
 - super adressage (ou bien CIDR et adressage privé)
- *Agrégation d'adresses dans les tables de routage*

Page 31

L'adressage IP: Le sous-adressage (subnetting)

- ➔ Le sous-adressage est une extension du plan d'adressage initial.
- ➔ Devant la croissance du nombre de réseaux de l'Internet, il a été introduit afin de limiter la consommation d'adresses IP .
- **Principes:**
 - A l'intérieur d'une entité associée à une adresse IP de classe A, B ou C, plusieurs réseaux physiques partagent cette adresse IP.
 - On dit alors que ces réseaux physiques sont des sous-réseaux (*Subnet*) du réseau d'adresse IP initial.
 - Le principe est qu'une **adresse de réseau d'une classe A, B ou C peut être découpée en plusieurs sous-réseaux.**

Page 32

L'adressage IP: Le sous-adressage (subnetting)

→ Réseau vu de l'extérieur:

Partie Réseau	Partie Locale
---------------	---------------

- En interne, découpage en pseudo classes:

Partie Réseau	Réseau sous réseau	Identifiant Machine
---------------	--------------------	---------------------

Une adresse IP comporte désormais 3 parties:

- **l'identifiant réseau «Partie Réseau» (NetId)** : il a la même signification que celui du plan d'adressage initial.
- **l'identifiant du sous-réseau** : identifie un segment ou un sous-réseaux.
- **l'identifiant de la machine** : identifie la machine sur le segment ou le sous-réseaux.
- La somme des longueurs de l'identifiant sous-réseau et l'identifiant de la machine doit toujours donner la longueur de la partie hôte dans l'adressage classique
- Les champs «sous Réseau» et «identifiant Machine» sont de taille variable.

Page 33

L'adressage IP: Le sous-adressage (subnetting)

Le sous adressage avec les différentes classes d'adresses.

8	24-N	N	
Réseau	Sous-réseau	Hôte	Classe A
16	16-N	N	
Réseau	Sous-réseau	Hôte	Classe B
24	8-N	N	
Réseau	Sous-réseau	Hôte	Classe C

Page 34

L'adressage IP: Le sous-adressage (subnetting)

Calcul des adresses avec le sous adressage:

Le sous-adressage consiste à déterminer :

- Le masque adéquat pour le sous-réseau.
- Le calcul des sous-réseaux correspondants:
 - Calculer l'adresse du sous-réseau.
 - Calculer l'adresse de diffusion correspondante.
 - Déterminer les adresses utilisables.
- Deux méthodes existent pour le calcul:
 - Le calcul binaire.
 - Le calcul décimal.

Page 35

L'adressage IP: Le sous-adressage (subnetting)

Algorithme de calcul des sous-réseaux:

- Déterminer le nombre de bits dans la partie sous-réseau qui permet d'avoir le nombre de sous-réseaux voulu. (**avec n bits on peut créer 2^n sous réseaux**)
- Déterminer le nombre de bits dans la partie machine qui permet d'avoir le nombre de machines. (**avec m bits on peut avoir $2^m - 2$ machines par sous réseau**)
- Déterminer le masque qui va être utilisé pour ses sous-réseaux.
- Écrire sous forme binaire l'adresse IP initial.
- Écrire sous forme binaire le masque initial.
- Écrire sous forme binaire le nouveau masque.
- Dédire les adresses de sous-réseaux en incrémentant la partie de sous-réseau dans l'adresse initial.
- Dédire l'adresse du broadcast en remplaçant par des 1 tous les bits de la partie machine de l'adresse IP.
- Enfin déduire les adresses utilisables.

Page 36

L'adressage IP: Adressage Privé et NAT

- Adresses privées,
- des adresses qui ne seront jamais attribuées (adresses illégales) et qui ne sont pas routables sur l'Internet,
- Ils peuvent être utilisés si :
 - ▶ Le réseau n'est pas connecté à Internet.
 - ▶ Sur un réseau avec un Firewall.

il sera dans tous les cas impossible de connecter directement à l'Internet un tel réseau (il faudra utiliser un traducteur d'adresse -NAT-, ou un proxy)

- Si une entreprise qui utilise des adresses privées souhaite tout de même disposer d'une connexion à l'Internet, il faut demander une adresse publique faire des conversions adresse privée <--> adresse publique.

