

INF3050 Réseaux Informatiques

Bassem Haidar

Plan du cours

- Introduction, Modèle OSI et TCP-IP
- Couche Physique – Supports de transmission
- Couche Liaison – Ethernet
- Couche Réseaux – Adressage IPv4
- **ARP - ICMP – DHCP**
- Routage statique
- Couche Transport (UDP - TCP)
- Introduction a la couche application

Couche Réseaux

ARP – ICMP - DHCP

Chapter 05

Résolution d'adresse - ARP

Adresses MAC et ARP

- Adresse IP 32 bits :
 - adresse de couche réseau pour l'interface
 - utilisé pour le transfert de couche 3 (couche réseau)
- Adresse MAC (ou LAN ou physique ou Ethernet) :
 - fonction : utilisé « localement » pour envoyer une trame d'une interface à une autre interface physiquement connectée (même réseau, au sens de l'adressage IP)
 - Adresse MAC 48 bits (pour la plupart des réseaux locaux) gravée dans la ROM NIC, parfois également réglable par logiciel
 - Ex : 1A-2F-BB-76-09-AD

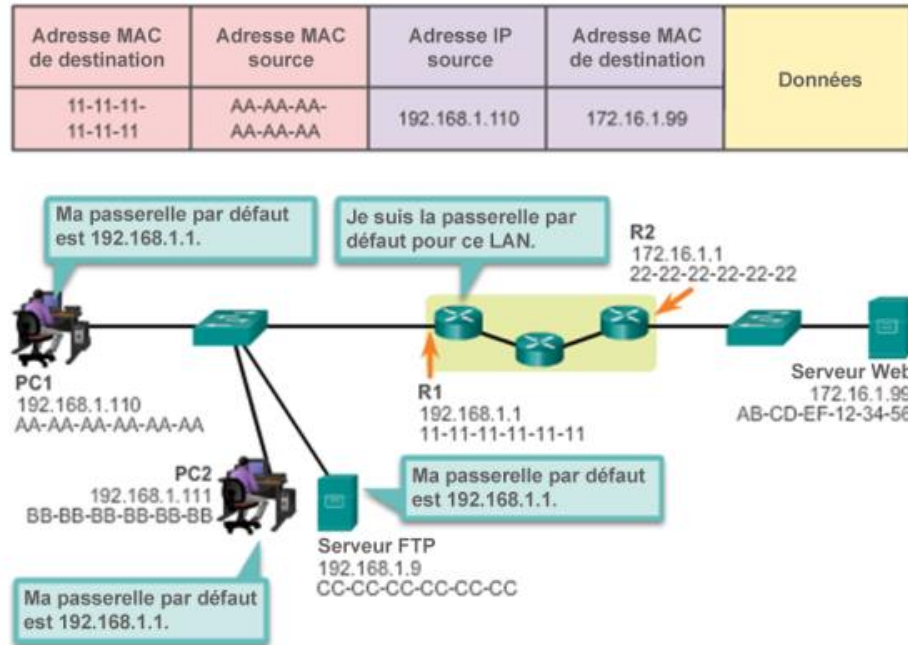
hexadecimal (base 16) notation
(each "numeral" represents 4 bits)

