IPv4 & IPv6 Addressing

Arquitetura de Redes

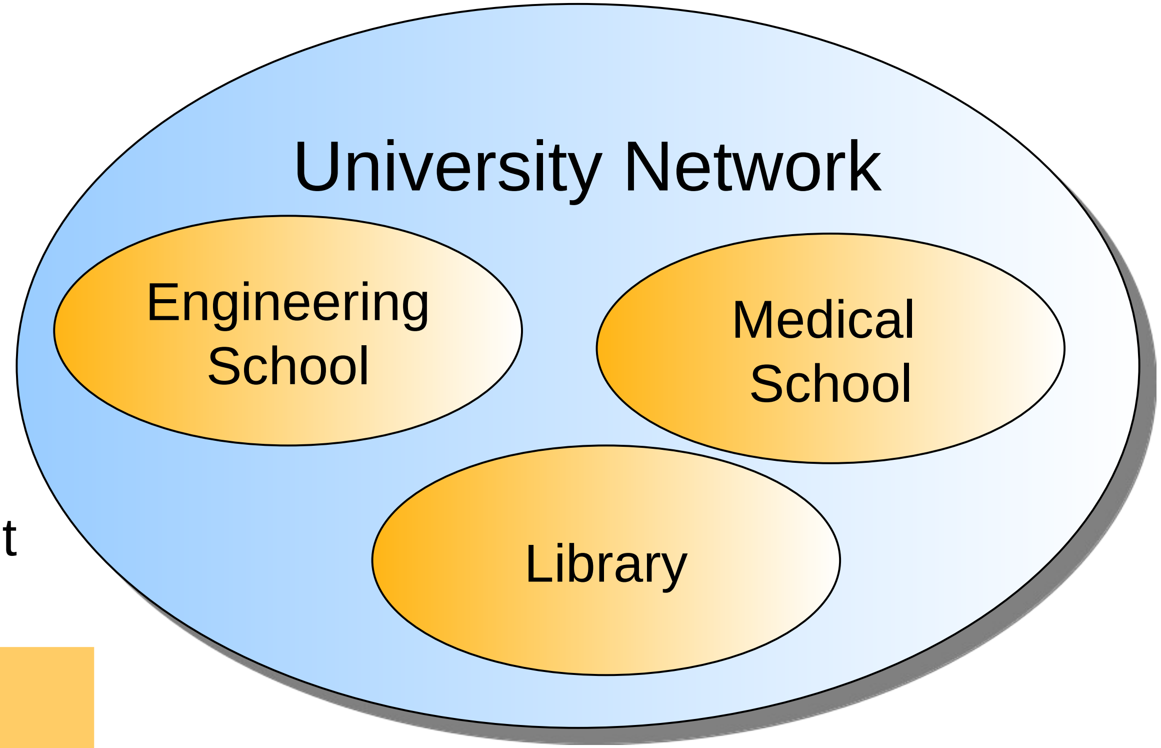
Mestrado Integrado em
Engenharia de Computadores e Telemática
DETI-UA

universidade de aveiro

deti.ua.pt

Subnetting

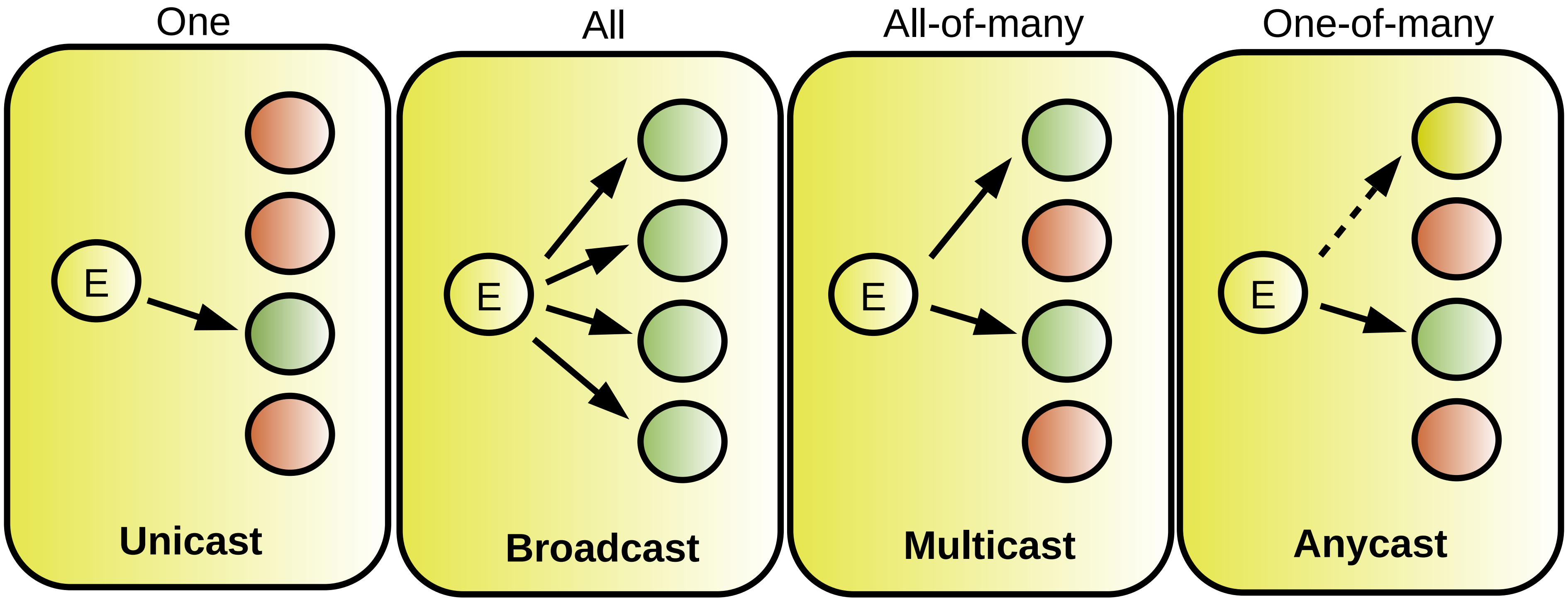
- **Problem**: Organizations have multiple networks which are independently managed
  - **Solution 1:** Allocate a separate network address for each network
    - Difficult to manage
    - From the outside of the organization, each network must be addressable.
  - **Solution 2:** Add another level of hierarchy to the IP addressing structure



→ **Subnetting**

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

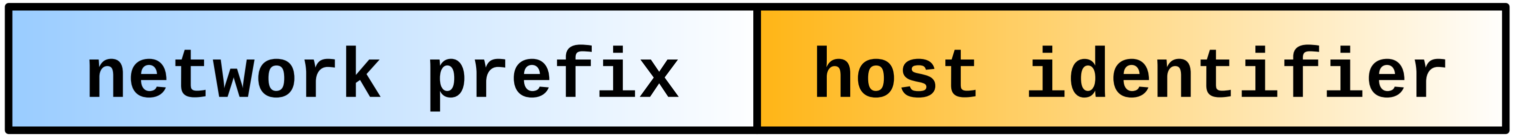
- An IPv4 address is a unique address for a network interface
- Exceptions:
  - Dynamically assigned IPv4 addresses (DHCP)
  - IP addresses in private networks (NAT)

- 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).



