Layer 3 - Addressing

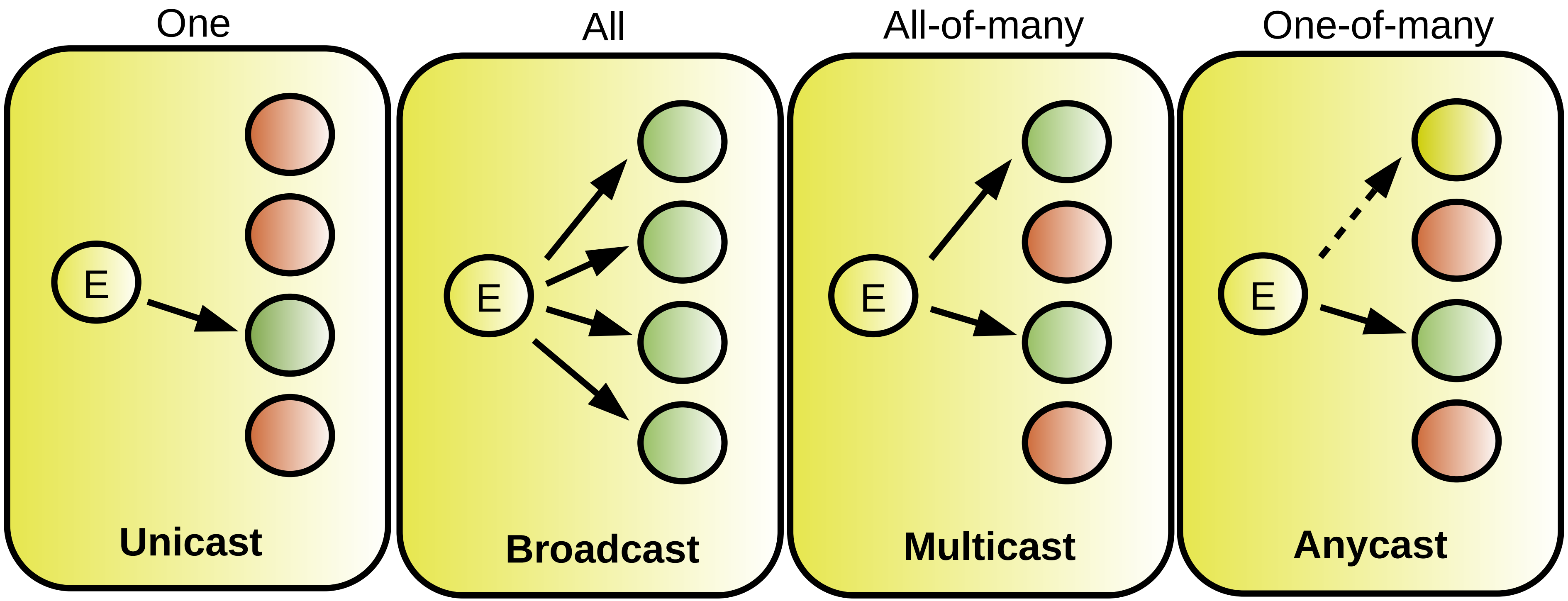
Fundamentos de Redes

Mestrado Integrado em
Engenharia de Computadores e Telemática
DETI-UA

universidade de aveiro
deti.ua.pt

Types of Addresses

- Unicast – Identify a single sender/receiver.
- Broadcast – All are receivers.
- Multicast – Identify all elements of a group as receivers (all-of-many)
- Anycast – Identifies any element of group as receiver (one-of-many)



IPv4 Addressing

- An IPv4 address is a unique address for a network interface
- Exceptions:
  - Dynamically assigned IPv4 addresses (DHCP)
  - IP addresses in private networks (NAT)

- An IPv4 address:
  - is a **32 bit long** identifier
  - encodes a network number (**network prefix**)
    and a **host identifier**

Network Prefix and Host Identifier

- The network prefix identifies a network and the host identifier identifies a specific host (actually, interface on the network).

network prefix	host identifier

- How do we know how long the network prefix is?
  - **Before 1993:** The boundary between network prefix and host identifier is implicitly defined (**class-based/classful addressing**)

  or

  - **After 1993:** The boundary between network prefix and host identifier is indicated by a **netmask.**

Classless Inter-Domain Routing (CIDR)

- New interpretation of the IP addressing to increase efficiency and flexibility.
  - Network Masks were created to define the boundary between the IP network prefix and host identifier.
  - A bit of the mask equal to one indicate that that bit (in that position) of the address belongs to the network prefix.
    - A bit of the mask equal to zero indicate that that bit (in that position) of the address belongs to the host identifier.
  - Called VLSM (Variable Length Subnet Mask).
  - Must be provided with the IP address.
- Allowed the partition of a network in smaller networks or sub-networks (subnets).
- Allowed to merge several network under a single prefix (aggregation or summary process).

	decimal		binary	
IPv4 Address	193.136.92.	1	11000001.10001000.01011100.	00000001
Mask	255.255.255.	0	11111111.11111111.11111111.	00000000
	network prefix	host identifier	network prefix	host identifier

Mask Notations

- There are two notations for IPv4 masks:
  - Decimal: 4 bytes separated by dots.
  - CIDR: A slash (/) a a number with the number of bits of the network prefix.
- Both notations still exist today.
  - CIDR starts to become prevalent.
  - IPv6 only supports CIDR.

CIDR	Decimal
/21	255.255.248.0
/20	255.255.240.0
/19	255.255.224.0
/18	255.255.192.0
/17	255.255.128.0
/16	255.255.0.0
/15	255.248.0.0
/14	255.240.0.0
/13	255.224.0.0

CIDR	Decimal
/30	255.255.255.252
/29	255.255.255.248
/28	255.255.255.240
/27	255.255.255.224
/26	255.255.255.192
/25	255.255.255.128
/24	255.255.255.0
/23	255.255.254.0
/22	255.255.252.0

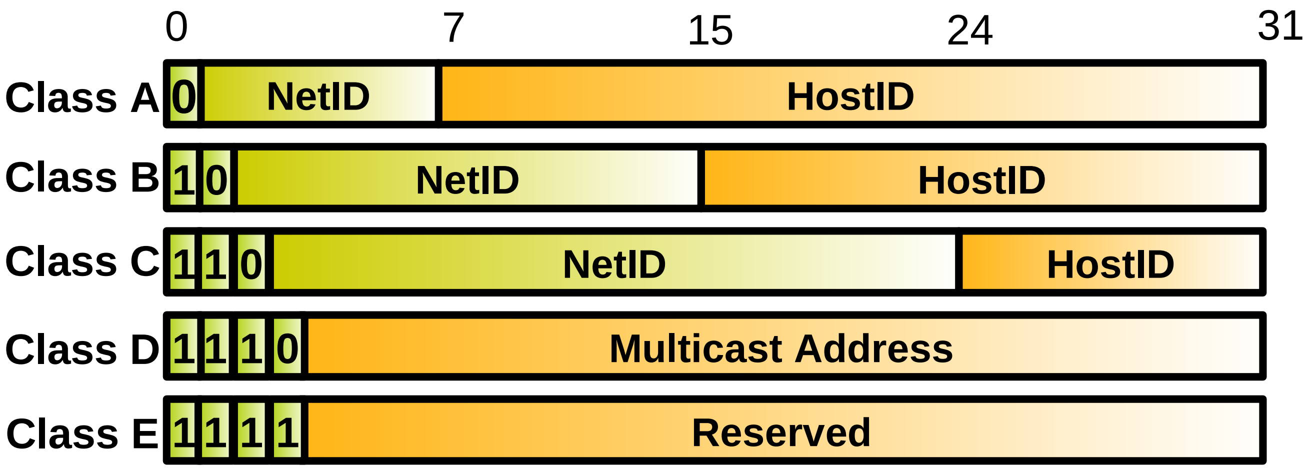
CIDR Address Blocks

- CIDR defines a block of addresses.
- The addresses blocks are used to assign
- #Addresses= 2^(32-CIDR)
  - Example: \24→ 2^(32-24)=2^8=256, \28→ 2^(32-28)=2^4=16
- #Usable_Addresses = #Addresses – 2 addresses
  - Network prefix and broadcast address

CIDR	# of addresses	# usable addresses
21	2048	2046
20	4096	4094
19	8192	8190
18	16384	16382
17	32768	32766
16	65536	65534
15	131072	131070
14	262144	262142
13	524288	524286

CIDR	# of addresses	# usable addresses
30	4	2
29	8	6
28	16	14
27	32	30
26	64	62
25	128	126
24	256	254
23	512	510
22	1024	1022

IPv4 Classful Addressing



- Initially (until 1993) the boundary between the network prefix and host identifier was predefined by the value of the first byte (class).
- Resulted in a huge waste of addresses:
  - Classes A and B were to big,
  - Not enough class C networks.
- Routing Tables were becoming very long
  - It was not possible to merge (aggregate) networks to simplify routing tables.

Class	First Address	Last Address
A	1.0.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.0.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.254

IPv4 Private Networks

Prefix	First Address	Last Address
10.0.0.0/8	10.0.0.0	10.255.255.255
172.16.0.0/12	172.16.0.0	172.31.255.255
192.168.0.0/16	192.168.0.0	192.168.255.255
169.254.0.0/16	169.254.0.0	169.254.255.255

- To be used within a local network.
- Packets with these addresses as destination are not routed to the Internet.
- Packets with these addresses as source should not be routed to the Internet.
  - Not default behavior!

IPv4 Address Planning

universidade de aveiro

deti.ua.pt

IPv4 Network Sub-netting

- Made allowed by Variable Length Subnet Mask.
- Division of an IPv4 networks into smaller IPv4 networks.
- Allows to save IPv4 addresses.
  - Assign a large network to a small network will have many address not assigned.
  - A large network may divided into smaller networks and each one assign to different LAN.

193.136.92.0/24 → 193.136.92.0**/25** + 193.136.92.128**/25**

$.92.000 = 01011100.00000000_2$

$.92.128 = 01011100.10000000_2$

IPv4 Network Aggregation

- Inverse process to network sub-netting.
- Used to obtain a single network prefix to multiple networks.
  - Mainly used to simplify routing.
- Example:

193.136.92.0/24 + 193.136.93.0/24 → 193.136.92.0**/23**

$.92. = 0101110\boxed{0}_2$

$.93. = 0101110\boxed{1}_2$

IPv4 Address Planning (1)

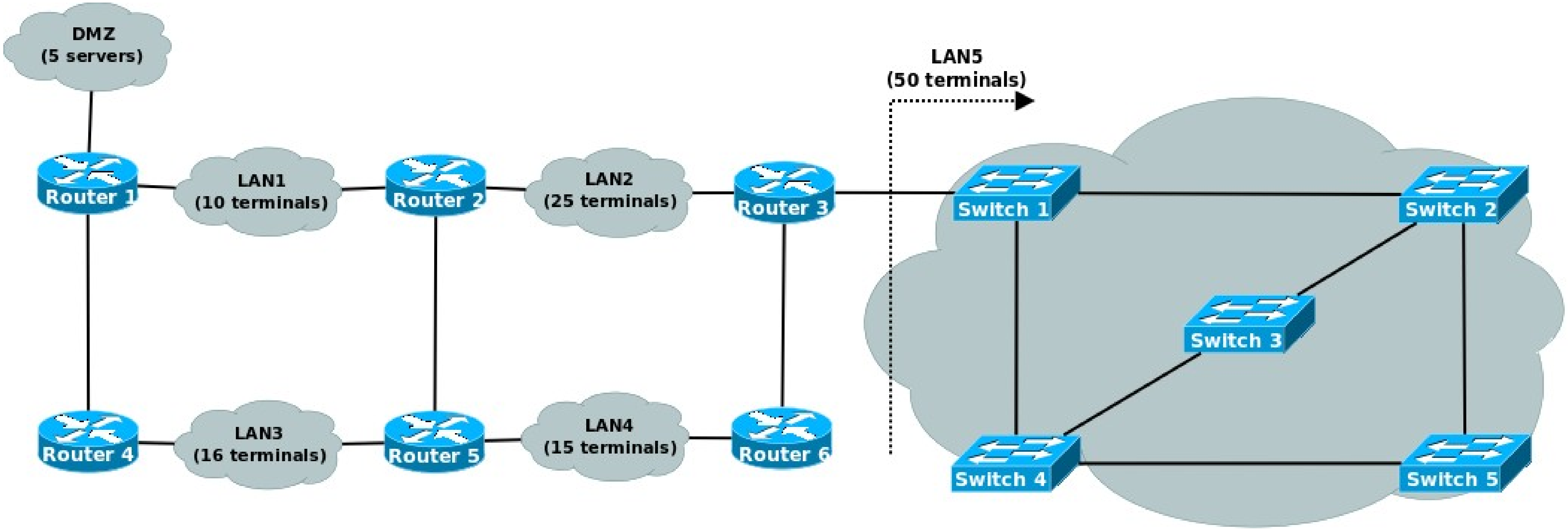
- Address planning is the assignment of an IP network to a (V)LAN.
  - To be assign address manually or dynamically (DHCP).
- Public addresses planning:
  - Limited number of available IPv4 addresses.
  - Planning ruled by the number of hosts in each LAN that require a public IPv4 address.
  - Not all LAN require IPv4 addresses.
  - Not all host in a LAN require IPv4 addresses.
  - Usually network managers receive /23, /24 or /25 networks.
- Private addresses planning:
  - Number of addresses is not an issue.
  - Number of hosts in a LAN is not so relevant.
    - Networks are usually divided in standard (/24), point-to-point (/30) and larger networks (may use /23, /22, /21, /20, etc…).

IPv4 Address Planning (2)

- Best practices:
  - Identify the available IPv4 network(s).
  - Identify the number of host in each (V)LAN.
    - Including terminals and routers (gateways).
  - Define each sub-network size.
    - Define network mask.
  - Sort sub-networks from larger to smaller.
    - Smaller CIDR to higher CIDR.
  - Start from the available network.
    - Sub-divide in half.
    - If sub-network size is required → **Assigned it** → ITS SUB-NETWORKS ARE NOT USABLE IN OTHER LAN.
    - If sub-network size is larger that required → **Sub-divide it in half**.
    - Repeat until all LAN have an assigned IPv4 network.
      - The overall available network may not be enough to assigned sub-networks to all LAN. The solution is to reevaluate requirements and assigned smaller sub-networks.

Example – IPv4 Public Planning (1)

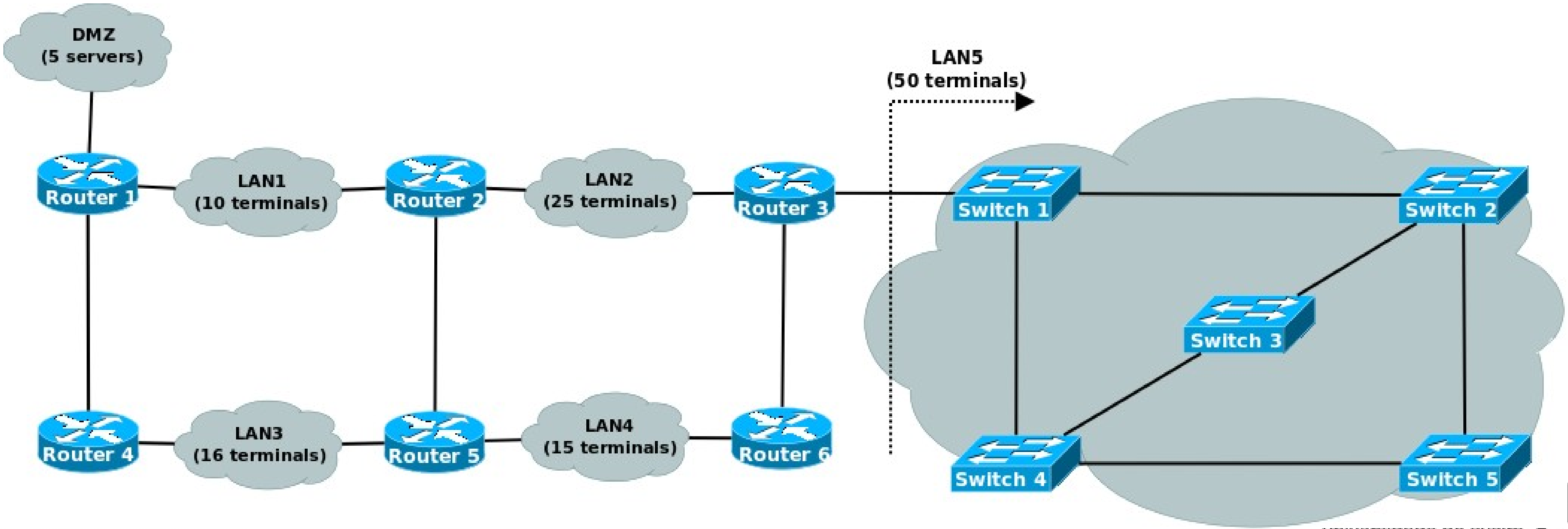
- Problem: Multiple (V)LAN require a small number of public IPv4 addresses. The public IPv4 network available is 193.1.1.0/24.
  - Note: All (V)LAN require IPv4 addresses, however may use private addresses (another IPv4 network).