- ▶ classe A : 10/8 : 10.0.0.0 → 10.255.255.255.
- ▶ classe B : 172.16/12 : 172.16.0.0 → 172.31.255.255.
- ▶ classe C : 192.168/16 : 192.168.0.0 → 192.168.255.255.

- Ces adresses ne doivent jamais être annoncées au niveau des tables de routage vers l'Internet.

Page 37

L'adressage IP: Adressage Privé et NAT

- **NAT (RFC 3022) - Network Address Translator**
 - mise en correspondance d'une adresse privée et d'une adresse publique
 - traduction statique ou dynamique (lors de la connexion)
 - une solution au manque d'adresses IP publiques :
 - quelques adresses IP publiques pour beaucoup d'adresses IP privées mais le NAT est coûteux en performance

The diagram illustrates a NAT setup. A Host with IP 10.0.0.1 is connected to a Private Network. The Private Network is connected to a Router + NAT with IP 150.150.0.1. The Router + NAT is connected to the Internet. Below the diagram, two tables show the translation of IP addresses.

Source IP	Destination IP	Source IP	Des
...	10.0.0.1	200.100.10.1	...

Changes according to NAT

Source IP	Destination IP	Source IP	Des
...	150.150.0.1	200	...

Page 38

La fragmentation des datagrammes IP

- Quand un datagramme est fragmenté, il n'est rassemblé que par la couche IP destinatrice finale. Cela implique trois remarques :
 - Cette opération est absolument transparente pour les couches de transport qui utilisent IP.
 - Chaque fragment est acheminé de manière indépendante.
 - Un temporisateur de réassemblage sur le destinataire est armé quand le premier fragment arrive.
- La perte d'un fragment IP provoque la retransmission de l'ensemble du datagramme.

Page 39

Le sous adressage

Quelque rappel sur le calcul binaire:

Une adresse IP est un entier sur 32 bit, et donc elle est décomposé en une somme de puissances de 2:

1	1	0	1	1	0	1	1
---	---	---	---	---	---	---	---

$2^0 + 2^1 + 2^3 + 2^4 + 2^6 + 2^7 = 219$

Le nombre de réseaux possible par adresse = $2^{\text{nombre de bits de la partie réseau}}$

Le nombre de machines par réseau = $2^{\text{nombre de bits de la partie hôte}} - 2$

Page 40

Le sous adressage

→ Les masques qu'on peut utiliser sont donc:

Dernier octet du Masque	Écriture binaire
0	0 0 0 0 0 0 0 0
128	1 0 0 0 0 0 0 0
192	1 1 0 0 0 0 0 0
224	1 1 1 0 0 0 0 0
240	1 1 1 1 0 0 0 0
248	1 1 1 1 1 0 0 0
252	1 1 1 1 1 1 0 0
254	1 1 1 1 1 1 1 0
255	1 1 1 1 1 1 1 1

Page 41

Le sous adressage

- Le nombre de réseau doit être une puissance de 2, or $8 = 2^3$ donc nous avons 3 bits dans la partie sous-réseau.
- Le nombre de machines doit être une puissance de 2 également, $32 = 2^5$, donc nous avons 5 bits dans la partie hôte.

