IPv4 & IPv6 Addressing

Arquitetura e Gestão de Redes

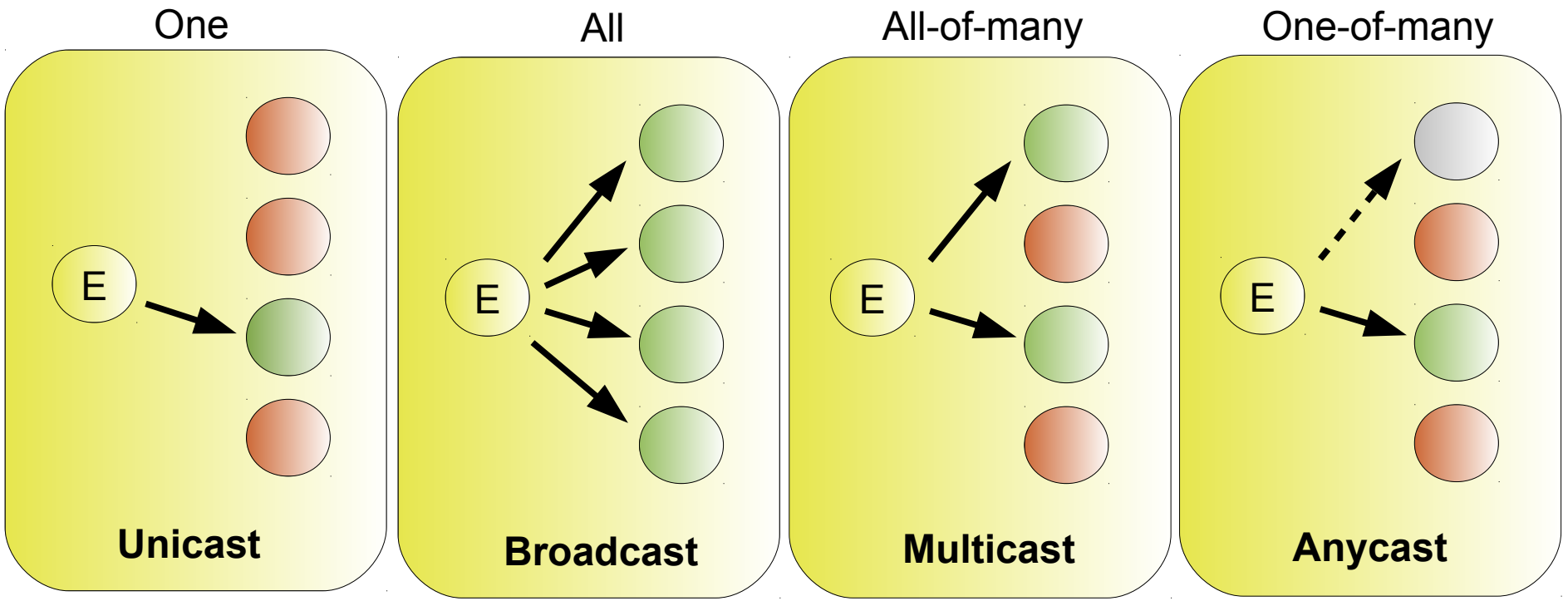
DETI-UA

universidade de aveiro

deti.ua.pt

Addressing Abstraction

- Types of addresses
  - Unicast – One receiver
  - Broadcast – All receivers
  - Multicast – All receivers of one group (all-of-many)
  - Anycast – One receiver of one group (one-of-many)



IPv4 Addressing, Subnetting and Summarization

IPv4 Addressing

- An IP address is a unique global 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 number**

Network prefix and host number

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

- How do we know how long the network prefix is?
  - **Before 1993:** The network prefix is implicitly defined (**class-based addressing**)

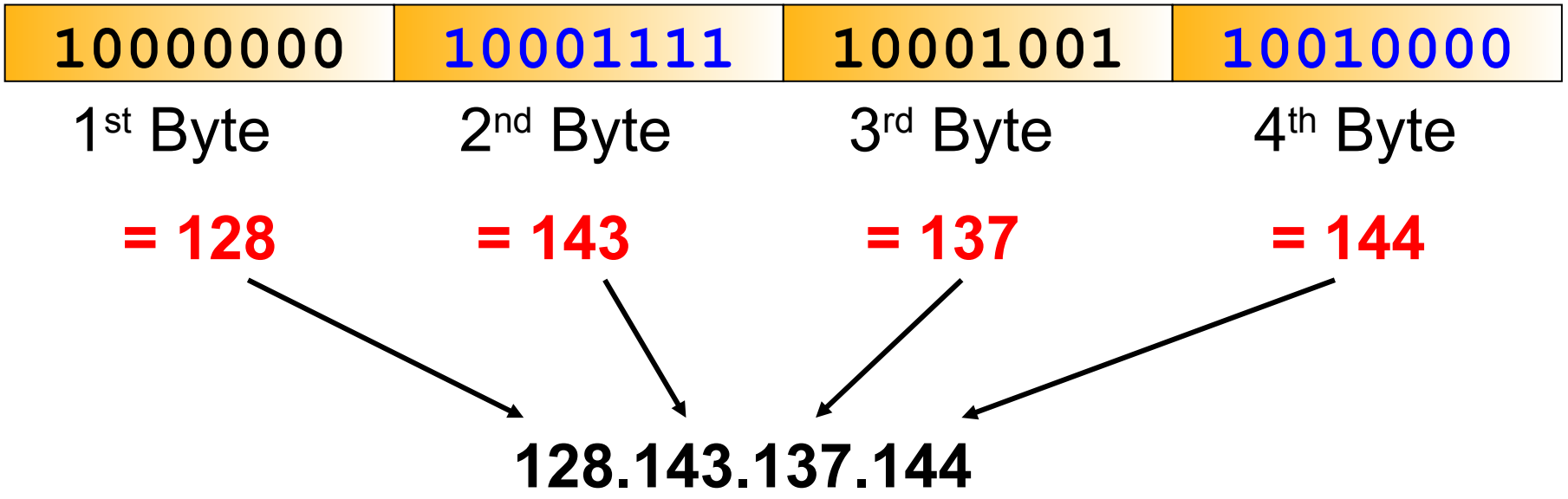
  or

  - **After 1993:** The network prefix is indicated by a **netmask.**

Dotted Decimal Notation

- IPv4 addresses are written in a so-called dotted **decimal notation**
- Each byte is identified by a decimal number in the range [0..255]:

- Example:



Classful IP Adresses (Until 1993)

- When Internet addresses were standardized (early 1980s), the Internet address space was divided up into classes:
  - **Class A:** Network prefix is 8 bits long
  - **Class B:** Network prefix is 16 bits long
  - **Class C:** Network prefix is 24 bits long

- Each IP address contained a key which identifies the class:
  - **Class A:** IP address starts with “0”
  - **Class B:** IP address starts with “10”
  - **Class C:** IP address starts with “110”

Problems with Classful IP Addresses

- By the early 1990s, the original classful address scheme had a number of problems
  - Flat address space. Routing tables on the backbone Internet need to have an entry for each network address. When Class C networks were widely used, this created a problem. By the 1993, the size of the routing tables started to outgrow the capacity of routers.