193.1.1.0/24

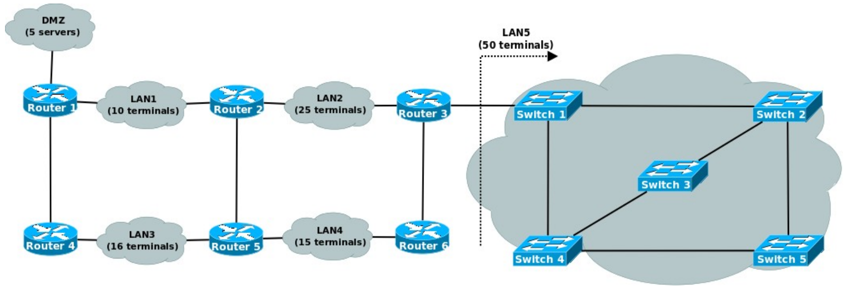
Example – IPv4 Public Planning (2)

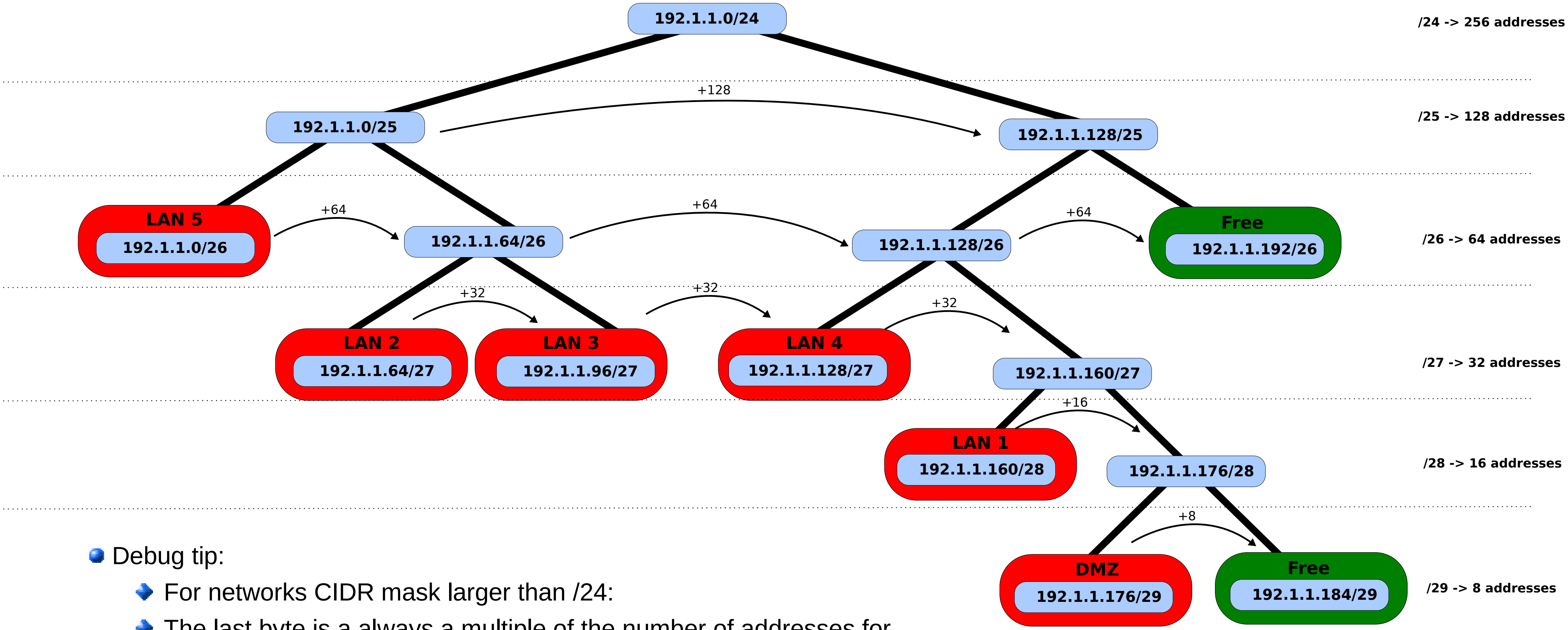
- LAN 1 → 10+2=12 → 16 → /28 net
- LAN 2 → 25+2=27 → 32 → /27 net
- LAN 3 → 16+2=18 → 32 → /27 net
- LAN 4 → 15+2=17 → 32 → /27 net
- LAN 5 → 50+1=51 → 64 → /26 net
- DMZ → 5+1=6 → 8 → /29 net



Example (3)

- LAN 1 → 10+2=12 → 16 → /28 net
- LAN 2 → 25+2=27 → 32 → /27 net
- LAN 3 → 16+2=18 → 32 → /27 net
- LAN 4 → 15+2=17 → 32 → /27 net
- LAN 5 → 50+1=51 → 64 → /26 net
- DMZ → 5+1=6 → 8 → /29 net

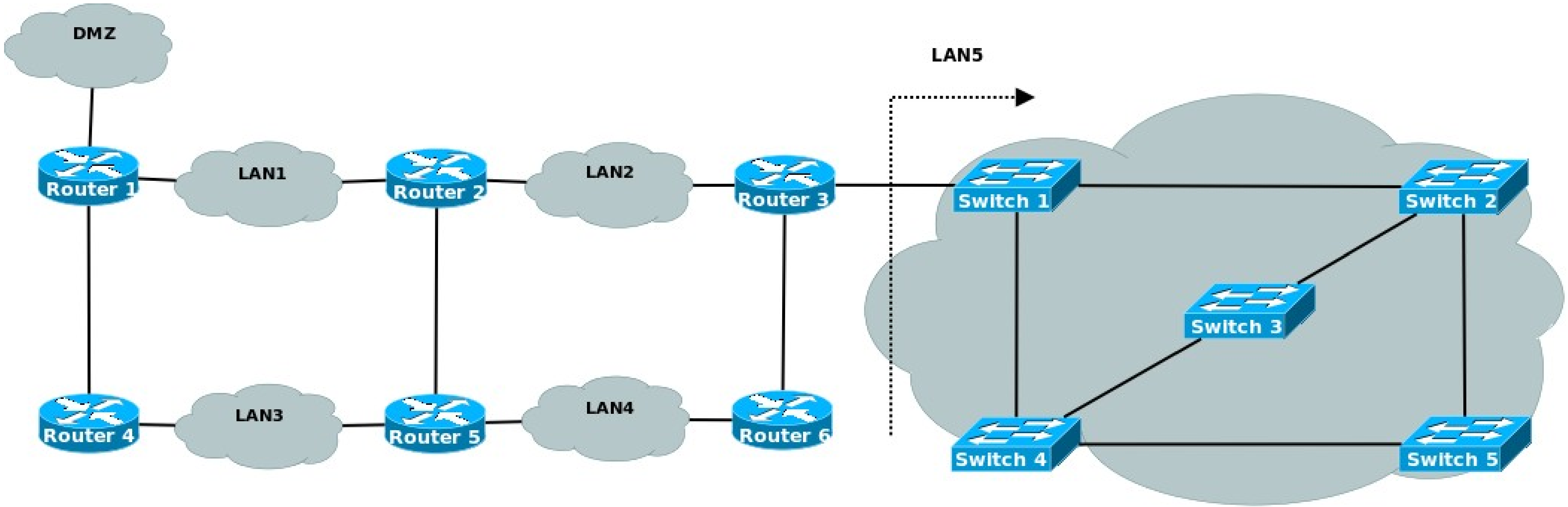




- Debug tip:
  - For networks CIDR mask larger than /24:
  - The last byte is a always a multiple of the number of addresses for that network size.
    - Example: 192 is multiple of 64, 176 is multiple of 16, and 184 is multiple of 8.

Example – IPv4 Private Planning (1)

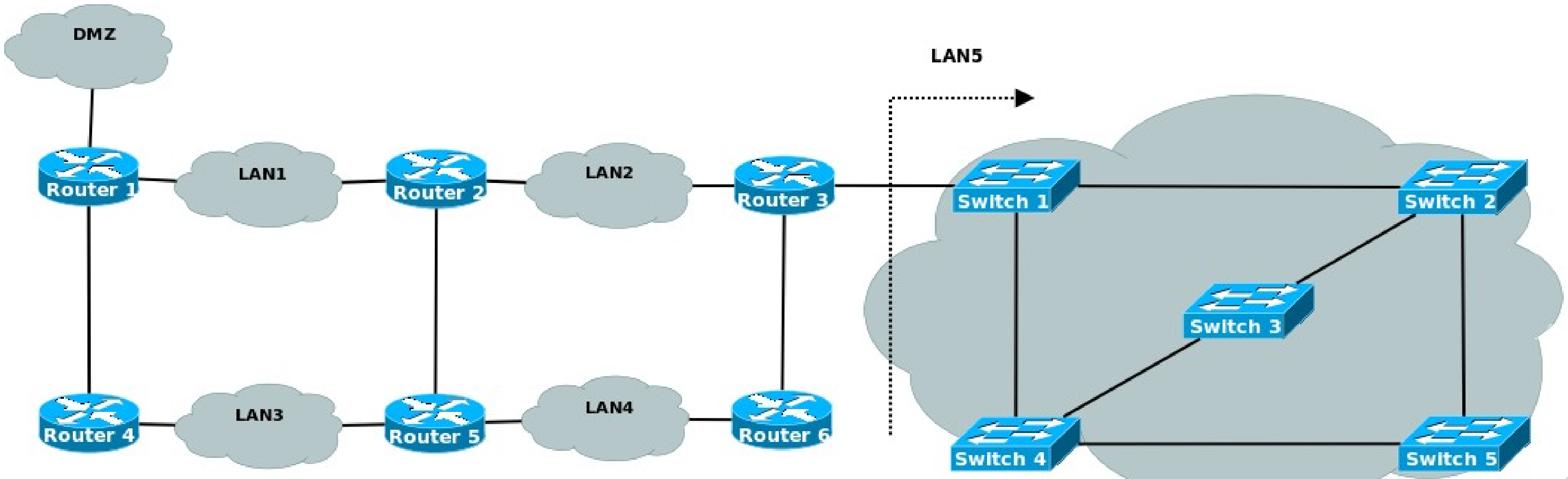
- Problem: All (V)LAN have a standard size, except LAN 5 that may have 1000 hosts.



10.0.0.0/8

Example – IPv4 Private Planning (2)

- Easier approach is to start from /24 networks and perform sub-netting/aggregation as required.
- Start with larger networks.
- LAN5 with 1000 users will be a /22 network (2^(32-22)-2=1022 usable addresses).
  - Aggregation of networks 10.0.0.0/24, 10.0.1.0/24, 10.0.2.0/24 and 10.0.3.0/24.
  - Assigned: 10.0.0.0/22
- LAN1 to LAN4 and DMZ have a standard size and will be a /24 network.
  - Assigned: 10.0.4.0/24, 10.0.5.0/24, 10.0.6.0/24, 10.0.7.0/24, 10.0.8.0/24
- Point-to-point networks R1-R4, R2-R5 and R3-R6 will be /30 networks.
  - Network 10.0.9.0/24 will be used to perform the sub-netting.
  - Assigned: 10.0.9.0/30, 10.0.9.4/30, 10.0.9.8/30
  - Free: 10.0.9.12/30+10.0.9.16/28+10.0.9.32/27+10.0.9.64/26+10.0.9.128/25



DHCP

universidade de aveiro

deti.ua.pt

Dynamic Host Configuration Protocol (DHCP)

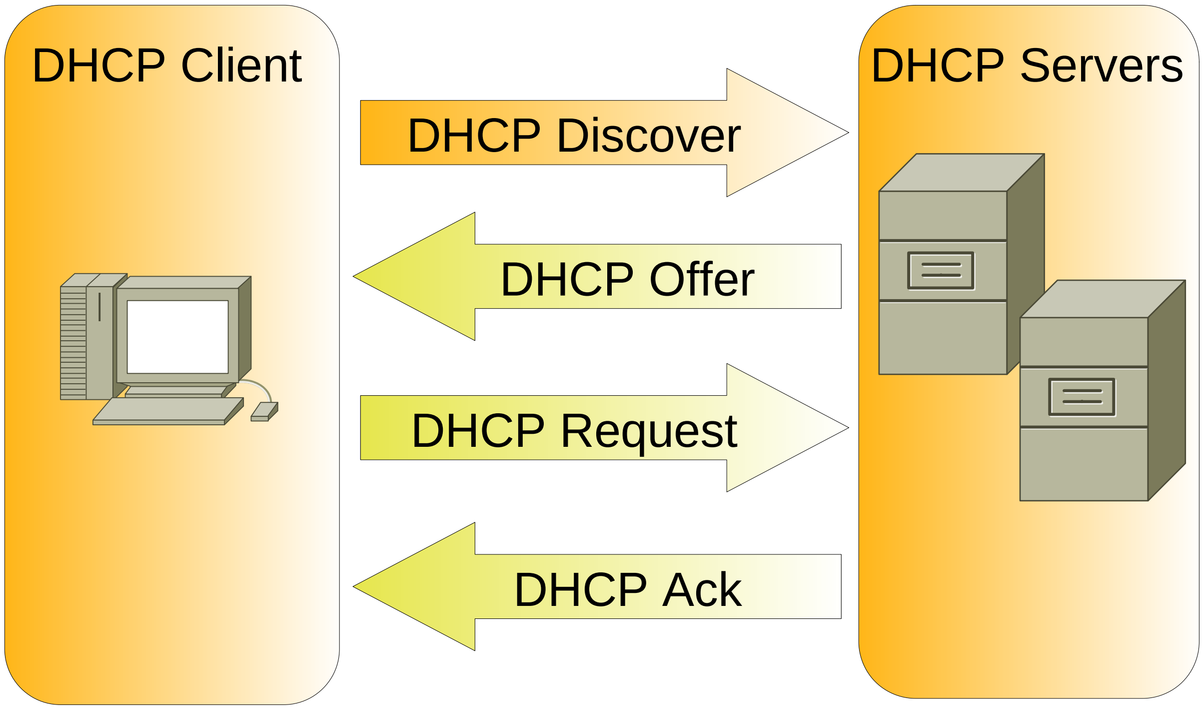
- Service for dynamic assignment of IP addresses.
  - Client-Server architecture.
- Extension of the Bootstrap Protocol, BOOTP, (RFC 1542)
  - Runs over UDP.
    - Server port 67 and client port 68.
- Address assignment follow a leasing paradigm.
- The assignment of address has four phases:
  - Discover
  - Offer
  - Request
  - Acknowledge
- DHCP servers provide:
  - Address, network mask and gateway.
  - May include additional information DNS server, Windows Domain Servers, etc…

DHCP Server

- Pool of (public) addresses
  - List of IPv4 public addresses to be assigned, usually defined as network or range of IPv4 addresses.
- Exclusion ranges
  - Set of IPv4 addresses that belong to a pool but must be assigned.
    - Usually manually assigned address to routers (gateways) and servers.
- Reserved addresses and static assignment
  - Based on the MAC address is possible to define a permanently assigned IPv4 address.
    - Usually used on servers, printers and other network devices.
    - Should not be used by routers.
- Lease time
  - Define for how long can a host use an assigned IPv4 address without a new interaction.
- To serve multiple IPv4 networks (LAN):
  - The server must have multiple pools of addresses,
  - The routers must have the BootP/DHCP Relay feature configured.
- A LAN may have multiple DHCP servers
  - For redundancy. Pools must be disjoint.