Page 42

Le sous adressage

	Notation décimal	0	24	27	31
Adresse initiale	192.168.64.0	1100 0000 1010 1000 010 0 0000		0 0 0	0 0 0 0 0
Masque	255.255.255.0	1111 1111 1111 1111 1111 1111		0 0 0	0 0 0 0 0
Nouveau Masque	255.255.255.224	1111 1111 1111 1111 1111 1111		1 1 1	0 0 0 0 0
Réseau N°=1	192.168.64.0	1100 0000 1010 1000 010 0 0000		0 0 0	0 0 0 0 0
Réseau N°=2	192.168.64.32	1100 0000 1010 1000 010 0 0000		0 0 1	0 0 0 0 0
Réseau N°=3	192.168.64.64	1100 0000 1010 1000 010 0 0000		0 1 0	0 0 0 0 0
Réseau N°=4	192.168.64.96	1100 0000 1010 1000 010 0 0000		0 1 1	0 0 0 0 0
Réseau N°=5	192.168.64.128	1100 0000 1010 1000 010 0 0000		1 0 0	0 0 0 0 0
Réseau N°=6	192.168.64.160	1100 0000 1010 1000 010 0 0000		1 0 1	0 0 0 0 0
Réseau N°=7	192.168.64.192	1100 0000 1010 1000 010 0 0000		1 1 0	0 0 0 0 0
Réseau N°=8	192.168.64.224	1100 0000 1010 1000 010 0 0000		1 1 1	0 0 0 0 0

Page 43

Page 43

Le sous adressage			
Adresse réseau	Adresse broadcast	Adresses utilisables	
192.168.64.000 00000 (192.168.64.0)	192.168.64.000 11111 (192.168.64.31)	192.168.64.000 0001 192.168.64.1	192.168.64.000 1110 192.168.64.30
192.168.64.001 00000 (192.168.64.32)	192.168.64.001 11111 (192.168.64.63)	192.168.64.001 0001 192.168.64.33	192.168.64.001 1110 192.168.64.62
192.168.64.010 00000 (192.168.64.64)	192.168.64.010 11111 (192.168.64.95)	192.168.64.010 0001 192.168.64.65	192.168.64.010 1110 192.168.64.96
192.168.64.011 00000 (192.168.64.96)	192.168.64.011 11111 (192.168.64.127)	192.168.64.011 0001 192.168.64.97	192.168.64.011 1110 192.168.64.126
192.168.64.100 00000 (192.168.64.128)	192.168.64.100 11111 (192.168.64.159)	192.168.64.100 0001 192.168.64.129	192.168.64.100 1110 192.168.64.158
192.168.64.101 00000 (192.168.64.160)	192.168.64.101 11111 (192.168.64.191)	192.168.64.101 0001 192.168.64.161	192.168.64.101 1110 192.168.64.190
192.168.64.110 00000 (192.168.64.192)	192.168.64.110 11111 (192.168.64.223)	192.168.64.110 0001 192.168.64.193	192.168.64.110 1110 192.168.64.222
192.168.64.111 00000 (192.168.64.224)	192.168.64.111 11111 (192.168.64.255)	192.168.64.111 0001 192.168.64.225	192.168.64.111 1110 192.168.64.254

Page 44

Le sous adressage

Calcul décimal:

- Déterminer l'octet qui va contenir le numéro du sous-réseau.
- Déterminer le nombre de bits dans la partie machine N, ce qui nous intéresse c'est 2^N qui est le nombre d'adresses possibles dans le sous-réseau (contenant l'adresse réseau est l'adresse de broadcast). Ce nombre est appelé **multiplicateur de sous-réseau**.
- Déterminer la première adresse de sous-réseaux (dont la partie sous-réseau doit être égale à 0).
- Pour obtenir la prochaine adresse IP de sous-réseau incrémenter de 2^N la première adresse.
- Pour obtenir la prochaine adresse augmenter de 2^N la dernière adresse obtenue et ainsi de suite.


Page 45

Le sous adressage

N=5, le nombre d'adresses possible= $2^5=32$ (nombre de sous réseaux est $2^{(8-5)}=8$)

Adresse réseau initial	192.168.64.0	
Masque initial	255.255.255.0	
Nouveau Masque	255.255.255.224	
Première adresse réseau	192.168.64.0 + 0	192.168.64.0
2ème adresse réseau	192.168.64.0 + 32	192.168.64.16
3ème adresse réseau	192.168.64.32 + 32	192.168.64.64
4ème adresse réseau	192.168.64.64 + 32	192.168.64.96
5ème adresse réseau	192.168.64.96 + 32	192.168.64.128
6ème adresse réseau	192.168.64.128 + 32	192.168.64.160
7ème adresse réseau	192.168.64.160 + 32	192.168.64.192
8ème adresse réseau	192.168.64.192 + 32	192.168.64.224