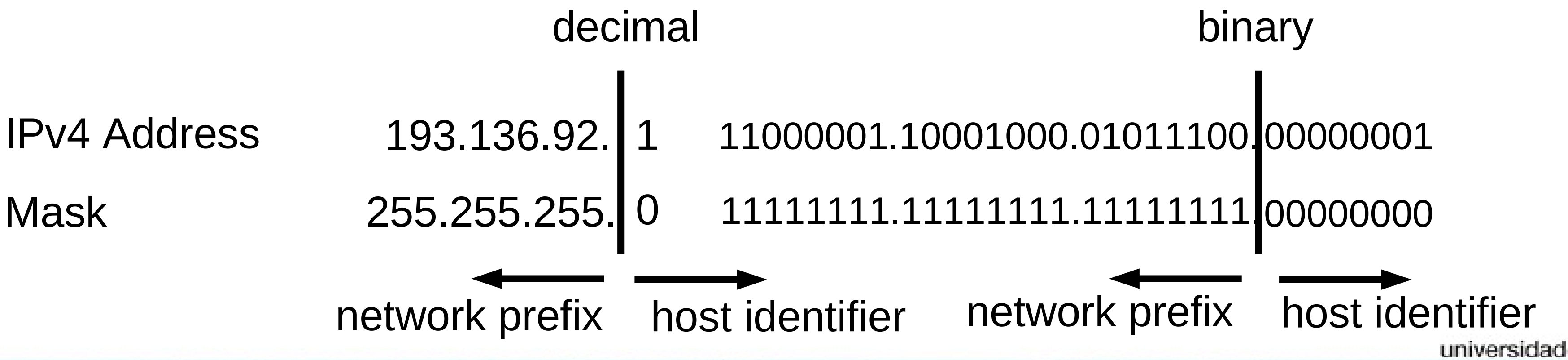
- How do we know how long the network prefix is?
  - **Before 1993:** The boundary between network prefix and host identifier is implicitly defined (**class-based/classful addressing**)

  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

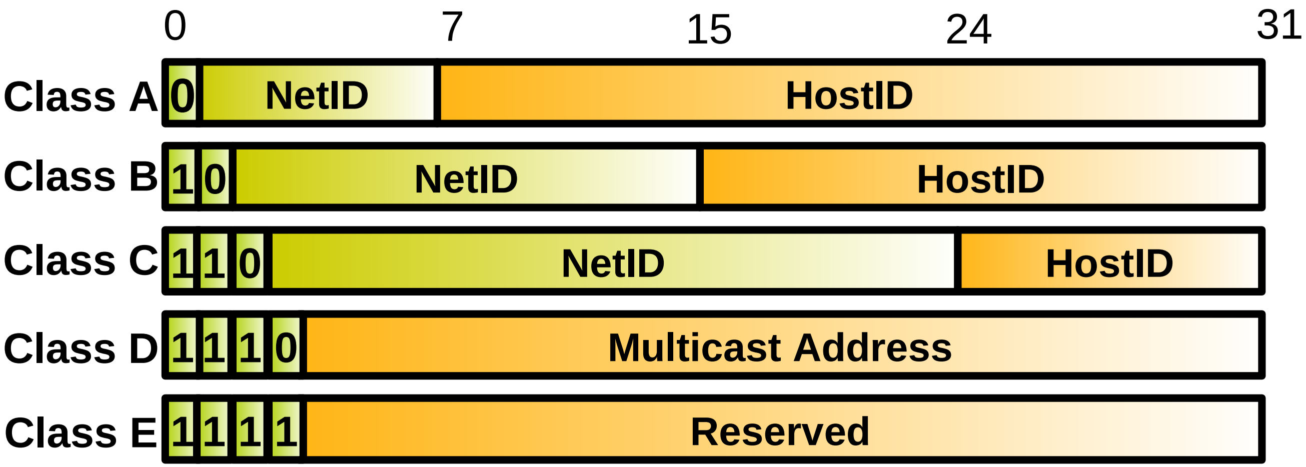
- CIDR defines a block of addresses.
- The addresses blocks are used to assign
- #Addresses= 2^(32-CIDR)
  - Example: \24→ 2^(32-24)=2^8=256, \28→ 2^(32-28)=2^4=16
- #Usable_Addresses = #Addresses – 2 addresses
  - Network prefix and broadcast address

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.


0 7 15 24 31

Class A 0 NetID HostID

Class B 1 0 NetID HostID

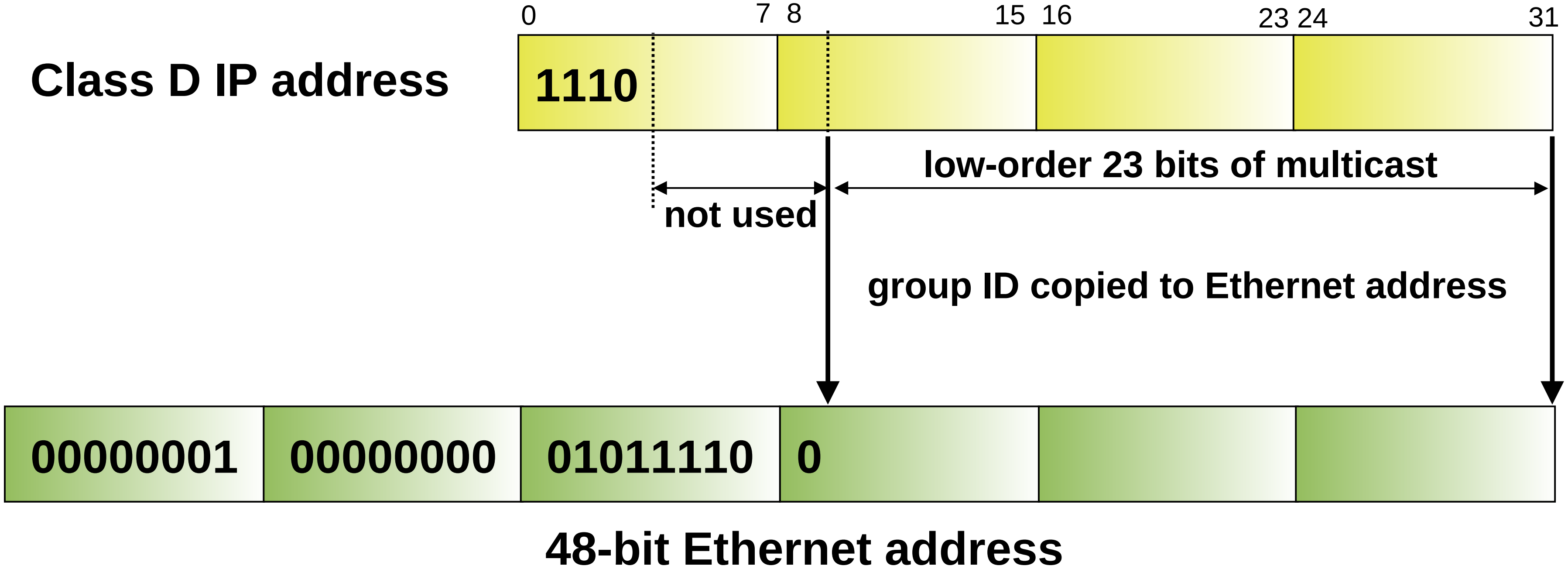
Class C 1 1 0 NetID HostID

Class D 1 1 1 0 Multicast Address

Class E 1 1 1 1 Reserved

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

Conversion of Multicast IPv4 Address to Ethernet Address



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!