- Other problems:
  - Too few network addresses for large networks
    - Class A and Class B addresses were gone
  - Limited flexibility for network addresses:
    - Class A and B addresses are overkill
    - Class C address is insufficient

CIDR - Classless Interdomain Routing

- IP backbone routers have one routing table entry for each network address:
  - With subnetting, a backbone router only needs to know one entry for each Class A, B, or C networks
  - This is acceptable for Class A and Class B networks
    - 2^7 = 128 Class A networks
    - 2^{14} = 16,384 Class B networks
  - But this is not acceptable for Class C networks
    - 2^{21} = 2,097,152 Class C networks
- In 1993, the size of the routing tables started to outgrow the capacity of routers
- Consequence: The Class-based assignment of IP addresses had to be abandoned

CIDR - Classless Interdomain Routing

- Goals:
  - New interpretation of the IP address space
  - Restructure IP address assignments to increase efficiency
  - Permits route aggregation to minimize route table entries
  -
- CIDR (Classless Interdomain routing)
  - Abandons the notion of classes
  - Key Concept: The length of the network prefix in the IP addresses is kept arbitrary
  - Consequence: Size of the network prefix must be provided with an IP address

CIDR Notation

- CIDR notation of an IP address:
  - 192.0.2.0/18
    - "18" is the prefix length. It states that the first 18 bits are the network prefix of the address (and 14 bits are available for specific host addresses)
    -
- CIDR notation can replace the use of subnetmasks (but is more general)
  - IP address 128.143.137.144 and subnetmask 255.255.255.0 becomes 128.143.137.144/24
- CIDR notation allows to drop trailing zeros of network addresses:
  - 192.0.2.0/18 can be written as 192.0.2/18

CIDR address blocks

- CIDR notation can nicely express blocks of addresses
- Blocks are used when allocating IP addresses for a company and for routing tables (route aggregation)
- # useable Addresses = # of Host Addresses – 2 Addresses
  - Network Identifier address + Network broadcast address

CIDR Block Prefix	# of Host Addresses	# useable 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 Block Prefix	# of Host Addresses	# useable Addresses
30	4	2
29	8	6
29	16	14
27	32	30
26	64	62
25	128	126
24	256	254
23	512	510
22	1024	1022

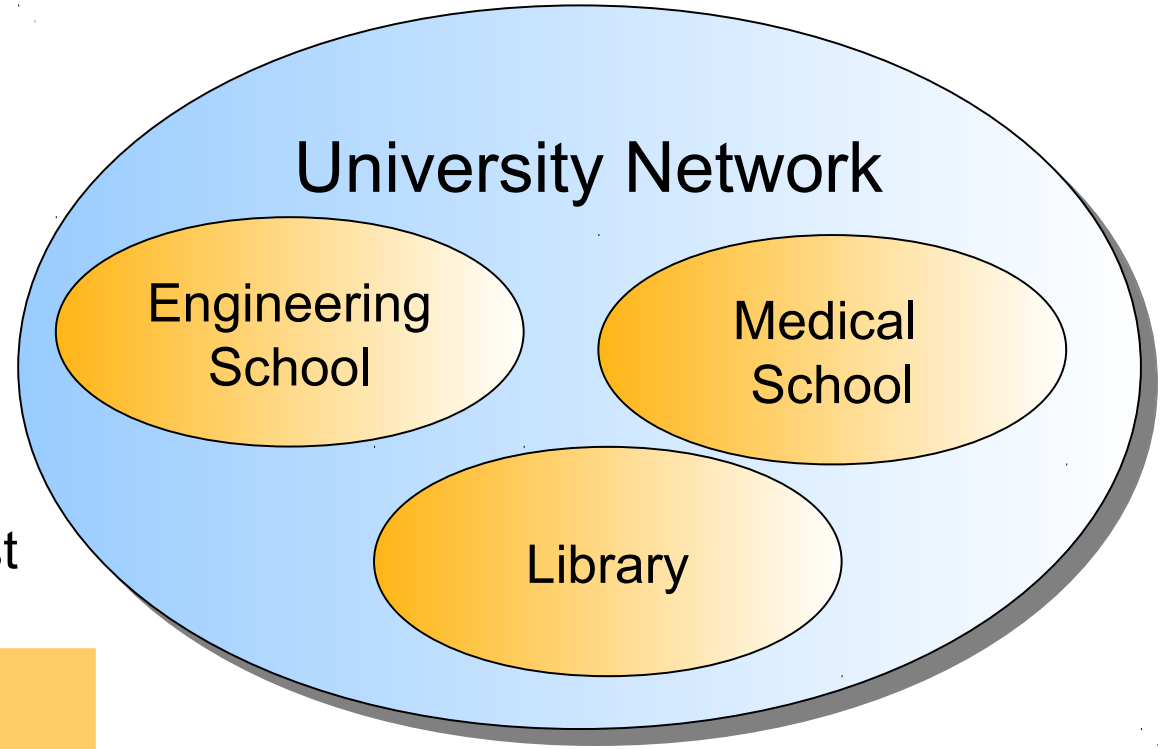
CIDR vs. (Sub)Netmask

CIDR Block Prefix	(Sub)Netmask
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 Block Prefix	(Sub)Netmask
30	255.255.255.252
29	255.255.255.248
29	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

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.