Page 46




Le sous adressage

Calcule de l'adresse de diffusion et les adresses utilisables:

L'adresse de broadcast = adresse sous-réseau + $2^N - 1$
 Les adresses utilisables = adresse sous-réseau + 1 jusqu'à adresse broadcast - 1

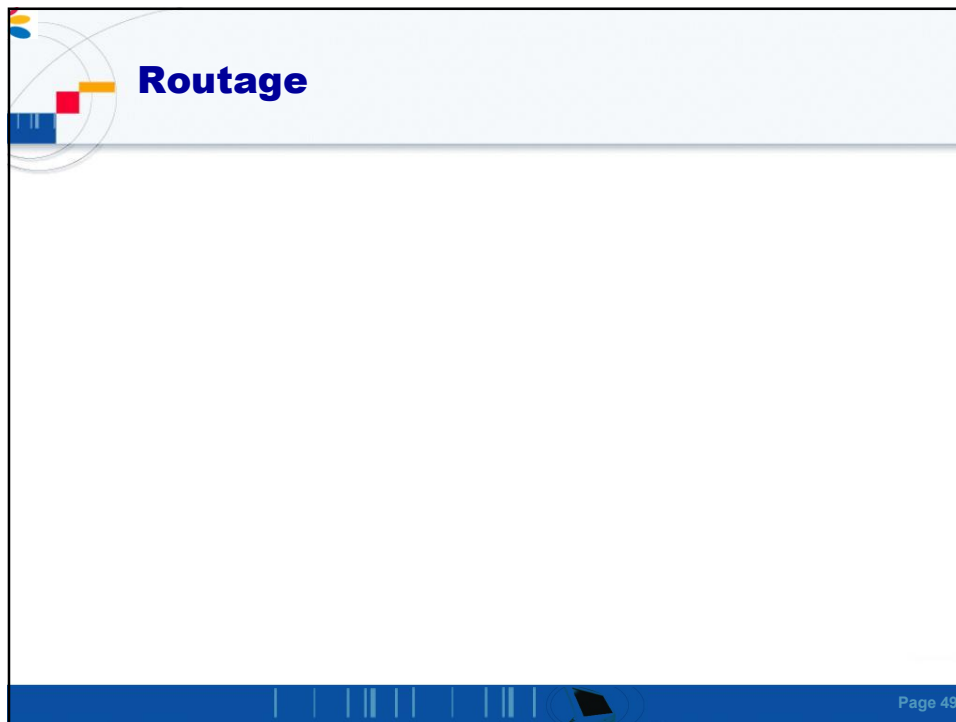
Page 47



Le sous adressage

Adresse sous-réseau	Adresse broadcast	Les adresses valides	
192.168.64.0	192.168.64.15	192.168.64.1	192.168.64.30
192.168.64.32	192.168.64.31	192.168.64.33	192.168.64.62
192.168.64.64	192.168.64.95	192.168.64.65	192.168.64.94
192.168.64.96	192.168.64.127	192.168.64.49	192.168.64.62
192.168.64.128	192.168.64.159	192.168.64.129	192.168.64.158
192.168.64.160	192.168.64.191	192.168.64.161	192.168.64.190
192.168.64.192	192.168.64.223	192.168.64.193	192.168.64.222
192.168.64.224	192.168.64.255	192.168.64.241	192.168.64.254


Page 48



Qu'est ce que le routage ?

- Processus par lequel un élément (courrier, appels téléphoniques, trains, paquets IP, ...) va être acheminé d'un endroit à un autre.
- Un élément faisant du routage doit connaître :
 - ✓ La destination,
 - ✓ De quelle source il peut apprendre les chemins d'accès à la destination voulue,
 - ✓ Les itinéraires possibles pour atteindre la destination,
 - ✓ Le(s) meilleur(s) itinéraire(s) pour atteindre la destination,
 - ✓ Un moyen d'actualiser les itinéraires.


Page 50



Pourquoi faire du routage sur un réseau ?