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

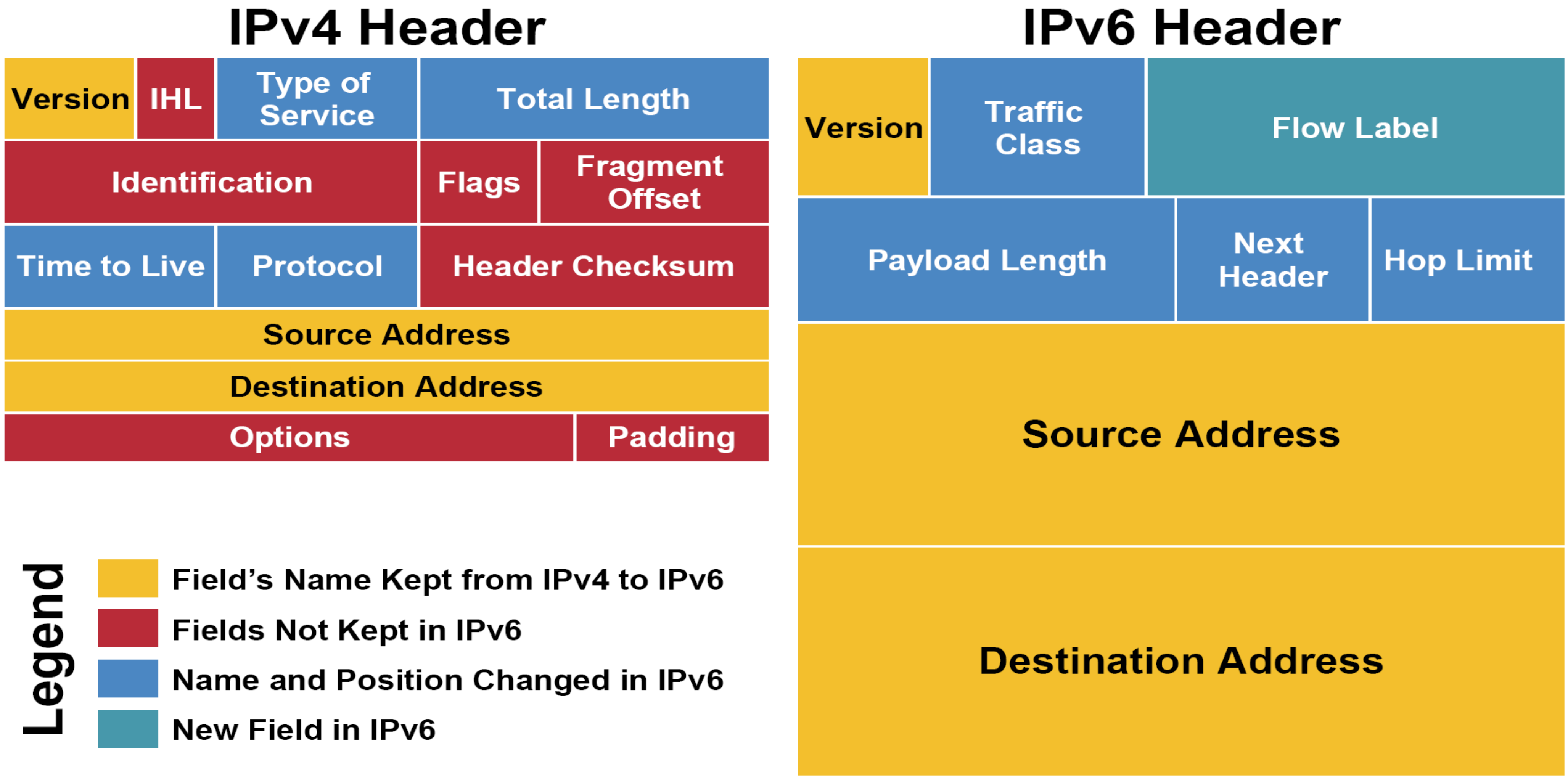
IPv6 Features

- 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



IPv4 Header

Version | IHL | Type of Service | Total Length

Identification | Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

Source Address

Destination Address

Options | Padding

IPv6 Header

Version | Traffic Class | Flow Label

Payload Length | Next Header | Hop Limit

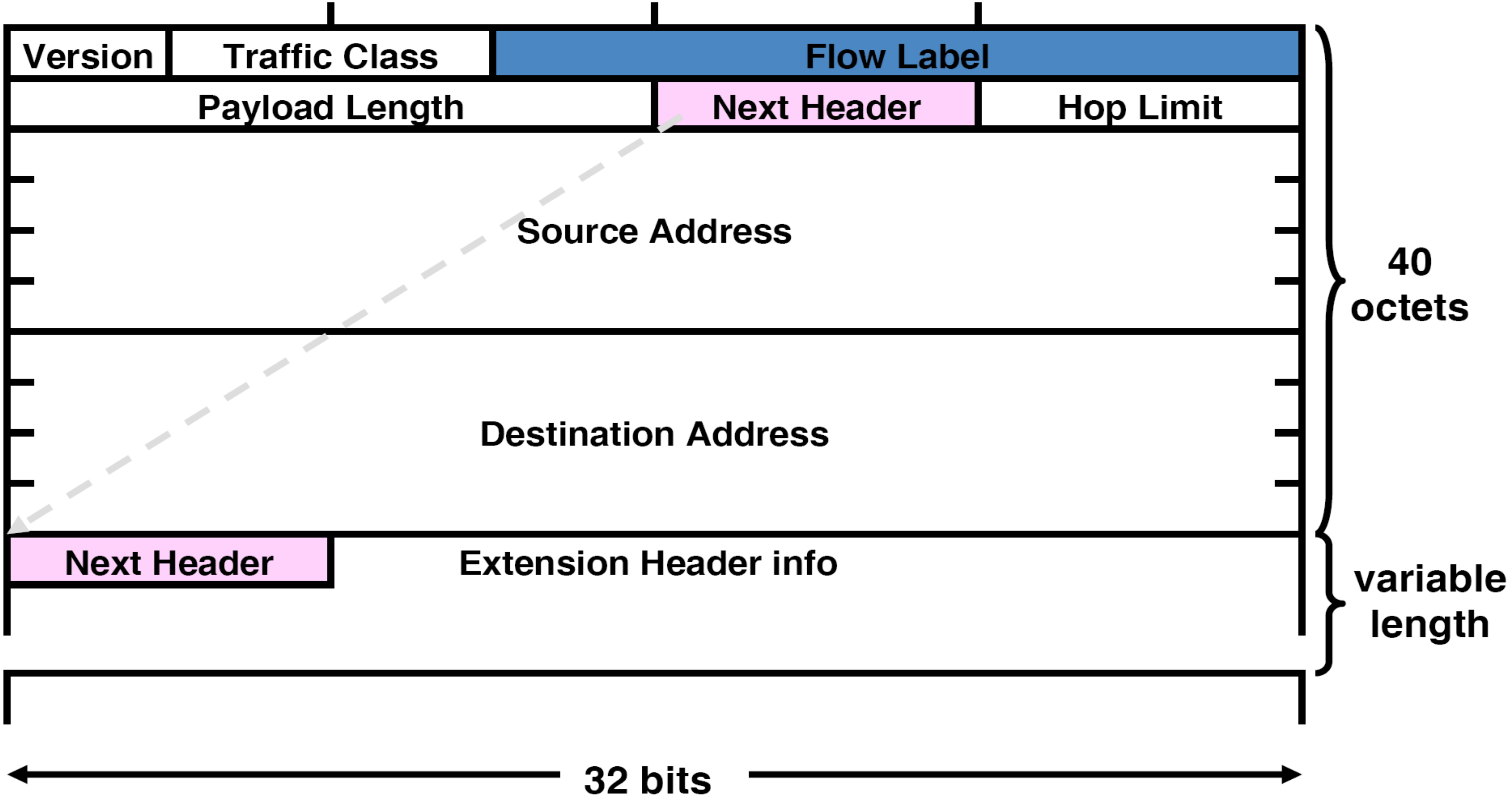
Source Address

Destination Address

Legend

- 🟨 Field’s Name Kept from IPv4 to IPv6
- 🟥 Fields Not Kept in IPv6
- 🟦 Name and Position Changed in IPv6
- 🟩 New Field in IPv6