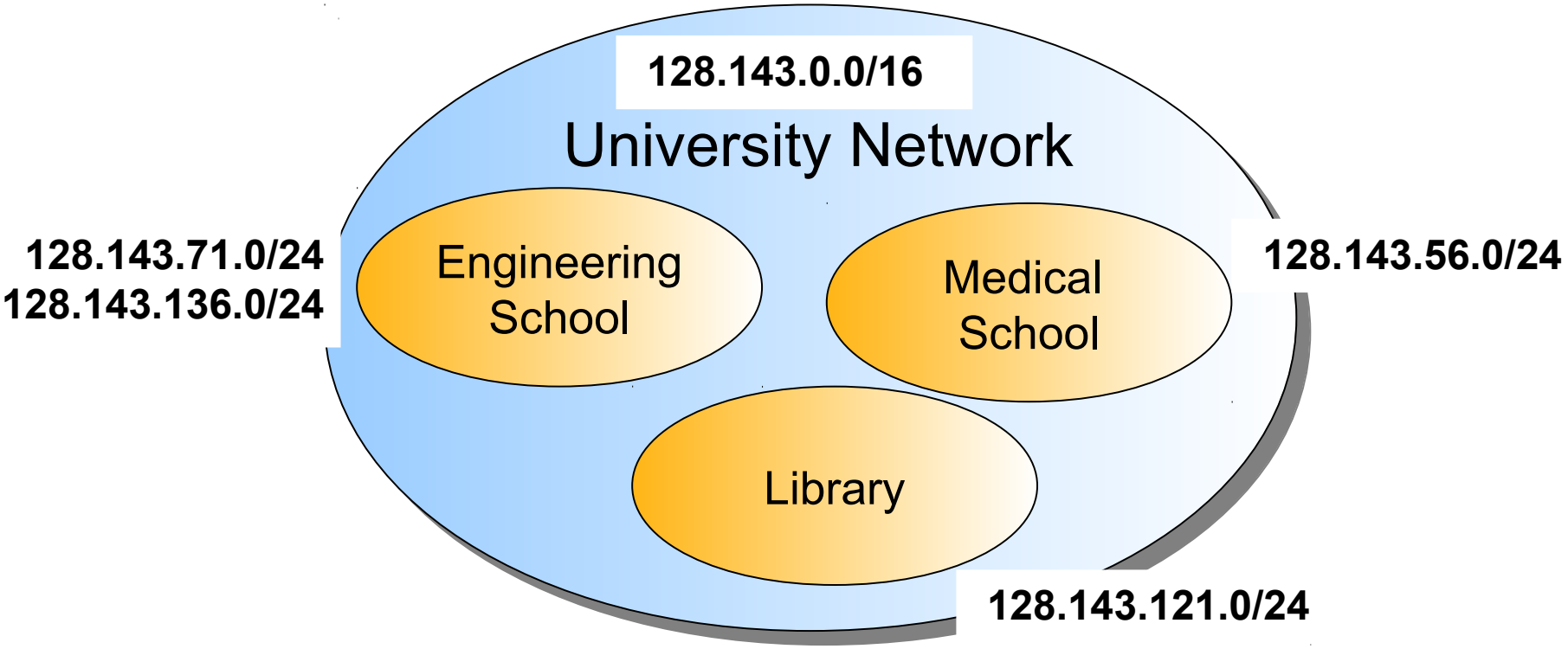


- **Solution 2:** Add another level of hierarchy to the IP addressing structure

Subnetting

Address assignment with subnetting

- Each part of the organization is allocated a range of IP addresses (subnetwork)
- Addresses in each subnet can be administered locally

