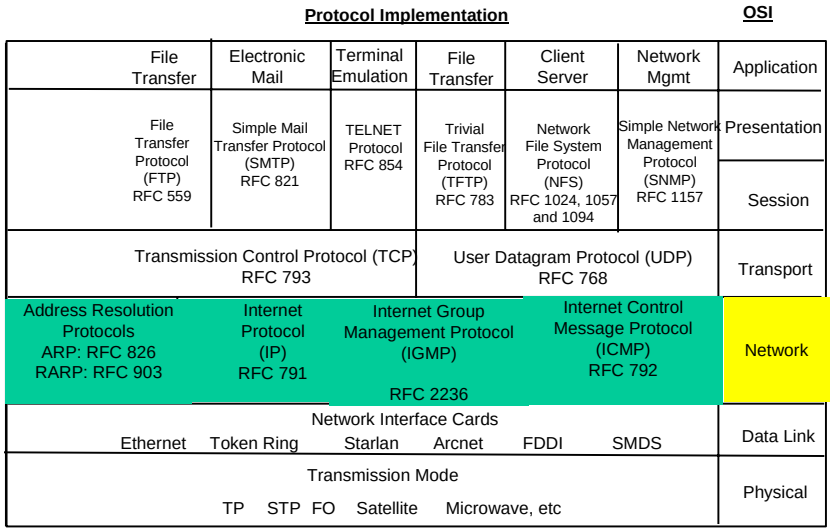
Cours 2: TCP/IP
Couche Réseau

Cours 2: plan

2.1 Introduction
2.2 IP: Adressage
2.3 IP: Routage
2.4 ARP Protocole
2.5 ICMP Protocole
2.6 IGMP Protocole

Introduction



3

IP ?

- IP est un service simple pour l'envoi de datagrammes en mode non connecté.
- IP est sensible à l'adressage, il s'assure que le routeur sait ce qu'il doit faire, lorsque les données arrivent.

Fonctions IP

- Acheminement de datagrammes vers un destinataire en mode non connecté (Datagramme)
  - @IP (Adresse IP)
- Routage : déterminer le chemin
  - Pour les paquets de la couche transport
  - Pour les trames de la couche liaison (Routeur)
  - Aucune connaissance complète de la carte du réseau
- Fragmentation/Réassemblage
  - Des micros aux gros systèmes
- Gestion des options IP
- Envoi et réception des messages de contrôle et d'erreur par ICMP

5

Ce que ne fait pas IP !

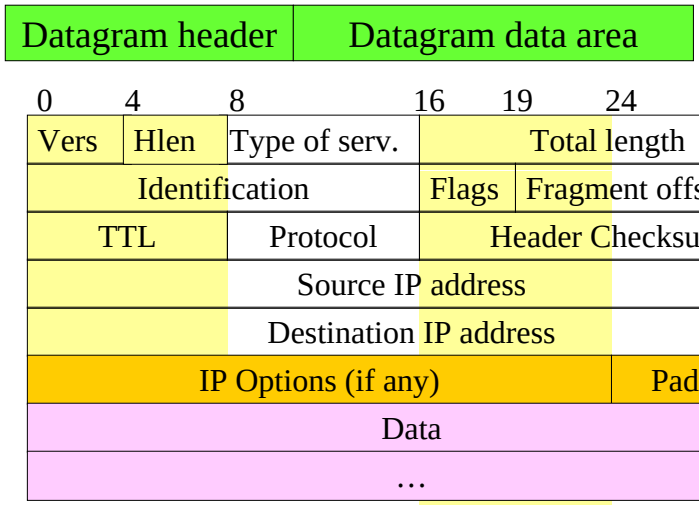
IP n'est pas fiable : il ne fait pas
- Multiplexage
- Séquencement
- Détection des duplications
- Détection de perte et retransmission
- Contrôle de flux

→ **IP est un protocole 'Best effort'**

6

Internet datagramme

- Unité de transfert basique
- Format de datagramme



7

IP datagramme

- **Vers** (4 bits): (IPv4=4)
- **Hlen (**4 bits): Header length (mot de 32 bits, sans options (cas général) = 20 octets)
- **Type of Service – TOS** (8 bits): n'est pas utilisé,
- **Total length** (16 bits): length de datagramme en octets en-tête inclus
- **identification, flags, fragmentation**
- **Time to live – TTL** (8bits): spécifie la durée de vie de datagramme
  - Routers decrement by 1
  - When TTL = 0 router discards datagram
  - Prevents infinite loops
- **Protocol** (8 bits): spécifie le format de la zone de données
  - Protocol numbers administered by central authority to guarantee agreement, e.g. TCP=6, UDP=17 …

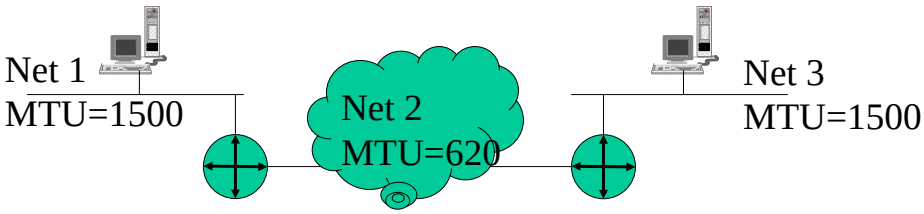
8

IP Datagramme

- **Checksum**
- **Source & destination IP address** (32 bits): contiennent les adresses IP source et destination
- **Options** (variable): infos. de routage et sécurité

IP Fragmentation

- Comment nous pouvons envoyer 1400 bytes à travers un réseau de *Maximum Transfer Unit (MTU) est* de 620 bytes?
- La réponse: fragmenter le datagramme



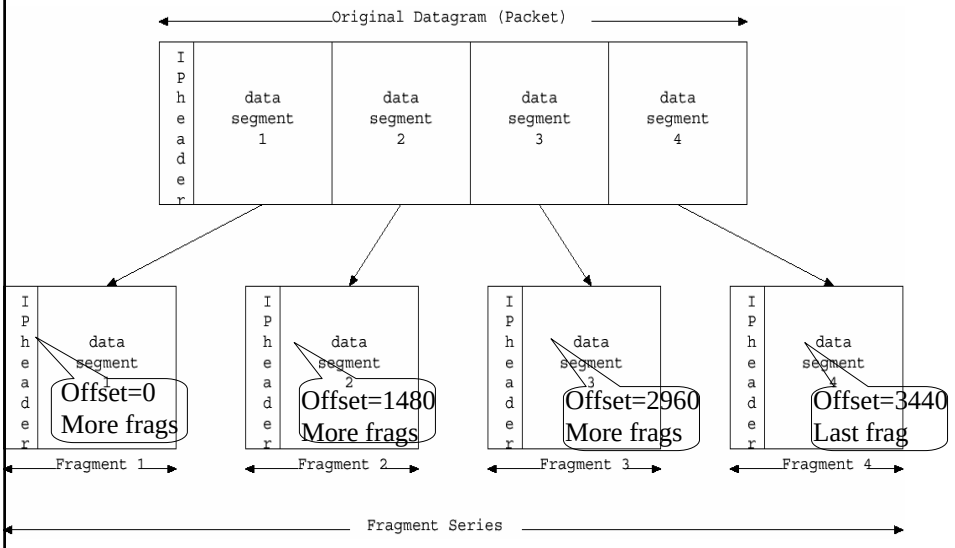
- Routeur fragmente les datagrammes de 1400 bytes
  - En 600 bytes, 600 bytes, 200bytes (20 bytes pour l'en-tête IP)
  - Routeurs ne re-assemblent pas les fragments

Contrôle de Fragmentation

- **Identification**: permet à la destination de connaître l'origine de chaque fragment
- **Fragment Offset** (13 bits): permet la localisation des données transportées dans le fragment courant par rapport au datagramme initial
  - Mesuré en unités de 8 bytes commençant par 0
- **Flags** (3 bits): contrôle la fragmentation
  - Réservé (0 bit)
  - Don't Fragment – DF (1er bit):
    - 1➔ n'est pas fragmenté
  - More Fragments –MF (2ieme bit): 1➔ données qui suivent
- Environ de 0.1% - 0.5% des paquets TCP sont fragmentés.