- **Un équipement sur un réseau local**
 - ✓ Peut atteindre directement les machines sur le même segment sans routage (ARP),
 - ✓ Ne peut pas atteindre les équipements sur un autre réseau (ou sous-réseau) sans un intermédiaire.
- **Qui doit faire du routage sur un réseau ?**
 - ✓ Équipement connecté à 2 réseaux ou sous réseaux au moins,
 - ☐ Station de travail avec 2 interfaces réseau au moins,
 - ☐ Routeur (CISCO, Juniper, BayNetworks, ...)


Page 51



PRINCIPES DU ROUTAGE IP

- Routage IP basé uniquement sur l'adresse du destinataire
- Chaque équipement du réseau sait atteindre un équipement d'un autre réseau, s'il existe au moins un équipement de routage pour acheminer les paquets à l'extérieur du réseau local.
- Les informations de routage sont mémorisées dans la table de routage des équipements (routeurs).
- Cette table doit être périodiquement mise à jour
 - ✓ Manuellement : routage STATIQUE
 - ✓ Automatiquement : routage DYNAMIQUE
- Le routage s'effectue sur deux opérations:
 - ✓ La sélection de la meilleure voie,
 - ✓ La commutation du paquet sur l'interface appropriée.


Page 52



Le routage IP

- **Routeur :**
 - passerelle entre sous-réseaux
 - une adresse IP par interface (par sous-réseau)
 - communications à l'intérieur d'un même sous-réseau se fait sans passer par un routeur
 - acheminement à partir de l'@ destination (& logique avec le netmask de chaque entrée de la table de routage)
- **Mise à jour de la table de routage :**
 - **Manuelle** = routage statique
 - commande "route" des stations unix
 - langage de commande des routeurs (ip route ...)
 - **Automatique** = routage dynamique
 - processus sur les stations et les routeurs
 - échanges d'informations de routage : protocoles de routage

Page 53



ROUTAGE IP STATIQUE

Avantages d'un routage statique

- ✓ Sécurité par masquage de certaines parties d'un interréseau
- ✓ Moins de surcharge par rapport au routage dynamique.


ip route 172.16.1.0 255.255.255.0 172.16.2.1 – STATIQUE

ip route 0.0.0.0 0.0.0.0 172.16.3.1 - DEFAULT

Route par défaut

- Facilite la circulation des données sur un réseau de grande taille,
- Pour atteindre une destination inconnue.
- utilisée si le prochain saut ne figure pas explicitement dans la table de routage.

Page 54



ROUTAGE IP STATIQUE

Configuration du routeur Cisco


- ❑ Configuration des interfaces d'un router
 - ✓ conf t
 - ✓ interface e0/0
 - ✓ ip address n.n.n.n m.m.m.m

Ajout de la route par défaut sur le PC


- ✓ route add default g.g.g.g

Afficher la table routage

- ✓ netstat -rn
- ✓ route get a.a.a.a (pour afficher la route par défaut)




Page 55



Routage dynamique

le routage dynamique permet d'avoir une plus grande flexibilité pour l'administrateur réseau, en cas de panne d'un lien, le calcul pour trouver un lien de secours se fera automatiquement entre les routeurs mais sa mise en œuvre est un peu plus complexe.



Page 56

Routage dynamique - Le protocole RIP

- ❑ Le protocole de routage RIP fait partie des protocoles de routage de vecteur de distance.
- ❑ Sa distance administrative est égal à 120 (La distance administrative définit la fiabilité d'un protocole de routage)
- ❑ La métrique utilisée est le nombre de saut (1 routeur = 1 saut)
- ❑ Le nombre de saut maximum est de 15, à partir de 16 routeurs le paquet est perdu.
- ❑ Trois instances de temporisation
 - ✓ Mise à jour de la table de routage toutes les 30 secondes
 - ✓ Temporisation d'invalidation = 180 secondes sans nouvelle de cette route, le routeur marque le routeur de destination injoignable
 - ✓ Temporisation d'effacement = 240 secondes sans nouvelle de la route injoignable, le routeur l'efface de sa table de routage au bout de 240s.
- ❑ Envoi ses mises de routage sur toutes les interfaces du routeur par défaut, et envoi la totalité de sa table de routage

