

# Niveau 3

IP – ARP – ICMP

# Protocoles – ARP – IP – TCP / UDP

- MAC Address – Ethernet
- IP Address – Subnet Mask – Gateway Address
- Unicast – Multicast – Broadcast (IP et MAC)
- TCP / UDP – Port
- ARP: correspondance entre une adresse de niveau 3 et une adresse de niveau 2.
- RARP
- ICMP

# Adresse IP (v4)

- Aujourd'hui (années 1990 – 2015) on est majoritairement en IPv4 (voir plus loin pour IPv6).
- 4 chiffres décimaux compris entre 0 et 255, séparés par des points.
- Exemple: 192.168.0.1 ou 15.125.42.89
- Normalement, une adresse par interface physique (ou logique)

# ARP

- Address Resolution Protocol
- Utilisé pour établir le lien (unique et univoque) entre une adresse de niveau 2 (MAC) et une adresse de niveau 3, connaissant l'adresse de niveau 3 !
- Le client envoie un 'ARP request', broadcast, à tout le monde
- La machine concernée répond par un 'ARP Reply'. C'est un unicast, destiné uniquement à la machine qui a envoyé l'ARP request
- Ethertype: 0x806

# Paquet ARP

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

Hardware Type										Protocol type									
Hardware address length					Protocol address length					Opcode									
Source Hardware Address																			
Source Protocol Address																			
Destination Hardware Address																			
Destination Protocol Address																			

# ARP – HW type – référence

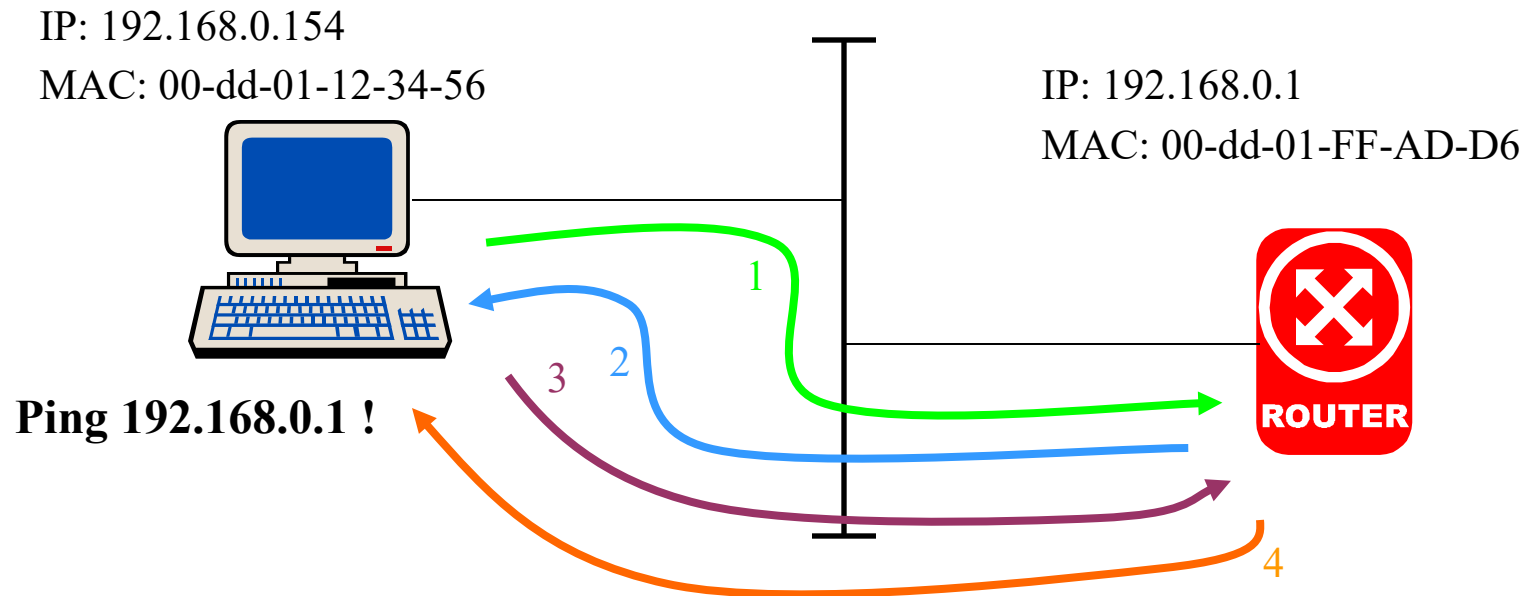
- |   |  |
|---|--|
| 1: Ethernet.                                | 17: HDLC.                                |
| 2: Experimental Ethernet.                   | 18: Fibre Channel.                       |
| 3: Amateur Radio AX.25.                     | 19: ATM, Asynchronous Transmission Mode. |
| 4: Proteon ProNET Token Ring.               | 20: Serial Line.                         |
| 5: Chaos.                                   | 21: ATM, Asynchronous Transmission Mode. |
| 6: IEEE 802.                                | 22: MIL-STD-188-220.                     |
| 7: ARCNET.                                  | 23: Metricom.                            |
| 8: Hyperchannel.                            | 24: IEEE 1394.1995.                      |
| 9: Lanstar.                                 | 25: MAPOS.                               |
| 10: Autonet Short Address.                  | 26: Twinaxial.                           |
| 11: LocalTalk.                              | 27: EUI-64.                              |
| 12: LocalNet (IBM PCNet or SYTEK LocalNET). | 28: HIPARP.                              |
| 13: Ultra link.                             | 29: IP and ARP over ISO 7816-3.          |
| 14: SMDS.                                   | 30: ARPSec.                              |
| 15: Frame Relay.                            | 31: IPsec tunnel.                        |
| 16: ATM, Asynchronous Transmission Mode.    | 32: Infiniband.                          |