Connexion des appareils

Les passerelles par défaut

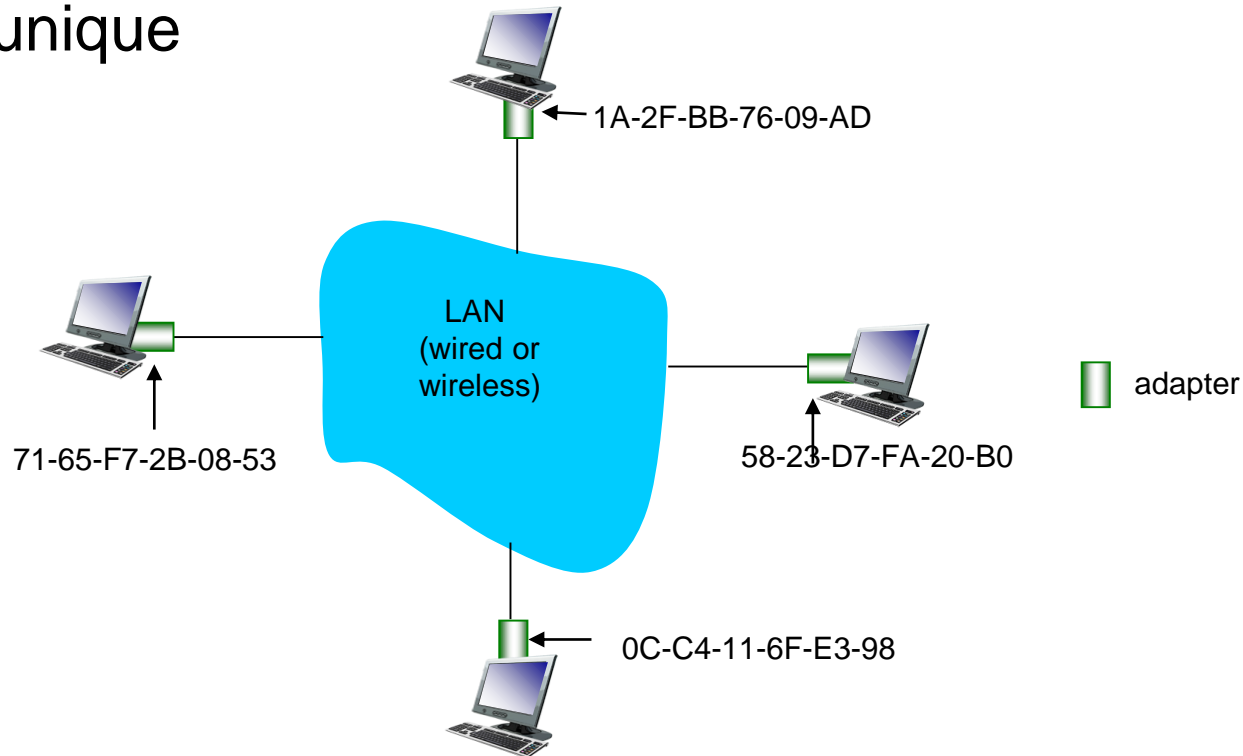
Pour assurer l'accès réseau, les appareils doivent être configurés avec les informations d'adresse IP suivantes :

- **Adresse IP** : identifie un hôte unique sur un réseau local.
- **Masque de sous-réseau** : identifie le sous-réseau du réseau de l'hôte.
- **Passerelle par défaut** : identifie le routeur auquel un paquet est envoyé lorsque la destination n'est pas sur le même sous-réseau du réseau local.



Adresses LAN et ARP

- chaque adaptateur sur le LAN a une adresse LAN unique



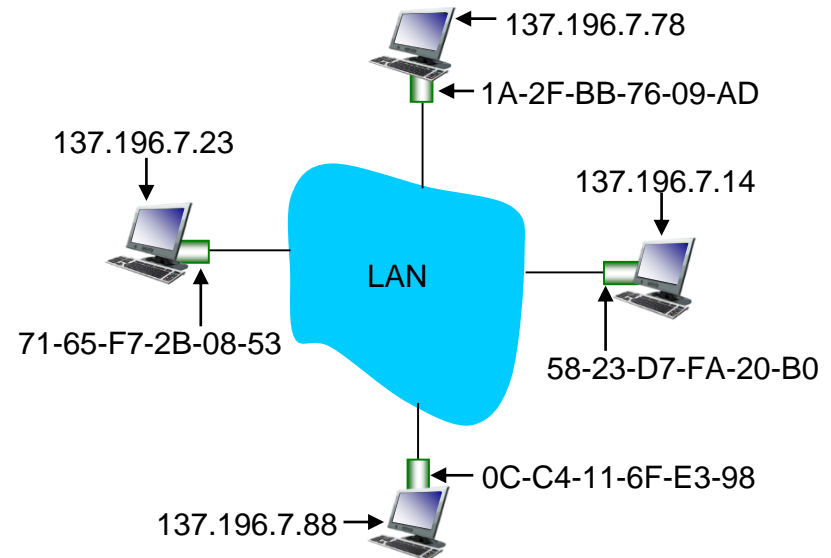
Adresses LAN

- Allocation d'adresse MAC administrée par IEEE
- le fabricant achète une partie de l'espace d'adressage MAC (pour assurer l'unicité)
- analogie:
 - Adresse MAC : comme le numéro de sécurité sociale
 - Adresse IP : comme l'adresse postale
- Adresse MAC plateforme → portabilité
 - peut déplacer la carte LAN d'un LAN à un autre
- Adresse IP hiérarchique non portable
 - l'adresse dépend du sous-réseau IP auquel le nœud est attaché

ARP: address resolution protocol

- Table ARP : chaque nœud IP (hôte, routeur) sur le réseau local a une table
 - Mappages d'adresses IP/MAC pour certains nœuds LAN :
- < IP address; MAC address; TTL>
 - TTL (Time To Live) : temps après lequel le mappage d'adresse sera oublié (typiquement 20 min)