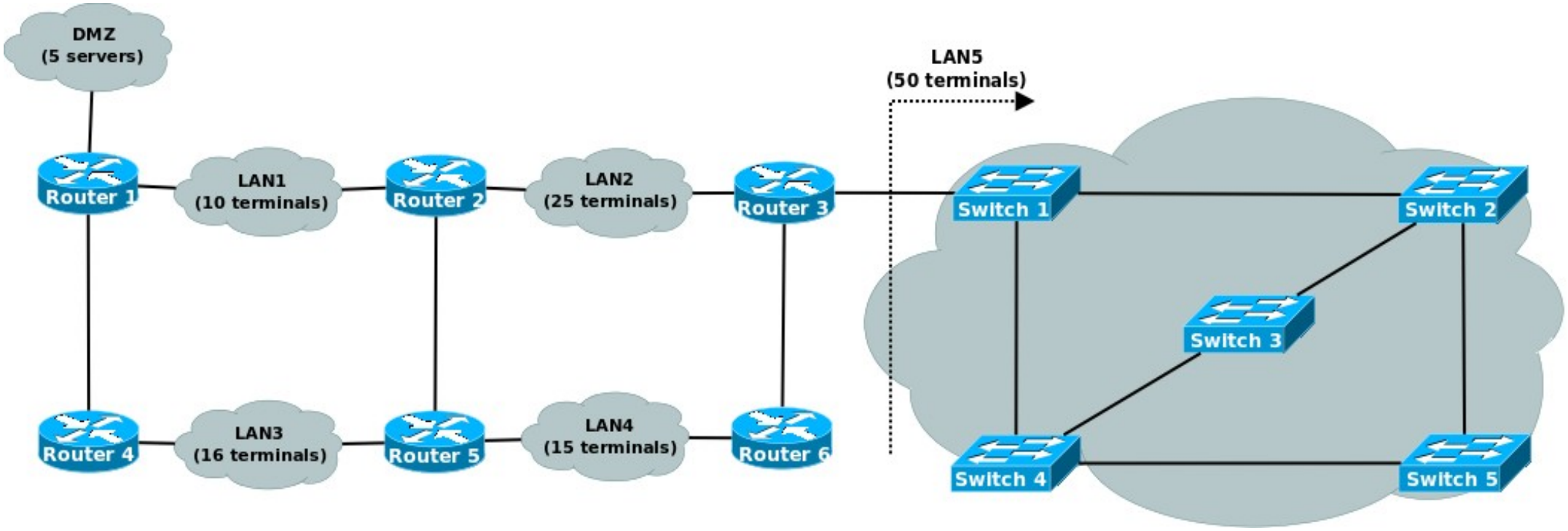


Advantages of Subnetting

- 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

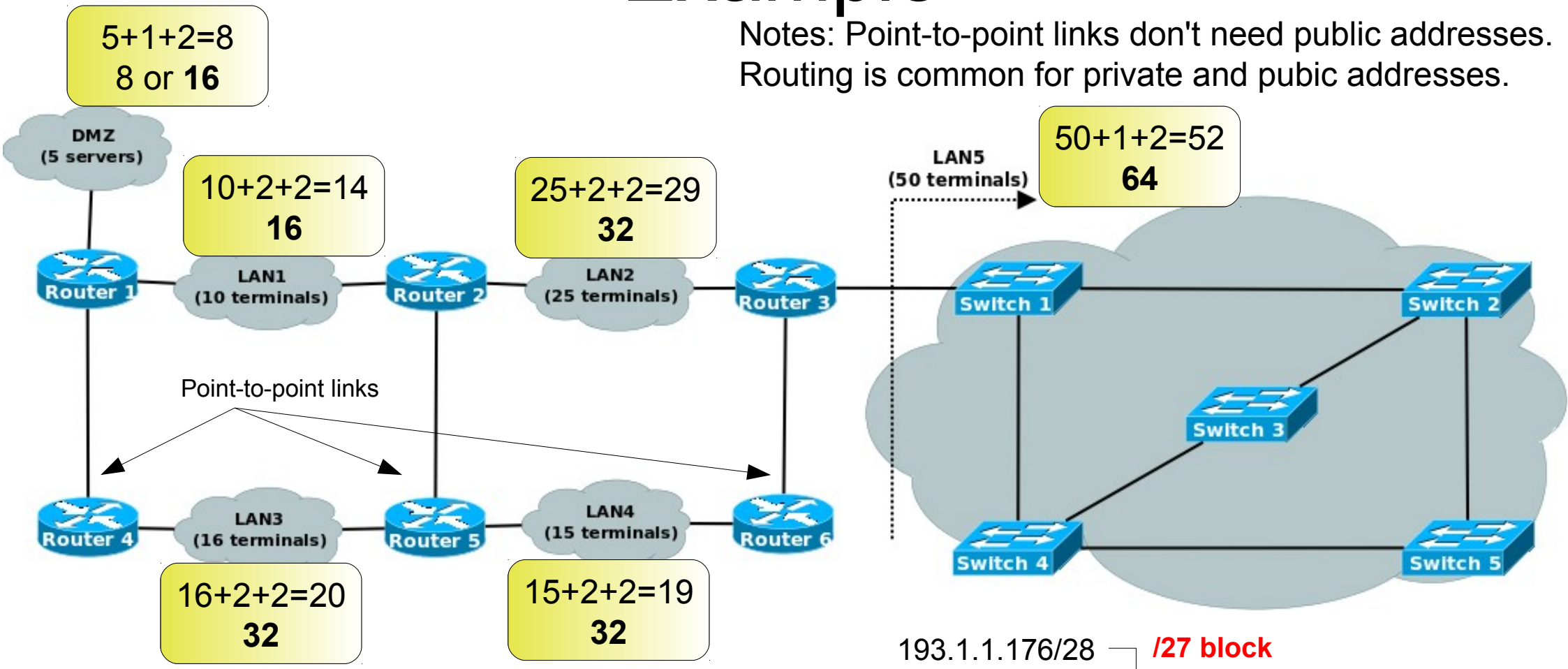
- Usually private network subnetting is not necessary!
- Common problem: small ranges of public addresses necessary in multiple (V)LANs.

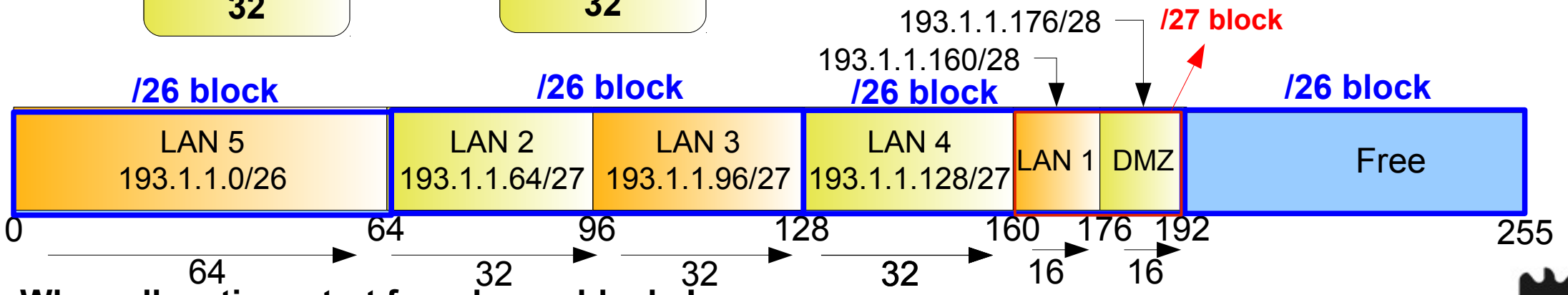


193.1.1.0/24

Example

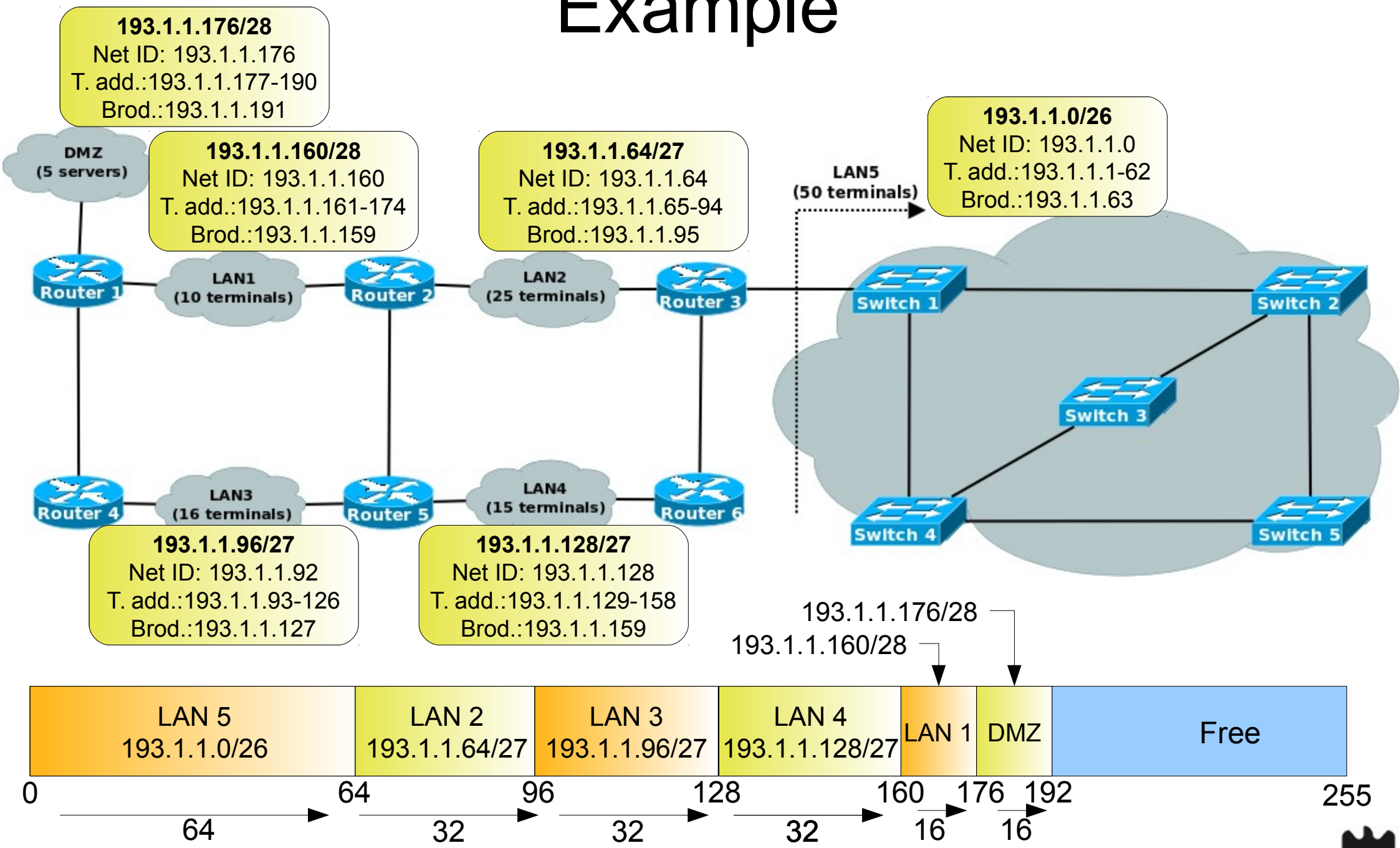
Notes: Point-to-point links don't need public addresses.
Routing is common for private and pubic addresses.