# ARP – Opcode – référence

- **1** Request.
- **2** Reply.
- **3** Request Reverse.
- **4** Reply Reverse.
- **5** DRARP Request.
- **6** DRARP Reply.
- **7** DRARP Error.
- **8** InARP Request.
- **9** InARP Reply.
- **10** ARP NAK.
- **11** MARS Request.
- **12** MARS Multi.
- **13** MARS MServ.
- **14** MARS Join.
- **15** MARS Leave.
- **16** MARS NAK.
- **17** MARS Unserv.
- **18** MARS SJoin.
- **19** MARS SLeave.
- **20** MARS Grouplist Request.
- **21** MARS Grouplist Reply.
- **22** MARS Redirect Map.
- **23** MAPOS UNARP.

Protocol Type: 0x800 = IP

# ARP – Fonctionnement



1: ARP REQUEST (Broadcast): Qui connaît 192.168.0.1 ???

2: ARP REPLY (Unicast): Moi ! La MAC est 00-dd-01-FF-AD-D6

3: ICMP ECHO REQUEST: Ouh ouh ? Es-tu là ???

4: ICMP ECHO REPLY: Oui, je suis là !!!

Cf: suite du cours...



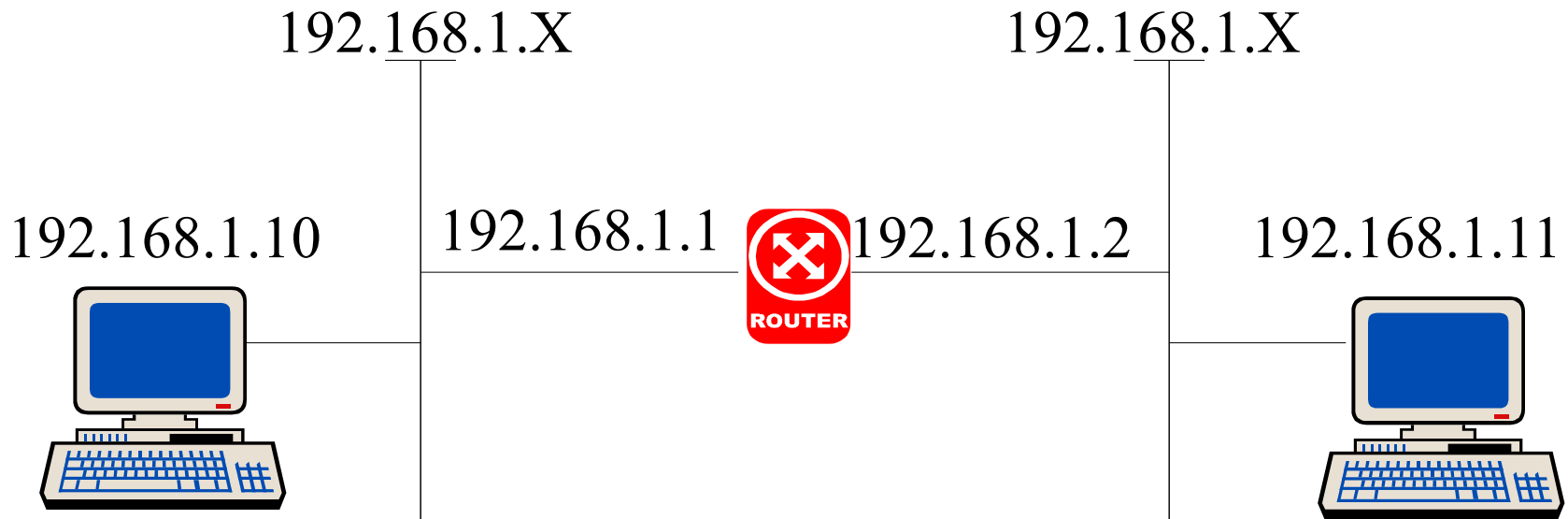
# ARP – Exemple

•	No.	Time	Source	Destination	Protocol	Info
•	1	0.000000	192.168.0.35	Broadcast	ARP	Who has 192.168.0.254? Tell 192.168.0.35
•	2	0.000419	192.168.0.254	192.168.0.35	ARP	192.168.0.254 is at 00:0a:e4:02:50:43
•	3	0.000440	192.168.0.35	10.10.10.10	ICMP	Echo (ping) request

# Proxy ARP

- Par défaut, les routeurs ne laissent pas passer les broadcasts
- Du proxy ARP peut être nécessaire si un broadcast domain est interrompu par un routeur
- Mauvais design réseau !

# Proxy ARP – Exemple



# RARP

- Reverse Address Resolution Protocol
- Utilisé pour établir le lien (unique et univoque) entre une adresse de niveau 2 (MAC) et une adresse de niveau 3, connaissant l'adresse de niveau 2 !
- Ethertype: 0x8035
- Nettement plus rare que ARP !
- Peut être utilisé pour obtenir une adresse IP automatiquement (comme BOOTP ou DHCP), mais UNIQUEMENT l'adresse IP... pas les autres paramètres. Utilisé donc uniquement sur un LAN.