Phase One: *Discover*

- The *DHCP Discover* message id encapsulated into a *BootP Request* packet.
  - Source address is 0.0.0.0.
- It is used to discover the available DHCP server(s).
- The client may include the desired address.
  - Server is not obliged to obey.



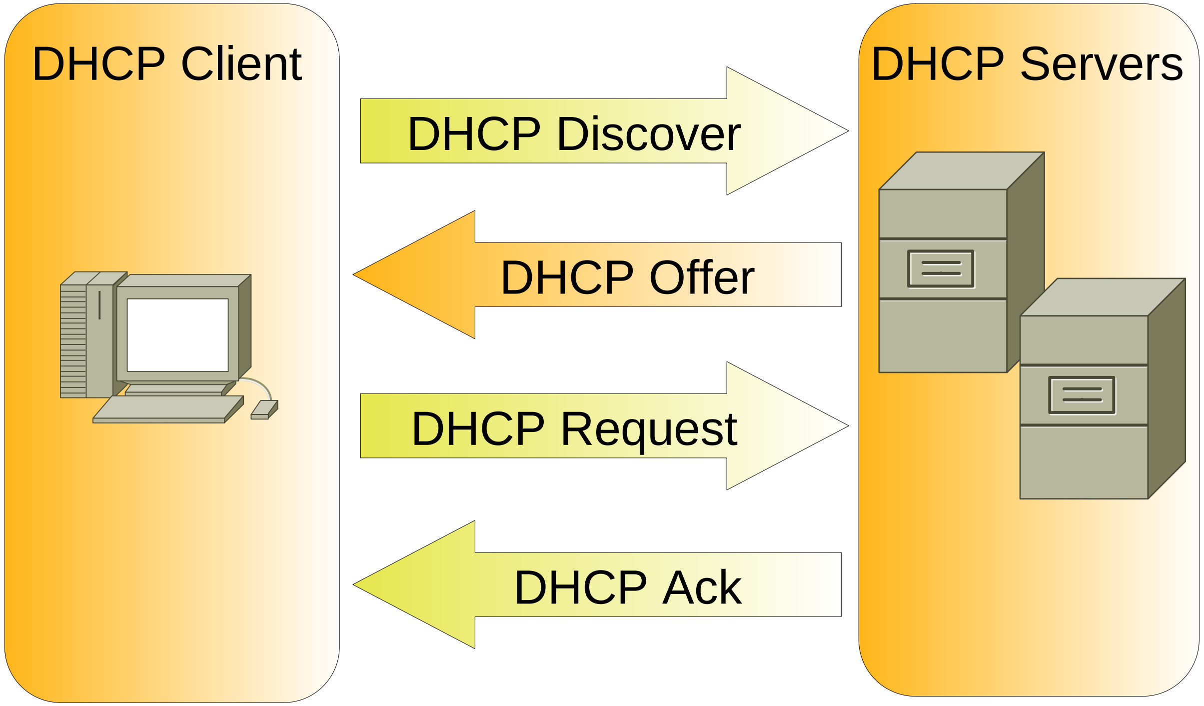
DHCP Discover

No.	Time	Source	Destination	Protocol	Info
1326	20.269579	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
1337	20.561380	193.136.92.65	193.136.93.228	DHCP	DHCP Offer
1338	20.561592	0.0.0.0	255.255.255.255	DHCP	DHCP Request
1340	20.569560	193.136.92.65	193.136.93.228	DHCP	DHCP ACK

```
▷ Frame 1326 (342 bytes on wire, 342 bytes captured)
▷ Ethernet II, Src: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e), Dst: ff:ff:ff:ff:ff:ff (ff
▷ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
▷ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
▽ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x42f5a54a
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ▷ Option: (t=53,l=1) DHCP Message Type = DHCP Discover
  ▷ Option: (t=50,l=4) Requested IP Address = 192.168.1.71
  ▷ Option: (t=12,l=15) Host Name = "salvador-laptop"
  ▷ Option: (t=55,l=13) Parameter Request List
    End Option
    Padding
```

Phase Two: *Offer*

- The *DHCP Offer* message is encapsulated into a *BootP Reply* packet.
- Each server proposes the lease of an IPv4 address to client.
  - If possible respect the client request (*Discovery*)



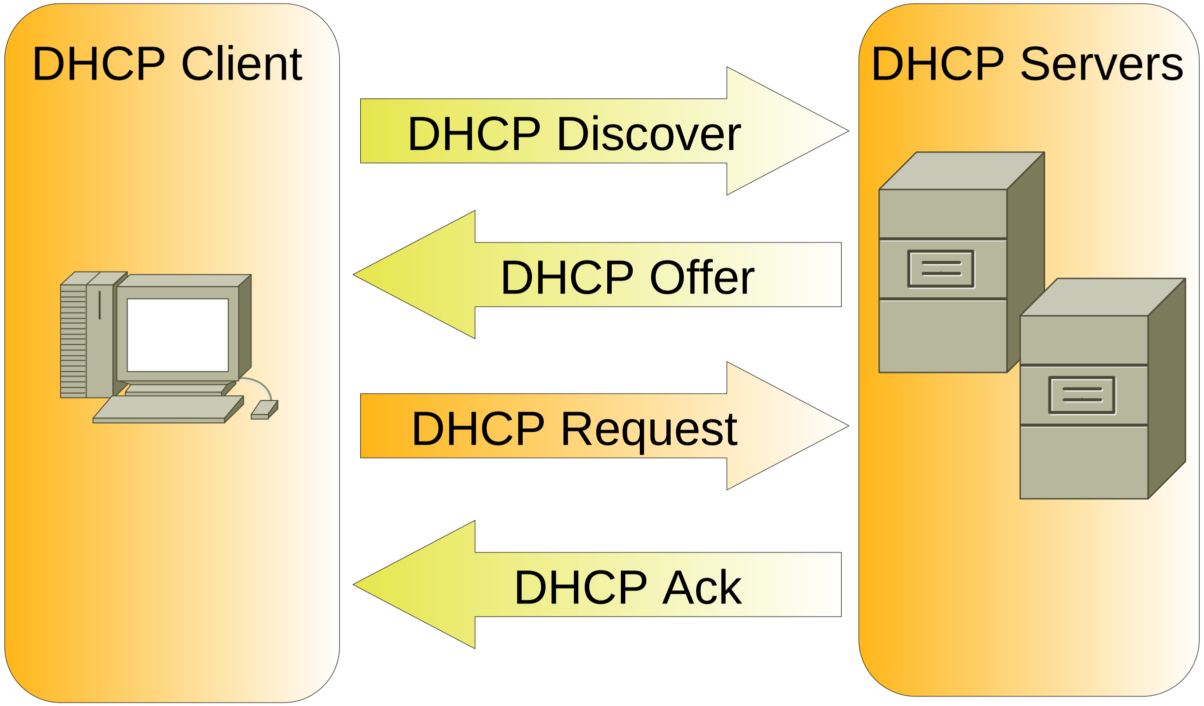
DHCP Offer

No.	Time	Source	Destination	Protocol	Info
1326	20.269579	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
1337	20.561380	193.136.92.65	193.136.93.228	DHCP	DHCP Offer
1338	20.561592	0.0.0.0	255.255.255.255	DHCP	DHCP Request
1340	20.569560	193.136.92.65	193.136.93.228	DHCP	DHCP ACK

```
▷ Frame 1337 (342 bytes on wire, 342 bytes captured)
▷ Ethernet II, Src: 00:d0:b7:17:5b:6d (00:d0:b7:17:5b:6d), Dst: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e)
▷ Internet Protocol, Src: 193.136.92.65 (193.136.92.65), Dst: 193.136.93.228 (193.136.93.228)
▷ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
▽ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x42f5a54a
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 193.136.93.228 (193.136.93.228)
    Next server IP address: 193.136.92.65 (193.136.92.65)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ▷ Option: (t=53,l=1) DHCP Message Type = DHCP Offer
  ▷ Option: (t=54,l=4) DHCP Server Identifier = 193.136.92.65
  ▷ Option: (t=51,l=4) IP Address Lease Time = 10 minutes
  ▷ Option: (t=1,l=4) Subnet Mask = 255.255.254.0
  ▷ Option: (t=3,l=4) Router = 193.136.92.1
  ▷ Option: (t=15,l=8) Domain Name = "av.it.pt"
  ▷ Option: (t=6,l=4) Domain Name Server = 193.136.92.65
    End Option
    Padding
```

Phase 3: *Request*

- The *DHCP Request* message id encapsulated into a *BootP Request* packet.
- The client may chooses the offered IPv4 address (and DHCP server if more than on *offer* is received).



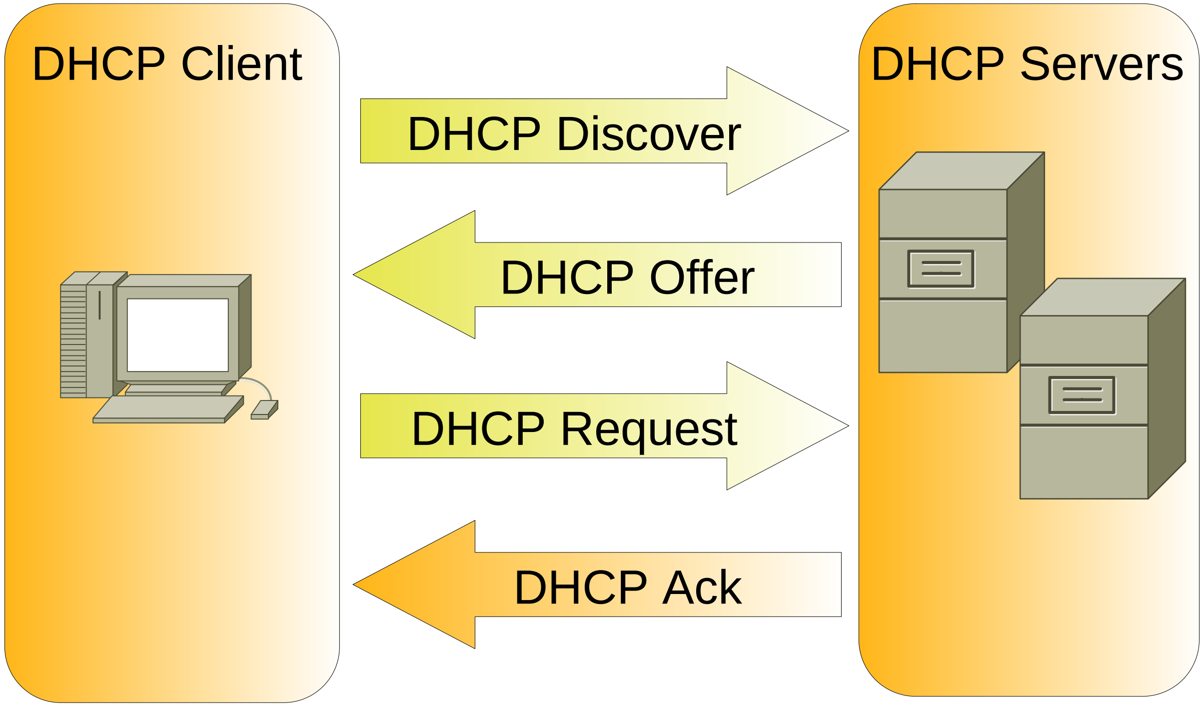
DHCP Request

No.	Time	Source	Destination	Protocol	Info
1326	20.269579	0.0.0.0	255.255.255.255	DHCP	
1337	20.561380	193.136.92.65	193.136.93.228	DHCP	
1338	20.561592	0.0.0.0	255.255.255.255	DHCP	
1340	20.569560	193.136.92.65	193.136.93.228	DHCP	

```
▷ Frame 1338 (342 bytes on wire, 342 bytes captured)
▷ Ethernet II, Src: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
▷ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
▷ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
▽ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x42f5a54a
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ▷ Option: (t=53,l=1) DHCP Message Type = DHCP Request
  ▷ Option: (t=54,l=4) DHCP Server Identifier = 193.136.92.65
  ▷ Option: (t=50,l=4) Requested IP Address = 193.136.93.228
  ▷ Option: (t=12,l=15) Host Name = "salvador-laptop"
  ▷ Option: (t=55,l=13) Parameter Request List
    End Option
    Padding
```

Phase 4: *Acknowledge*

- The *DHCP Ack* message is encapsulated into a *BootP Reply* packet.
- The server confirms the IPv4 address lease and provides additional information:
  - Lease time, Gateway(s), DNS server, etc...



DHCP Ack

No.	Time	Source	Destination	Protocol	Info
1326	20.269579	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
1337	20.561380	193.136.92.65	193.136.93.228	DHCP	DHCP Offer
1338	20.561592	0.0.0.0	255.255.255.255	DHCP	DHCP Request
1340	20.569560	193.136.92.65	193.136.93.228	DHCP	DHCP ACK

```
Frame 1340 (342 bytes on wire, 342 bytes captured)
Ethernet II, Src: 00:d0:b7:17:5b:6d (00:d0:b7:17:5b:6d), Dst: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e)
Internet Protocol, Src: 193.136.92.65 (193.136.92.65), Dst: 193.136.93.228 (193.136.93.228)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x42f5a54a
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 193.136.93.228 (193.136.93.228)
    Next server IP address: 193.136.92.65 (193.136.92.65)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option: (t=53,l=1) DHCP Message Type = DHCP ACK
    Option: (t=54,l=4) DHCP Server Identifier = 193.136.92.65
    Option: (t=51,l=4) IP Address Lease Time = 10 minutes
    Option: (t=1,l=4) Subnet Mask = 255.255.254.0
    Option: (t=3,l=4) Router = 193.136.92.1
    Option: (t=15,l=8) Domain Name = "av.it.pt"
    Option: (t=6,l=4) Domain Name Server = 193.136.92.65
    End Option
    Padding
```

DHCP Operational Details

- Address Leasing Times
  - T1 Time (50% of Lease Time) – time after which the client must renew the address lease.

    T2 Time (85% of Lease Time) – time after which the client must renew the address lease if the first attempt failed.

    Lease Time – time after which the client can not used the leased address.
- DHCP allows multiple servers
  - Recommended for redundancy.
    - Requires
  - Advantage: resilience to operational failures.
  - Requirement: Disjointed pool of addresses in different servers.

DHCP Other Messages

- DHCP *Decline*:
  - Used by a client to reject the offer made by a server and musr restart the leasing process.
- DHCP *Nack*:
  - Used by a server informing that cannot satisfy the received request (DHCP *Request*).
- DHCP *Release*:
  - Used by a client informing the server that no longer requires an address. The lease is terminated.
- DHCP *Inform*:
  - Used by a client to request additional information after receiving an address.