Page 57

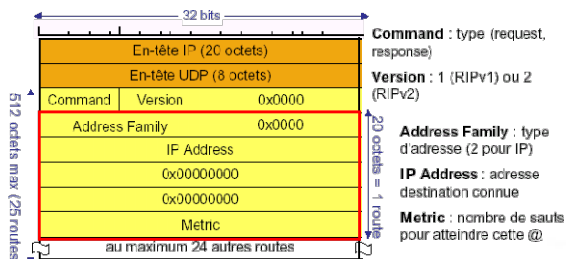
Le routage IP: le routage RIP

Principe:

- Un nœud construit sa table de routage en fonction des vecteurs de distance reçus de ses voisins,
- distance = nombre de sauts (entre 1 et 15), 16 = valeur maximum (représente l'infini),
- utilisable uniquement à l'intérieur de domaines peu étendus,
- Le routeur diffuse toutes les 30 secondes un message RIP à ses voisins contenant la liste des réseaux qu'il peut atteindre avec leur distance,
- si aucun message pendant 180s, route inaccessible (d=16)
- Implantation : sous Unix ou matériel propriétaire (Cisco, ...)

Message RIPv1

Encapsulé dans un datagramme UDP (port 520)



Page 58

Routage dynamique Protocole RIP v2

```

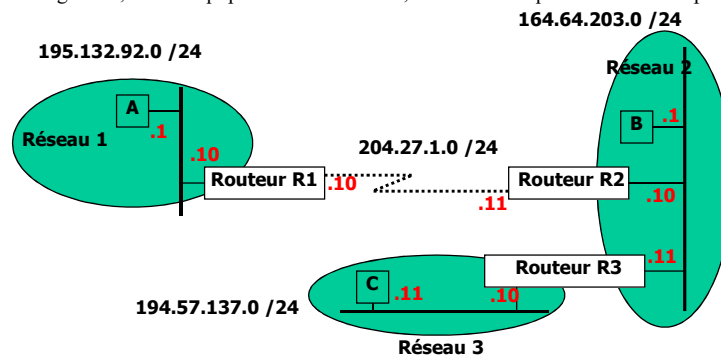
R1(config)#router rip // activation du processus RIP
R1(config-router)#version 2 // utilisation de la version 2 de RIP
R1(config-router)#no auto-summary // désactivation de
                                   // l'agrégation de routes
R1(config-router)#network 192.168.3.0 //déclaration d'un
                                   //réseau
R1(config-router)#network 10.1.1.0
Le Mans(config-router)#network 10.1.2.0
R1(config-router)#exit
  
```

Page 59

Le routage IP

Routage statique:

- La commande route permet d'indiquer une route :
 - vers un réseau (net) ou vers un équipement (host)
 - ou une route par défaut (default)
- Syntaxe :
 - route add |delete [net|host] destination |default gateway metric
- En général, sur les équipements non routeur, on définit uniquement une route par défaut



Page 60

Le routage IP: le routage RIP

- Avantages:
 - très utilisé et très répandu sur tous les équipements,
 - s'adapte automatiquement (panne, ajout de réseau, ...).
- Désavantages:
 - la distance ne tient pas compte de la charge, du débit, du coût des lignes, ...
 - distance maximale = 15,
 - trafic important (toutes les 30s) + temps de convergence,
 - pas d'authentification des messages (attaques de routeurs en générant des "faux" messages RIP)
- Conclusion:
 - utiliser RIP sur un petit réseau que l'on contrôle est très efficace mais pas adapté aux grands domaines.
- RIPv2:
 - permet le routage des sous-réseaux (véhicule le netmask dans le vecteur de distance)
 - possibilité d'authentification (cryptée ou non) des messages.