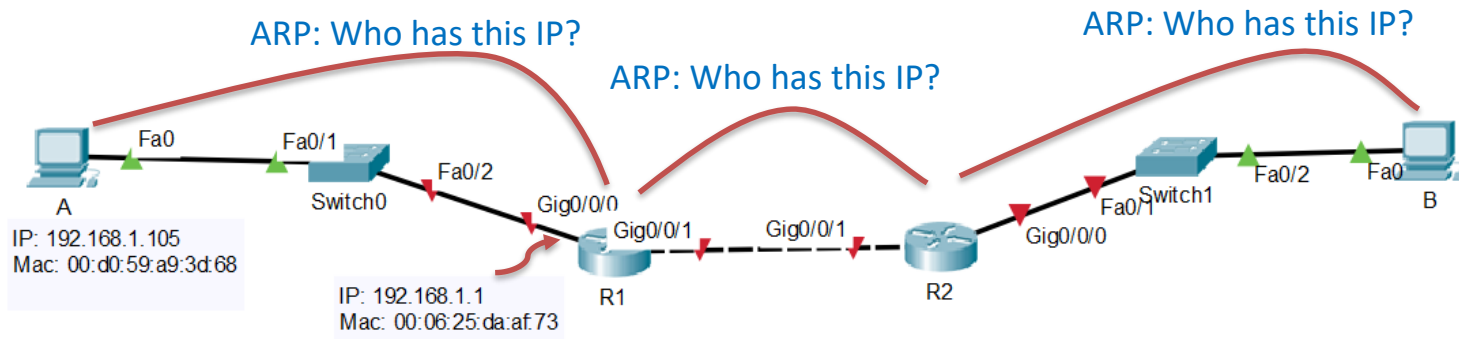
Question: comment déterminer l'adresse MAC de l'interface, connaissant son adresse IP?



IP address	MAC address	TTL
137.196.7.14	58-23-D7-FA-20-B0	20

Protocole ARP : même LAN

- A veut envoyer un datagramme à B
 - L'adresse MAC de B n'est pas dans la table ARP de A.
- A **diffuse** un paquet de requête ARP, contenant l'adresse IP de B
 - adresse MAC de destination = FF-FF-FF-FF-FF-FF
 - tous les nœuds du LAN reçoivent une requête ARP
- B reçoit le paquet ARP, répond à A avec son adresse MAC (B)
 - trame envoyée à l'adresse MAC de A (unicast)
- Une paire d'adresses IP-MAC en cache (sauvegarde) dans sa table ARP jusqu'à ce que les informations deviennent obsolètes (expiration du délai)
- ARP est « plug-and-play » :
 - les nœuds créent leurs tables ARP sans intervention de l'administrateur réseau



ethernet-ethertrace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Source	Destination	Protocol	Length	Info
10.000000	AmbitMic_a9:3...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
20.001018	LinksysG_da:a...	AmbitMic_a9:3d...	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
613.542...	CnetTech_73:8...	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104

<

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)

> Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Destination: Broadcast (ff:ff:ff:ff:ff:ff)

> Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

Type: ARP (0x0806)

> Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

Sender IP address: 192.168.1.105

Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.1.1

The image shows a Wireshark packet capture analysis of an ARP request. The top toolbar includes File, Edit, View, Go, Capture, Analysis, Statistics, Wireless, Tools, and Help. The main display area shows three packets:

No.	Time	Source	Destination	Protocol	Length	Info
10	0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
20	0.001018	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
613	542....	CnetTech_73:8...	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104

Below the packet list, the details of the selected packet (No. 20) are shown:

- Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
- Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
 - Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
 - Source: LinksysG_da:af:73 (00:06:25:da:af:73)
 - Type: ARP (0x0806)
 - Padding: 00000000000000000000000000000000
- Address Resolution Protocol (reply)
 - Hardware type: Ethernet (1)
 - Protocol type: IPv4 (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: reply (2)
 - Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
 - Sender IP address: 192.168.1.1
 - Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
 - Target IP address: 192.168.1.105

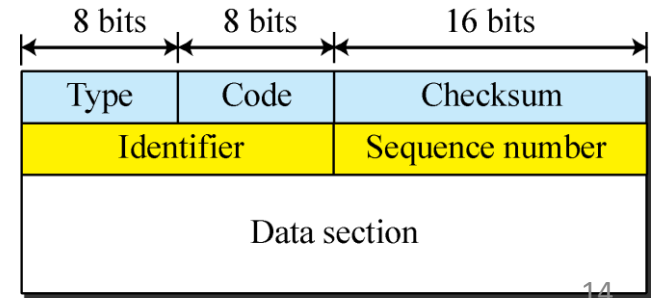
Internet Control Message Protocol version 4 ICMP

Internet Control Message Protocol version 4

- L'IPv4 n'a pas de mécanisme de rapport d'erreur ou de correction d'erreur.
- Le protocole IP manque également d'un mécanisme pour les requêtes d'hôte et de gestion.
- L'Internet Control Message Protocol version 4 (ICMPv4) a été conçu pour compenser les deux lacunes ci-dessus.