# Paquet IP

**IP = « Best Effort »**

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Version				IHL				Type of Service								Total length															
Identification																Flags		Fragment Offset													
Time To Live								Protocol ID								Header Checksum															
Source Address																															
Destination Address																															
Options et données																															

# Default Gateway

- Quand une machine veut envoyer un paquet, elle doit comparer l'adresse destination avec sa propre adresse grâce au subnet mask (ET logique)
- Si les deux machines sont sur le même réseau, on envoie directement (ARP)
- Si les deux machines ne sont pas sur le même réseau, on s'adresse au default gateway (ARP aussi !)

# Le champ ToS – 1

- Défini dans la RFC 1349
- 3 bits de précedence (définit le PHB, utilisé pour la gestion des queues)
  - 111: network control (protocoles de routage)
  - 110: Internetwork control
  - 101: Critic / ECP
  - 100: Flash override
  - 011: Flash
  - 010: Immediat
  - 001: Priorité
  - 000: Routine (BE)

1	2	3	4	5	6	7	8
Prec			Type of Service				0

# Le champ ToS – 2

- 4 bits de Type of Service (Rarement implémenté, complexe, beaucoup de CPU)
  - 1000: D : Minimiser le délai
  - 0100: T : Maximiser le débit
  - 0010: R : Maximiser la fiabilité
  - 0001: C : Minimiser le coût financier
  - 0000: Service normal
  - 1111: Maximiser la sécurité

1	2	3	4	5	6	7	8
Prec			D	T	R	C	0



# Le champ FLAG

- Le champ FLAG est composé de 3 bits:
  - 0: Pas utilisé !
  - 1: 0 = may fragment, 1 = don't fragment
  - 2: 0 = last fragment, 1 = other fragment coming...

# ICMP

- Internet Control Message Protocol
- Application ‘ping’, ‘traceroute’ et autres...
- RFC 792
- Tourne sur IP: Protocol ID numéro 1 !
- Utilité: problèmes de base !