11

Exemple de Fragmentation



12

Cours 2: plan

2.1 Introduction
2.2 IP: Adressage
2.3 IP: Routage
2.4 ARP Protocole
2.5 ICMP Protocole
2.6 IGMP Protocole

13

Internet Adressage

- 32 bits par adresse
  - L'adresse réfère une interface qu'une machine
  - Composée de deux parties
    - Identificateurs de network et host
  - Class A, B, C for unicast
  - Class D for multicast
  - Class E réservée
- 4 octets/bytes en format décimal
  - E.g. 134.79.16.1, 127.0.0.1

14

Classes d'adresses d'Internet

- Class A: plus de hosts, peu de networks
  - 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh
    - 7 bits network (0 et 127 réservés, soit 126 networks), 24 bits host (> 16M hosts/net)
- Class B: nombre de hosts et networks
  - 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh
    - 16,384 class B networks, 65,534 hosts/network
    - Plage d'adressage 128-191 (décimal)
- Class C: grand nombre de networks
  - 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh
    - 2,097,152 networks, 254 hosts/network
    - Initial byte 192-223 (decimal)
- Class D: 224-247 (decimal) (RFC 1112)
- Class E: 248-255 (decimal)

15

Subnets: sous adressage

- Le mask du réseau est appliqué pour déterminer comment le réseau est sous adressé
- exemple :

137.138.28.228, et le mask sous réseau 255.255.255.0 alors 228 représente la machine est 137.138.28.0 le réseau

16

Conversions de subnet mask

Prefix Length	Subnet Mask	Prefix Length	Subnet Mask
/1	128.0.0.0	/17	255.255.128.0
/2	192.0.0.0	/18	255.255.192.0
/3	224.0.0.0	/19	255.255.224.0
/4	240.0.0.0	/20	255.255.240.0
/5	248.0.0.0	/21	255.255.248.0
/6	252.0.0.0	/22	255.255.252.0
/7	254.0.0.0	/23	255.255.254.0
/8	255.0.0.0	/24	255.255.255.0
/9	255.128.0.0	/25	255.255.255.128
/10	255.192.0.0	/26	255.255.255.192
/11	255.224.0.0	/27	255.255.255.224
/12	255.240.0.0	/28	255.255.255.240
/13	255.248.0.0	/29	255.255.255.248
/14	255.252.0.0	/30	255.255.255.252
/15	255.254.0.0	/31	255.255.255.254
/16	255.255.0.0	/32	255.255.255.255

Decimal Octet	Binary Number
128	1000 0000
192	1100 0000
224	1110 0000
240	1111 0000
248	1111 1000
252	1111 1100
254	1111 1110
255	1111 1111

17

Problèmes d'Adressage

- En 1991 IAB (Internet Architecture Board) identifié 3 dangers
  - Pénurie des adresses de classe B
  - Augmentation des réseaux va exploser les tables de routage
  - Augmentation des nets/hosts dépasse l'espace d'adressage de 32 bits
- Quatre stratégies d'adressage
  - Creative address space allocation {RFC 2050}
  - adresses privées{RFC 1918}, Network Address Translation (NAT) {RFC 1631}
  - Classless InterDomain Routing (CIDR) {RFC 1519}
  - IP version 6 (IPv6) {RFC 1883}

18

Creative IP address allocation

- Trois organisations d'attribution d'adresses
  - APNIC – Asia & Pacific www.apnic.net
  - ARIN – N. & S. America, Caribbean & sub-Saharan Africa www.arin.net
  - RIPE – Europe and surrounding areas www.ripe.net

19

Adresses privées

- IP adresses non routables, utilisées par les entreprises en interne "ne sont pas assignées à des réseaux au sein de l'Internet global"
- Trois plages:
  - 10.0.0.0 - 10.255.255.255 a single class A net
  - 172.16.0.0 - 172.31.255.255 16 contiguous class Bs
  - 192.168.0.0 – 192.168.255.255 256 contiguous class Cs
- Connectivité fournit par Network Address Translator (NAT)
  - correspondre une adresse privée à une adresse IP publique (routable)
  - seulement pour les paquets TCP/UDP

20

Classless InterDomain Routing (CIDR)

- Beaucoup d'organisation ont > 256 machines mais peu ont plusieurs milliers
- À la place d'attribuer une class B (16384 nets), on attribue des adresses de classe C
  - < 256 adresses ➔ 1 class C
  - ...
  - < 8192 adresses ➔ 32 Class C

21

CIDR & Supernetting

- Blocs d'adresses CIDR représentés par un préfixe et préfixe long
  - **Préfixe** = seule adresse représente le bloc de réseaux
    - 192.32.136.0 = 11000000 00100000 10001000 00000000
    - 192.32.143.0 = 11000000 00100000 10001111 00000000

Préfixe 21 bits (2048 machines)

  - **Préfixe long** indique le nombre de bits de routage

    192.32.136.0/21 ➔ 21 bits utilisés pour le routage
    - CIDR regroupe tous les réseaux entre 192.32.136.0 et 143.0 en une seule entrée dans le routeur- **réduire les entrées dans la table de routeur**
- Voir en détail RFC 1519

22

IPV6

- **Pourquoi un nouveau Protocole IP ?**

  Actuellement la taille de l'Internet double tous les 12mois
  - problèmes à résoudre l'épuisement des adresses IP (2008 +/- 3 ans)
  - Et l'explosion de la taille des tables de routage
  - le nouveau protocole doit permettre d'adresser un espace (beaucoup) plus grand (10 E+9 réseaux au minimum)
  - un routage plus efficace

23

de IPv4 à IPv6

Pour résoudre ces problèmes :

Nouvelle version de Internet Protocol : Version 6

- actuellement : IPv4
- IANA: Internet Assignment Numbers Authority (RFC 1700) Ce nouveau protocole (IPv6) :
  - garde ce qui a fait le succès de l'Internet
  - étend la fonction d'adressage et de routage
  - tend à résoudre les problèmes qui vont devenir critiques

  (applications temps réel, multipoint, sécurité...)

24

IPV6 :Quelques Caractéristiques

- Adresse plus longue : 128 bits (16 octets)
- Adressage de 340 x 10 e36 équipements
- Adressage hiérarchique

- 3 types d'adresses :
  - Unicast
  - Multicast
  - *Broadcast*

25

IPV6 :Quelques Caractéristiques

- En-tête simplifié
  - nombre de champs réduit de moitié => augmente l'efficacité de commutation des équipements de routage
- Extension de l'en-tête pour les options
  - Les options IPv6 sont placées dans des en-têtes séparés,

  intercalés entre l'en-tête IPv6 et l'en-tête de la couche transport => introduction aisée de nouvelles fonctionnalités
  - la longueur des options n'est plus limitée à 40 octets

26

IPV6 : Nouvelles fonctionnalités

- Autoconfiguration : "*plug and play*"
  - Gestion de la mobilité
  - Renumérotation facile si changement de prestataire
  - Serveurs d'adresses (DHCP : *Dynamic Host Configuration Protocol)*
  - et SAA : *Stateless Address Autoconfiguration (RFC 1971)*
- Multipoint (*Multicast*) inclus de base pour les routeurs et les clients
  - "scope" = meilleur routage des paquets multicast => plus besoin de Mbone ni de mrouted

27

IPV6: Nouvelles fonctionnalités

- "Marquage" des flux particuliers : (*Flow Label*)
  - applications temps réel, Qualité de Service (QoS)
  - Priorité du trafic de contrôle
- Sécurité :
  - authentification et intégrité des données
  - *en option* : confidentialité
- Routage à partir de la source
  - Source Demand Routing Protocol

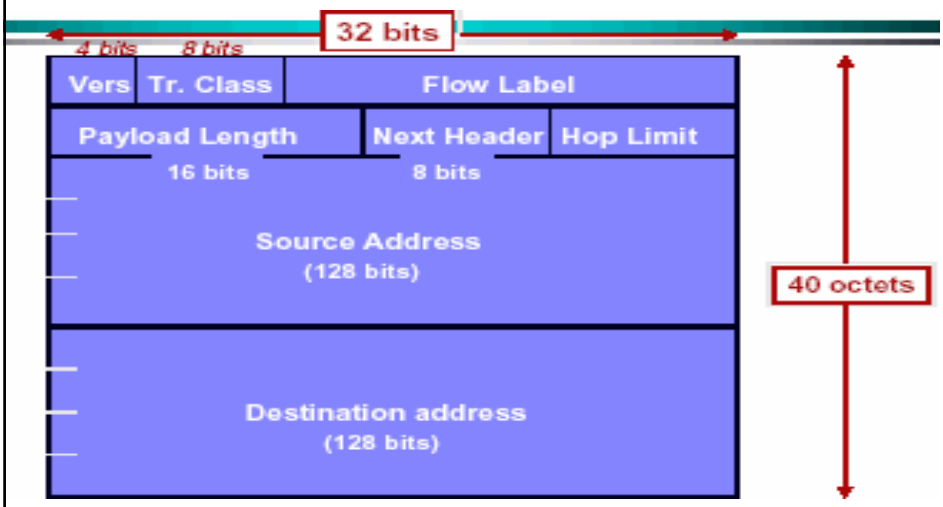
28

IPv4 -> IPv6
changements de l'en-tête

- Header Length (IHL) : supprimé
- ToS --> Flow Label
- Total Length (TL) --> Payload Length
- ID, Flags et Fragment Offset (FO) : supprimés
- TTL --> Hop Limit
- Protocol --> Next header (mêmes valeurs que dans IPv4)
- Header CS : supprimé
- Adresses : 32 --> 128 bits (4 --> 16 octets)
- Alignement 32 --> 64 bits