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

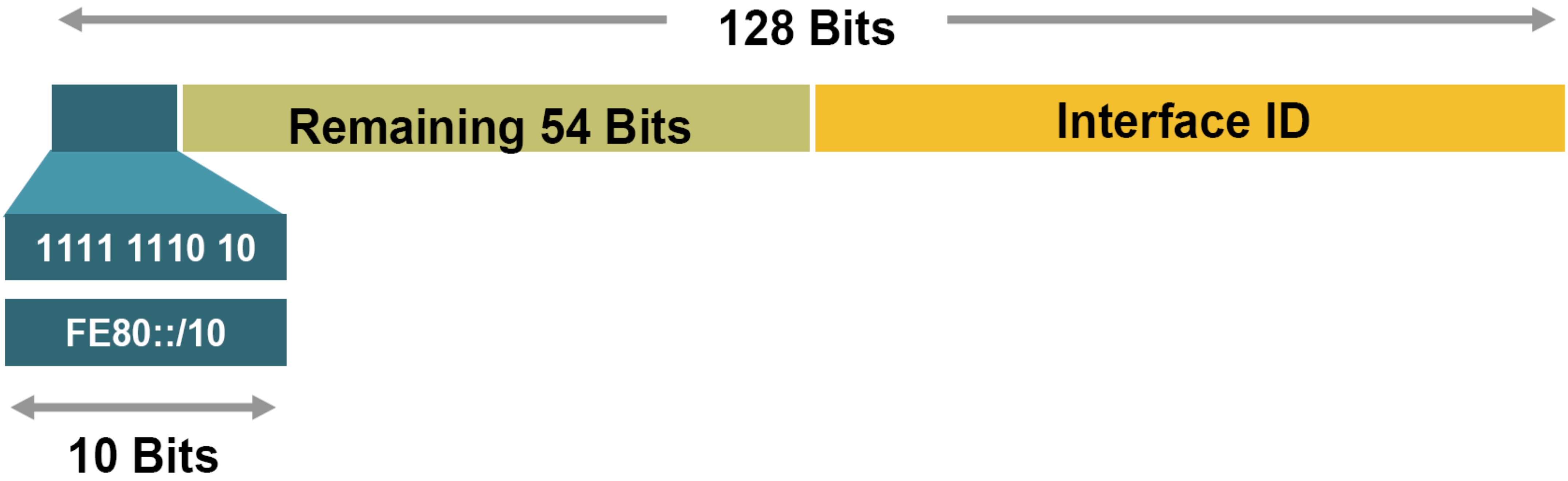
Types of IPv6 Addresses

- 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

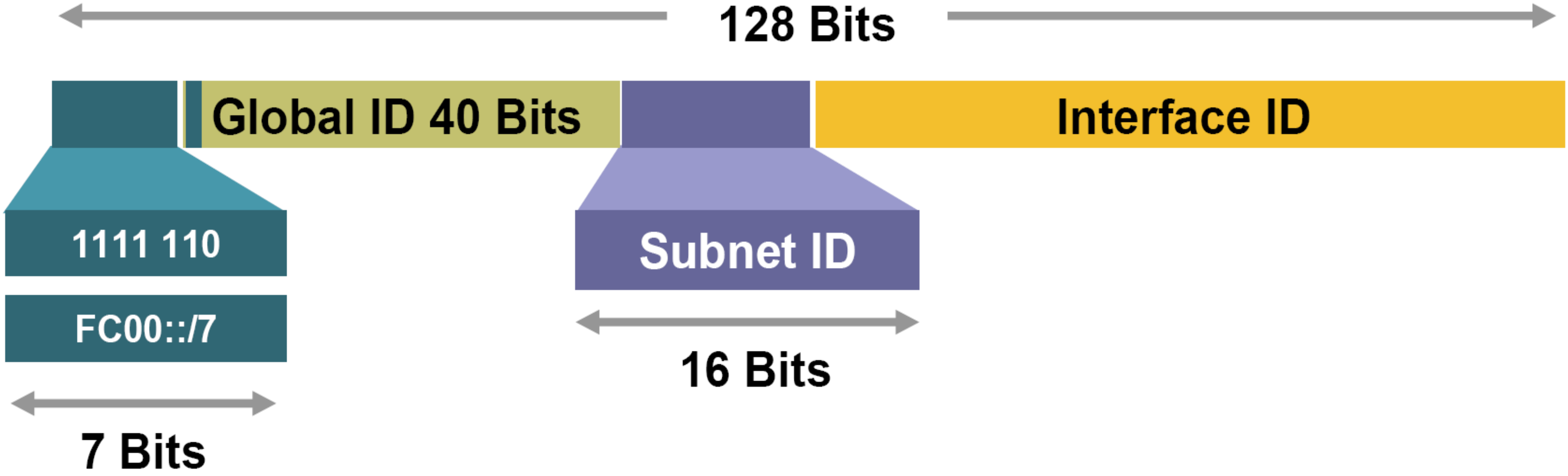
Type	Binary	Hexadecimal
Global Unicast Address	0010	2
Link-Local Unicast Address	1111 1110 10	FE80::/10
Unique-Local Unicast Address	1111 1100 1111 1101	FC00::/8 FD00::/8
Multicast Address	1111 1111	FF00::/16

Link-Local Address



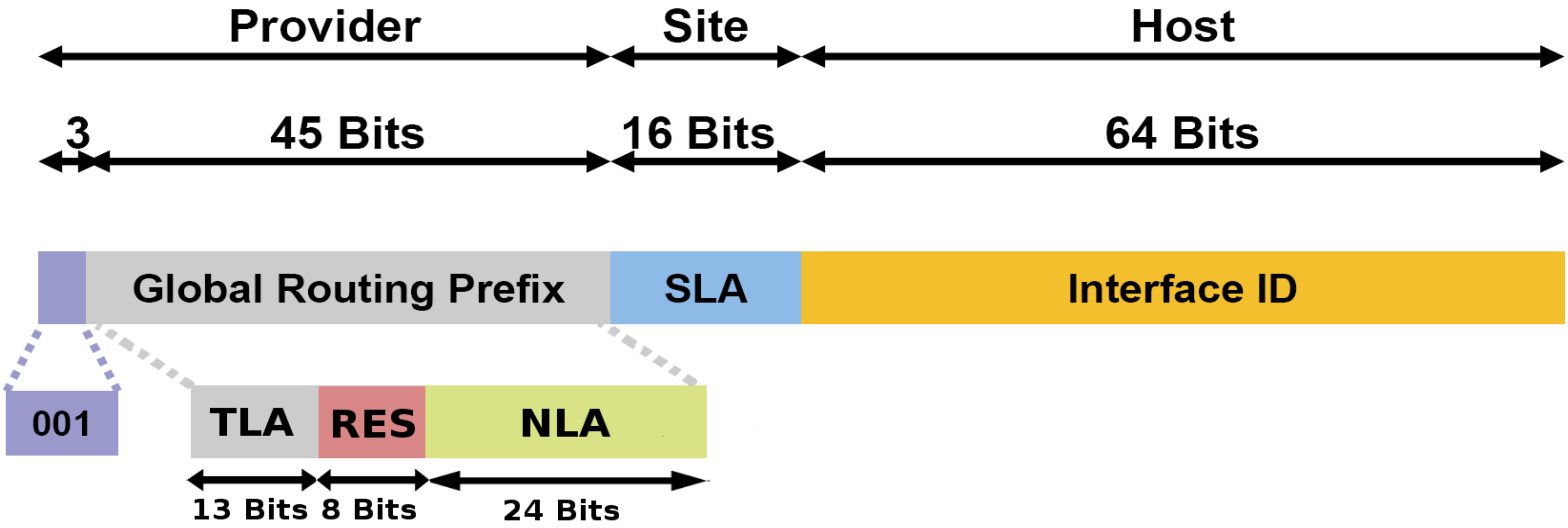
- Used For:
  - Mandatory address for local communication between two IPv6 devices
  - Next-Hop calculation in Routing Protocols
- Automatically assigned as soon as IPv6 is enabled
- Remaining 54 bits could be Zero or any manual configured value

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



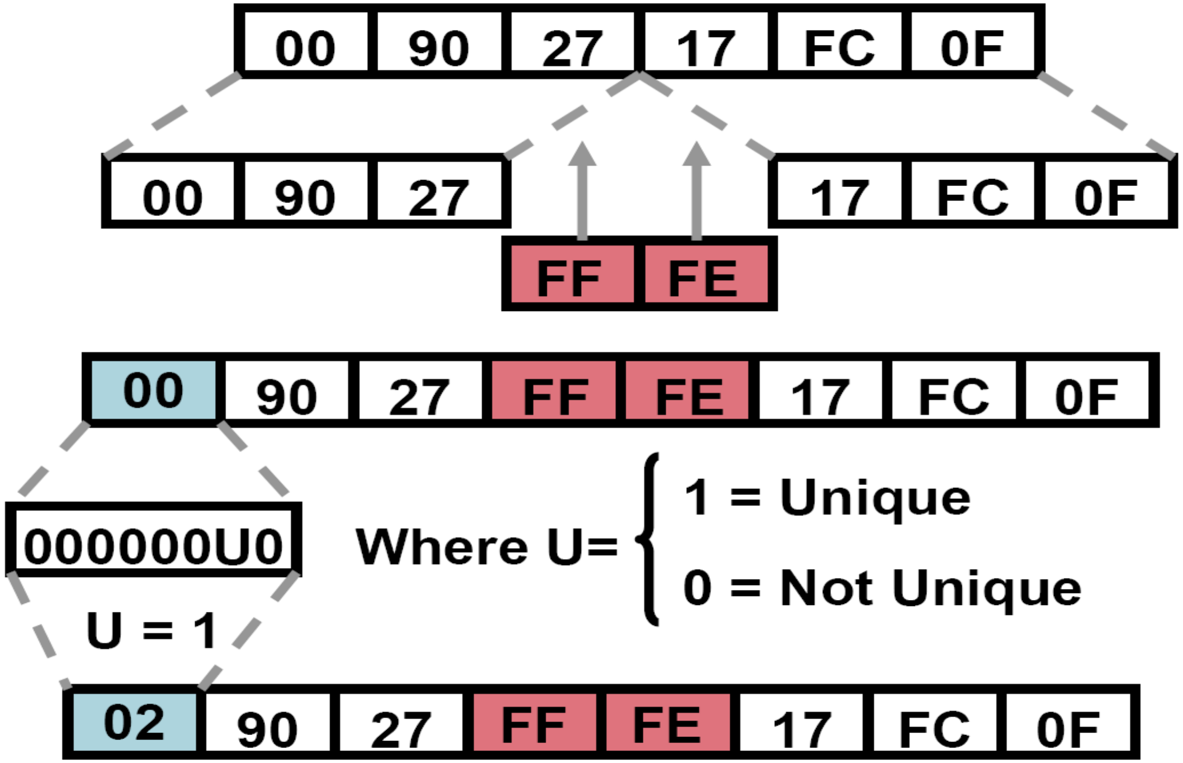
- LA, NLA and SLA used for hierarchical addressing
  - TLA - Top-Level Aggregation
  - RES – Reserved (must be zero)
  - NLA - Next-Level Aggregation Identifier
  - SLA - Site-Level Aggregation Identifier