# Paquet ICMP

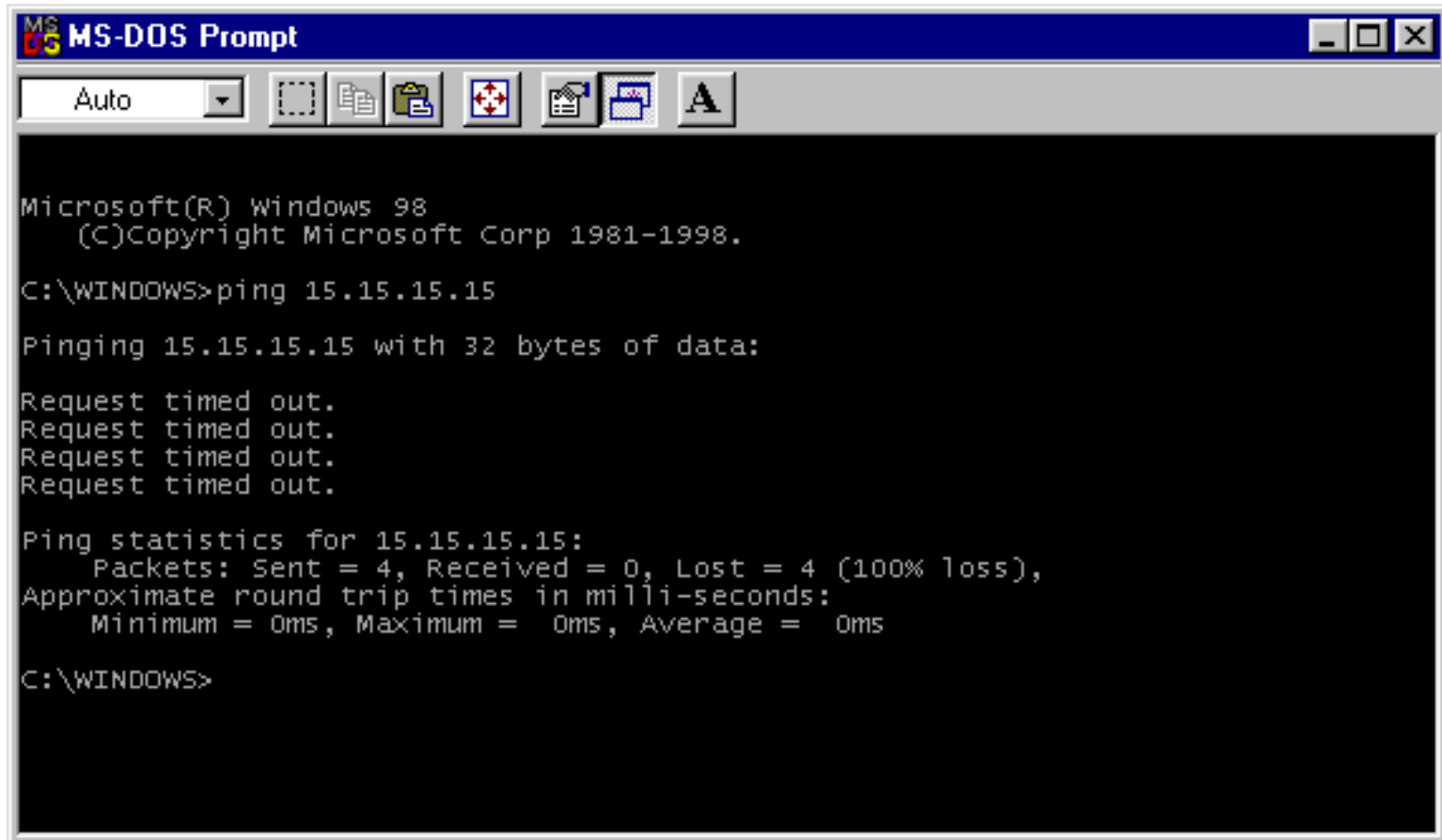
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Type								Code								ICMP Header Checksum															
ICMP DATA																															

- Le type détermine le type de paquet
- Le code est déterminé par le type

# ICMP – Type – Référence

- 0: Echo reply
- 3: Destination unreachable
- 4: Source quench
- 5: Redirect
- 8: Echo request
- 9: Router advertisement
- 10: Router solicitation
- 11: TTL exceeded
- 12: Parameter problem
- 13: Timestamp request
- 14: Timestamp reply
- 15: Information request
- 16: Information reply
- 17: Address mask request
- 18: Address mask reply
- 30: Traceroute
- 31: Conversion error
- 32: Mobile host redirect
- 33: IPv6 Where-are-you
- 34: IPv6 I-am-here
- 35: Mobile registration request
- 36: Mobile registration reply
- 37: Domain name request
- 38: Domain name reply
- 39: SKIP protocol
- 40: Security failures