DHCP Release

No.	Time	Source	Destination	Protocol	Info
1330	24.011686	193.136.93.228	193.136.92.65	DHCP	DHCP Release

```
▷ Frame 1330 (342 bytes on wire, 342 bytes captured)
▷ Ethernet II, Src: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e), Dst: 00:d0:b7:17:5b:6d (00:d0:b7:17:5b:6d)
▷ Internet Protocol, Src: 193.136.93.228 (193.136.93.228), Dst: 193.136.92.65 (193.136.92.65)
▷ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
▽ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xc099a870
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 193.136.93.228 (193.136.93.228)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ▷ Option: (t=53,l=1) DHCP Message Type = DHCP Release
  ▷ Option: (t=54,l=4) DHCP Server Identifier = 193.136.92.65
  ▷ Option: (t=12,l=15) Host Name = "salvador-laptop"
    End Option
    Padding
```

DHCP Inform

No.	Time	Source	Destination	Protocol	Info
4107	65.374546	193.136.93.173	255.255.255.255	DHCP	DHCP Inform
5446	86.143470	193.136.93.102	255.255.255.255	DHCP	DHCP Inform

```
▷ Frame 4107 (342 bytes on wire, 342 bytes captured)
▷ Ethernet II, Src: d0:df:9a:cb:d1:3c (d0:df:9a:cb:d1:3c), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
▷ Internet Protocol, Src: 193.136.93.173 (193.136.93.173), Dst: 255.255.255.255 (255.255.255.255)
▷ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
▽ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xfb8eebf9
    Seconds elapsed: 0
  ▷ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 193.136.93.173 (193.136.93.173)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: d0:df:9a:cb:d1:3c (d0:df:9a:cb:d1:3c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ▷ Option: (t=53,l=1) DHCP Message Type = DHCP Inform
  ▷ Option: (t=61,l=7) Client identifier
  ▷ Option: (t=12,l=7) Host Name = "IT-TOSH"
  ▷ Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  ▷ Option: (t=55,l=13) Parameter Request List
    End Option
    Padding
```

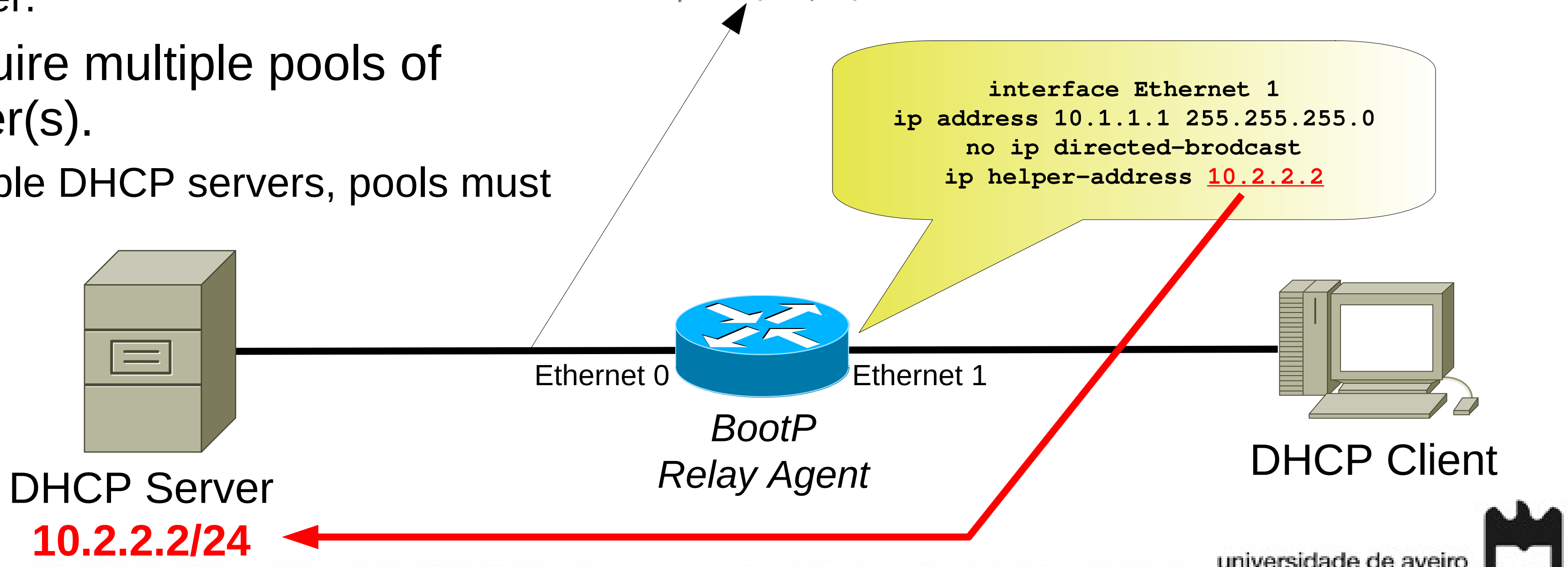
```
▽ Option: (t=55,l=13) Parameter Request List
    Option: (55) Parameter Request List
    Length: 13
    Value: 010F03062C2E2F1F2179F92BFC
    1 = Subnet Mask
    15 = Domain Name
    3 = Router
    6 = Domain Name Server
    44 = NetBIOS over TCP/IP Name Server
    46 = NetBIOS over TCP/IP Node Type
    47 = NetBIOS over TCP/IP Scope
    31 = Perform Router Discover
    33 = Static Route
    121 = Classless Static Route
    249 = Private/Classless Static Route (Microsoft)
    43 = Vendor-Specific Information
    252 = Private/Proxy autodiscovery
```

DHCP in Complex Environments

- In complex network environments where one (or more) DHCP server provide addresses to multiple (V)LAN.
  - Router must have a “BootP Relay Agent” configured and active.
  - Router redirects the client DHCP (broadcast) packets to DHCP server(s) using unicast,
    - Append information of the network/interface where it received the DHCP packet from client.
  - Router redirects server responses to the client.
  - From the client point of view, the Router behaves like a DHCP server.
- Multiple VLAN require multiple pools of addresses at server(s).
  - When using multiple DHCP servers, pools must be disjoint.

No.	Time	Source	Destination	Protocol	Info
3	2.933744	10.1.1.1	10.2.2.2	DHCP	DHCP Discover
4	5.935516	10.1.1.1	10.2.2.2	DHCP	DHCP Discover
5	8.939088	10.1.1.1	10.2.2.2	DHCP	DHCP Discover

```
▷ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootps (67)
▽ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0xd668f173
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 10.1.1.1 (10.1.1.1)
    Client MAC address: 00:aa:00:2a:15:00 (00:aa:00:2a:15:00)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ▷ Option: (t=53,l=1) DHCP Message Type = DHCP Discover
  ▷ Option: (t=61,l=7) Client identifier
  ▷ Option: (t=12,l=3) Host Name = "box"
```



NAT and PAT

universidade de aveiro

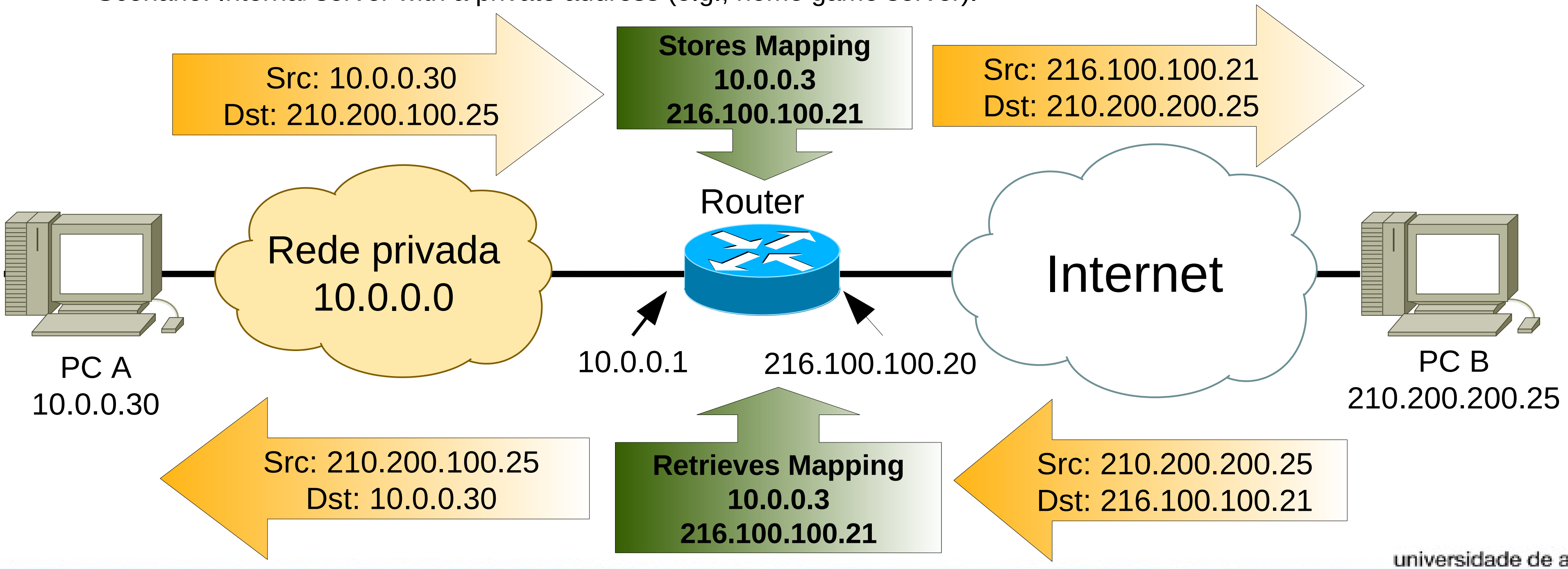
deti.ua.pt

NAT (Network Address Translation) e PAT (Port Address Translation)

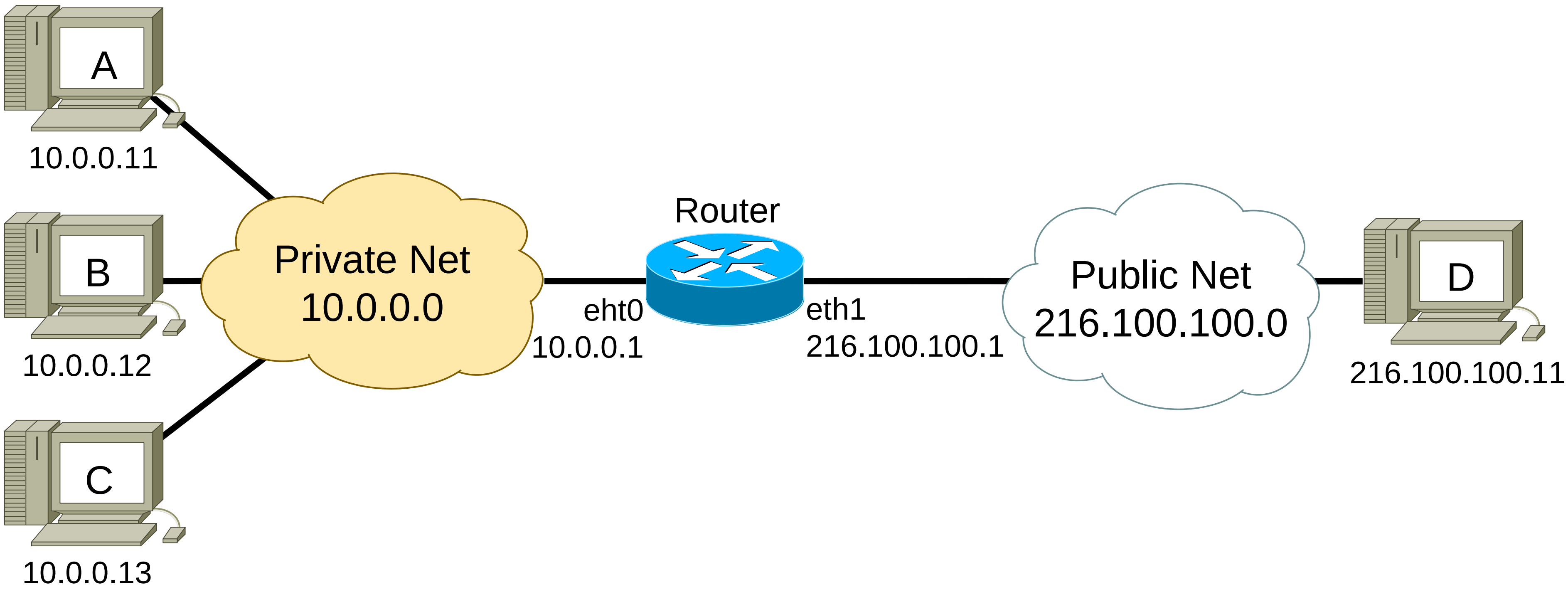
- NAT – Translates private address into public addresses.
- PAT – Translates address and also UDP/TCP ports.
  - ICMP does not have ports. ICMP identifier field is used instead.
  - Also called NAPT (Network Address and Port Translation)
- Mapping between a private and public address may be dynamic or static.
- Allows a LAN that has a limited number of IPv4 public address allow the connectivity of many internal host to the Internet.
  - The available IPv4 addresses are called the address pool.
  - A packet passing from a private network to a public network will have its IPV4 source address (and UDP/TCP port) changed to one of the available IPv4 public addresses (and ports).
  - That change will be store on the device on the boundary between the private and public network (Router, Firewall or Security Appliance).
    - Its called mapping or translation table.
  - The answer to that packet will have a reverse change.

NAT/PAT Mapping

- Dynamic Mapping:
  - Static: To allow an external host to access an internal host with a private address.
    - External host contacts the public address/port statically mapped to the private address/port.
    - Scenario: Internal server with a private address (e.g., home game server).
  - The choice of public address (and port) and mapping to the private address (and port) is done automatically by the Router when it receives a packet from an inside host.
  - An external host cannot initiate a conversation with a inside host.
    - May respond to conversation initiated from an inside host.
- Static Mapping:
  - The choice of public address (and port) and mapping to the private address (and port) is done by configuration.
  - Allows an external host to initiate a conversation with an internal host with a private address.
    - External host contacts the public address/port statically mapped to the private address/port.
    - Scenario: Internal server with a private address (e.g., home game server).

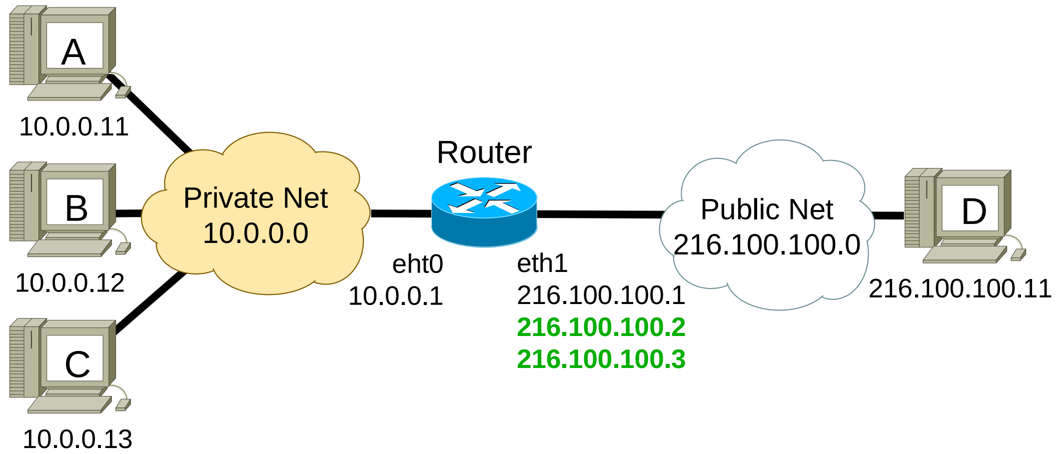


Example – NAT (1)



- Router configures with Dynamic NAT.
- Public IPv4 addresses:
  - 216.100.100.2 and 216.100.100.3 to NAT mappings,
  - 216.100.100.1 to be used by the interface.
    - The IPv4 on the interface may also be used for mapping.