MESSAGES

- Les messages ICMP sont divisés en deux grandes catégories :
 1. Messages de rapport d'erreur : signalent les problèmes qu'un routeur ou un hôte (destination) peut rencontrer lors du traitement d'un paquet IP.
 2. Messages de requête : qui se produisent par paires, aident un hôte ou un gestionnaire de réseau à obtenir des informations spécifiques d'un routeur ou d'un autre hôte. Par exemple, les nœuds peuvent découvrir leurs voisins. En outre, les hôtes peuvent découvrir et se renseigner sur les routeurs de leur réseau et les routeurs peuvent aider un nœud à rediriger ses messages.



ICMP: internet control message protocol

- Utilisé par les hôtes et les routeurs pour communiquer des informations au niveau du réseau
 - rapport d'erreurs : hôte, réseau, port, protocole inaccessible
 - requête/réponse d'écho (utilisée par ping)
- IP de la couche réseau « au-dessus » :
 - Messages ICMP transportés dans des datagrammes IP
- Message ICMP : type, code plus les 8 premiers octets du datagramme IP provoquant une erreur

Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

Outils de débogage

- Il existe plusieurs outils qui peuvent être utilisés sur Internet pour le débogage. Nous pouvons déterminer la viabilité d'un hôte ou d'un routeur. Nous pouvons tracer la route d'un paquet.
- Nous présentons deux outils qui utilisent ICMP pour le débogage :
- Ping :
 - Nous pouvons utiliser le programme ping pour déterminer si un hôte est vivant et répond. L'hôte source envoie des messages de demande d'écho ICMP.
- Traceroute ou Tracert :
 - Le programme traceroute sous UNIX ou tracert sous Windows peut être utilisé pour tracer le chemin d'un paquet d'une source à la destination. Il peut trouver les adresses IP de tous les routeurs visités le long du chemin.
- Le programme traceroute obtient l'aide de deux messages de rapport d'erreur :
 - Message dépassé.
 - Message de destination inaccessible.


```
C:\Users\samova>ping www.google.com
```

```
Pinging www.google.com [216.58.213.164] with 32 bytes of data:
```

```
Reply from 216.58.213.164: bytes=32 time=8ms TTL=116
```

```
Reply from 216.58.213.164: bytes=32 time=11ms TTL=116
```

```
Reply from 216.58.213.164: bytes=32 time=10ms TTL=116
```

```
Reply from 216.58.213.164: bytes=32 time=10ms TTL=116
```

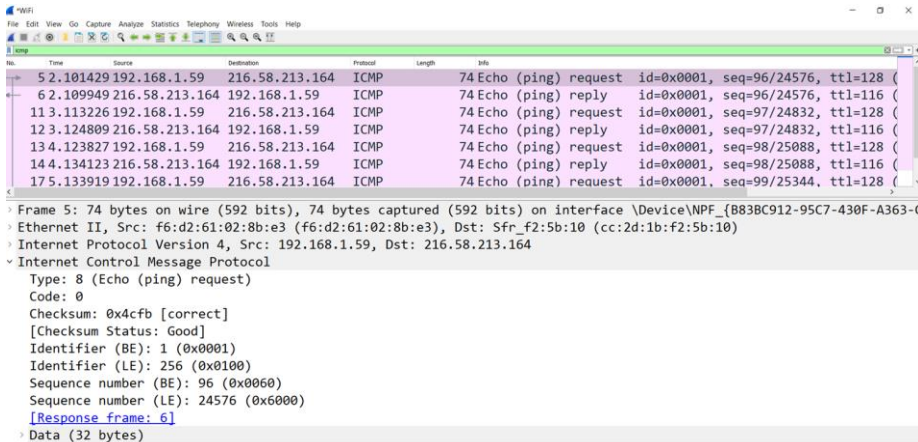
```
Ping statistics for 216.58.213.164:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 8ms, Maximum = 11ms, Average = 9ms
```

Command ping



Wireshark packet capture showing ping results to 216.58.213.164. The capture shows four ICMP Echo (ping) requests and four replies. The first request is at time 5.2.101429, and the first reply is at time 6.2.109949. The capture is filtered on the interface \Device\NPF_{B83BC912-95C7-430F-A363-...}.