When allocating, start from larger blocks!

Example

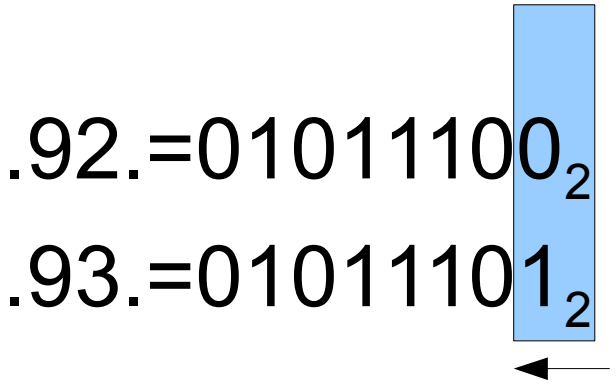


universidade de aveiro

IPv4 (Route) Summarization

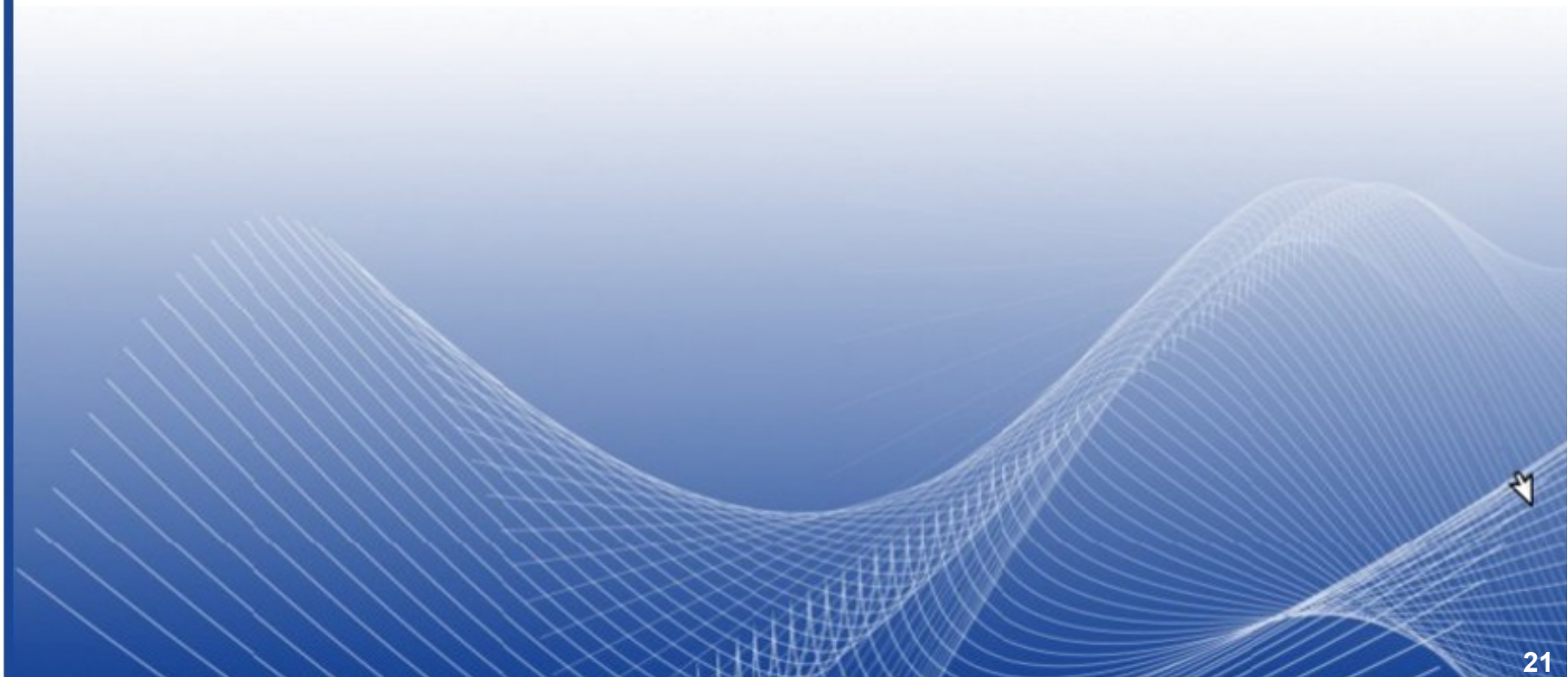
- Inverse process of sub-netting.
- Used to create a network identifier that merges “many” IP (sub)networks.
- Used for public and private IPv4 networks.
- Example:

193.136.92.0/24 + 193.136.93.0/24



=> 193.136.92.0/**23**

IP-IP Tunnels
&
Loopback/Logical interfaces



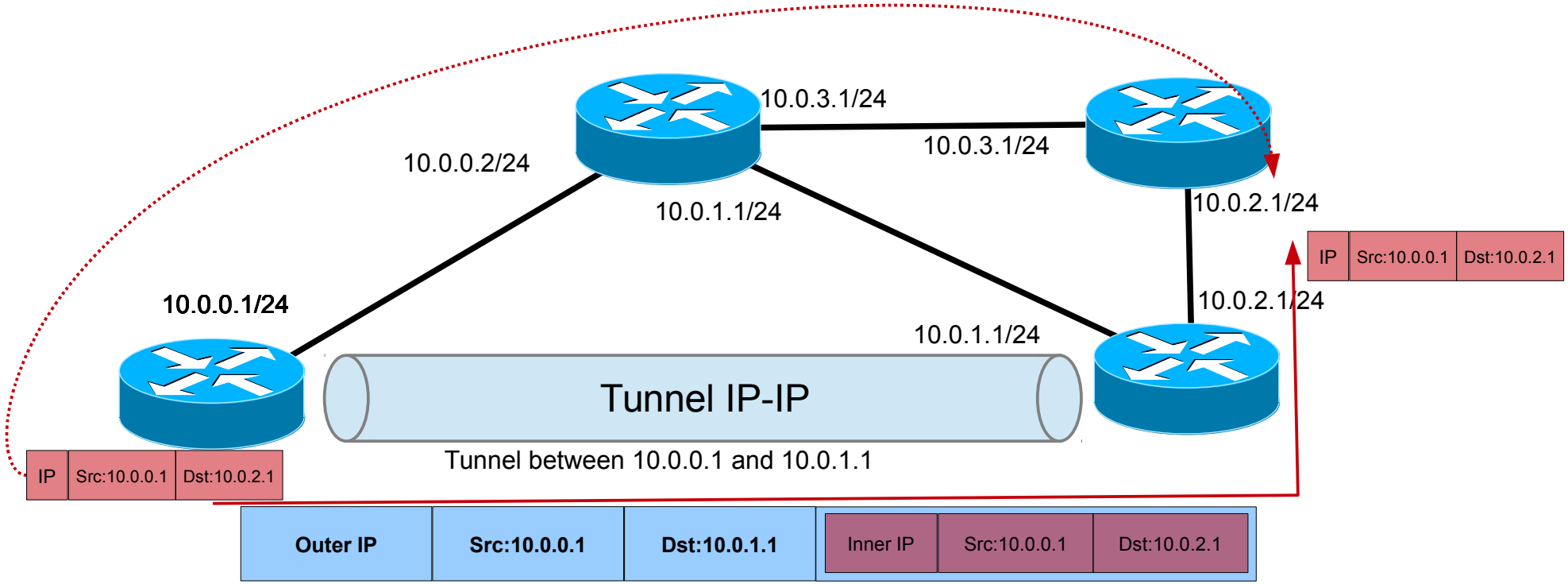
IP-IP tunnels (1)