29

IPV6 : En-tête



30

IPV6: les champs de l'en-tête

- Vers : Version Number (= 6)
- Traffic Class : priorité ou classes de trafic (Differentiated Services)
- Flow label : marquage des paquets «spéciaux»
- Payload length : longueur du paquet après en-tête (en octets).
  autorise des paquets > 64 Koctets => Payload length = 0
- Next header : indique le type d'entête suivant immédiatement l'entête IPv6
  On utilise les mêmes valeurs que dans le champ "Protocol" de IPv4 pour référencer les protocoles de niveau 4 **(TCP=6 , UDP=17, ICMP=1)**

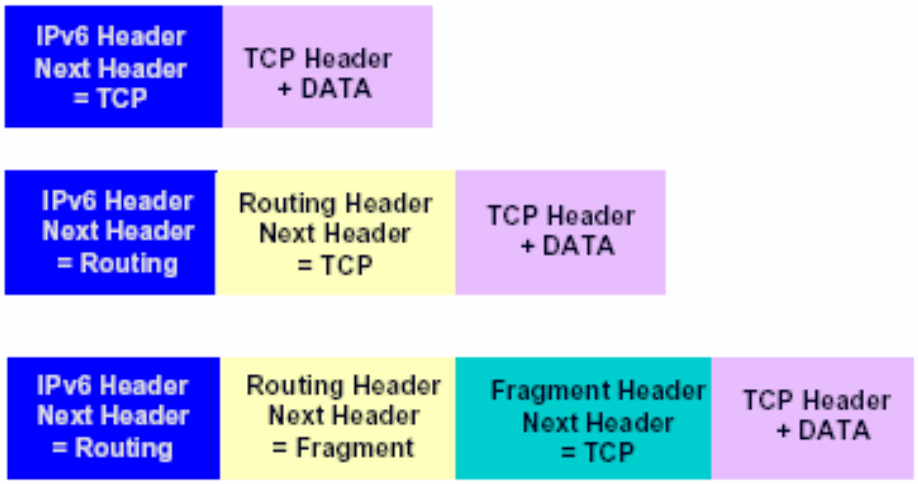
31

IPV6:les champs de l'en-tête

- Hop_limit : -1 chaque fois que le paquet est commuté par un équipement si hop_limit = 0 => le paquet est détruit.
  permet de réduire l'effet des boucles de routage.
- Source address : @ de l'émetteur initial du paquet
- Destination adress : Une adresse de destination ...
  peut-être différente de l'adresse destination finale si l'option "Routing Header" est présente.

32

IPV6: en-têtes optionnelles



33

IPV6: Les options

- Hop-by-Hop Header :transport d'information qui doit être examinée sur chaque noeud du chemin suivi par le datagramme IP.
- End-to-end Header : transport d'information qui n'est à examiner que par le destinataire du datagramme.
- Routing Header : routage à partir de la source

  liste un ou plusieurs noeuds intermédiaires "à visiter" au cours de l'acheminement du datagramme "Reverse bit" :

  si = 1 => utiliser l'information de routage pour le retour

  sinon => résoudre le routage à partir de l'extrémité destinataire

34

IPV6 : en-têtes optionnelles

- Fragment header :dans IPv6, la fragmentation n'est réalisée que par la source
- Authentication Header :authentification et intégrité des données
- Privacy Header : chiffrement des données à protéger datagramme TCP/ UDP ou datagramme IPv6 entier, à la demande

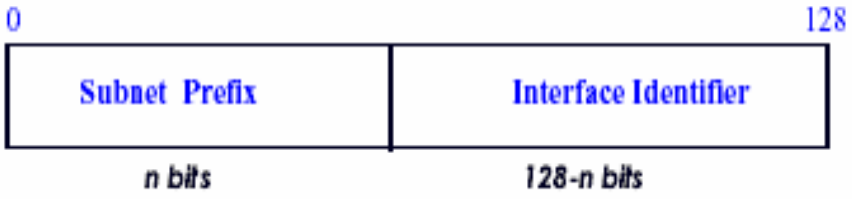
35

IPV6: Allocation des Adresses

- Allocation initiale des adresses : # 15% @ Unicast des prestataires de connectivité (*ISP*)
  @ Multicast
  @ à usage local
  @ compatibles IPv4
  autres : ISO NSAP,IPX, téléphone ?
  Réserve pour la croissance : # 85%

36

IPV6 : Format des adresses



Dans le plan d'adressage agrégé, n=64

37

IPV6: Préfixes et plan d'adressage agrégé

- 48 (3+13+8+24) bits — topologie publique
- 80 (16+64) bits — topologie privée (site)

Préfixes :
TLA = /16
NLA = /48
SLA = /64

« Frontières » fixes

38

IPV6: La Mobilité

La mobilité IPv6 s'appuie sur :

- L'expérience acquise dans IPv4
- Les nouvelles fonctionnalités d'IPv6
- L'opportunité du déploiement d'une nouvelle version d'IP
- La mobilité IPv6 permet le support des communications avec un mobile en effectuant un routage soit :
  - ✓ vers le point d'attachement du mobile sur l'Internet
  - ✓ vers l'adresse du mobile dans son sous-réseau mère

39

IPV6: Les principales fonctionnalités de la Mobilité

- Les correspondants d'un mobile doivent :
  - Disposer d'une liaison dans leur cache des liaisons
  - Apprendre la position du mobile en traitant des options «Binding Update»
  - Effectuer le routage des paquets directement vers le mobile (Routing Header)
- L'agent mère d'un mobile doit :
  - Être un routeur dans le sous-réseau mère du mobile
  - Intercepter les paquets dans le sous-réseau mère
  - Tunneler (encapsulation IPv6) ces paquets directement au mobile

40

IPV6: L'adressage d'un mobile

- Un mobile est toujours *joignable* par son adresse mère
- Un mobile en déplacement possède toujours une adresse temporaire (autoconfiguration) :
  - Réception de « Router Advertisement » indiquant le préfixe du sous réseau visité
  - Concaténation de ce préfixe avec l'adresse MAC de l'interface
- La détection de mouvement s'effectue également à l'aide des mécanismes de « Neighbor Discovery »

41

IPV6 : Gestion des caches de liaisons

- Un mobile envoie à chaque déplacement un Binding Update (BU):
  - Chaque BU inclut une durée de vie
  - Un mobile maintient une liste des correspondants à qui il a envoyé un BU
- L'adresse temporaire envoyée dans le BU destiné à l'agent mère est appelée adresse temporaire principale

42

IPV6: Format de l'option Binding Update

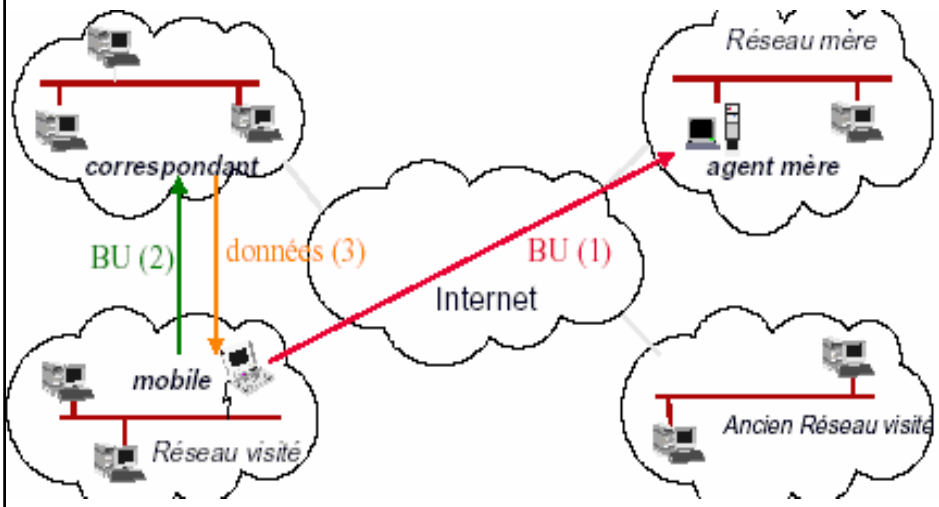
- La mobilité IPv6 définit une nouvelle option destination appelée Binding Update

Option Type	Option Length
A H L Reserved	Lifetime
Identification	
Care-of Address	
Home Link-Local Address (present only if L bit set)	

Tout paquet qui inclut l'option destination Binding Update doit également contenir un en-tête d'authentification