IPv6 Interface Identifier

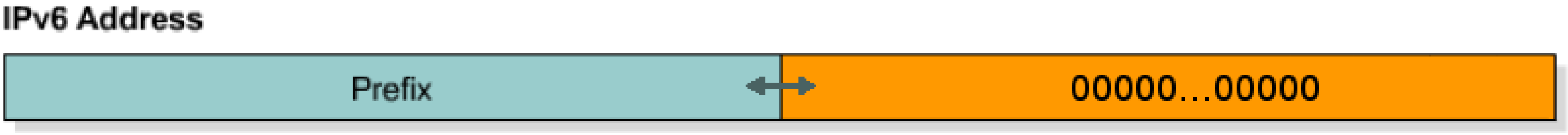
- Lowest-Order 64-Bit field of any address:
  - Auto-configured from a 64-bit EUI-64, or expanded from a 48-bit MAC address (e.g. Ethernet address)
  - Auto-generated pseudo-random number
  - Assigned via DHCP
  - Manually configured

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

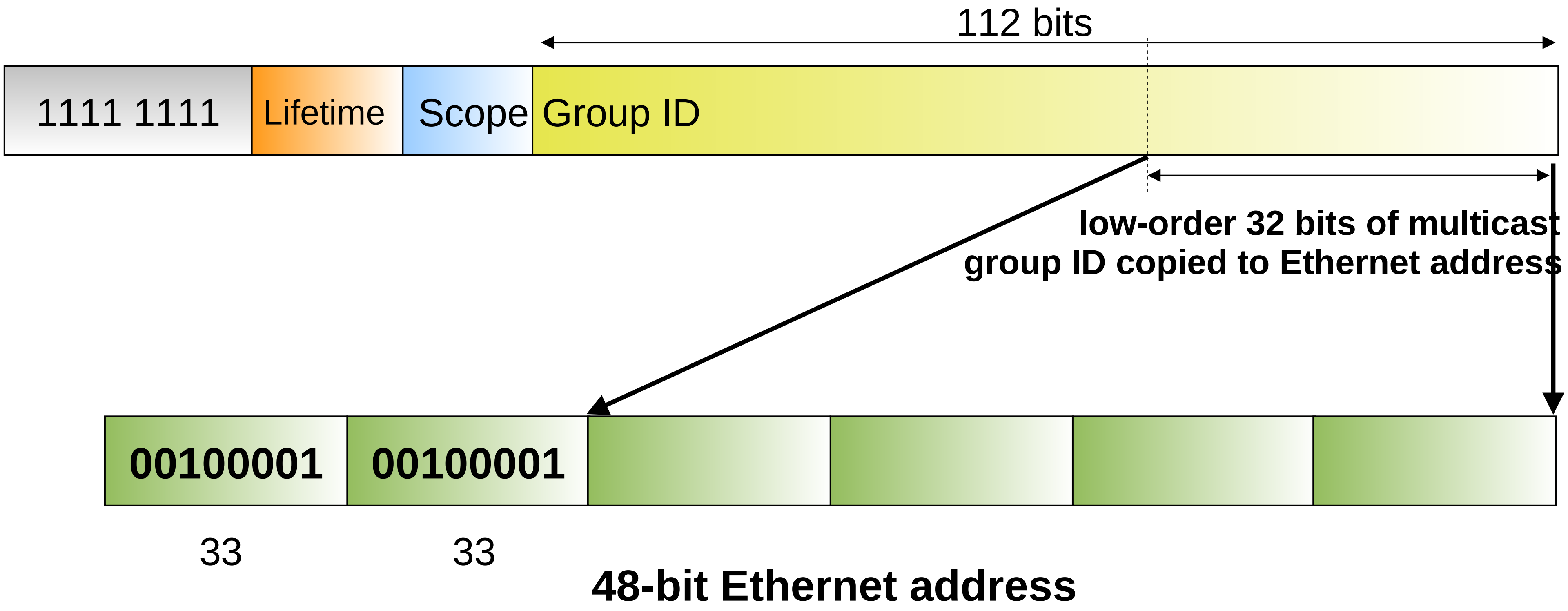
8-bit	4-bit	4-bit	112-bit
1111 1111	Lifetime	Scope	Group-ID

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.

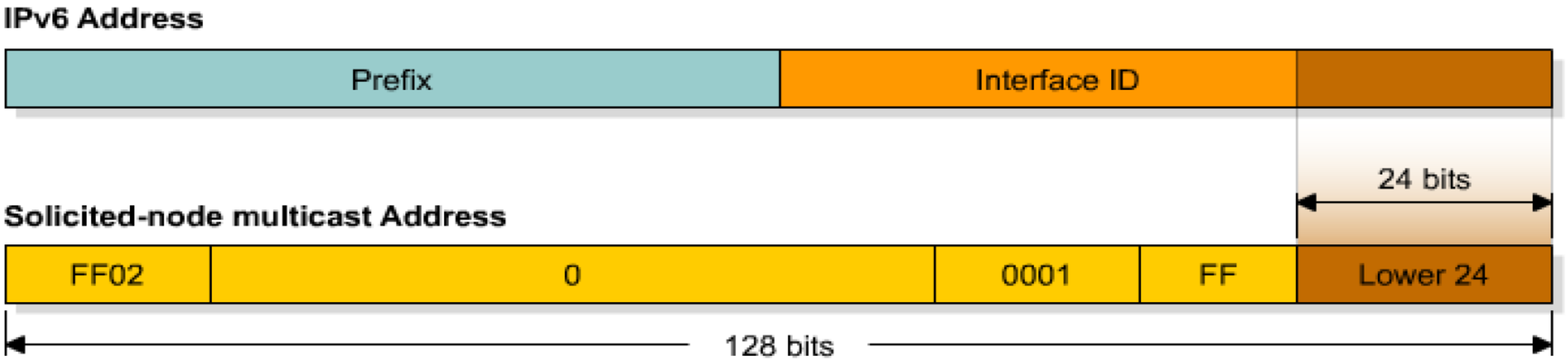
Mapping a IPv6 Multicast Address to Ethernet Address



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

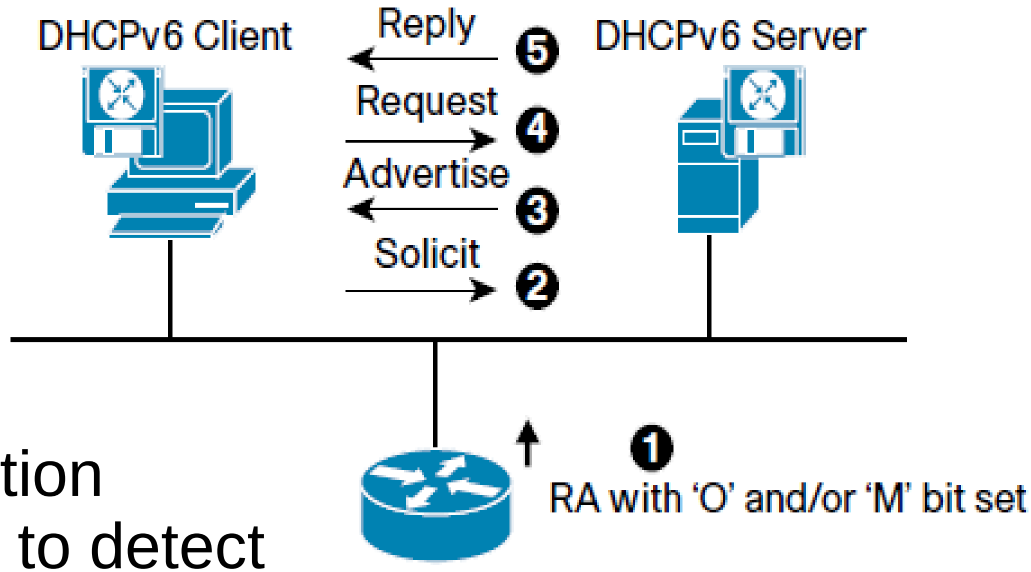
- Redirect is used by a router to signal the reroute of a packet to a better router

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



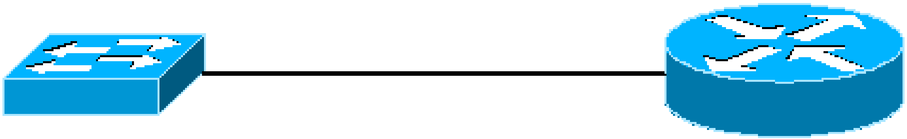
- Basic DHCPv6 concept is similar to DHCP for IPv4.
- If a client wishes to receive configuration parameters, it will send out a request to detect available DHCPv6 servers.
  - This done through the “Solicit” and “Advertise” messages.
  - Well known DHCPv6 Multicast addresses are used for this process.
- 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.