Example – NAT (2)



Ping from 10.0.0.11 to 216.100.100.11:

No.	Time	Source	Destination	Protocol	Length	Info
6	15.892528	10.0.0.11	216.100.100.11	ICMP	98	Echo (ping) request id=0x6c3a, seq=1/256, ttl=64
7	15.911436	216.100.100.11	10.0.0.11	ICMP	98	Echo (ping) reply id=0x6c3a, seq=1/256, ttl=63
8	16.912087	10.0.0.11	216.100.100.11	ICMP	98	Echo (ping) request id=0x6d3a, seq=2/512, ttl=64
9	16.932449	216.100.100.11	10.0.0.11	ICMP	98	Echo (ping) reply id=0x6d3a, seq=2/512, ttl=63
10	17.933103	10.0.0.11	216.100.100.11	ICMP	98	Echo (ping) request id=0x6f3a, seq=3/768, ttl=64
11	17.952490	216.100.100.11	10.0.0.11	ICMP	98	Echo (ping) reply id=0x6f3a, seq=3/768, ttl=63
12	18.954005	10.0.0.11	216.100.100.11	ICMP	98	Echo (ping) request id=0x703a, seq=4/1024, ttl=64
13	18.974316	216.100.100.11	10.0.0.11	ICMP	98	Echo (ping) reply id=0x703a, seq=4/1024, ttl=63
14	19.975028	10.0.0.11	216.100.100.11	ICMP	98	Echo (ping) request id=0x713a, seq=5/1280, ttl=64
15	19.986293	216.100.100.11	10.0.0.11	ICMP	98	Echo (ping) reply id=0x713a, seq=5/1280, ttl=63

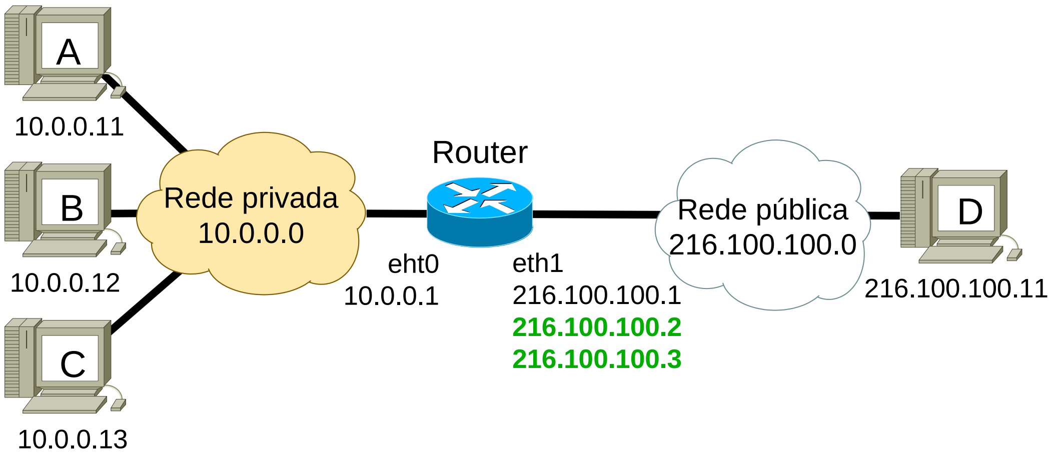
Private Network

No.	Time	Source	Destination	Protocol	Length	Info
2	3.913049	216.100.100.2	216.100.100.11	ICMP	98	Echo (ping) request id=0x6c3a, seq=1/256, ttl=63 (
3	3.913320	216.100.100.11	216.100.100.2	ICMP	98	Echo (ping) reply id=0x6c3a, seq=1/256, ttl=64 (
4	4.934041	216.100.100.2	216.100.100.11	ICMP	98	Echo (ping) request id=0x6d3a, seq=2/512, ttl=63 (
5	4.934405	216.100.100.11	216.100.100.2	ICMP	98	Echo (ping) reply id=0x6d3a, seq=2/512, ttl=64 (
6	5.954132	216.100.100.2	216.100.100.11	ICMP	98	Echo (ping) request id=0x6f3a, seq=3/768, ttl=63 (
7	5.954324	216.100.100.11	216.100.100.2	ICMP	98	Echo (ping) reply id=0x6f3a, seq=3/768, ttl=64 (
8	6.975911	216.100.100.2	216.100.100.11	ICMP	98	Echo (ping) request id=0x703a, seq=4/1024, ttl=63
9	6.976473	216.100.100.11	216.100.100.2	ICMP	98	Echo (ping) reply id=0x703a, seq=4/1024, ttl=64
10	7.987741	216.100.100.2	216.100.100.11	ICMP	98	Echo (ping) request id=0x713a, seq=5/1280, ttl=63
11	7.988265	216.100.100.11	216.100.100.2	ICMP	98	Echo (ping) reply id=0x713a, seq=5/1280, ttl=64

Public Network

```
Router#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 216.100.100.2      10.0.0.11          ---                ---
```

Example – NAT (3)



Ping from 10.0.0.12 to 216.100.100.11:

No.	Time	Source	Destination	Protocol	Length	Info
53	311.240021	10.0.0.12	216.100.100.11	ICMP	98	Echo (ping) request id=0x943b, seq=1/256, ttl=64
54	311.258670	216.100.100.11	10.0.0.12	ICMP	98	Echo (ping) reply id=0x943b, seq=1/256, ttl=63
56	312.259967	10.0.0.12	216.100.100.11	ICMP	98	Echo (ping) request id=0x953b, seq=2/512, ttl=64
57	312.280140	216.100.100.11	10.0.0.12	ICMP	98	Echo (ping) reply id=0x953b, seq=2/512, ttl=63
58	313.281645	10.0.0.12	216.100.100.11	ICMP	98	Echo (ping) request id=0x963b, seq=3/768, ttl=64
59	313.302003	216.100.100.11	10.0.0.12	ICMP	98	Echo (ping) reply id=0x963b, seq=3/768, ttl=63
60	314.303181	10.0.0.12	216.100.100.11	ICMP	98	Echo (ping) request id=0x973b, seq=4/1024, ttl=64
61	314.323635	216.100.100.11	10.0.0.12	ICMP	98	Echo (ping) reply id=0x973b, seq=4/1024, ttl=63
62	315.325157	10.0.0.12	216.100.100.11	ICMP	98	Echo (ping) request id=0x983b, seq=5/1280, ttl=64
63	315.345519	216.100.100.11	10.0.0.12	ICMP	98	Echo (ping) reply id=0x983b, seq=5/1280, ttl=63

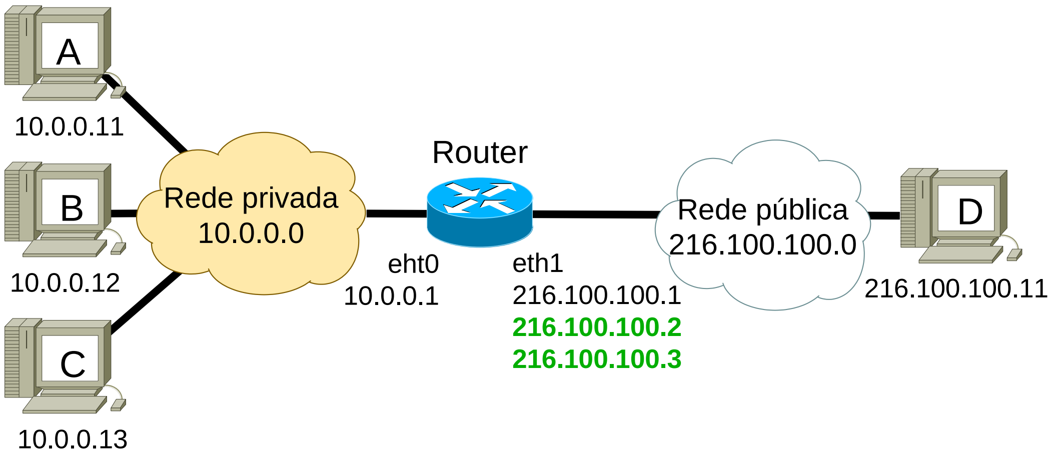
Private Network

No.	Time	Source	Destination	Protocol	Length	Info
47	299.260334	216.100.100.3	216.100.100.11	ICMP	98	Echo (ping) request id=0x943b, seq=1/256, ttl=63
48	299.260929	216.100.100.11	216.100.100.3	ICMP	98	Echo (ping) reply id=0x943b, seq=1/256, ttl=64
50	300.281677	216.100.100.3	216.100.100.11	ICMP	98	Echo (ping) request id=0x953b, seq=2/512, ttl=63
51	300.282286	216.100.100.11	216.100.100.3	ICMP	98	Echo (ping) reply id=0x953b, seq=2/512, ttl=64
52	301.303570	216.100.100.3	216.100.100.11	ICMP	98	Echo (ping) request id=0x963b, seq=3/768, ttl=63
53	301.304103	216.100.100.11	216.100.100.3	ICMP	98	Echo (ping) reply id=0x963b, seq=3/768, ttl=64
54	302.325227	216.100.100.3	216.100.100.11	ICMP	98	Echo (ping) request id=0x973b, seq=4/1024, ttl=63
55	302.325755	216.100.100.11	216.100.100.3	ICMP	98	Echo (ping) reply id=0x973b, seq=4/1024, ttl=64
56	303.347148	216.100.100.3	216.100.100.11	ICMP	98	Echo (ping) request id=0x983b, seq=5/1280, ttl=63
57	303.347704	216.100.100.11	216.100.100.3	ICMP	98	Echo (ping) reply id=0x983b, seq=5/1280, ttl=64

Public Network

```
Router#show ip nat translation
Pro Inside global     Inside local      Outside local     Outside global
--- 216.100.100.2     10.0.0.11         ---               ---
--- 216.100.100.3     10.0.0.12         ---               ---
```

Example – NAT (4)



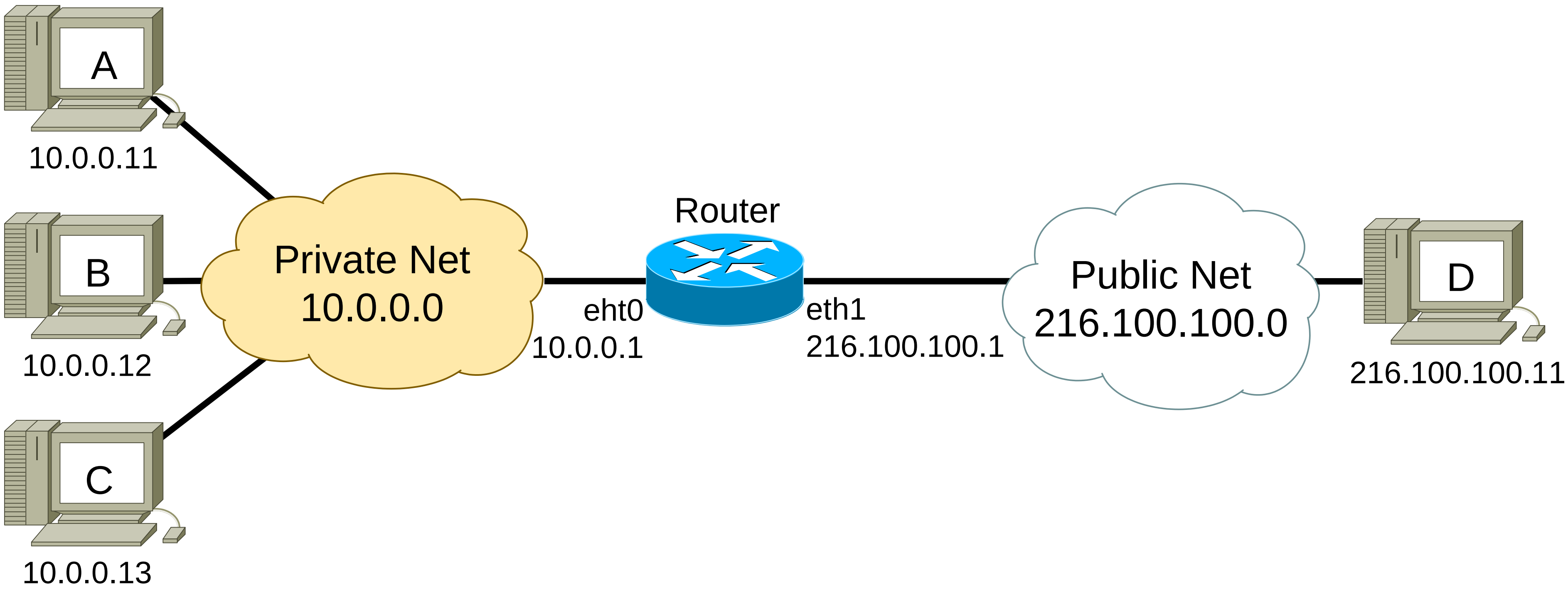
Ping from 10.0.0.13 to 216.100.100.11:

No.	Time	Source	Destination	Protocol	Length	Info
113	506.016226	10.0.0.13	216.100.100.11	ICMP	98	Echo (ping) request id=0x573c, seq=1/256, ttl=64
114	506.035020	10.0.0.1	10.0.0.13	ICMP	70	Destination unreachable (Host unreachable)
115	507.036014	10.0.0.13	216.100.100.11	ICMP	98	Echo (ping) request id=0x583c, seq=2/512, ttl=64
116	507.046188	10.0.0.1	10.0.0.13	ICMP	70	Destination unreachable (Host unreachable)
117	508.047177	10.0.0.13	216.100.100.11	ICMP	98	Echo (ping) request id=0x593c, seq=3/768, ttl=64
118	508.057193	10.0.0.1	10.0.0.13	ICMP	70	Destination unreachable (Host unreachable)
119	509.058553	10.0.0.13	216.100.100.11	ICMP	98	Echo (ping) request id=0x5a3c, seq=4/1024, ttl=64
120	509.068436	10.0.0.1	10.0.0.13	ICMP	70	Destination unreachable (Host unreachable)
121	510.069971	10.0.0.13	216.100.100.11	ICMP	98	Echo (ping) request id=0x5b3c, seq=5/1280, ttl=64
122	510.079907	10.0.0.1	10.0.0.13	ICMP	70	Destination unreachable (Host unreachable)

Private Network

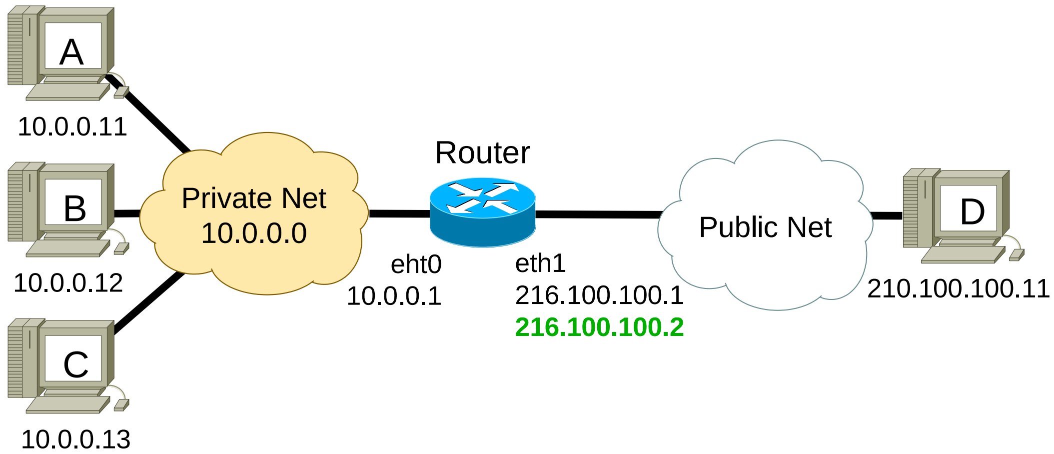
- Host C (10.0.0.13) cannot access the public network.
  - All IPv4 public address available on the Router have been mapped to Host A and Host B.
- All NAT mappings have a limited lifetime (*timeout*).
  - After some time without traffic to the public network the mappings will be deleted.

Example – NAT/PAT (1)



- Host D has a UDP server (ECHO) on port 5005.
- Public IPv4 addresses:
  - 216.100.100.2 and 216.100.100.3 to NAT mappings,
  - 216.100.100.1 to be used by the interface.