43

IPV6: Gestion de la mobilité



44

Cours 2: plan

2.1 Introduction
2.2 IP: Adressage
2.3 IP: Routage
2.4 ARP Protocole
2.5 ICMP Protocole
2.6 IGMP Protocole

45

Concepts de routage

- Deux types basics de routage IP :
  - **Routage Direct**.
    - ✓ La machine destination est directement attachée au même support physique “réseau” comme la machine source
    - ✓ Le datagramme IP est encapsulé dans une trame physique (i.e. Ethernet).
  - **Routage Indirect.**
    - ✓ **Attachement** physique de la source et la destination n’est pas nécessaire
    - ✓ Un seul chemin pour rejoindre la destination via un ou plusieurs routeurs
    - ✓ L’adresse du premier routeur(default gateway) est la seule adresse exigée par la source

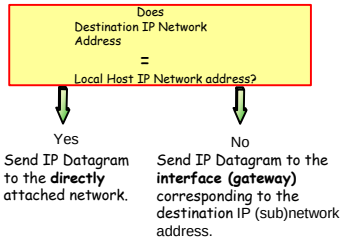
46

Concepts de routage

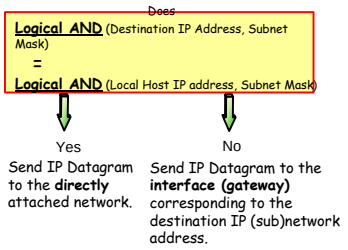
Table de routage IP

- Chaque host/router garde un ensemble de chemins avec **le routeur next** dans la direction de la Destination
- Ces chemins sont stockés dans la **table de Routage IP**. Cette table contiendra trois chemins différents:
  - **Routes directes** pour les réseaux attachés localement.
  - **Routes indirectes** pour les réseaux atteints via un ou plusieurs réseaux
  - Une **default route** dans le cas où le réseau destination n'a pas de table de routage
- Un Algorithme de routage

IP Routing without Subnets

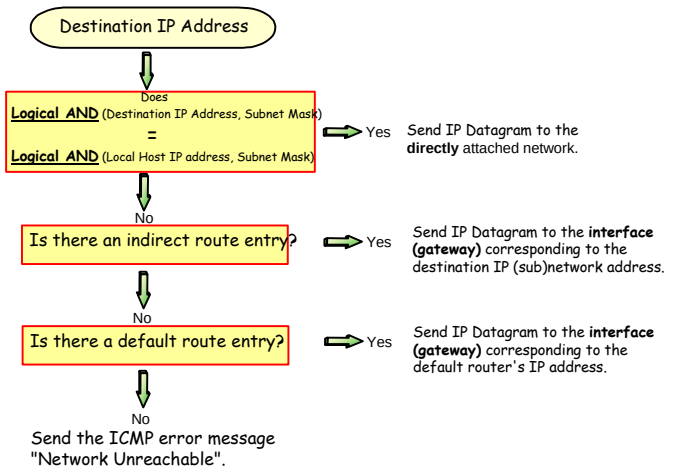


IP Routing with Subnets



47

Algorithme de routage w/ Subnets



48

Cours 2: plan

2.1 Introduction
2.2 IP: Adressage
2.3 IP: Routage
2.4 ARP Protocole
2.5 ICMP Protocole
2.6 IGMP Protocole

49

ADDRESS RESOLUTION PROTOCOL (ARP)/ REVERSE ARP(RARP)

50

ARP

- **Problème**
  - **IP** est une méthode d'adressage utilisée au niveau réseau pour identifier les machines et les réseaux
    - C'est une adresse logique et n'est pas physique/ MAC adresse.
    - Physique/ MAC adresses identifient les stations au niveau liaison
  - méthode d'adressage TCP/IP n'était pas désignée pour les LANs
    - LANs exigent que les stations connaissent chaque adresse physique pour établir la communication.

La station **connaît l'adresse IP destination** mais ne connaît pas **l'adresse MAC destination**

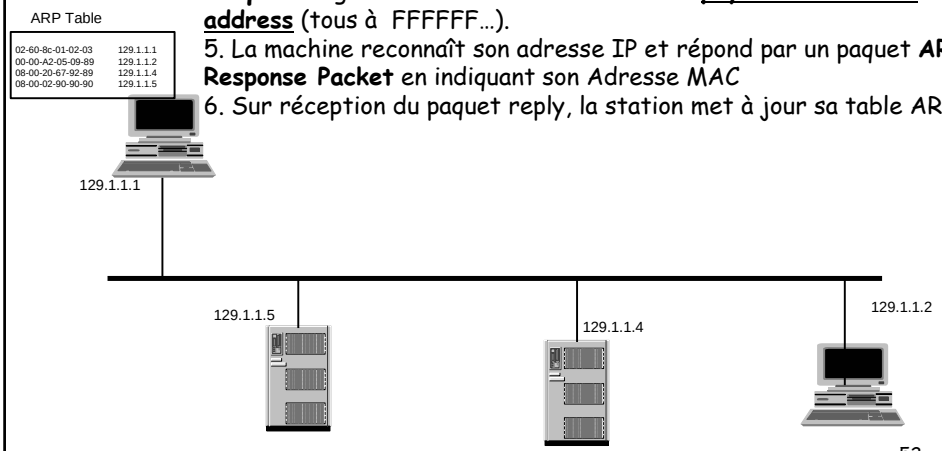
Comment la station obtiendra-t-elle l'adresse MAC destination?

- **Solution**
  - Mappage (correspondre) de l'**address IP (32 bits)** dans l'**adresse MAC (48 bits)**
  - TCP/IP utilisera **ARP** pour trouver l'adresse physique de la station destination

51

ARP : CONCEPT

1 IP demande une **MAC address** de la table **ARP**
2. Station recherche dans l'entrée dans la table ARP
3. Si l'adresse est dans la table alors retourne MAC address à IP
4. Si l'adresse MAC n'est pas dans la table, un paquet **ARP Request** généré sur le réseau en utilisant **physical Broadcast address** (tous à FFFFFF…).
5. La machine reconnaît son adresse IP et répond par un paquet **ARP Response Packet** en indiquant son Adresse MAC
6. Sur réception du paquet reply, la station met à jour sa table ARP



52

ARP Table

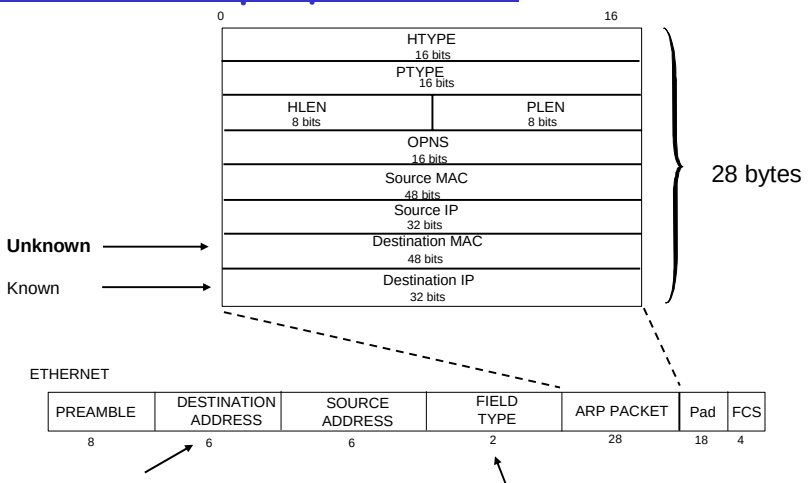
- ARP Table Size: adresses IP
  - Routeurs peut avoir plusieurs centaines d'entrées
  - les hosts quelques entrées.
- ARP Timeout

Variable entre 120s à 4heures, indique le temps d'expiration (effacement) de l'adresse de la table

- Adresses MAC

53

Format de paquet ARP

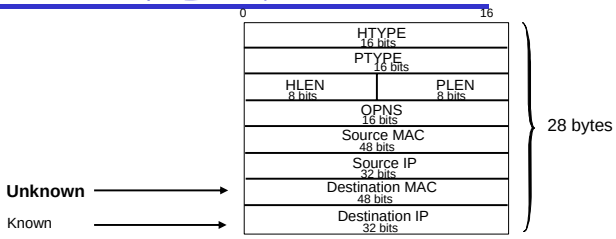


- A **Broadcast** for an ARP Request.
- A **Unicast** for a ARP Reply

0806_{16} = Ethernet type for ARP Request and Response.

54

ARP PACKET FORMAT



- **HTYPE.** The **hardware type field** indicates the network (hardware interface type) for which the sender seeks an answer. This will be **1** for Ethernet.
- **PTYPE.** The **protocol type field** specifies the type of high-level protocol address the sender has supplied. This is normally **0800h** for IP addresses.
- **HLEN.** The **hardware address length** field specifies the size in bytes of the hardware address. This field will normally contain the **value 6** (the length of the MAC address field is 48 bits).
- **PLEN.** The **protocol address length** field specifies the size in bytes of the high-level protocol address. This field will normally contain the **value 4** (the length of the IP address is 32 bits).
- **OPNS.** The **operations field** specifies whether the packet is an **ARP request** (a value of **1**) or an **ARP reply** (a value of **2**). The field is required since the **Ethernet field type** will contain the same value for both ARP request and ARP reply.