No.	Time	Source	Destination	Protocol	Length	Info
5	5.2.101429	192.168.1.59	216.58.213.164	ICMP	74	Echo (ping) request id=0x0001, seq=96/24576, ttl=128 (
6	6.2.109949	216.58.213.164	192.168.1.59	ICMP	74	Echo (ping) reply id=0x0001, seq=96/24576, ttl=116 (
11	11.3.113226	192.168.1.59	216.58.213.164	ICMP	74	Echo (ping) request id=0x0001, seq=97/24832, ttl=128 (
12	13.124809	216.58.213.164	192.168.1.59	ICMP	74	Echo (ping) reply id=0x0001, seq=97/24832, ttl=116 (
13	13.4.123827	192.168.1.59	216.58.213.164	ICMP	74	Echo (ping) request id=0x0001, seq=98/25088, ttl=128 (
14	14.4.134123	216.58.213.164	192.168.1.59	ICMP	74	Echo (ping) reply id=0x0001, seq=98/25088, ttl=116 (
17	17.5.133919	192.168.1.59	216.58.213.164	ICMP	74	Echo (ping) request id=0x0001, seq=99/25344, ttl=128 (

Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B83BC912-95C7-430F-A363-...} Ethernet II, Src: f6:d2:61:02:8b:e3 (f6:d2:61:02:8b:e3), Dst: Sfr_f2:5b:10 (cc:2d:1b:f2:5b:10)

Internet Protocol Version 4, Src: 192.168.1.59, Dst: 216.58.213.164

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x4cfb [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

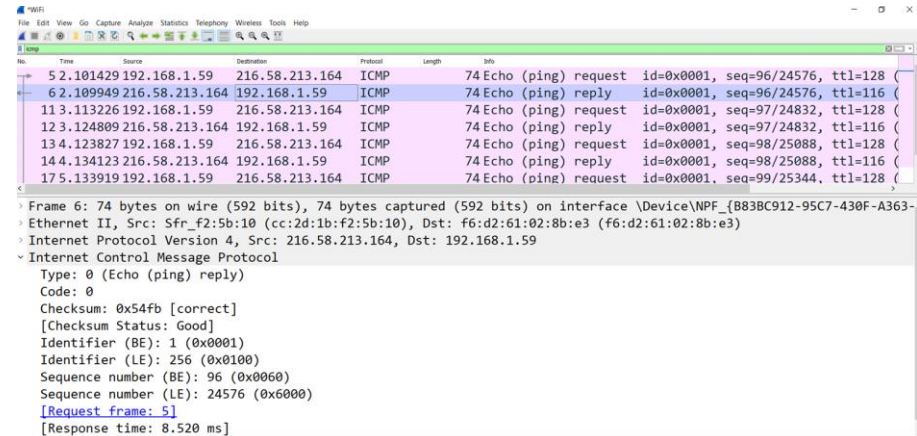
Identifier (LE): 256 (0x0100)

Sequence number (BE): 96 (0x0060)

Sequence number (LE): 24576 (0x6000)

[Response frame: 6]

Data (32 bytes)



Wireshark packet capture showing ping results to 216.58.213.164. The capture shows four ICMP Echo (ping) requests and four replies. The first request is at time 5.2.101429, and the first reply is at time 6.2.109949. The capture is filtered on the interface \Device\NPF_{B83BC912-95C7-430F-A363-...}.

No.	Time	Source	Destination	Protocol	Length	Info
5	5.2.101429	192.168.1.59	216.58.213.164	ICMP	74	Echo (ping) request id=0x0001, seq=96/24576, ttl=128 (
6	6.2.109949	216.58.213.164	192.168.1.59	ICMP	74	Echo (ping) reply id=0x0001, seq=96/24576, ttl=116 (
11	11.3.113226	192.168.1.59	216.58.213.164	ICMP	74	Echo (ping) request id=0x0001, seq=97/24832, ttl=128 (
12	13.124809	216.58.213.164	192.168.1.59	ICMP	74	Echo (ping) reply id=0x0001, seq=97/24832, ttl=116 (
13	13.4.123827	192.168.1.59	216.58.213.164	ICMP	74	Echo (ping) request id=0x0001, seq=98/25088, ttl=128 (
14	14.4.134123	216.58.213.164	192.168.1.59	ICMP	74	Echo (ping) reply id=0x0001, seq=98/25088, ttl=116 (
17	17.5.133919	192.168.1.59	216.58.213.164	ICMP	74	Echo (ping) request id=0x0001, seq=99/25344, ttl=128 (

Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B83BC912-95C7-430F-A363-...} Ethernet II, Src: Sfr_f2:5b:10 (cc:2d:1b:f2:5b:10), Dst: f6:d2:61:02:8b:e3 (f6:d2:61:02:8b:e3)

Internet Protocol Version 4, Src: 216.58.213.164, Dst: 192.168.1.59

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0x54fb [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 96 (0x0060)

Sequence number (LE): 24576 (0x6000)

[Request frame: 5]

[Response time: 8.520 ms]

Traceroute et ICMP

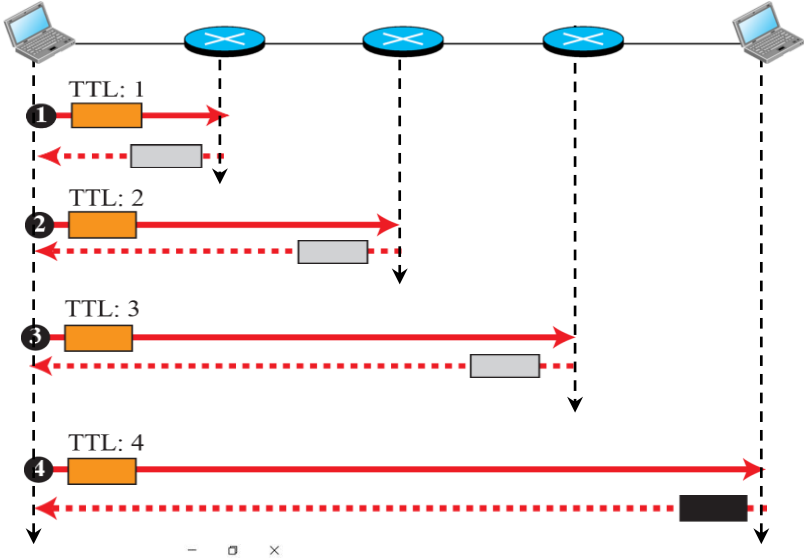
- la source envoie une série de segments UDP à la destination
 - le premier ensemble a un TTL =1
 - le deuxième ensemble a TTL=2, etc.
 - numéro de port improbable
- lorsque le datagramme du nième ensemble arrive au nième routeur :
 - le routeur supprime le datagramme et envoie le message ICMP source (type 11, code 0)
 - Le message ICMP inclut le nom du routeur et l'adresse IP
- lorsque le message ICMP arrive, la source enregistre les RTT
 - critère d'arrêt :*
 - Le segment UDP arrive finalement à l'hôte de destination*
 - la destination renvoie le message ICMP « port inaccessible » (type 3, code 3)*
 - la source s'arrête*

```
C:\Users\samova>tracert www.google.com

Tracing route to www.google.com [172.217.22.132]
over a maximum of 30 hops:

 1    3 ms    1 ms    1 ms    box [192.168.1.1]
 2    5 ms    5 ms    3 ms    78nsa1-nro-1.nro.gaoland.net [109.24.76.75]
 3    6 ms    6 ms    34 ms   j-1.0.154.77.rev.sfr.net [77.154.0.161]
 4    5 ms    5 ms    7 ms    89.144.6.194.rev.sfr.net [194.6.144.89]
 5   10 ms   11 ms   14 ms   136.144.6.114.rev.sfr.net [194.6.144.186]
 6    9 ms    7 ms    7 ms    140.144.6.154.rev.sfr.net [194.6.144.186]
 7   10 ms    7 ms   19 ms   14.14.194.10
 8   13 ms    9 ms   12 ms   103.170.231.111
 9   10 ms    7 ms    7 ms    60.249.95.247
10    9 ms    6 ms   10 ms   par21s12-in-f4.1e100.net [172.217.22.132]

Trace complete.
```