Example – NAT/PAT (2)



Hosts A, B and C access Host D (UDP Port 5005):

Source	Destination	Protocol	Length	Info
10.0.0.11	216.100.100.11	UDP	98	22147 → 5005
216.100.100.11	10.0.0.11	UDP	98	5005 → 22147
10.0.0.11	216.100.100.11	UDP	98	22147 → 5005
216.100.100.11	10.0.0.11	UDP	98	5005 → 22147

Source	Destination	Protocol	Length	Info
10.0.0.12	216.100.100.11	UDP	98	40521 → 5005
216.100.100.11	10.0.0.12	UDP	98	5005 → 40521
10.0.0.12	216.100.100.11	UDP	98	40521 → 5005
216.100.100.11	10.0.0.12	UDP	98	5005 → 40521

Source	Destination	Protocol	Length	Info
10.0.0.13	216.100.100.11	UDP	98	61252 → 5005
216.100.100.11	10.0.0.13	UDP	98	5005 → 61252
10.0.0.13	216.100.100.11	UDP	98	61252 → 5005
216.100.100.11	10.0.0.13	UDP	98	5005 → 61252

Private Network

Source	Destination	Protocol	Length	Info
216.100.100.2	216.100.100.11	UDP	98	1024 → 5005
216.100.100.11	216.100.100.2	UDP	98	5005 → 1024
216.100.100.2	216.100.100.11	UDP	98	1024 → 5005
216.100.100.11	216.100.100.2	UDP	98	5005 → 1024

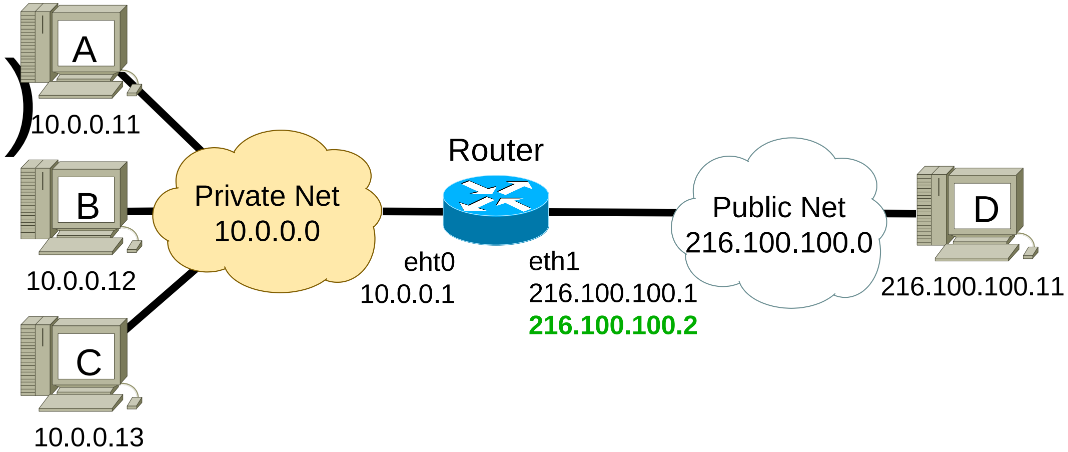
Source	Destination	Protocol	Length	Info
216.100.100.2	216.100.100.11	UDP	98	1025 → 5005
216.100.100.11	216.100.100.2	UDP	98	5005 → 1025
216.100.100.2	216.100.100.11	UDP	98	1025 → 5005
216.100.100.11	216.100.100.2	UDP	98	5005 → 1025

Source	Destination	Protocol	Length	Info
216.100.100.2	216.100.100.11	UDP	98	1026 → 5005
216.100.100.11	216.100.100.2	UDP	98	5005 → 1026
216.100.100.2	216.100.100.11	UDP	98	1026 → 5005
216.100.100.11	216.100.100.2	UDP	98	5005 → 1026

Public Network

- Mapping choices by the Router depends on local algorithm, is not defined by standards.
- All hosts were mapped to IPv4 216.100.100.2.
  - Host A used the UDP client port 22147, and was mapped to port 1024.
  - Host B used the UDP client port 40521, and was mapped to port 1025.
  - Host C used the UDP client port 61252, and was mapped to port 1025.

Example – NAT/PAT (3)



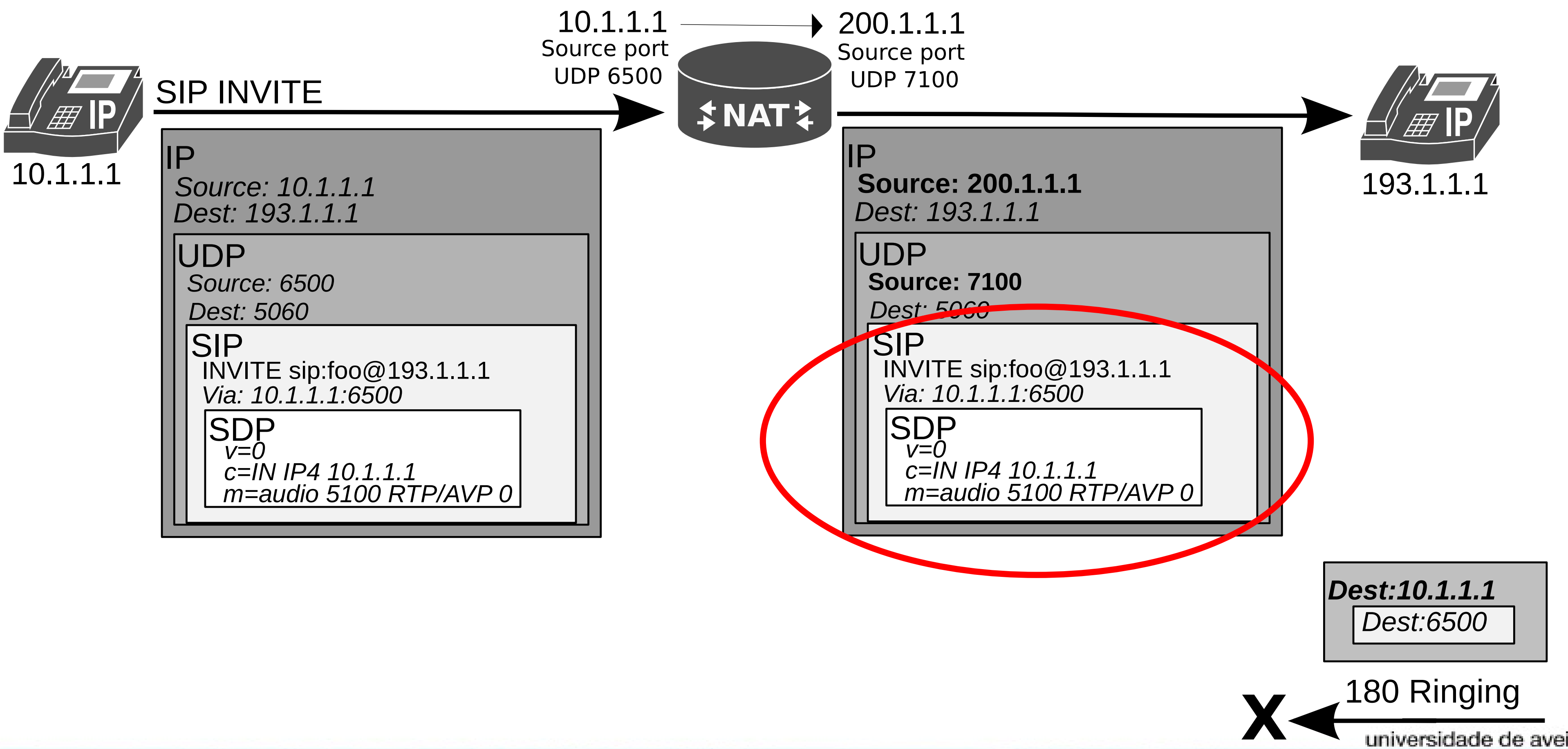
Hosts A, B and C access Host D (UDP Port 5005):

```
Router#show ip nat translation
Pro Inside global       Inside local        Outside local       Outside global
udp 216.100.100.2:1024 10.0.0.11:22147    216.100.100.11:5005 216.100.100.11:5005
udp 216.100.100.2:1025 10.0.0.12:40521    216.100.100.11:5005 216.100.100.11:5005
udp 216.100.100.2:1026 10.0.0.13:61252    216.100.100.11:5005 216.100.100.11:5005
```

- All hosts were mapped to IPv4 address 216.100.100.2.
- Host A used the UDP client port 22147, and was mapped to port 1024.
- Host B used the UDP client port 40521, and was mapped to port 1025.
- Host C used the UDP client port 61252, and was mapped to port 1025.

Some Protocols Require Translation at the Application Level

- Some protocols (e.g., SIP) require the translation of addresses and ports also at the application protocol level.
  - Very computational demanding and not all devices allow it.



IPv6 Addressing

IPv6 Background

- ETF IPv6 WG began to work on a solution to solve addressing growth issues in early 1990s
- Reasons to late deployment
  - Classless Inter-Domain Routing (CIDR) and Network address translation (NAT) were developed
  - Investments on field equipments (not IPv6 aware) had to reach the predicted “return of investment”
  - Massive re-equipment price

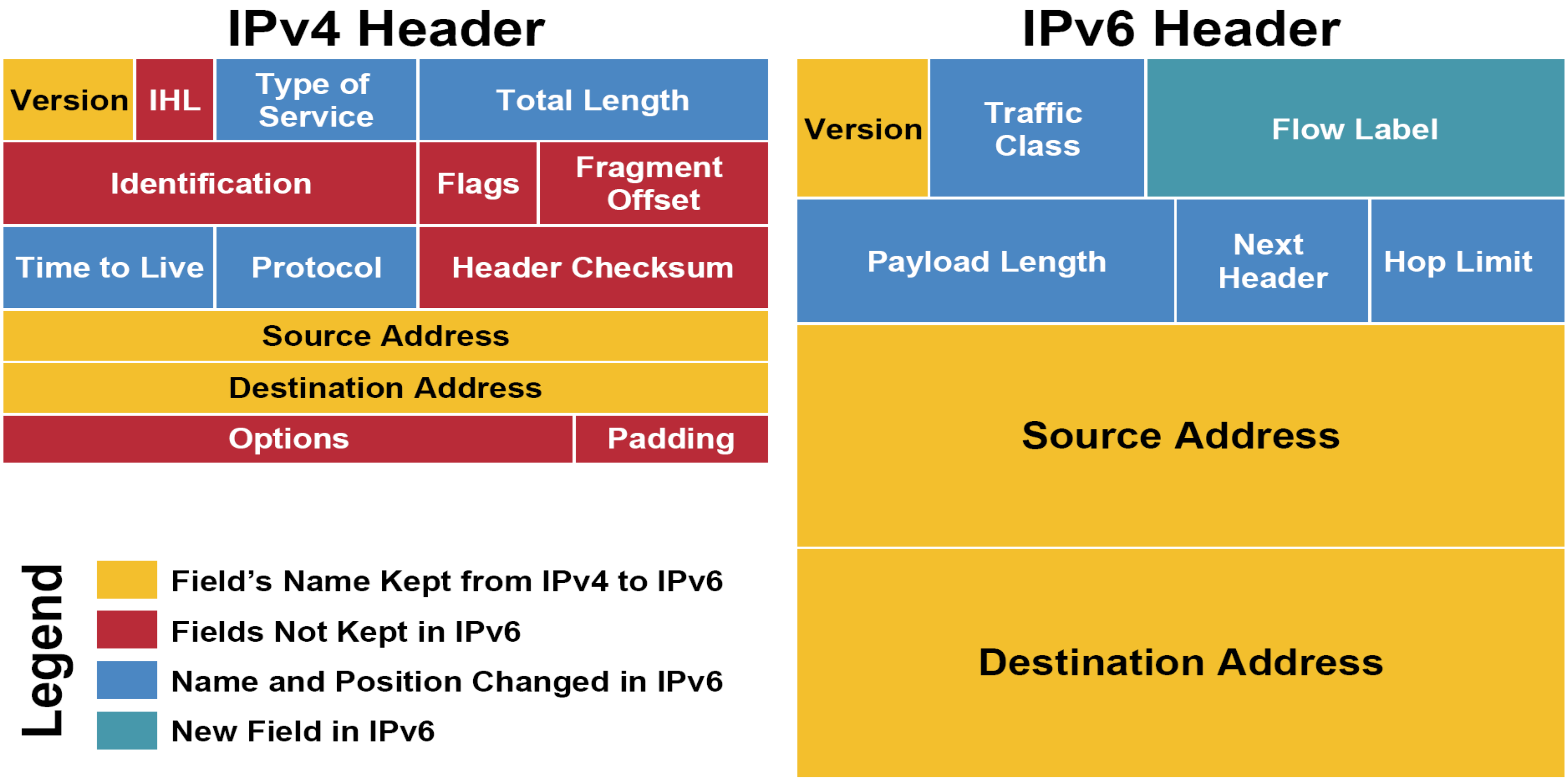
IPv6 Features

- Larger address space enabling:
  - Global reachability, flexibility, aggregation, multihoming, autoconfiguration, “plug and play” and renumbering
- Simpler header enabling:
- Routing efficiency, performance and forwarding rate scalability
- Improved option support

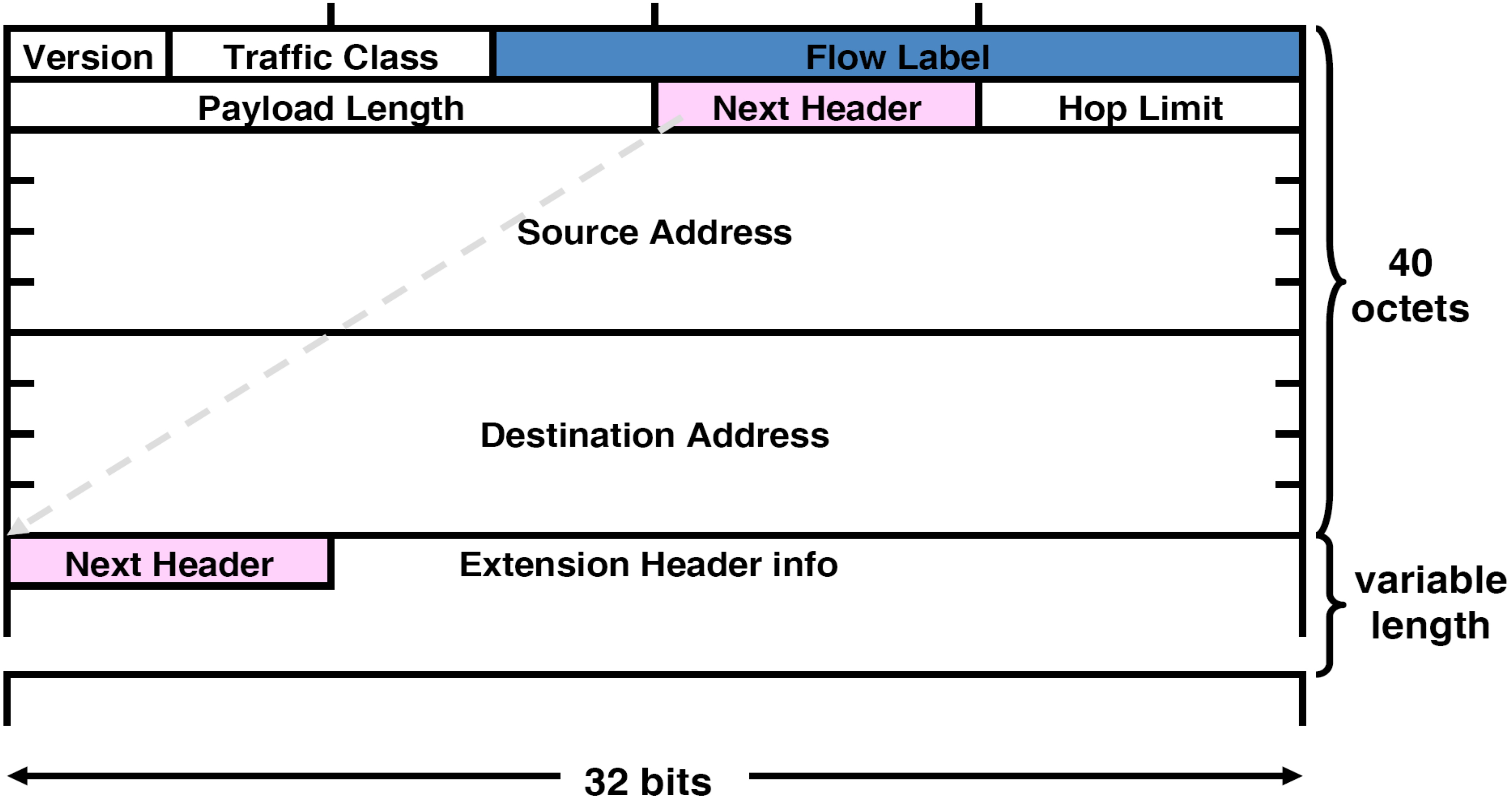
IPv6 Addressing

- IPv4: 4bytes/32 bits
  - ~ 4,294,967,296 possible addresses
- IPv6: 16bytes/128 bits
  - 340,282,366,920,938,463,463,374,607,431,768,211,456 possible addresses
- Representation
  - 16-bit hexadecimal numbers
    - Hex numbers are not case sensitive
  - Numbers are separated by (:)
    - Abbreviations are possible
      - Leading zeros in contiguous block could be represented by (::)
      - Example:
      - 2001:0db8:0000:130F:0000:0000:087C:140B = 2001:0db8:0:130F::87C:140B
      - Double colon only appears once in the address
  - Address's prefix is represented as: prefix/mask_number_of_bits