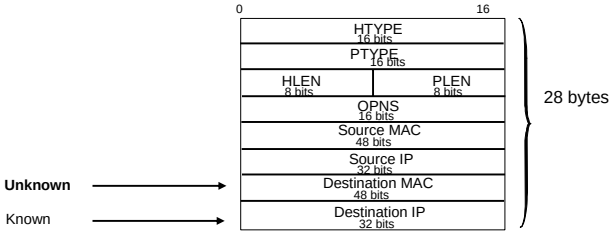
55

Hardware Types

Hardware Type	Decimal Code
DIX -Ethernet and FDDI	1
IEEE 802 (802.3 and 802.5)	6
ARCnet	7
LocalTalk	11
SMDS	14
Frame Relay	15
ATM	19
Serial Line	20

56

ARP : format de paquet



- **Source MAC**. The **physical/MAC address** of the source station requesting the address resolution.
- **Source IP**. The **IP address** of the source station requesting the address resolution.
- **Destination MAC**. The **physical/MAC address** of the destination station which will resolve the address mapping. This field will normally be set to **all 0s** in the request packet because this field is unknown.
- **Destination IP**. The **IP address** of the destination station which will resolve the address mapping.

NOTE:
1. For an **ARP Request** all the fields are filled in **except** the destination MAC address.
2. When the host receives the ARP request, it **fills in** its hardware address and **swaps** the two sender addresses with the two destination address.
3. The **OPNS field** is set to 2(this indicates a reply) and a reply is sent back to the requesting station.
4. The reply can either be broadcast of unicast but is normally unicast.

57

RARP

❑**Problème**
- o **MAC dépend du matériel** cependant **IP** adresses sont **indépendantes**.
- o Les programmes d'Application utilisent **IP adresse** pour spécifier une destination. Cette adresse est enregistrée sur le disque de l'ordinateur, le système au démarrage lit cette adresse
- o Stations sur le réseaux utilisent Physical/ **MAC adresses** pour spécifier la destination.

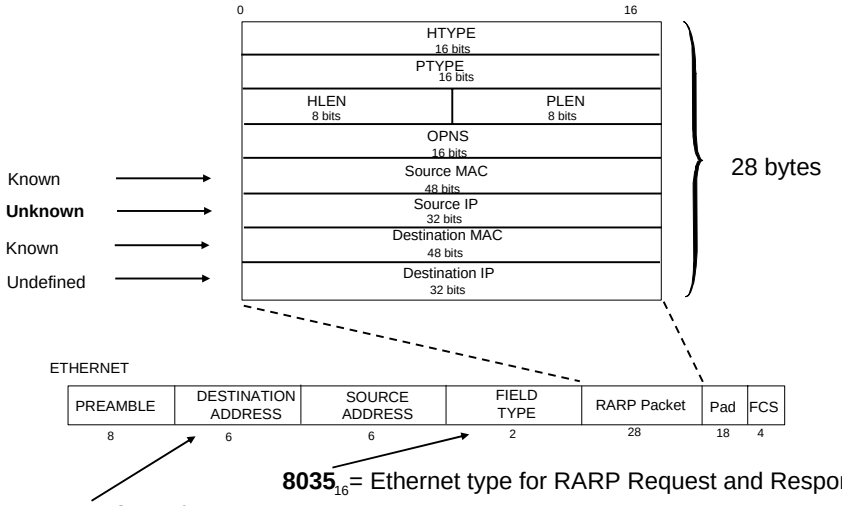
ARP est utilisé pour accomplir la correspondance entre deux adresses

La station source **connaît son MAC address** mais **pas son IP address**
Comment une station du travail **diskless** obtient une IP address**?**

❑**Solution**
- o TCP/IP utilisera **RARP** pour trouver **Internet Address** à travers le réseau via **RARP server**
- o Chaque réseau doit posséder au moins **un RARP server**
- oIP fait correspondre une IP adresse avec une adresse MAC

58

ARP/RARP PACKET FORMAT



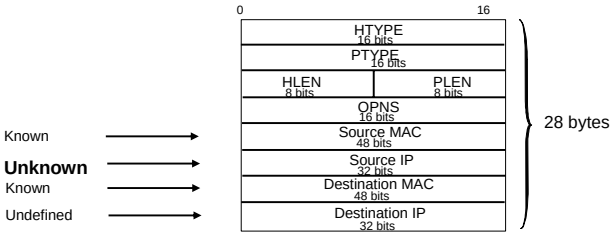
8035$_{16}$= Ethernet type for RARP Request and Response.

A **Broadcast** for an RARP Request.
A **Unicast** for a RARP Reply

RARP will normally reside on a prom in the network adapter card.

59

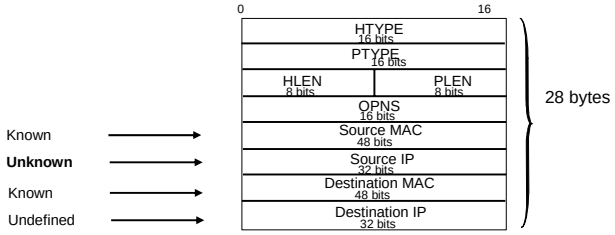
ARP/RARP PACKET FORMAT



- **HTYPE**. The **hardware type field** indicates the network(hardware interface type) for which the sender seeks an answer. This will be 1 for Ethernet.
- **PTYPE**. The **protocol type field** specifies the type of high-level protocol address the sender has supplied. This is normally 0800h for IP addresses.
- **HLEN**. The **hardware address length** field specifies the size in bytes of the hardware address. This field will normally contain the value 6(the length of the MAC address field is 48 bits).
- **PLEN**. The **protocol address length** field specifies the size in bytes of the high-level protocol address. This field will normally contain the value 4 (the length of the IP address is 32 bits).
- **OPNS**. The **operations field** specifies whether the packet is an **RARP request** (a value of 3) or an **RARP reply** (a value of 4). The field is required since the **Ethernet field type** will contain the same value for both RARP request and RARP reply.

60

ARP/RARP PACKET FORMAT



- **Source MAC**. The **Physical/MAC address** of the **source station** requesting the address resolution. This field is known.
- **Source IP**. The **IP address** of the **source station** requesting the address resolution.This field is unknown and will normally be set to **all 0s**. It will be filled in by the responding RARP server.
- **Destination MAC**. For a **RARP Request**, the **physical/MAC address** of the **source station** requesting the address resolution.
- **Destination IP**. The **IP address** of the RARP server. This is unknown.

NOTE:
1. For an **RARP Request** , the **Source MAC and Destination MAC** addresses are filled in with the **physical address of the requesting station.** The **Source IP is Unknown** and will be filled in by RARP server. The **Destination IP is unknown**.
2. For an **Rarp Response**, the **Source MAC and Source IP** addresses contain **the physical address and logical address** of the RARP server. **The Destination MAC** contains the physical address of the requesting station while the **Destination IP** contains the IP address of the requesting station assigned by the RARP server.
3. The **OPNS field** is set to **4** to indicate a reply.

61

Cours 2: plan

62

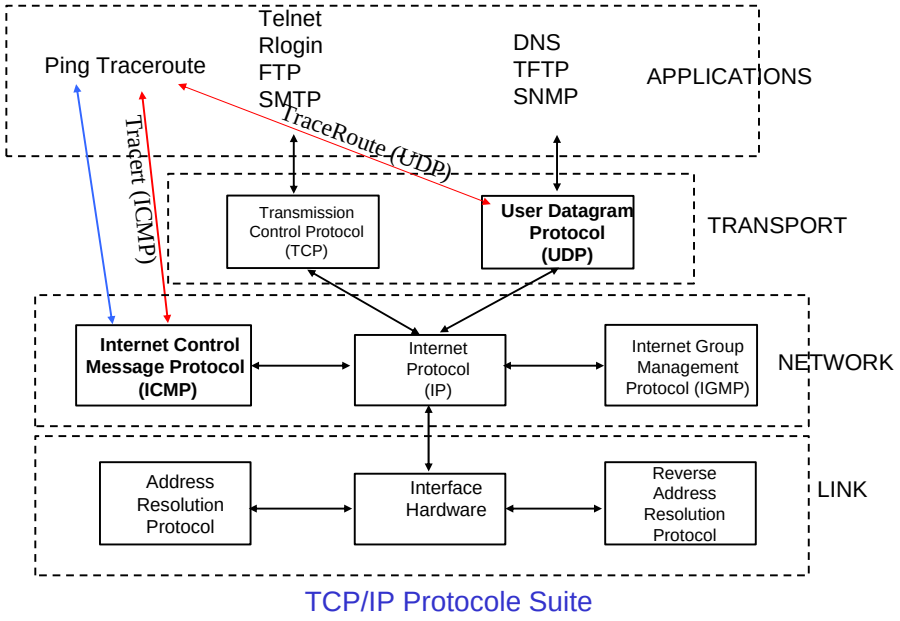
INTERNET CONTROL MESSAGE PROTOCOL
-ICMP -