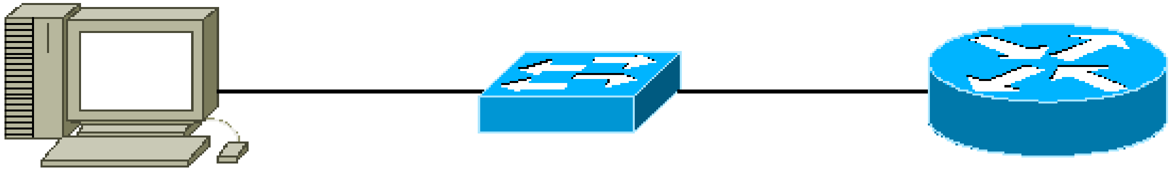
IPv6 Start-up - Router



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)

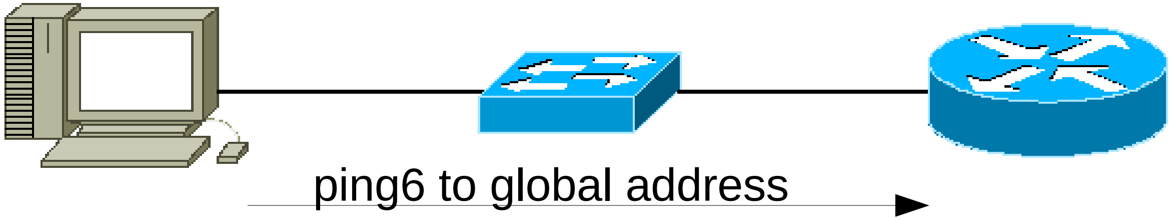
Only if global address is configured

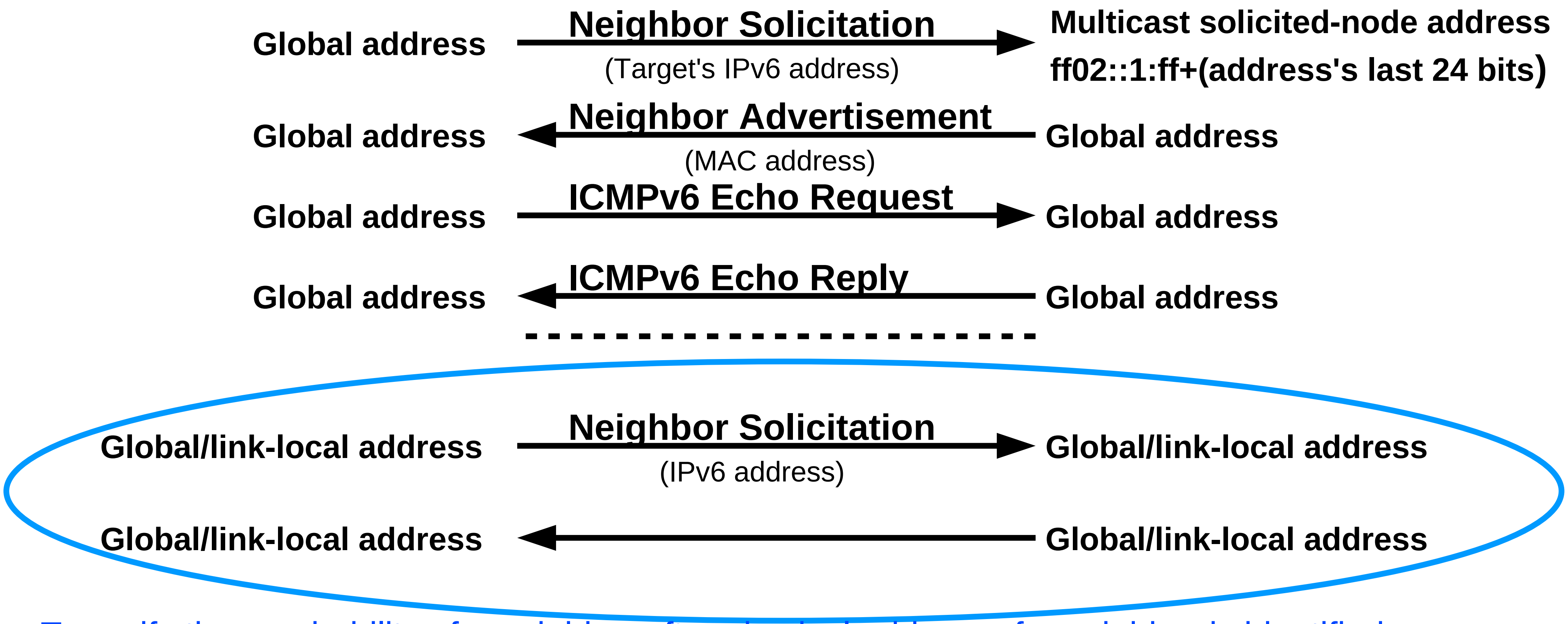
IPv6 Start-up – Terminal/Router Interaction



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





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.
    - More “large” masks also work.
  - Some tools/services may break.
  - Requires manual, DHCPv6 address configuration or modified auto-configuration mechanisms.

IP Addresses Allocation Planning

universidade de aveiro

deti.ua.pt

Physical vs. Logical Networks

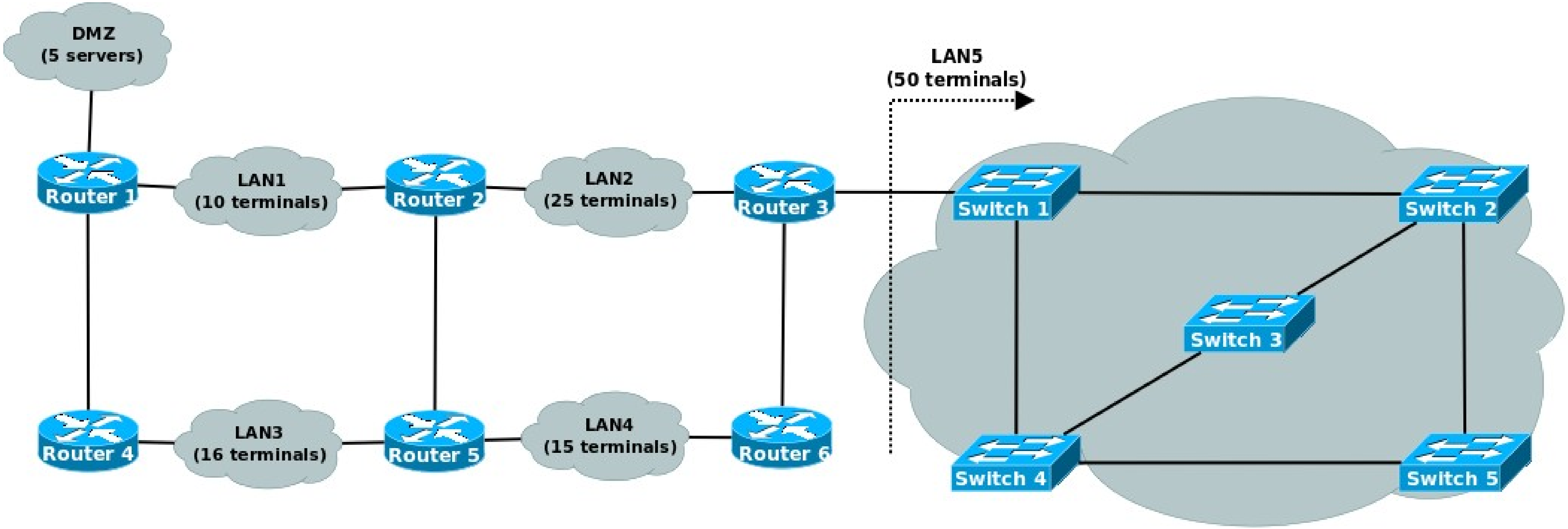
- A physical (or VLAN) network can have multiple IP logical (sub)networks,
  - One or more IPv4 public networks,
  - One or more IPv4 private networks,
  - One or more IPv6 networks.
- Requires
  - Terminals that support multiple IP addresses in the same NIC (normal!).
  - Configuration of sub-interfaces in routers or L3 switches
- IPv4 private and public routing is the same.
- IPv4 routing and IPv6 routing are independent.