# ICMP – Exemple 1



The image shows a screenshot of an MS-DOS Prompt window. The title bar reads "MS-DOS Prompt" with standard window controls. Below the title bar is a toolbar with icons for "Auto", a list, a folder, a network, a printer, and a large "A" icon. The main text area is black with white text. It shows the output of a ping command to 15.15.15.15, which failed with 100% loss.

```
Microsoft(R) Windows 98
(C)Copyright Microsoft Corp 1981-1998.

C:\WINDOWS>ping 15.15.15.15

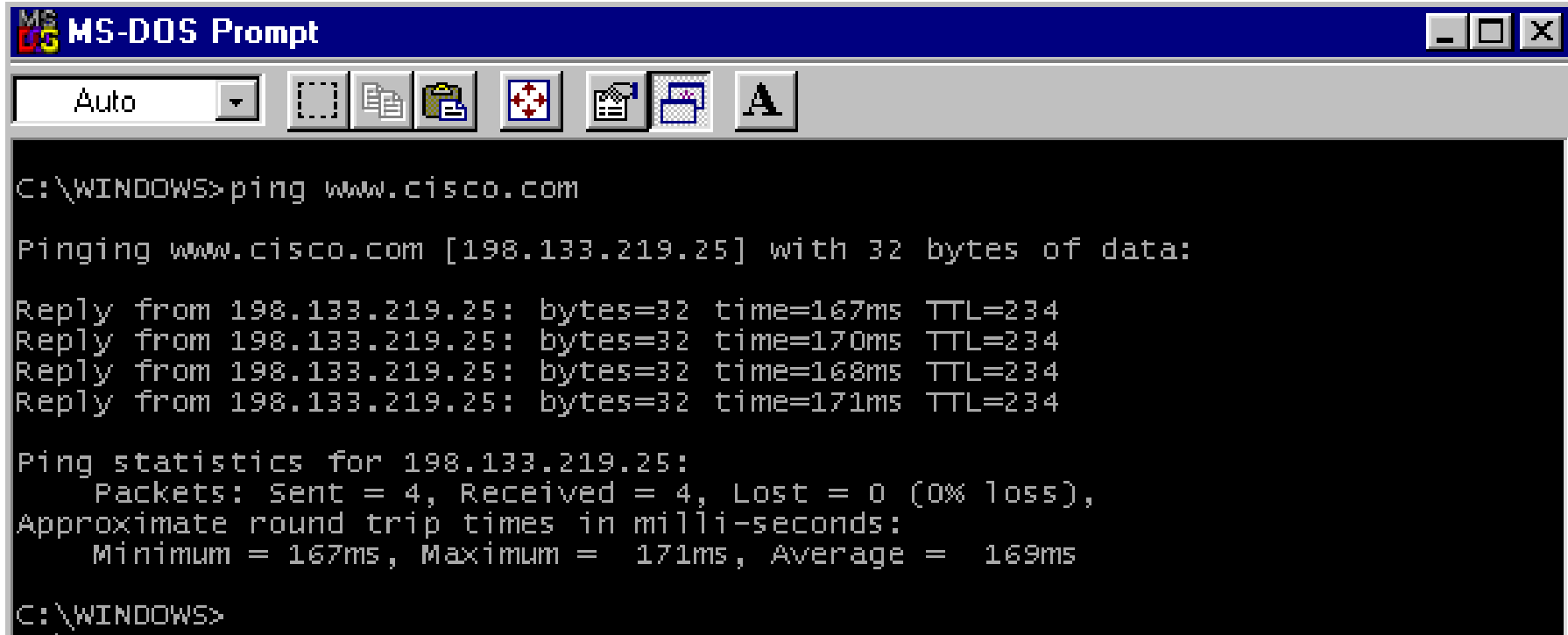
Pinging 15.15.15.15 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 15.15.15.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\WINDOWS>
```