- IP-IP is: one IP packet encapsulated inside another IP packet.
- An IP-IP tunnel is configured between two end-points.
  - Adds an additional header with source/destination equal to the end-points addresses.
  - Defines a Virtual “1-hop” link between two remote nodes.
- Tunnel types:
  - IP-IP

  - IP-GRE-IP
    - The main advantage of using Generic Routing Encapsulation (GRE) instead of IP-IP is that it supports IP multicast packets.

IP-IP tunnels (2)

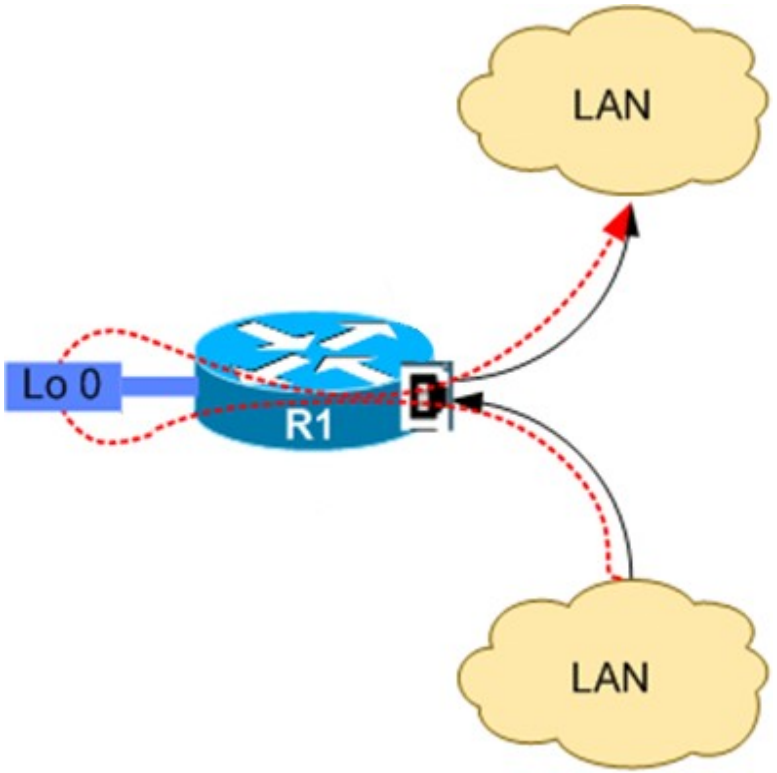
- Allows the routing of traffic via a specific node, independently of the underlying routing protocols.



- May have associated Security/QoS features.
  - E.g., IPsec, MPLS, ...

Loopback/Logical Interfaces

- Loopback/Logical interface is a Virtual interface which is always up (while the router is up).
- Allows to make router-to-router connections independently of physical interfaces.
  - Ideal for Tunnel end-points
  - Point-to-point neighbor relations (e.g., BGP routing protocol).
- Also used as “base identifier” in several network mechanisms.
- Configured as any other layer 3 interface.