IPv4 vs. IPv6 Headers



IPv6 Header Format



IPv6 Addressing Model

- Interface have multiple addresses
- Addresses have scope:
  - Link Local
    - Valid within the same LAN or link
  - Unique Local
    - Valid within the same private domain
    - Can not be used in Internet
  - Global
- Addresses have lifetime
  - Valid and preferred lifetime

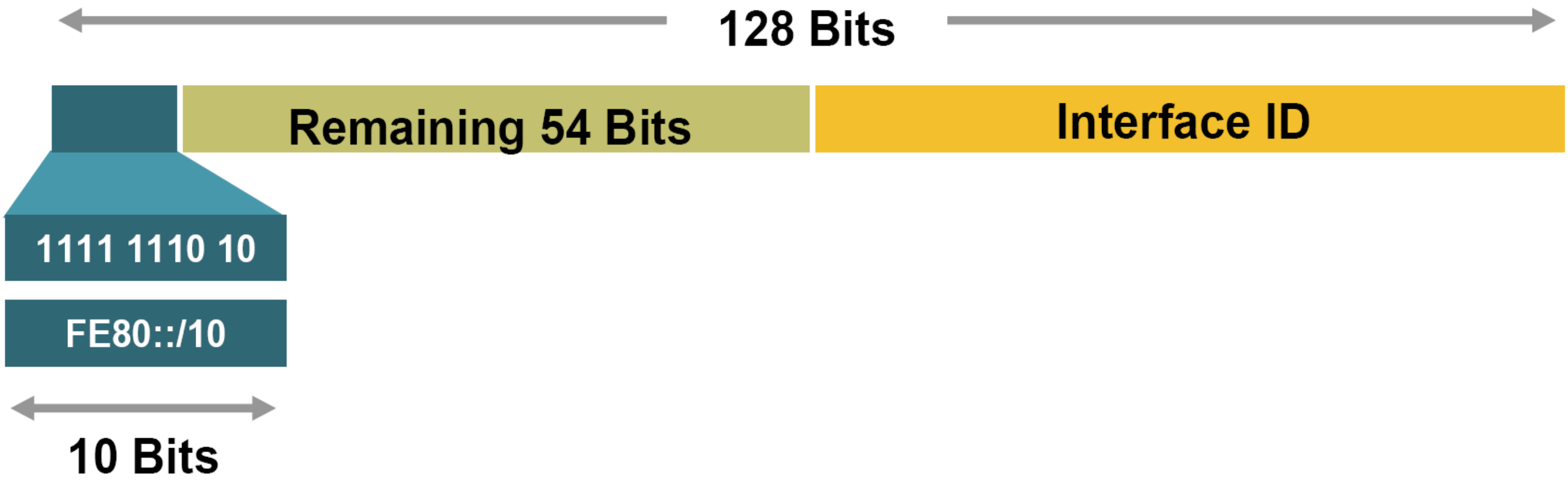
Types of IPv6 Addresses

- Unicast
  - Address of a single interface.
  - One-to-one delivery to single interface
- Multicast
  - Address of a set of interfaces.
  - One-to-many delivery to all interfaces in the set
- Anycast
  - Address of a set of interfaces.
  - One-to-one-of-many delivery to a single interface in the set that is closest
- No more broadcast addresses

IPv6 Addressing

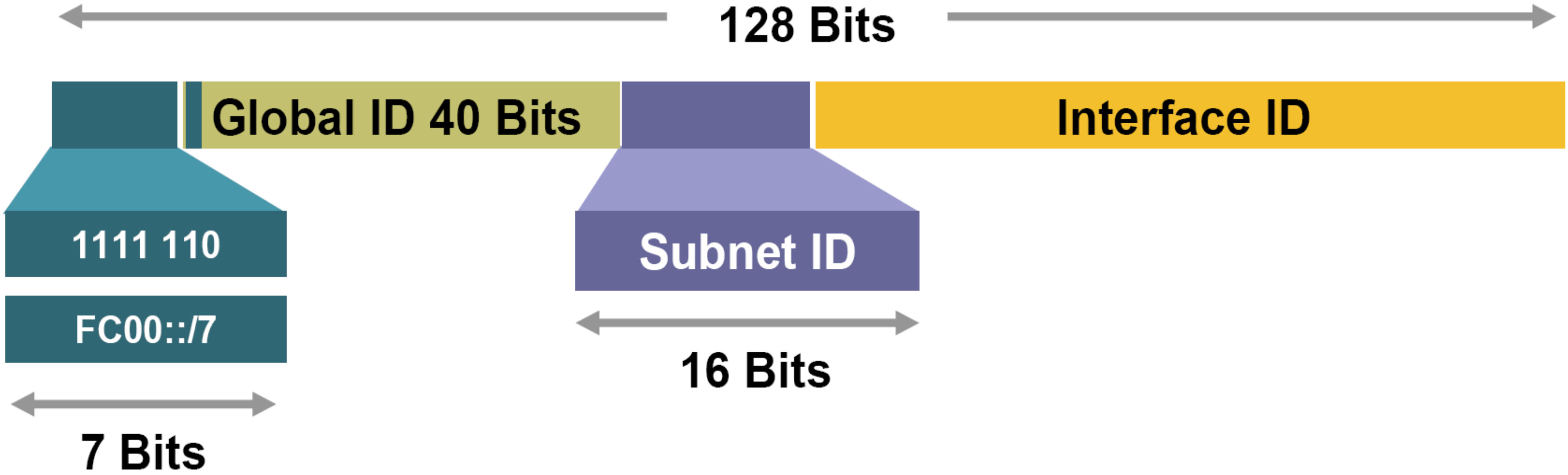
Type	Binary	Hexadecimal
Global Unicast Address	0010	2
Link-Local Unicast Address	1111 1110 10	FE80::/10
Unique-Local Unicast Address	1111 1100 1111 1101	FC00::/8 FD00::/8
Multicast Address	1111 1111	FF00::/16

Link-Local Address



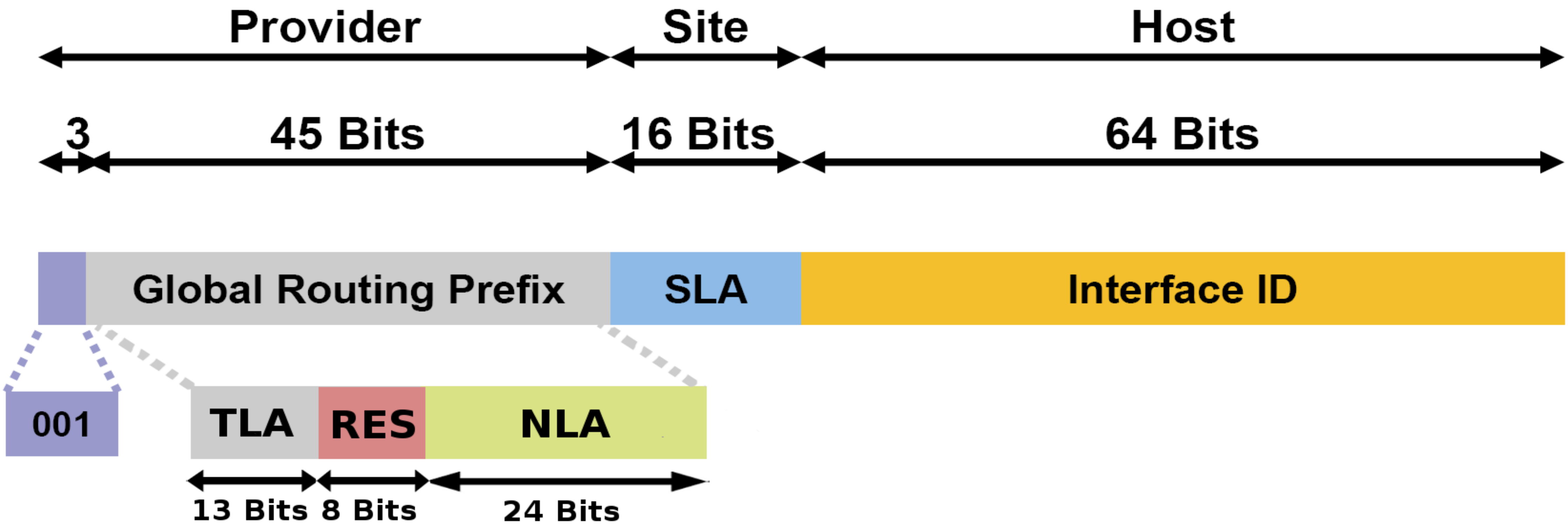
- Used For:
  - Mandatory address for local communication between two IPv6 devices
  - Next-Hop calculation in Routing Protocols
- Automatically assigned as soon as IPv6 is enabled
- Remaining 54 bits could be Zero or any manual configured value

Unique-Local Address



- Used For:
  - Local communications
  - Inter-site VPNs
- Can be routed only within the same Autonomous System
  - Can not be used on the Internet

Global Unicast Addresses



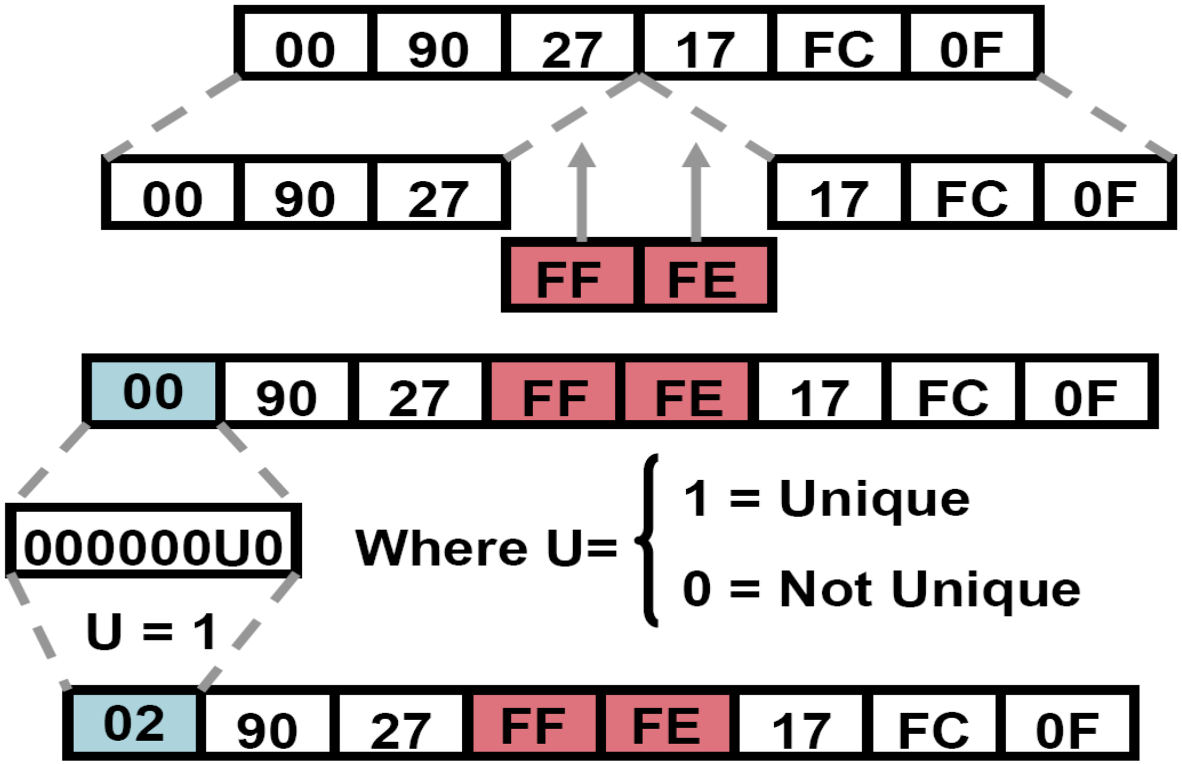
- LA, NLA and SLA used for hierarchical addressing
  - TLA - Top-Level Aggregation
  - RES – Reserved (must be zero)
  - NLA - Next-Level Aggregation Identifier
  - SLA - Site-Level Aggregation Identifier

IPv6 Interface Identifier

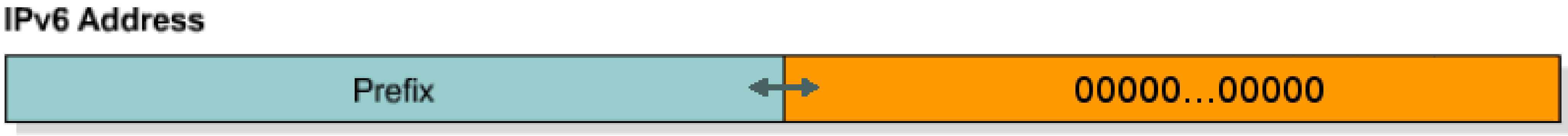
- Lowest-Order 64-Bit field of any address:
  - Auto-configured from a 64-bit EUI-64, or expanded from a 48-bit MAC address (e.g. Ethernet address)
  - Auto-generated pseudo-random number
  - Assigned via DHCP
  - Manually configured

MAC to Interface ID (EUI-64 format)

- Stateless auto-configuration
- Expands the 48 bit MAC address to 64 bits by inserting FFFE into the middle 16 bits
- To make sure that the chosen address is from a unique Ethernet MAC address
  - “u”bit is set to 1 for global scope
  - “u”bit is set to 0 for local scope



Anycast Address



- Address that is assigned to a set of interfaces
  - Typically belong to different nodes
- A packet sent to an Anycast address is delivered to the closest interface (determined by routing and timings)
- Anycast addresses can be used only by routers, not hosts
- Must not be used as the source address of an IPv6 packet
- Nodes to which the anycast address is assigned must be explicitly configured to recognize that the address is an Anycast address