63

ICMP

- ICMP fait un compte rendu sur les conditions d'erreur à la source
- ICMP permet aux routeurs d'envoyer des messages d'erreur ou de supervision à d'autres routeurs ou machines
- ICMP offre un mécanisme de communication entre le logiciel IP d'une machine et celui d'une autre machine
- Le message ICMP est **encapsulé** dans un datagramme IP et il est considéré comme une partie intégrante du protocole IP
- Le message d'erreur ICMP contient **l'en-tête IP** et **8 premiers bytes** de message
- Dans l'ordre d'éviter la congestion, un message ICMP n'est jamais envoyé en réponse au:
  - Un message d'erreur ICMP
  - Une adresse broadcast ou multicast
  - Un autre fragment que le premier
  - Une adresse source qui ne définit pas une seule machine

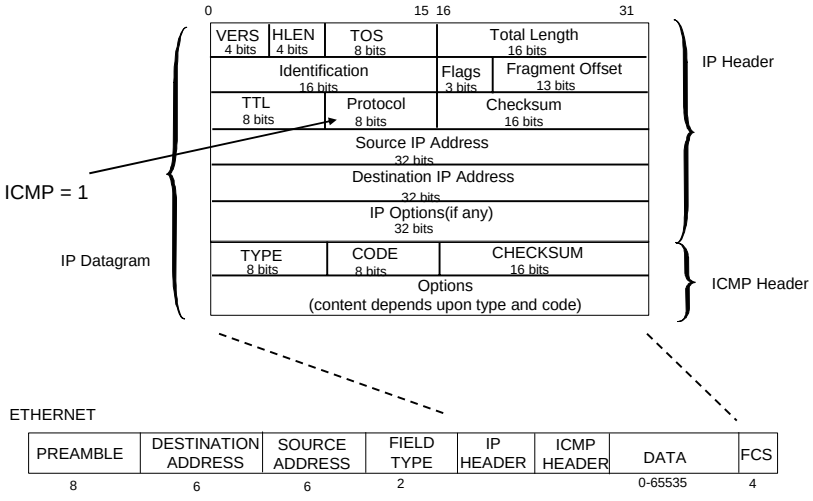
64



TCP/IP Protocole Suite

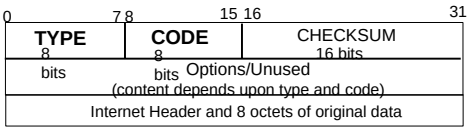
65

ICMP ENCAPSULATION



66

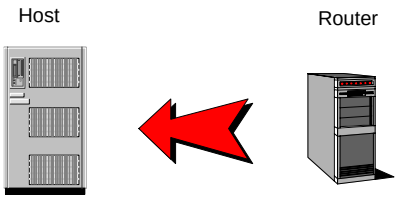
ICMP: ENCAPSULATION



- **TYPE.** Type de message (**20 ICMP type messages**)
- **CODE.** Fournit des infos. Supplémentaires sur le type de message
- **CHECKSUM.** Le même comme IP, mais pour le message ICMP (y compris les données)
- **OPTION FIELD.** Le contenu dépend de **type de message** .

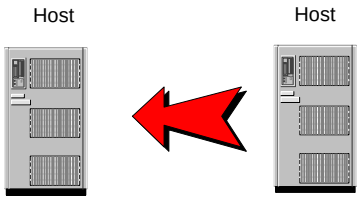
67

ICMP: Messages d'erreurs



Router Error Messages

- Destination is unreachable.
- Time-to-Live expired at router.
- Bad parameter in the IP header
- A better route is available



Host Error Messages

- Service is unreachable.
- Fragment reassembly time has expired.
- Bad parameter in the IP header

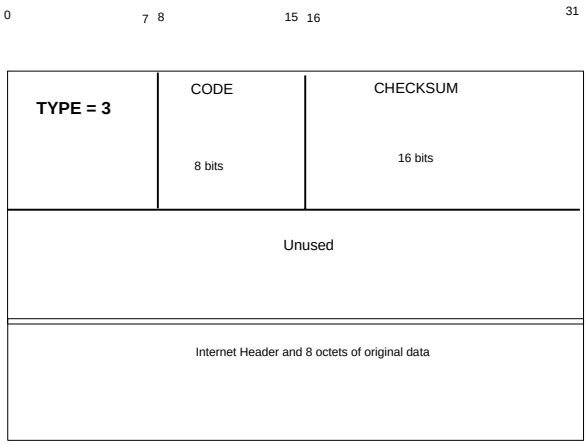
68

ICMP : Types de messages

0	Echo Reply	RFC 792
3	Destination Unreachable	RFC 792
4	Source Quench	RFC 792
5	Redirect	RFC 792
8	Echo	RFC 72
9	Router Advertisement	RFC 1256
10	Router Solicitation	RFC 1256
11	Time Exceeded	RFC 792
12	Parameter Problem	RFC 792
13	Timestamp	RFC 792
15	Information Request	RFC 792
16	Information Reply	RFC 792
17	Address Mask Request	RFC 950
18	Address Mask Reply	RFC 950
30	Traceroute	RFC 1393
32	Mobile Host Redirect	
33	IPv6 Where-Are-You	
34	IPv6 I-Am-Here	
35	Mobile Registration Request	
36	Mobile registration Reply	

69

Destination inaccessible



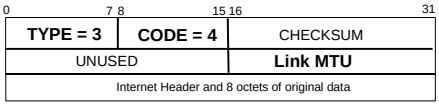
70

Destination inaccessible

Code	Description
0	Network is unreachable
1	Host is unreachable
2	Protocol is not supportable at destination
3	Port unreachable (application is probably not available)
4	**Fragmentation required but DF bit is set**
5	Source route failed
6	Destination network unknown
7	Destination host unknown
8	Source host isolated (obsolete)
9	Destination network administratively prohibited
10	Destination host administratively prohibited
11	Network unreachable for TOS
12	Host unreachable for TOS
13	Communication administratively prohibited by filtering
14	Host precedence violated
15	Precedence cutoff in effect

71

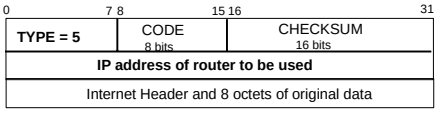
Path MTU Discovery



- Path MTU Discovery est une méthode pour déterminer le MTU Maximum Transmission Unit de bout en bout
  - Le bit **DF** dans IP Header est positionné à 1
  - La sélection initiale de MTU se fait:
    - ✓ **Pour le TCP** la valeur la plus petite est annoncée par les stations locale et distante 576 octets
    - ✓ **Pour UDP** la longueur de MTU de l'interface locale est sélectionnée
  - Au premier routeur avec un MTU le plus court, un ICMP ***Destination Unreachable*** message avec le **CODE = 4** est envoyé à la station source
  - la station source ajuste son MTU jusqu'à elle passe
  - la station recontrôle périodiquement le chemin

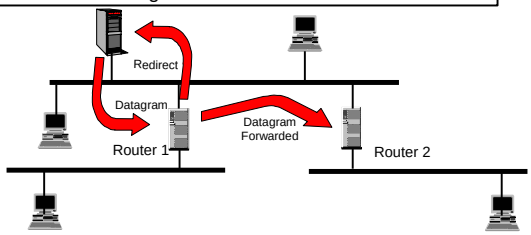
72

Message de redirection(changement de route)



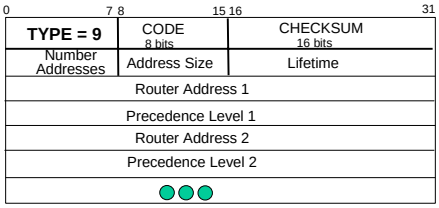
- Le host/routeur retourne un "**ICMP redirect message**" s'il y a un meilleur chemin à la destination
  - Ce message est limité à l'interaction entre host et routeur sur le même réseau
  - IP Address est l'adresse de routeur utilisé par la source pour atteindre la destination. Host alors met à jour son table de routage

Code	Description
0	Redirect datagrams for the network(périmé).
1	Redirect datagrams for the host.
2	Redirect datagrams for the TOS and the network.
3	Redirect datagrams for the TOS and the host.