# ICMP – Exemple 2



The image shows a screenshot of an MS-DOS Prompt window. The title bar is blue with the text "MS-DOS Prompt" and standard window control buttons (minimize, maximize, close). Below the title bar is a toolbar with icons for file operations (Auto, Find, Print, Copy, Paste, etc.). The main area of the window is black with white text. The text shows a command prompt session where the user has entered "ping www.cisco.com". The output shows four successful replies from 198.133.219.25 with varying times and a TTL of 234. Ping statistics are also displayed, showing 0% loss and an average round trip time of 169ms.

```
C:\WINDOWS>ping www.cisco.com

Pinging www.cisco.com [198.133.219.25] with 32 bytes of data:

Reply from 198.133.219.25: bytes=32 time=167ms TTL=234
Reply from 198.133.219.25: bytes=32 time=170ms TTL=234
Reply from 198.133.219.25: bytes=32 time=168ms TTL=234
Reply from 198.133.219.25: bytes=32 time=171ms TTL=234

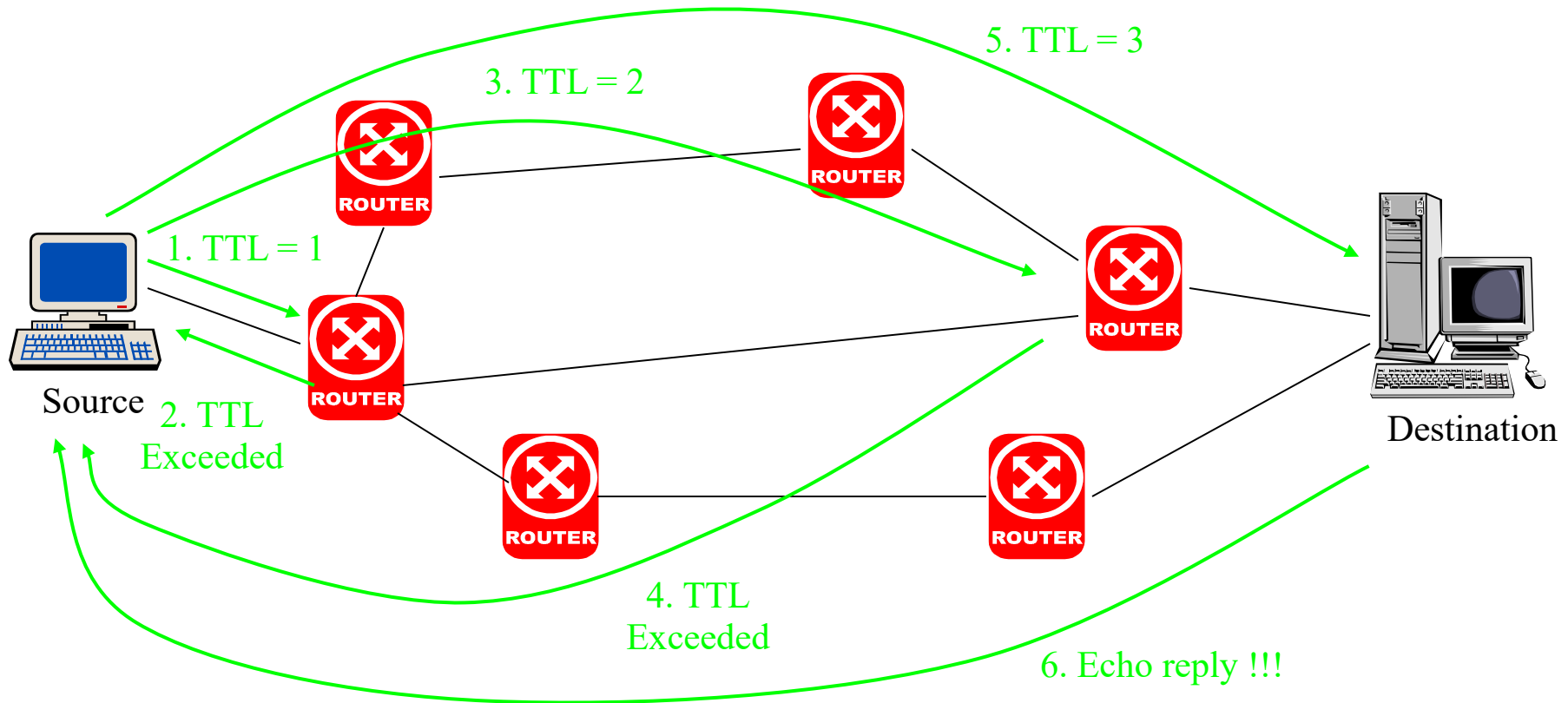
Ping statistics for 198.133.219.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 167ms, Maximum = 171ms, Average = 169ms

C:\WINDOWS>
```

# Traceroute

- Qu'est ce que c'est ?
- Application basée sur ICMP.
- Comment ça marche ?
- On envoie des paquets vers la même destination avec des TTL de plus en plus grand, en partant de 1 !
- Parfois (souvent) limité à 32 hops, diamètre maximum de l'Internet de nos jours...