Page 61

Le protocole ARP: Address Resolution Protocol

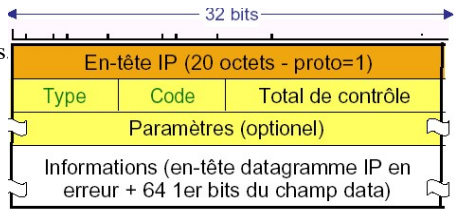
- Le besoin:
 - La communication entre machines ne peut s'effectuer qu'à travers l'interface physique
 - Les applicatifs ne connaissant que des adresses IP, comment établir le lien adresse IP / adresse physique?
- La solution : ARP
 - Mise en place dans TCP/IP d'un protocole de bas niveau appelé Address Resolution Protocol (ARP)
 - Rôle de ARP : fournir à une machine donnée l'adresse physique d'une autre machine située sur le même réseau à partir de l'adresse IP de la machine destinatrice
- La technique :
 - Diffusion d'adresses sur le réseau physique
 - La machine d'adresse IP émet un message contenant son adresse physique
 - Les machines non concernées ne répondent pas
 - Gestion cache pour ne pas effectuer de requête ARP à chaque émission
- L'association **adresse physique - adresse IP** de l'émetteur est incluse dans la requête ARP de manière à ce que les récepteurs enregistrent l'association dans leur propre mémoire cache

Page 62

Le protocole ICMP

Le besoin:

- Le **protocole ICMP** (Internet control message Protocol) permet d'envoyer des messages de **contrôle**, de **diagnostique** ou d'**erreur** vers d'autres machines ou passerelles.
- ICMP rapporte les messages d'erreur à l'émetteur initial.
- utilisé par des utilitaires (ping, traceroute, Network Time Protocol)
- permet de pallier au manque de service d'IP
- Beaucoup d'erreurs sont causées par l'émetteur, mais d'autres sont dues à des problèmes d'interconnexions rencontrées sur l'Internet :
 - ▶ Machine destination déconnectée.
 - ▶ Durée de vie du datagramme expirée.
 - ▶ Congestion de passerelles intermédiaires.
- **Format des messages ICMP**



Page 63

Le protocole ICMP

TYPE	8 bits; type de message
CODE	8 bits; informations complémentaires
CHECKSUM	16 bits; champ de contrôle
HEAD-DATA	en-tête datagramme + 64 premiers bits des données.

<u>TYPE</u>	<u>Message ICMP</u>	<u>TYPE</u>	<u>Message ICMP</u>
0	Echo Reply	13	Timestamp Request
3	Destination Unreachable	14	Timestamp Reply
4	Source Quench	15	Information Request (obsolete)
5	Redirect (change a route)	16	Information Reply (obsolete)
8	Echo Request	17	Address Mask Request
11	Time Exceeded (TTL)	18	Address Mask Reply
12	Parameter Problem with a Datagram		

Page 64



Le protocole ICMP

Signification des messages ICMP:

- 0 et 8 Echo Reply / Echo Request Demande et réponse écho: utilisé par la commande [ping](#) et [traceroute](#) pour déterminer si une machine est opérationnel, et également pour déterminer la validité du chemin emprunté.
- 3 [Destination Unreachable](#) : Message d'erreur émis par un routeur si une destination est inaccessible.
- 4 [Source Quench](#) : message émis par un routeur pour demander a une machine de diminuer sa vitesse d'émission afin d'éviter la congestion.
- 5 [Redirect \(change a route\)](#) : message émis en cas de détection d'un chemin plus court pour atteindre une destination donnée.
- 11 [Time Exceeded \(TTL\)](#) : lorsqu'un paquet atteint un routeur avec un TTL=0 ce dernier le détruit et génère un message d'erreur a l'émetteur (utilisé aussi par traceroute).
- 12 [Parameter Problem with a Datagram](#): Message d'erreur émis lorsqu'une erreur est détectée sur l'entête d'un datagramme et le type de cette erreur n'est pas couvert par les message ICMP.
- 13 et 14 [Timestamp Request / Timestamp Reply](#) : Demande et réponse d'horodatage: utilisé pour la synchronisation entre les horloges des machines sur le réseau.
- 15 et 16 [Information Request / Information Reply \(obsolète\)](#)
- 17 et 18 [Address Mask Request / Address Mask Reply](#) : demande et réponse pour l'obtention du masque de sous réseau.

Page 65