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

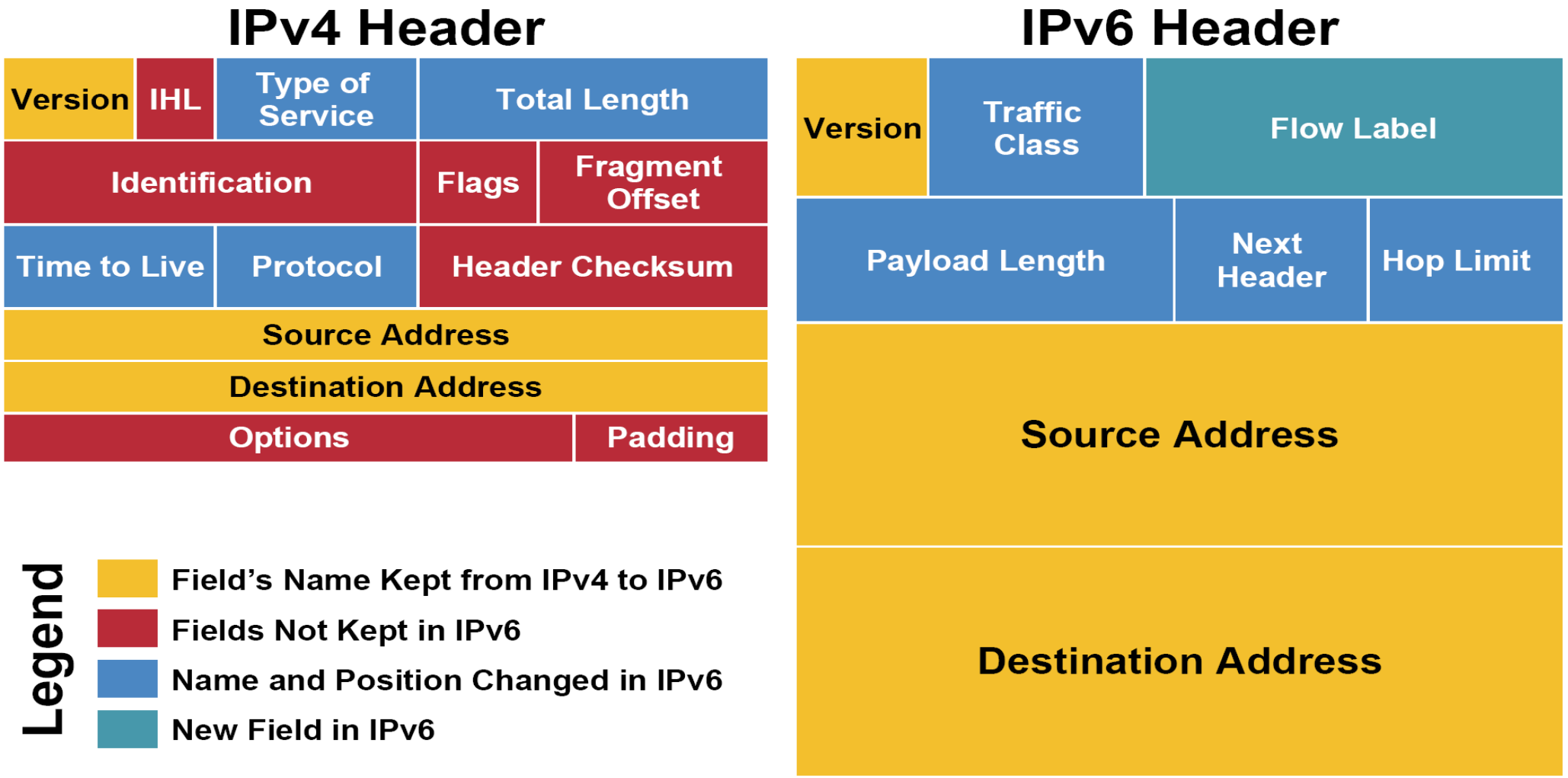
IPv6 Features

- 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

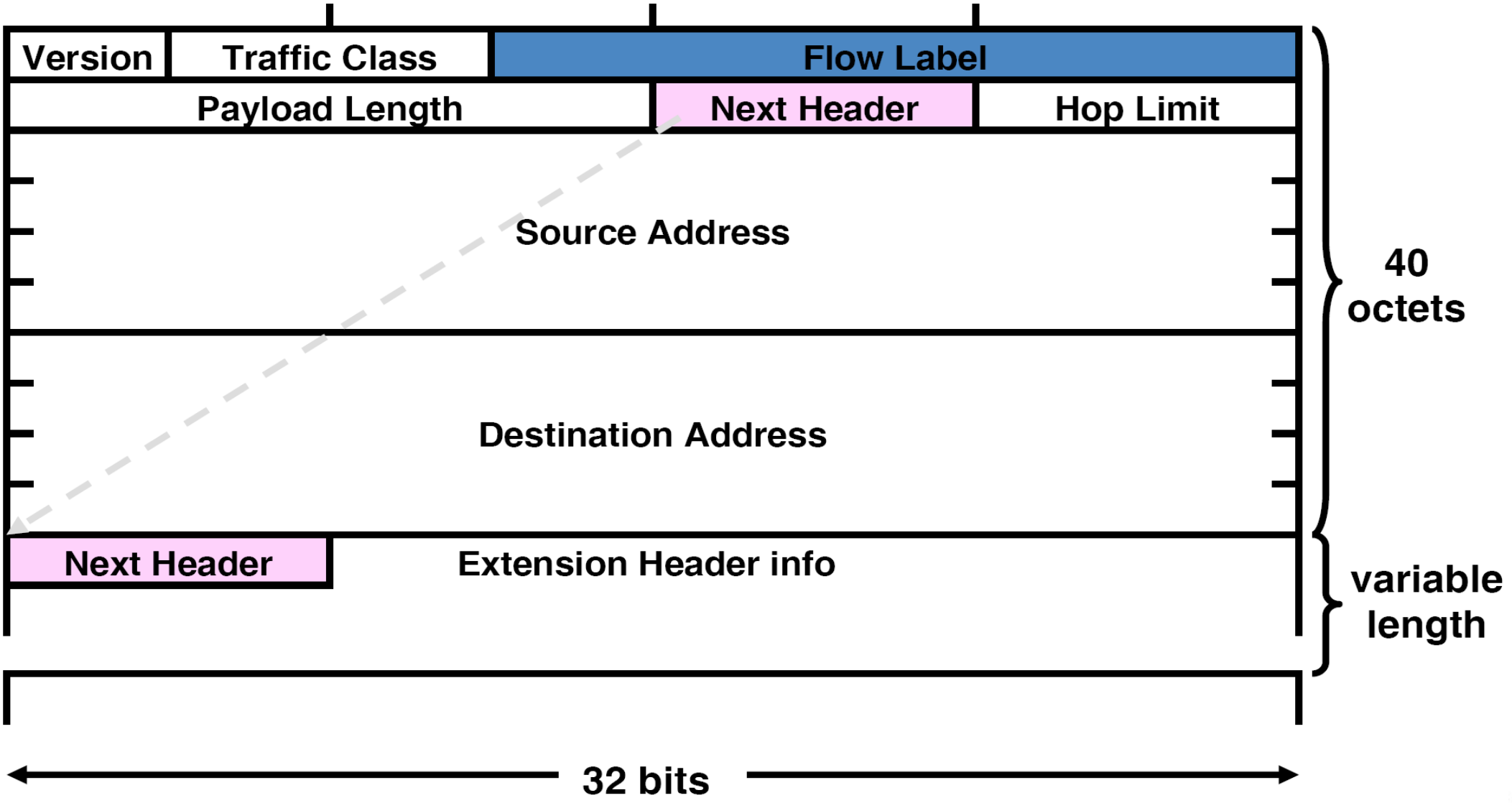
IPv6 Addressing

- 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

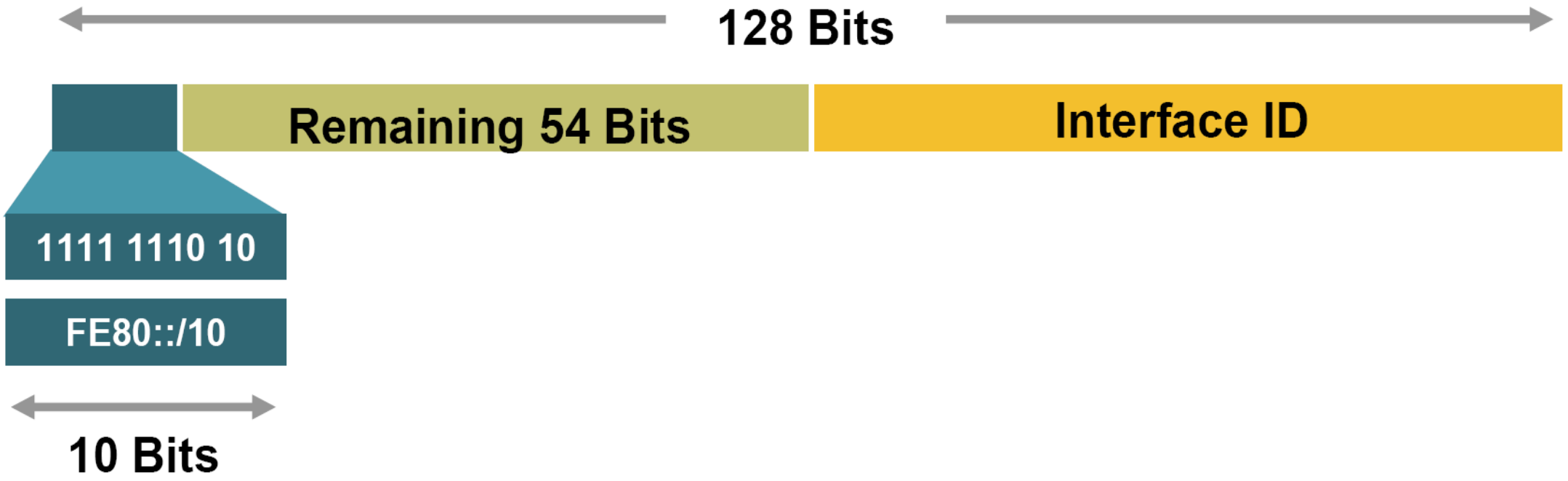
Types of IPv6 Addresses

- 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

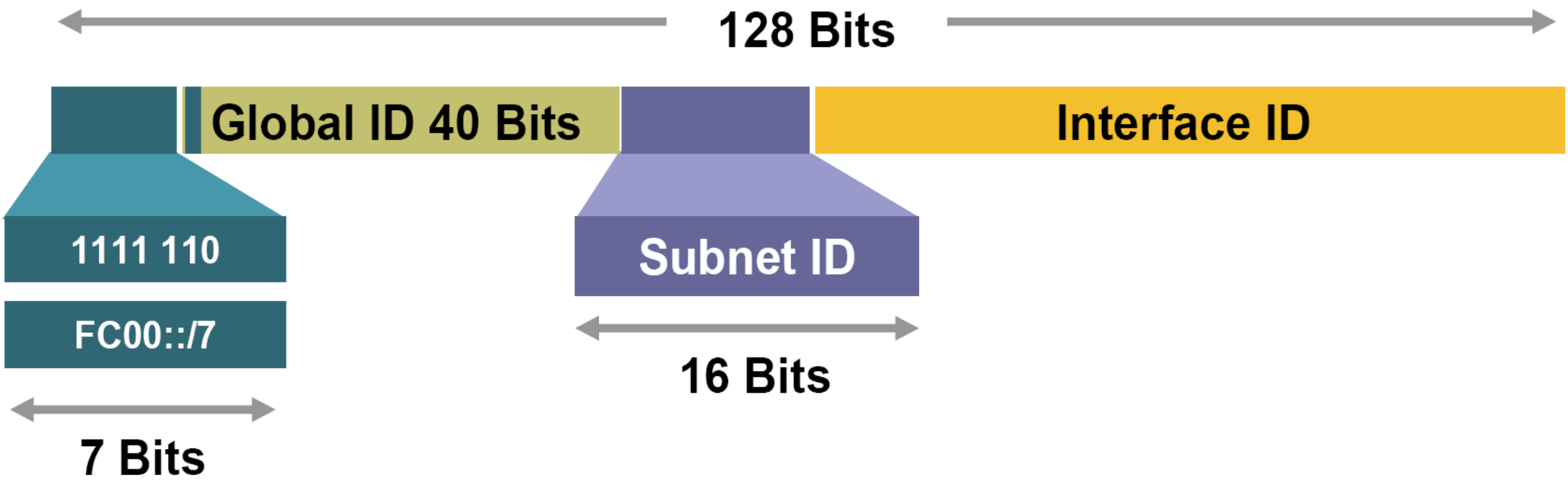
Type	Binary	Hexadecimal
Global Unicast Address	0010	2