Advantages of Subnetting

- With subnetting, IP addresses use a 3-layer hierarchy:
  - Network
  - Subnet
  - Host
- Reduces router complexity. Since external routers do not know about subnetting, the complexity of routing tables at external routers is reduced.
- Note: Length of the subnet mask **does not need** to be identical in all subnetworks.
  - Address blocks with mask /x contain 2 address blocks with mask /(2*x)
  - /24 block contains 2 /25 blocks
  - /25 block contains 2 /26 blocks
  - …
  - /27 block contains 2 /28 blocks

Example – IPv4 Public Planning (1)

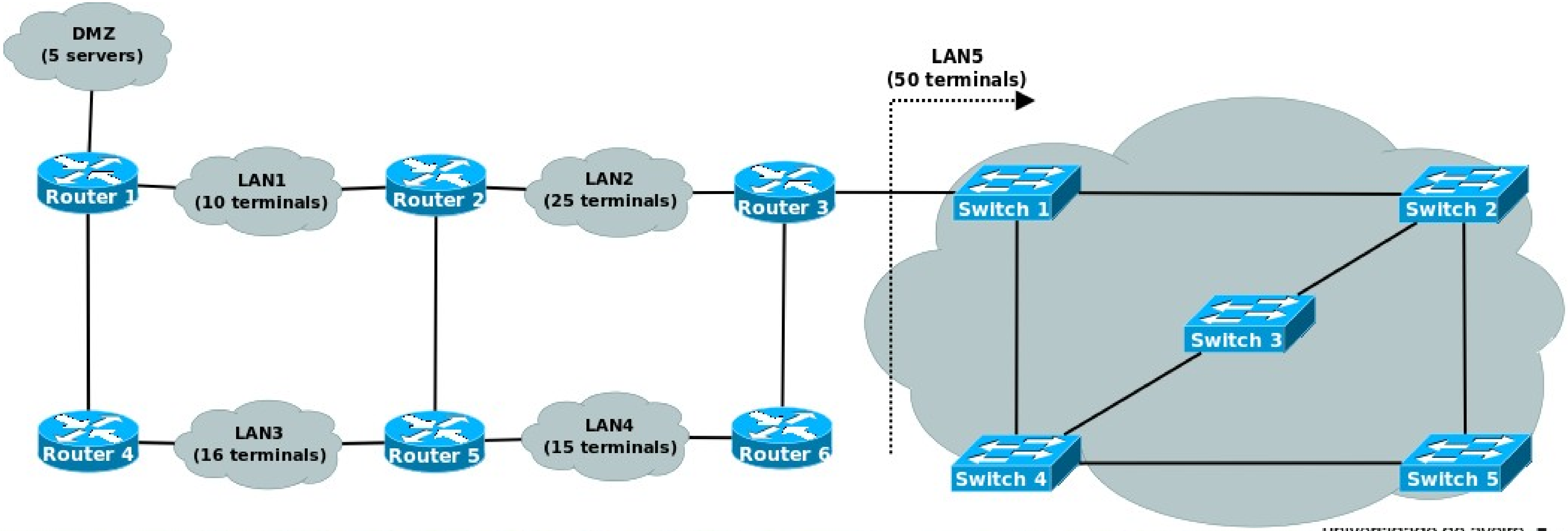
- Problem: Multiple (V)LAN require a small number of public IPv4 addresses. The public IPv4 network available is 193.1.1.0/24.
  - Note: All (V)LAN require IPv4 addresses, however may use private addresses (another IPv4 network).



192.1.1.0/24

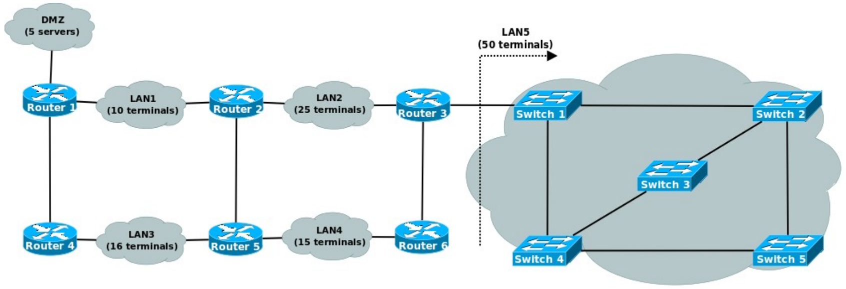
Example – IPv4 Public Planning (2)

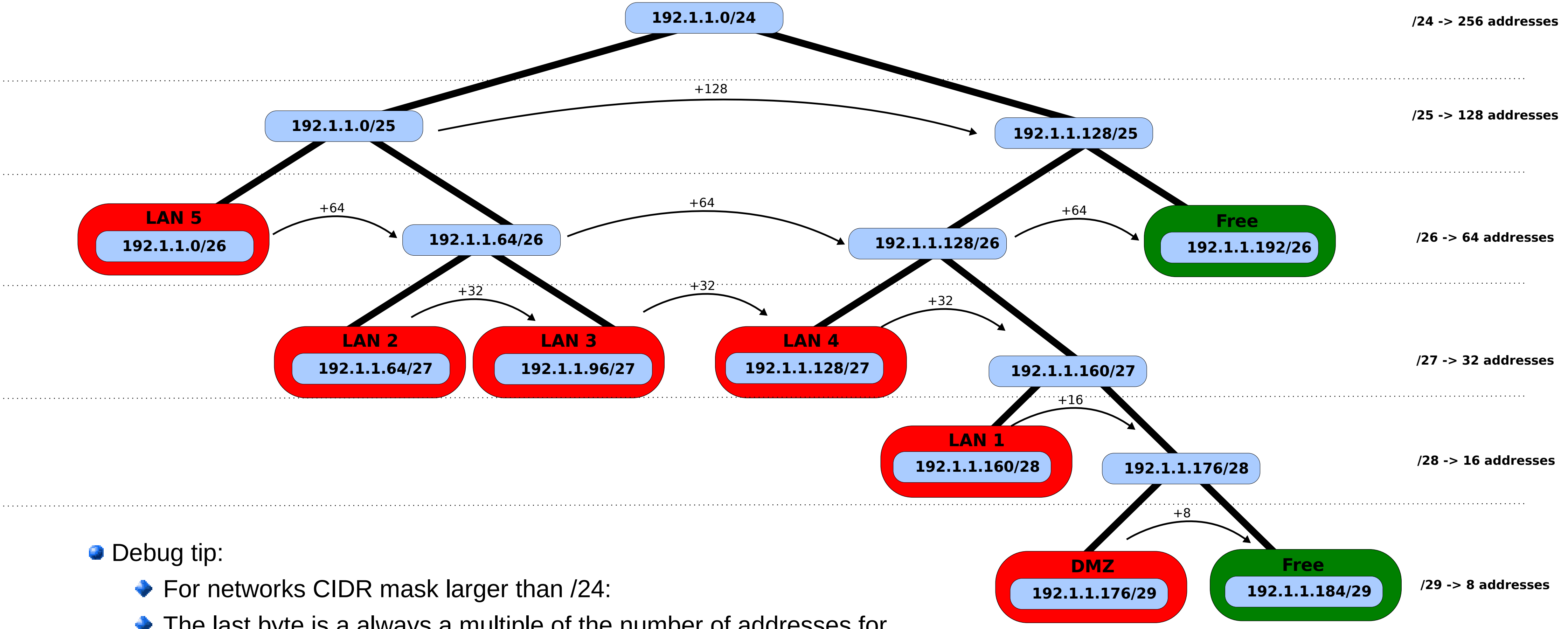
- LAN 1 → **10**+2 routers/gw+prefix+broadcast= 14 → 16 → /28 net
- LAN 2 → **25**+2 routers/gw+prefix+broadcast= 29 → 32 → /27 net
- LAN 3 → **16**+2 routers/gw+prefix+broadcast= 20 → 32 → /27 net
- LAN 4 → **15**+2 routers/gw+prefix+broadcast= 19 → 32 → /27 net
- LAN 5 → **50**+1 router/gw+prefix+broadcast= 53 → 64 → /26 net
- DMZ → **5**+1 router/gw+prefix+broadcast = 8 → 8 → /29 net



Example (3)