73

Annonce Routeur



- A l'initialisation, un ordinateur a besoin de connaître IP address de routeur
  - BootP
  - DHCP
  - Static Configuration
- Si le routeur supporte le multicast, il utilise l'adrese **224.0.0.1**. sinon, il utilise le broadcast **255.255.255.255**. pour les annonces
- Annonces toutes les 10 minutes avec default TTL de 30 minutes

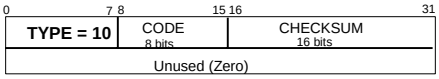
74

Annonce Routeur

- **Number Addresses.** Le nombre d'adresses de routeurs portées dans le message (le plus souvent une seule adresse)
- **Address Size.** Définit la taille d'une adresse en mots de 32bits (1 mot pour les adresses IPV4)
- **Lifetime.** Le nombre en seconde pendant lequel, la machine peut utiliser les adresses annoncées dans le message (30 minutes)
- **Router Address.** Adresse IP d'un routeur
- **Precedence Level**. Niveau de priorité est un entier représenté en complément à 2, un ordinateur choisit en général la route de plus haut niveau de priorité

75

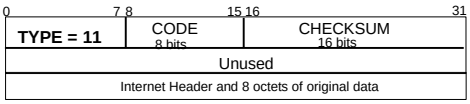
Sollicitation d'un routeur



- la valeur par défaut d'annonce est de **10 minutes**
- Router Solicitation message exige une annonce immédiate de routeur
  - Sollicitation messages sont envoyés toutes les **3 secondes**
- Si les hosts supportent le multicast, ils envoient la sollictation à **224.0.0.2**. Si non ils envoient à l'adresse de diffusion tout à 1
- À chaque fois la machine reçoit un advertisement, elle met à jour son routeur par défaut si l' advertisement contient un plus haute priorité.

76

Délai excessif

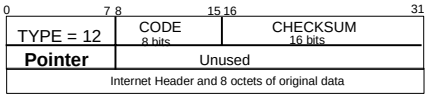


- **Time-to-Live** est expiré au routeur ou **Fragment Reassembly Time** est expiré à la destination avant l'arrivée des fragments➔ route circulaire ou excessivement longue
  - **Time-to-Live** field sets an upper bound on how many routers a datagram can transit.
    - ✓ initialisé par l'emetteur (32 ou 64) et décrémenté à chaque passage par un routeur
    - ✓ il est basiquement limité au lifetime de datagramme afin d'éviter la boucle
    - ✓ quand le TTL zéro ,le **datagramme est écarté** et l'émetteur est notifié ICMP message
  - A **Fragment Reassembly Timer** est positionné par le récepteur à la réception du premier fragment (**60 et 120 secondes**), quand le timer expire **datagramme est écarté** et l'émetteur est notifié ICMP message

Code	Description
0	**Time-to-Live** expired while the datagram was in transit. Generated by the router.
1	**Fragment Reassembly** Time has expired. Generated by the host.

77

Problème de paramètre

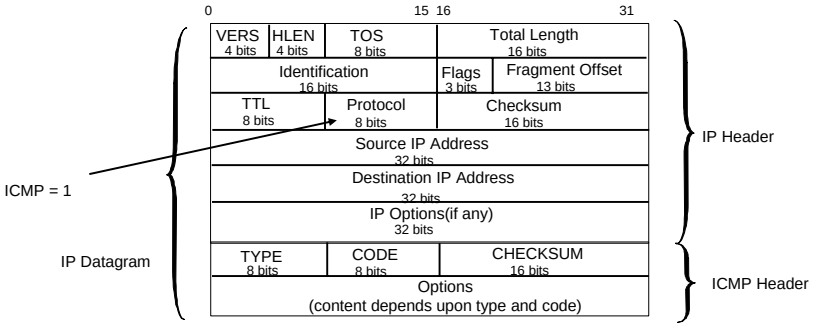


- The **Parameter Problem** est envoyé en cas d'erreur non prise en compte la première fois
  - Par exemple, une erreur d'en-tête
  - Le champ **Pointer** identifie l'octet du datagramme qui est la cause du problème,

Code	Description
0	The value in the pointer field indicates the octet where an error occurred. This will probably be due to inconsistent or missing information that makes it impossible to process the datagram.
1	A required option is missing (e.g., the military security option). The pointer field is filled with zeroes.
2	Bad length(offset was probably invalid).

78

PING: ENCAPSULATION



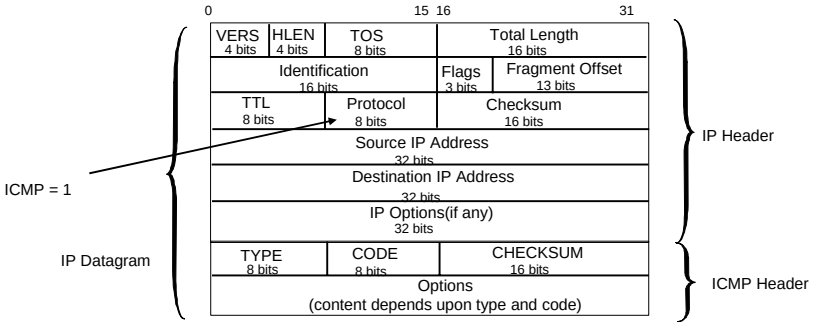
The Packet InterNet Grouper(PING)

c'est un programme test l'accessibilité à une machine

- Il emploie **ICMP Echo Request (type 8)/Echo Reply (type 0)**.
- PING sera difficilement utilisé avec l'augmentation **Internet security** (firewalls etc)

79

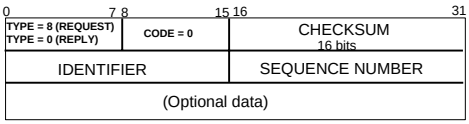
PING: ENCAPSULATION

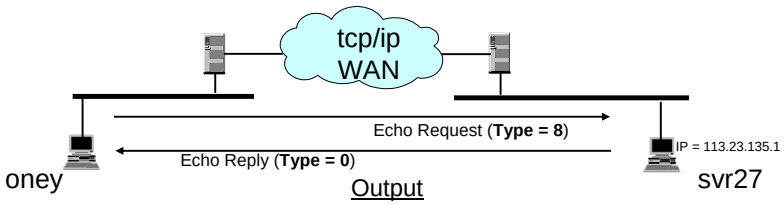


- **IDENTIFIER**. Permet à l'expéditeur d'associer les réponses reçues avec ses propres demandes
- **SEQUENCE NUMBER**. Comme IDENTIFIER
  - pour un programme ping ce champ est initialisé à 0 puis il est incrémenté de 1 à chaque demande envoyée
  - Utilisé pour détecter l'absence, duplication ou re-odre des pings
- **OPTIONAL DATA**. Data envoyées par la source et retournées par un Echo Reply

80

PING



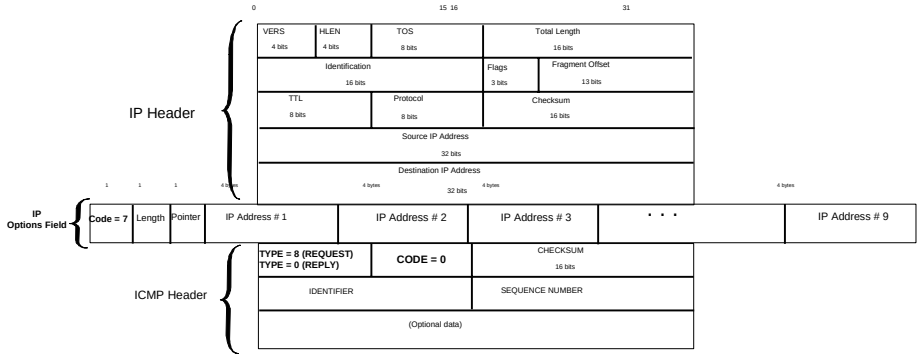


Output

```
oney % ping svr27
PING svr27: (113.23.135.1): 56 data bytes
64 bytes from (113.23.135.1): icmp_seq=0 ttl  = 240 time=600 ms
64 bytes from (113.23.135.1): icmp_seq=1 ttl  = 240 time=800 ms
64 bytes from (113.23.135.1): icmp_seq=3 ttl  = 240 time=500 ms
64 bytes from (113.23.135.1): icmp_seq=4 ttl  = 240 time=380 ms
64 bytes from (113.23.135.1): icmp_seq=5 ttl  = 240 time=270 ms
^c
-------svr27 PING statistics--------
6 packets sent, 5 packets received, 16% packet loss
round-trip min/avg/max = 270/510/800 ms
```

81

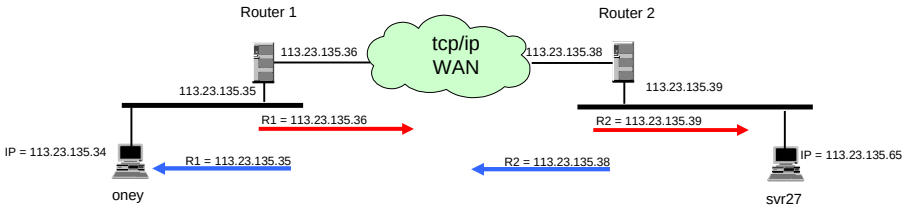
PING W/IP RECORD ROUTE



- Le **ping program** avec **- R** options active l' **IP Record Route** option **(Code = 7)**
  - L'expéditeur envoies un ICMP **Echo Request** avec l' IP **Record Route** activé
- Chaque routeur le long de **transmit path** ajoute son adresse IP à la liste l' **IP options field** et incrémente le champ pointeur par 4 bytes
- le récepteur **copie** cette liste des IP adresses ICMP **Echo Reply options field.**
- Chaque routeur le long de **return path adds** ajoute son adresse IP à la liste l' **IP options field** et incrémente le champ pointeur par 4 bytes
- À la réception une liste d'adresses sera imprimé