Capturing from WiFi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
82	10.817...	192.168.1.59	172.217.22.132	ICMP	106	Echo (ping) request id=0x0001, seq=100/25600, ttl=1 (no
83	10.821...	192.168.1.1	192.168.1.59	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
84	10.821...	192.168.1.59	172.217.22.132	ICMP	106	Echo (ping) request id=0x0001, seq=101/25856, ttl=1 (no
85	10.822...	192.168.1.1	192.168.1.59	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
86	10.823...	192.168.1.59	172.217.22.132	ICMP	106	Echo (ping) request id=0x0001, seq=102/26112, ttl=1 (no
87	10.824...	192.168.1.1	192.168.1.59	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
1...	16.384...	192.168.1.59	172.217.22.132	ICMP	106	Echo (ping) request id=0x0001, seq=103/26368, ttl=2 (no
1...	16.390...	109.24.76.75	192.168.1.59	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
1...	16.393...	192.168.1.59	172.217.22.132	ICMP	106	Echo (ping) request id=0x0001, seq=104/26624, ttl=2 (no
1...	16.398...	109.24.76.75	192.168.1.59	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
1...	16.401...	192.168.1.59	172.217.22.132	ICMP	106	Echo (ping) request id=0x0001, seq=105/26880, ttl=2 (no
1...	16.404...	109.24.76.75	192.168.1.59	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
1...	21.997...	192.168.1.59	172.217.22.132	ICMP	106	Echo (ping) request id=0x0001, seq=106/27136, ttl=3 (no
1...	22.004...	77.154.0.161	192.168.1.59	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1...	22.007...	192.168.1.59	172.217.22.132	ICMP	106	Echo (ping) request id=0x0001, seq=107/27392, ttl=3 (no

> Frame 82: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{B83BC912-95C7-430F-A3^
> Ethernet II, Src: f6:d2:61:02:8b:e3 (f6:d2:61:02:8b:e3), Dst: Sfr_f2:5b:10 (cc:2d:1b:f2:5b:10)
> Internet Protocol Version 4, Src: 192.168.1.59, Dst: 172.217.22.132
> Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0

Traceroute - Tracert

DHCP

Dynamic Host Configuration Protocol

IP addresses: how to get one?

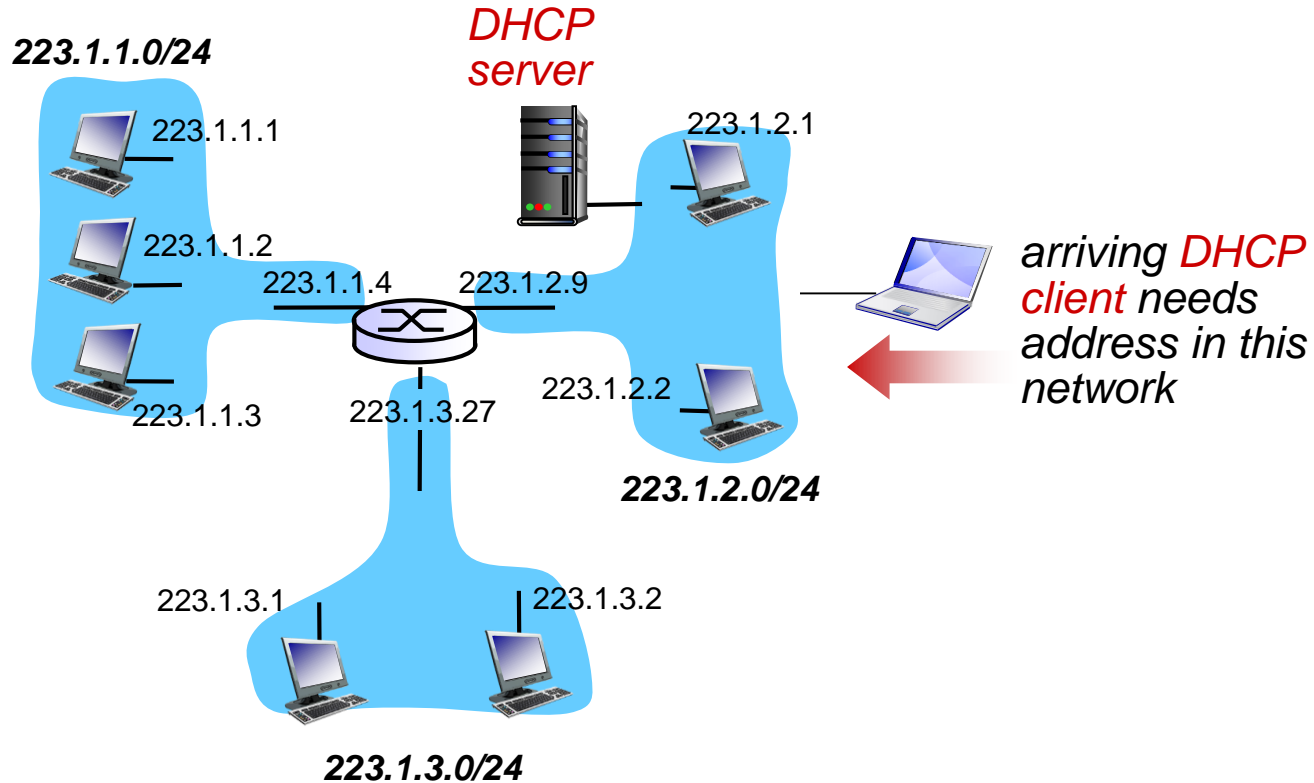
Q: How does a *host* get IP address?