Multicast Addresses

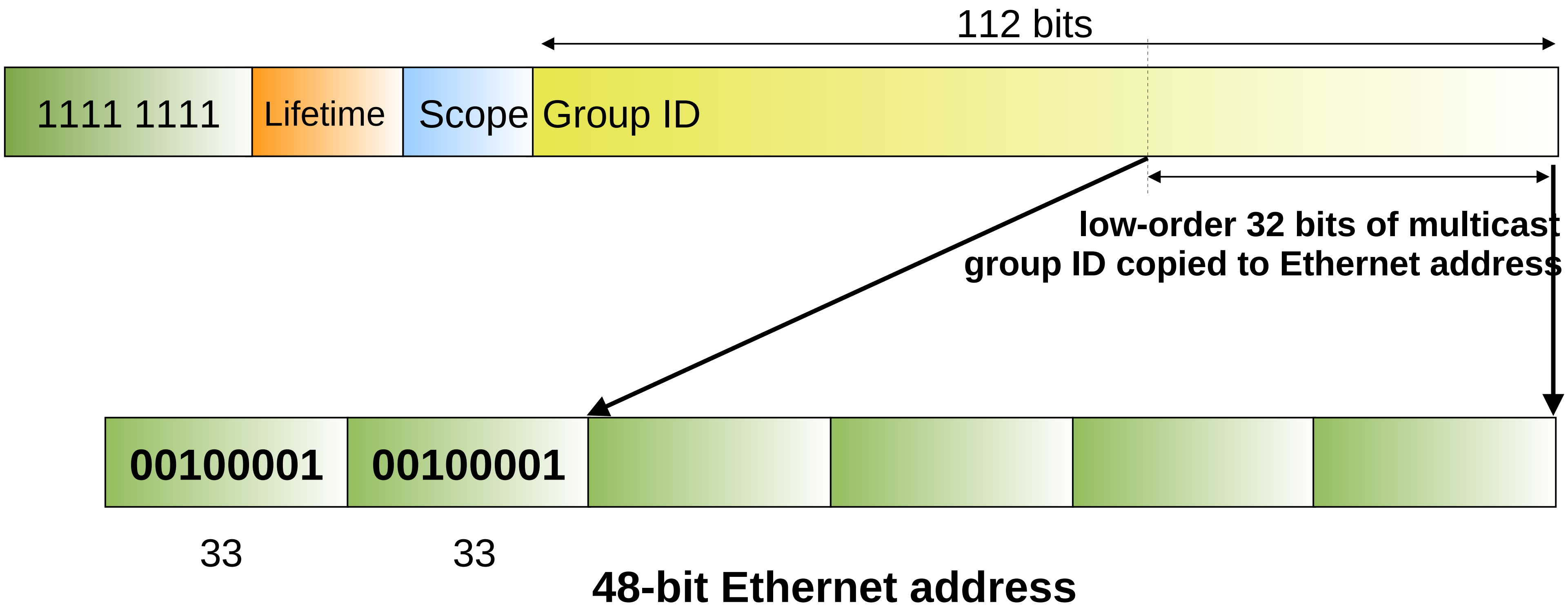
8-bit	4-bit	4-bit	112-bit
1111 1111	Lifetime	Scope	Group-ID

Lifetime	
0	If Permanent
1	If Temporary

Scope	
1	Node
2	Link
5	Site
8	Organization
E	Global

- Multicast addresses have a prefix FF00::/8
- The second byte defines the lifetime and scope of the multicast address.

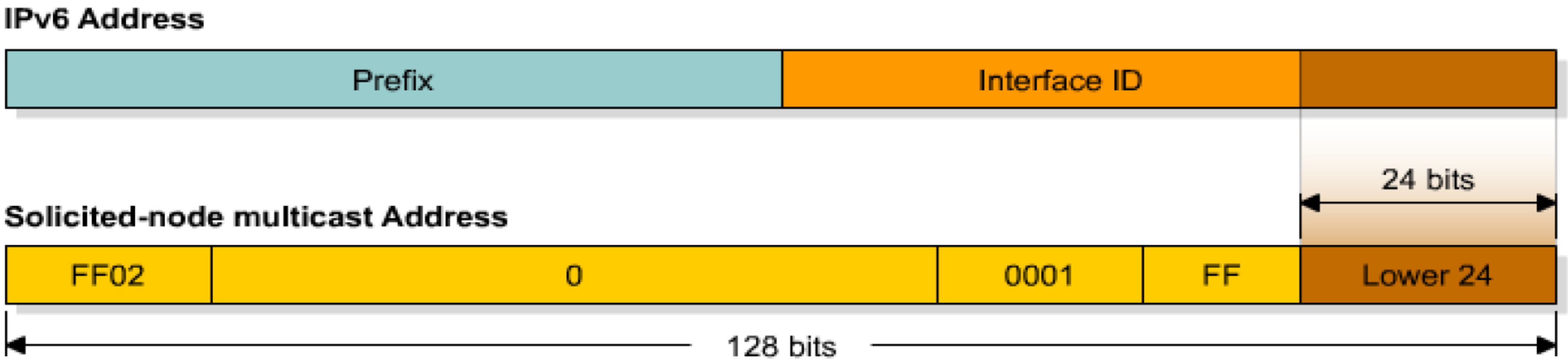
Mapping a IPv6 Multicast Address to Ethernet Address



Common Multicast Addresses

- Node Scope
  - FF01:::1 All Nodes Address (Node scope)
  - FF01:::2 All Routers Address (Node scope)
- Link Scope
  - FF02::1 All Nodes Address (Node scope)
  - FF02::2 All Routers Address
  - FF02::4 DVMRP Routers
  - FF02::5 OSPF IGP
  - FF02::6 OSPF IGP Designated Routers
  - FF02::9 RIP Routers
  - FF02::B Mobile-Agents
  - FF02::D All PIM Routers
  - FF02::E RSVP-ENCAPSULATION
  - FF02::16 All MLDv2-capable routers
  - FF02:::1:2 All DHCP agents

Solicited-Node Multicast Address



- For each unicast and anycast address configured there is a corresponding solicited-node multicast
- FF02::1:FF:<interface ID's lower 24 bits>
- This address has link local significance only
- Used in “Neighbour Solicitation Messages”
  - MAC/Physical addresses resolution
  - Duplicate Address Detection (DAD)
    - Random or assigned interface IDs may result in equal global/link addresses

Physical Addresses Resolution

- In IPv6 ARP does not exist anymore.
- ARP table is now called **NDP table**
  - NDP: Neighbor Discovery Protocol
  - Maintains a list of known neighbors (IPv6 addresses and MAC addresses).
- Uses ICMPv6 “Neighbor Solicitation” and “Neighbor Advertisement” messages.
  - To resolve an address a Neighbor Solicitation message is sent to the Solicited-Node multicast address of the target machine (IPv6 address).
  - Response is sent in unicast using a Neighbor Advertisement message.

ICMPv6

- Internet Control Message Protocol version 6 (ICMPv6) is the implementation ICMP for IPv6
    - RFC 4443
    - ICMPv6 is an integral part of IPv6.
- Have the same functionalities of ICMP, plus:
    - Replaces and enhances ARP,
        - ICMPv6 implements a Neighbor Discovery Protocol (NDP),
    - Hosts use it to discover routers and perform auto configuration of addresses,
    - Used to perform Duplicate Address Detection (DAD),
    - Used to test reachability of neighbors.

Neighbor Discovery

- Neighbor discovery uses ICMPv6 messages, originated from node on link local with hop limit of 255
- Consists of IPv6 header, ICMPv6 header, neighbor discovery header, and neighbor discovery options
- Five neighbor discovery messages
  - Router solicitation (ICMPv6 type 133)
  - Router advertisement (ICMPv6 type 134)
  - Neighbor solicitation (ICMPv6 type 135)
  - Neighbor advertisement (ICMPv6 type 136)
  - Redirect (ICMPV6 type 137)

Router Solicitation

- Host send to inquire about presence of a router on the link
- Send to all routers multicast address of FF02::2 (all routers multicast address)
- Source IP address is either link local address or unspecified IPv6 address

Router advertisement

- Sent out by routers periodically, or in response to a router solicitation
- Includes auto-configuration information
- Includes a "preference level" for each advertised router address
- Also includes a "lifetime" field

Neighbor Solicitation

- Send to discover link layer address of IPv6 node
- IPv6 header, source address is set to unicast address of sending node, or :: for DAD
- Destination address is set to
  - Unicast address for reachability
  - Solicited node multicast for address resolution and DAD

Neighbor Advertisement

- Response to neighbor solicitation message
- Also send to inform change of link layer address

Redirect

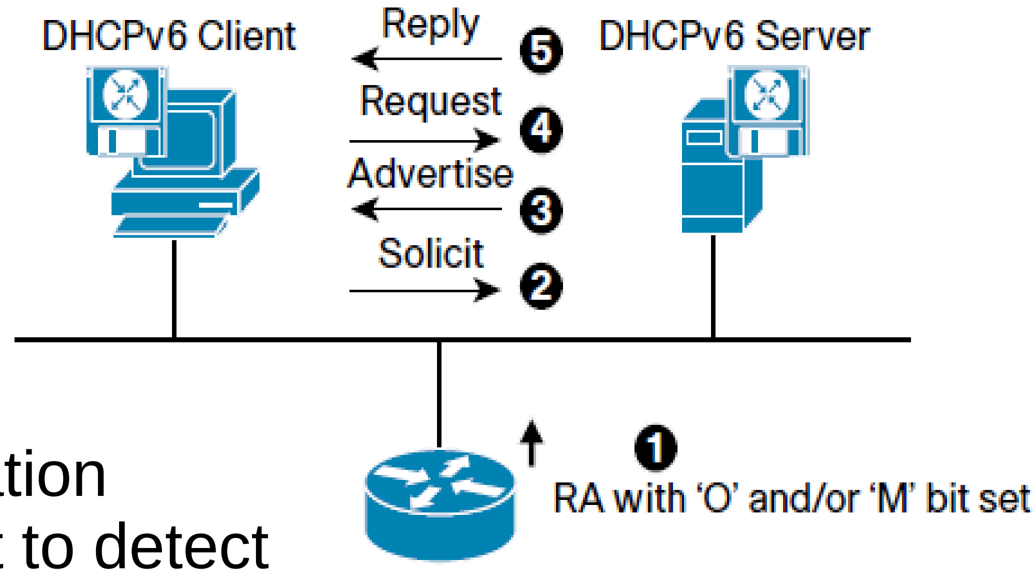
- Redirect is used by a router to signal the reroute of a packet to a better router

Auto-configuration

- Stateless
  - A node on the link can automatically configure global IPv6 addresses by appending its interface identifier (64 bits) to the prefixes (64 bits) included in the Router Advertisement messages
  - Additional/Other network information may be obtained
    - Additional fields in Router Advertisement messages,
    - Using a stateless DHCPv6 server.
- Stateful
  - Addresses are obtained using DHCPv6.

- The default gateway may send two configurable flags in Router Advertisements (RA)
  - Other flag bit: client can use DHCPv6 to retrieve other configuration parameters (e.g.: DNS server addresses)
  - Managed flag bit: client may use DHCPv6 to retrieve a Managed IPv6 address from a server

DHCPv6



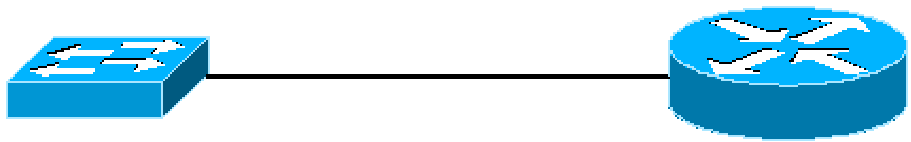
- Basic DHCPv6 concept is similar to DHCP for IPv4.
- If a client wishes to receive configuration parameters, it will send out a request to detect available DHCPv6 servers.
  - This done through the "Solicit" and "Advertise" messages.
  - Well known DHCPv6 Multicast addresses are used for this process.
- Next, the DHCPv6 client will "Request" parameters from an available server which will respond with the requested information with a "Reply" message.
- DHCPv6 relaying works differently from DHCP for IPv4 relaying
  - Relay agent will encapsulate the received messages from the directly connected DHCPv6 client (RELAY-FORW message)
  - Forward these encapsulated DHCPv6 packets towards the DHCPv6 server.
  - In the opposite direction, the Relay Agent will decapsulate the packets received from the central DHCPv6 Server (RELAY-REPL message).

Multicast Listener Discovery (MLD)

- MLD permits the creation/management of multicast groups
- MLD is used by an IPv6 router to:
  - Discover the presence of multicast listeners on directly attached links
  - And to discover which multicast addresses are of interest to those neighboring nodes
  - Report interest in router specific multicast addresses
- Routers and hosts use MLD to report interest in respective Solicited-Node Multicast Addresses

- MLD will be studied later in detail.

IPv6 Start-up - Router



Multicast (all MLDv2-capable routers) **ff02::16**	**MLDv2 Report Message** (Multicast all routers)	**Null address** **::**
Multicast (all MLDv2-capable routers) **ff02::16**	**MLDv2 Report Message** (Multicast solicited-node address)	**Null address** **::**
Multicast solicited-node address **ff02::1:ff+(address's last 24 bits)**	**Neighbor Solicitation** (DAD link-local address)	**Null address** **::**
Multicast (all hosts) **ff02::1**	**Neighbor Advertisement**	**Link-local address** **fe80::+(interface ID 64-bits)**
Multicast (all MLDv2-capable routers) **ff02::16**	**MLDv2 Report Message** (Multicast all routers)	**Link-local address** **fe80::+(interface ID 64-bits)**
Multicast (all MLDv2-capable routers) **ff02::16**	**MLDv2 Report Message** (Multicast solicited-node address)	**Link-local address** **fe80::+(interface ID 64-bits)**
Multicast solicited-node address **ff02::1:ff+(address's last 24 bits)**	**Neighbor Solicitation** (DAD global address)	**Null address** **::**
Multicast (all hosts) **ff02::1**	**Router Advertisement**	**Link-local address** **fe80::+(interface ID 64-bits)**

Only if global address is configured

IPv6 Start-up – Terminal/Router Interaction

Null address **::**	**Neighbor Solicitation** → (DAD link-local address)	**Multicast solicited-node address** **ff02::1:ff+(address's last 24 bits)**
Link-local address **fe80::+(interface ID 64-bits)**	**Router Solicitation** →	**Multicast (all routers)** **ff02::2**
Null address **::**	**MLDv2 Report Message** → (Multicast solicited-node address)	**Multicast (all MLDv2-capable routers)** **ff02::16**
Multicast (all hosts) **ff02::1**	← **Router Advertisement**	**Link-local address** **fe80::+(interface ID 64-bits)**
Null address **::**	**Neighbor Solicitation** → (DAD global address)	**Multicast solicited-node address** **ff02::1:ff+(address's last 24 bits)**

Address Resolution and Ping6

Global address → **Neighbor Solicitation** (Target's IPv6 address) → **Multicast solicited-node address ff02::1:ff+(address's last 24 bits)**

Global address ← **Neighbor Advertisement** (MAC address) ← **Global address**

Global address → **ICMPv6 Echo Request** → **Global address**

Global address ← **ICMPv6 Echo Reply** ← **Global address**

Global/link-local address → **Neighbor Solicitation** (IPv6 address) → **Global/link-local address**

Global/link-local address ← **Global/link-local address**

To verify the reachability of a neighbor after physical address of a neighbor is identified

IPv6 Subnetting/Aggregation

- In IPv6 the same principles of IPv4 subnetting and aggregation are still valid.
  - Using the TLA, NLA and SLA bits of the IPv6 addresses.
  - Example: network 2001:A:A:/48 can be divided in 2^16 sub-networks with identifiers 2001:A:A:****:/64
- By standard, the maximum mask size is /64, however it is possible to subnet also the host part of the IPv6 address.
  - Usage of mask /120 to protect the network from NDP Table Exhaustion attacks.
    - With mask /120 the maximum size of the NDP table is limited to 2^8.
    - “Larger” masks also work.
  - Some tools/services may break.
  - Point-to-point links may use /126.
    - Some devices accept use /127, however in others may not work.
  - Requires manual, DHCPv6 address configuration or modified auto-configuration mechanisms.

IPv6 Addresses Planning

- Due to IPv6 nature, there are many networks and networks are large.
  - Number of hosts in LAN is not an issue!
  - Usually network managers receive /48 networks:
    - Allows for 2^16 /64 networks.
    - Standard LAN use /64
      - or /120 to protect against attacks, however breaks stateless assignment.
    - Point-to-point links use /126.
      - Usually a /64 network is sub-netted into multiple /126.