82

PING W/IP RECORD ROUTE

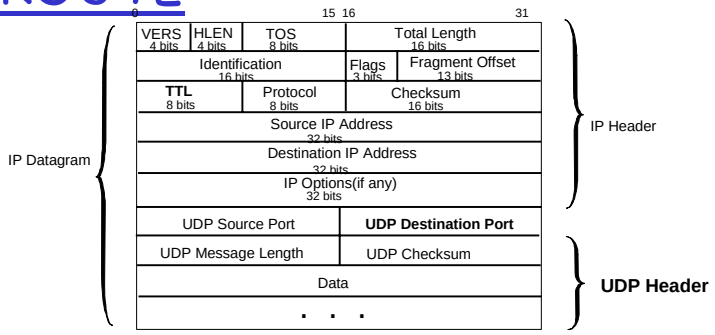


Output

```
oney % ping -R svr27
PING svr27: (113.23.135.65): 56 data bytes
64 bytes from (113.23.135.34): icmp_seq=0 ttl=220 time=600 ms
RR:     router 1 (113.23.135.36)
        router 2 (113.23.135.39)
        router 2 (113.23.135.38)
        router 1 (113.23.135.35)
^?
-------svr27 PING statistics--------
6 packets sent, 6 packets received, 0% packet loss
round-trip min/avg/max = 280/270/280 ms
```

83

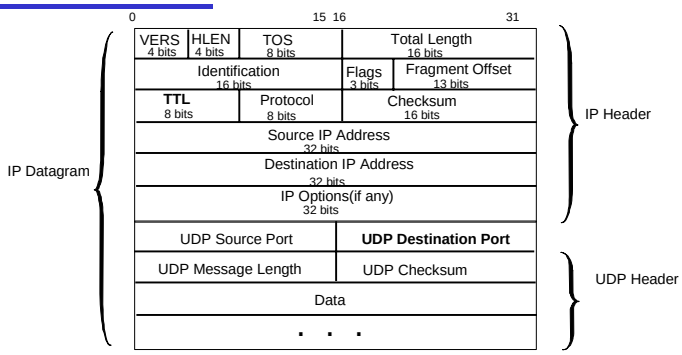
TRACEROUTE



1. Un outil de debugage écrit par Van Jacobson. Il trace la route des **UDP packets** de la machine locale jusqu'à la machine distante. Traceroute est nécessaire parceque:
   a. Tous les routeurs ne supportent pas l'**IP RR** option
   b. IP RR est normalement **one-way** option
   c. L'espace d'IP Options n'est pas assez grand pour manipuler beaucoup de routes
2. Traceroute encapsule **UDP avec an unreachable port** dans un paquet IP packet avec leurs **TTL variables**
   a. Il envoie un datagramme IP avec un **TTL = 1** à la destination.
   b. Le premier routeur décrémente le TTL, rejete le datagramme et renvoie un ICMP **Time Exceeded** message. cela identifie le premier routeur le long du chemin

84

TRACEROUTE

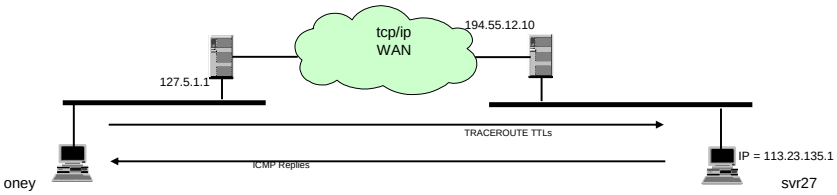


c. Traceroute envoie un IP datagram avec **TTL = 2** à la destination
d. Le second routeur décrémente the TTL, rejete le datagramme et renvoie un ICMP **Time Exceeded** message. Cela identifie le second routeur le long du chemin. Etc.
e. Traceroute montre une ligne de sortie pour chaque ICMP Time Exceeded message

3. Le UDP datagram utilise une destination **UDP port number plus grand 30,000**. Ce plus haut numéro de port sera normalement non utilisé
4. Traceroute fait la différence entre **Time Exceeded** et **Port Unreachable** message

85

TRACEROUTE



Output

oney % **traceroute svr27**
traceroute to svr27(113.23.135.1), 30 hops max, 40 byte packets

1 127.5.1.1 (127.5.1.1) 100ms 115ms 127ms
2 128.5.1.1 (128.5.1.1) 200ms 225ms 222ms
3 129.5.1.1 (129.5.1.1) 230ms 227ms 200ms
4 192.55.12.10 (192.55.12.10) 250ms 240ms 255ms
5 193.55.12.10 (193.55.12.10) 294ms 300ms 294ms
6 194.55.12.10 (194.55.12.10) 324ms 324ms 324ms
7 113.23.135.1 (113.23.135.1) 325ms 300ms 310ms

86

Cours 2: plan

2.1 Introduction
2.2 IP: Adressage
2.3 IP: Routage
2.4 ARP Protocole
2.5 ICMP Protocole
2.6 IGMP Protocole

Internet Group Management Protocol (IGMP)

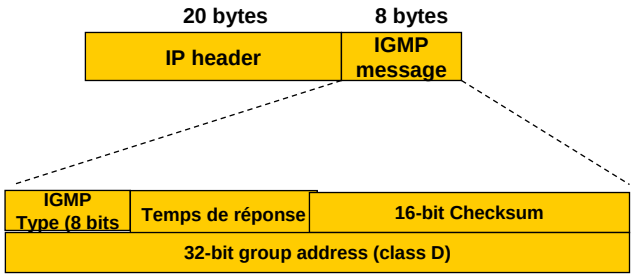
IGMP

- Version 1 d' IGMP était basée sur des messages primaires
  - Members Group Query: 1 query envoyé par le routeur
  - Members Group Reports: 0 report envoyé par la machine
- Version 2 fournit un champ maximum de temps de réponse dans le paquet Query packet
- Version 3 ajoute une fonction de filtrage à la source et la possibilité de spécifier les sources qui peuvent envoyer au multicast group

89

IGMP

- IGMP fait partie de la couche IP
- IGMP messages sont encapsulés dans des paquets IP



90

IGMP: Opération

- Pour joindre le groupe, les hosts envoient un report message
  - Adresse de groupe pour joindre
  - Toutes les hosts dans le groupe reçoivent le message
- Routeurs envoient périodiquement request message
  - Envoie à toutes les machines du groupe
  - Host qui veut rester dans les groupes doit lire tous les messages et répond avec un report pour chaque groupe

91

IGMP Host Queries

- Les routeurs utilisent IGMP "query" messages périodiquement pour découvrir les membres de groupe multicast
  - Hosts qui sont membres des groupes multicast répondent avec un message IGMP "report" pour chaque groupe où il est membre
  - Pour améliorer efficacement, hosts attendent un temps moyen aléatoire avant de répondre (de 0 à 10 secondes)
    - ✓ Pendant le temps d'attente, hosts écoutent les réponses des autres
    - ✓ Si une host du groupe répond, alors les autres hosts du même groupe ne répondent pas

92

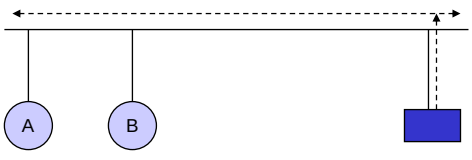
IGMP Host Queries

un Exemple

Exemple: A et B sont membres de multicast group G_1

93

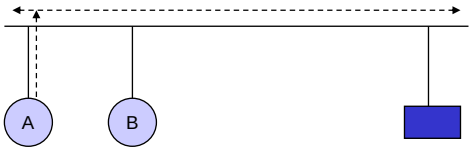
IGMP query, TTL=1
IGMP destination group = 0
IP destination address = 224.0.0.1
IP source address = router address



A waits 100 ms B waits 200 ms

94

IGMP report, TTL=1
IGMP destination group = G_1
IP destination address = G_1
IP source address = A



A responds 100 ms later

B aborts response because it hears A's report

Router is now aware that at least one host on its subnet is a member of G_1

95

IGMP Reports

- Hosts peuvent aussi envoyer des IGMP reports quand elles rejoient la première fois le multicast group
  - Dans ce cas elles n'ont pas besoin d'attendre un IGMP query
- Quand les hosts quittent le groupe, ils envoient d'annonces

96