- hard-coded by system admin in a file
 - Windows: control-panel->network->configuration->tcp/ip->properties
 - UNIX: /etc/rc.config
- **DHCP: Dynamic Host Configuration Protocol:** dynamically get address from as server
 - “plug-and-play”

DHCP: Dynamic Host Configuration Protocol

- goal: allow host to dynamically obtain its IP address from network server when it joins network
 - can renew its lease on address in use
 - allows reuse of addresses (only hold address while connected/“on”)
 - support for mobile users who want to join network (more shortly)
- DHCP overview:
 - host broadcasts “DHCP discover” msg [optional]
 - DHCP server responds with “DHCP offer” msg [optional]
 - host requests IP address: “DHCP request” msg
 - DHCP server sends address: “DHCP ack” msg

DHCP client-server scenario



DHCP client-server scenario

DHCP server: 223.1.2.5



DHCP discover

Broadcast: is there a
DHCP server out there?
.....

arriving
client



DHCP offer

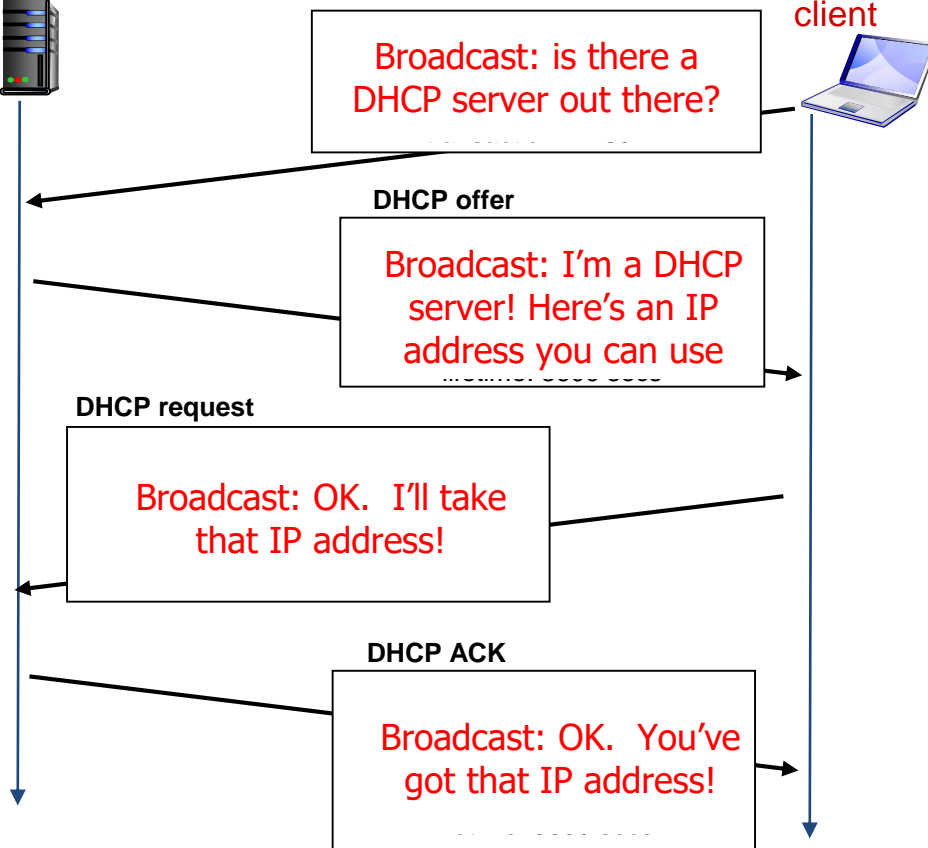
Broadcast: I'm a DHCP
server! Here's an IP
address you can use
.....

DHCP request

Broadcast: OK. I'll take
that IP address!

DHCP ACK

Broadcast: OK. You've
got that IP address!
.....



DHCP: more than IP addresses

- DHCP can return more than just allocated IP address on subnet:
 - address of first-hop router for client
 - name and IP address of DNS sever
 - network mask (indicating network versus host portion of address)