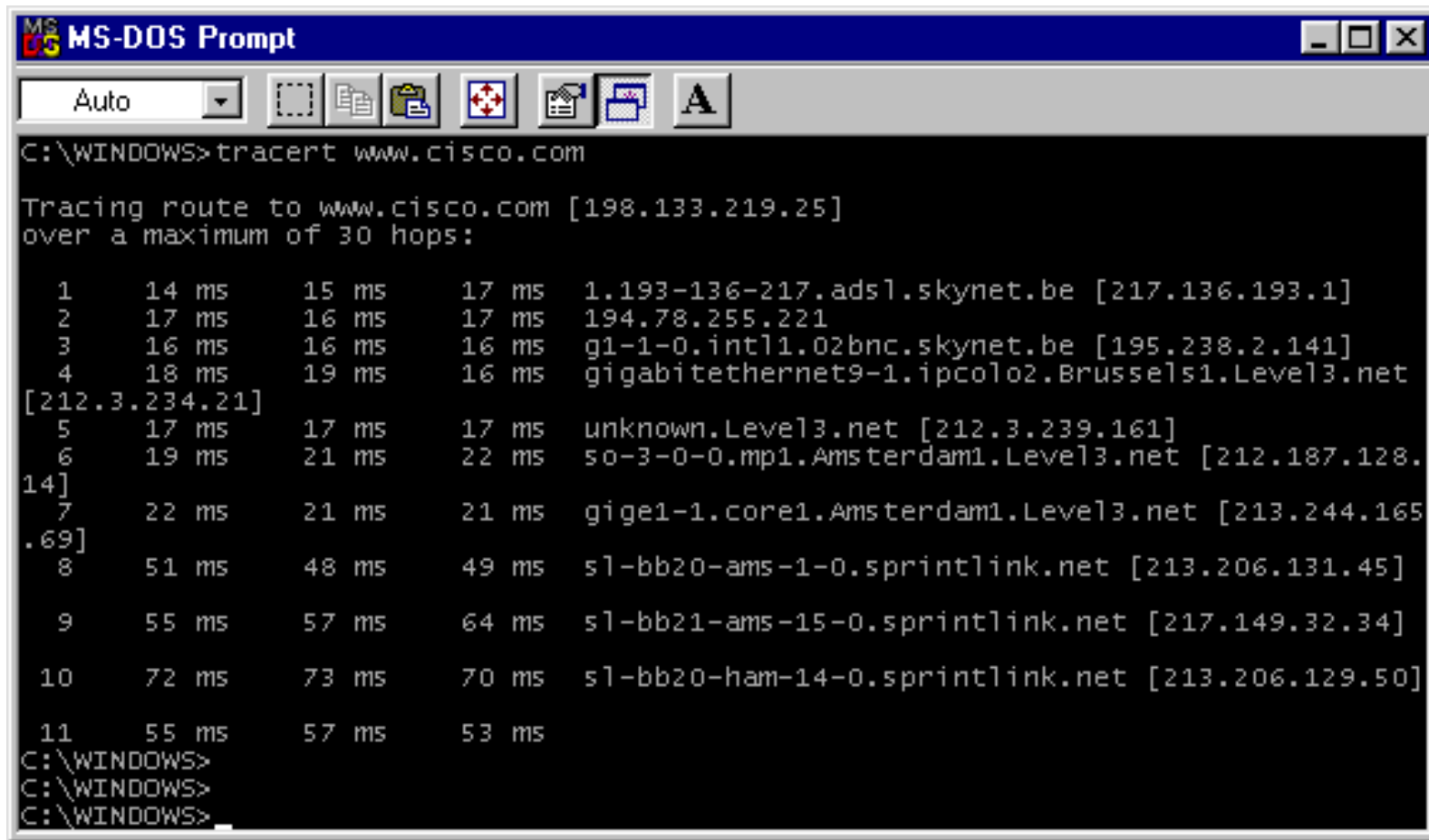
# Traceroute – Exemple théorique



**!!! IP ne garantit pas le chemin utilisé !!!**



# Traceroute – Exemple



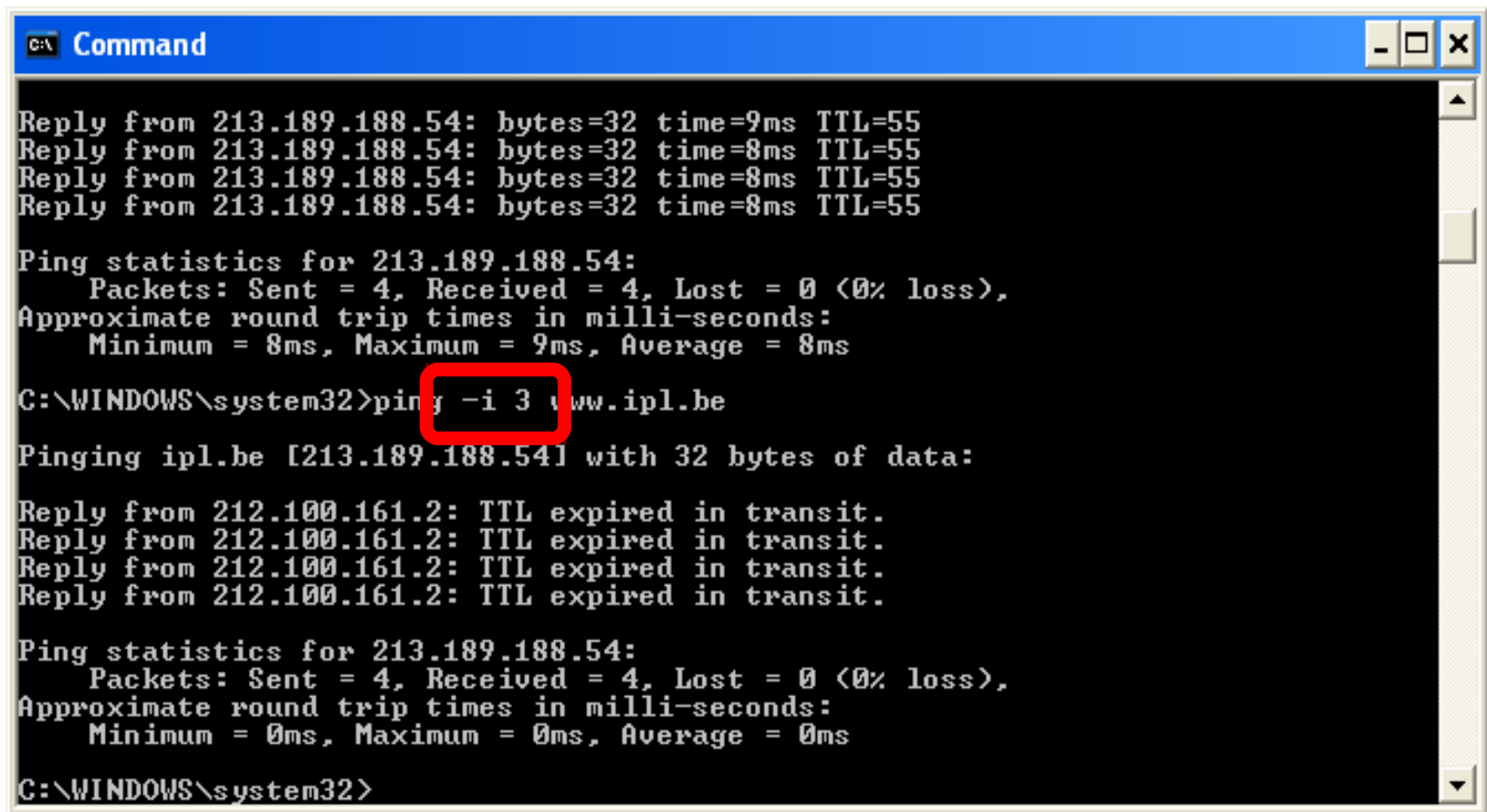
```
C:\WINDOWS>tracert www.cisco.com

Tracing route to www.cisco.com [198.133.219.25]
over a maximum of 30 hops:

  0  14 ms    15 ms    17 ms    1.193-136-217.ads1.skynet.be [217.136.193.1]
  1  17 ms    16 ms    17 ms    194.78.255.221
  2  16 ms    16 ms    16 ms    g1-1-0.intl1.02bnc.skynet.be [195.238.2.141]
  3  18 ms    19 ms    16 ms    gigabitethernet9-1.ipcolo2.Brussels1.Level3.net
  4  [212.3.234.21]
  5  17 ms    17 ms    17 ms    unknown.Level3.net [212.3.239.161]
  6  19 ms    21 ms    22 ms    so-3-0-0.mp1.Amsterdam1.Level3.net [212.187.128.
  7  14]
  7  22 ms    21 ms    21 ms    gige1-1.core1.Amsterdam1.Level3.net [213.244.165
  8  .69]
  8  51 ms    48 ms    49 ms    s1-bb20-ams-1-0.sprintlink.net [213.206.131.45]
  9  55 ms    57 ms    64 ms    s1-bb21-ams-15-0.sprintlink.net [217.149.32.34]
 10  72 ms    73 ms    70 ms    s1-bb20-ham-14-0.sprintlink.net [213.206.129.50]
 11  55 ms    57 ms    53 ms

C:\WINDOWS>
C:\WINDOWS>
C:\WINDOWS>
```

# Contrôle du TTL



The screenshot shows a Windows Command Prompt window with a blue title bar labeled "Command". The window contains the following text:

```
Reply from 213.189.188.54: bytes=32 time=9ms TTL=55
Reply from 213.189.188.54: bytes=32 time=8ms TTL=55
Reply from 213.189.188.54: bytes=32 time=8ms TTL=55
Reply from 213.189.188.54: bytes=32 time=8ms TTL=55

Ping statistics for 213.189.188.54:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 9ms, Average = 8ms

C:\WINDOWS\system32>ping -i 3 www.ipl.be

Pinging ipl.be [213.189.188.54] with 32 bytes of data:

Reply from 212.100.161.2: TTL expired in transit.
Reply from 212.100.161.2: TTL expired in transit.
Reply from 212.100.161.2: TTL expired in transit.
Reply from 212.100.161.2: TTL expired in transit.

Ping statistics for 213.189.188.54:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\WINDOWS\system32>
```

The command `ping -i 3 www.ipl.be` is highlighted with a red rectangle. The output shows that the TTL expired in transit for the second ping attempt, resulting in a 0ms round trip time.