- LAN 1 → 10+2+2=14 → 16 → /28 net
- LAN 2 → 25+2+2=29 → 32 → /27 net
- LAN 3 → 16+2+2=20 → 32 → /27 net
- LAN 4 → 15+2+2=19 → 32 → /27 net
- LAN 5 → 50+1+2=53 → 64 → /26 net
- DMZ → 5+1+2=8 → 8 → /29 net





192.1.1.0/24

+128

192.1.1.0/25

192.1.1.128/25

LAN 5
192.1.1.0/26

+64

192.1.1.64/26

+64

192.1.1.128/26

+64

Free
192.1.1.192/26

+32

+32

+32

LAN 2
192.1.1.64/27

LAN 3
192.1.1.96/27

LAN 4
192.1.1.128/27

192.1.1.160/27

+16

LAN 1
192.1.1.160/28

192.1.1.176/28

+8

DMZ
192.1.1.176/29

Free
192.1.1.184/29

/24 -> 256 addresses

/25 -> 128 addresses

/26 -> 64 addresses

/27 -> 32 addresses

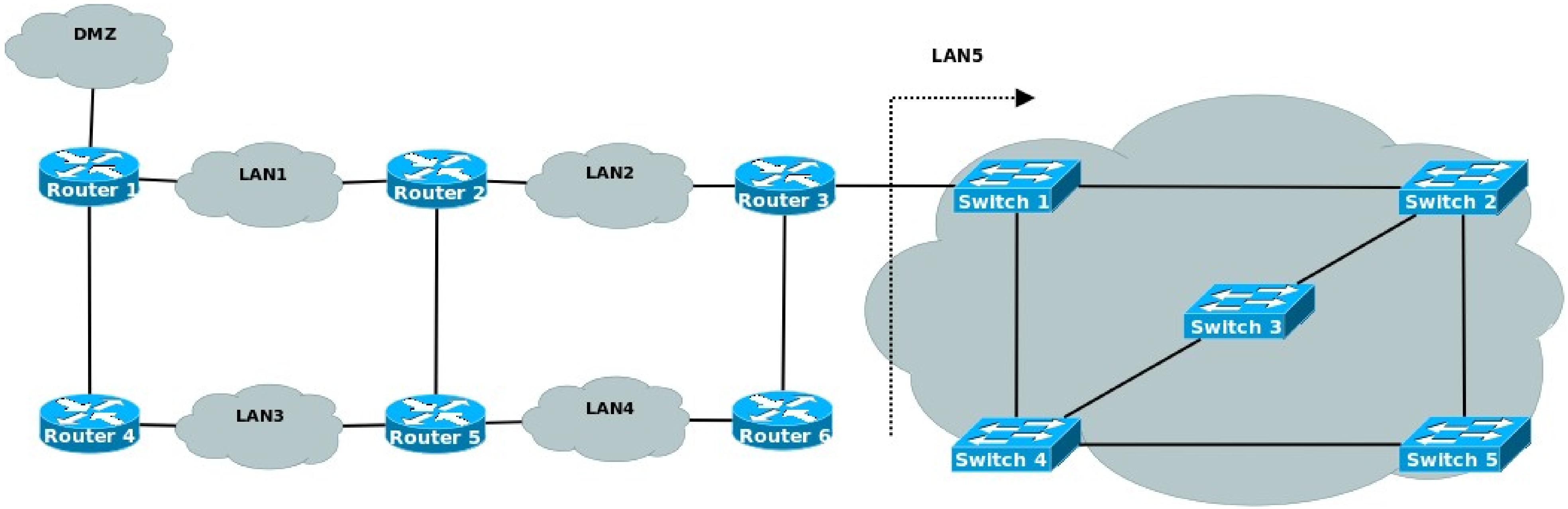
/28 -> 16 addresses

/29 -> 8 addresses

- 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.

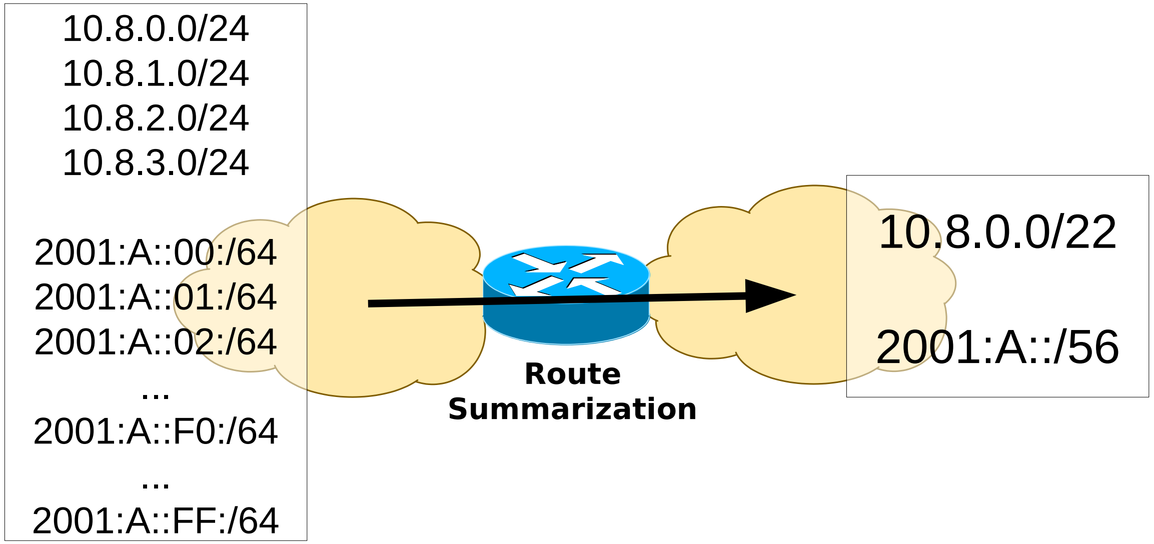
Example – IPv4 Private Planning (2)

- Easier approach is to start from /24 networks and perform sub-netting/aggregation as required.
- Point-to-point networks 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



IP Address Allocation (1)

- IP addresses allocation (blocks)
  - Separate VLANs for video, voice and data, and even user role-based
  - Data-center and DMZ
  - Network Address Translation (NAT/PAT)
  - Addressing for virtual private network (VPN) clients
  - Inner layer (point-to-point) links
  - Lookback addresses
- The same (V)LAN may/should have an IPv4 private network, IPv4 public network (if required), IPv6 global network, and IPv6 site-local network (optional).
- Allocate address blocks that allow route summarization (addresses aggregation) for “similar” (sub)networks
  - Important in scaling any routing protocol.
    - Simpler configurations, reduces routing tables (and routes databases) sizes, number/size of exchanged packets, faster convergence.
  - Efficient and easily managed address rules for quality of service (QoS) and security purposes.



10.8.0.0/24
10.8.1.0/24
10.8.2.0/24
10.8.3.0/24

2001:A::00:/64
2001:A::01:/64
2001:A::02:/64
...
2001:A::F0:/64
...
2001:A::FF:/64

10.8.0.0/22

2001:A::/56

IP Address Allocation (2)

- IPv4 private versus public address allocation
  - Reserve small public subnets for equipments/services that really need a public address
    - Router network interfaces with ISPs
      - Usually ISPs give/define extra addresses for this interfaces.
      - Company's (paid) IP addresses ranges used to everything else.
    - NAT/PAT
    - Video-conference terminals, public servers, etc...
  - For private addressing available addresses are not an issue (usually!)
    - A simple scheme that can be used to avoid binary arithmetic,
    - e.g., use network 10.0.0.0/8 → to cretate subnetworks 10.<aaaabbbb>.<ccccdddd>.0/24
    - aaaa bits: location encoding; bbbb bits: building/zone encoding; cccc bits: group encoding; dddd bits: service encoding.
- IPv6 address allocation
  - Available addresses are not an issue.
  - Usage of summarization must be considered.
    - e.g., for network 2001:A:A::/48 → 2001:A:A:<aaaabbbbccccdddd>:/64 subnetworks
    - Example for summarization per location first, and after by service: aaaa bits: location encoding; bbbb bits: service encoding; cccc bits: group encoding; dddd bits: building/zone encoding.
    - Example for sumarization per location first, and after by building/zone: aaaa bits: location encoding; bbbb bits: building/zone encoding; cccc bits: group encoding; dddd bits: service encoding.
- Point-to-point links and *loopback* interfaces
  - For IPv4 prefer to use
    - /30 prefixes for point-to-point links, /32 prefixes for *loopback* interfaces.
  - For IPv6 prefer to use
    - /126 prefixes for point-to-point links, /128 prefixes for *loopback* interfaces.