Link-Local Unicast Address	1111 1110 10	FE80::/10
Unique-Local Unicast Address	1111 1100 1111 1101	FC00::/8 FD00::/8
Multicast Address	1111 1111	FF00::/16

Link-Local Address



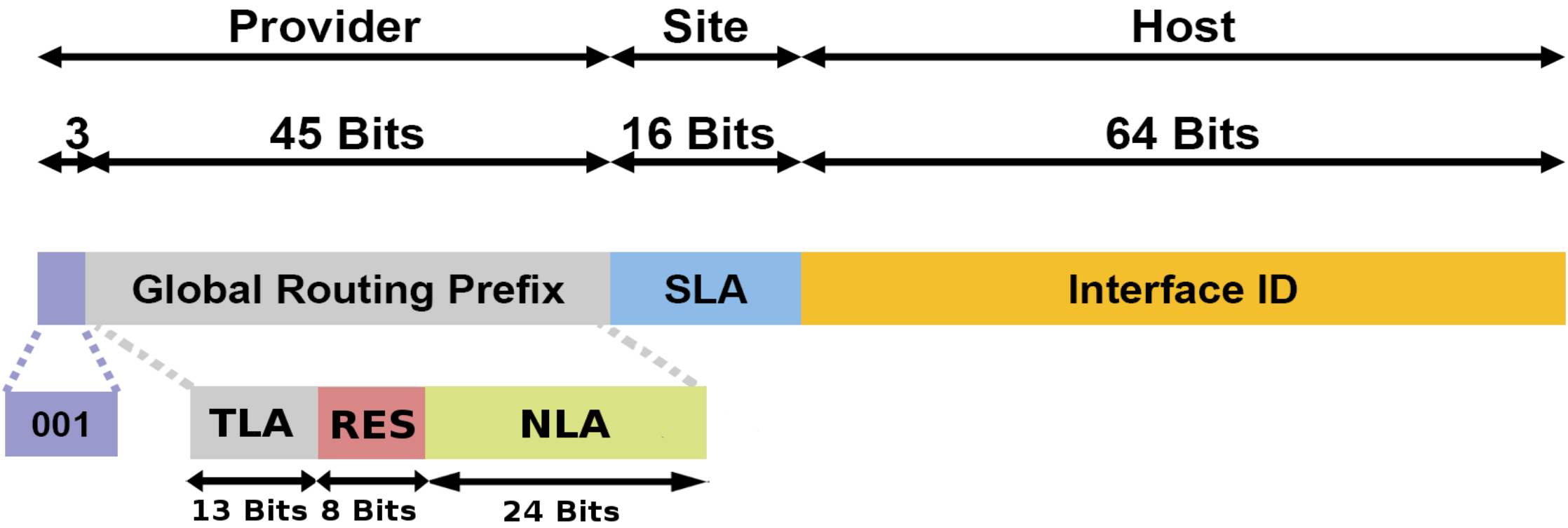
- Used For:
  - Mandatory address for local communication between two IPv6 devices
  - Next-Hop calculation in Routing Protocols
- Automatically assigned as soon as IPv6 is enabled
- Remaining 54 bits could be Zero or any manual configured value

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



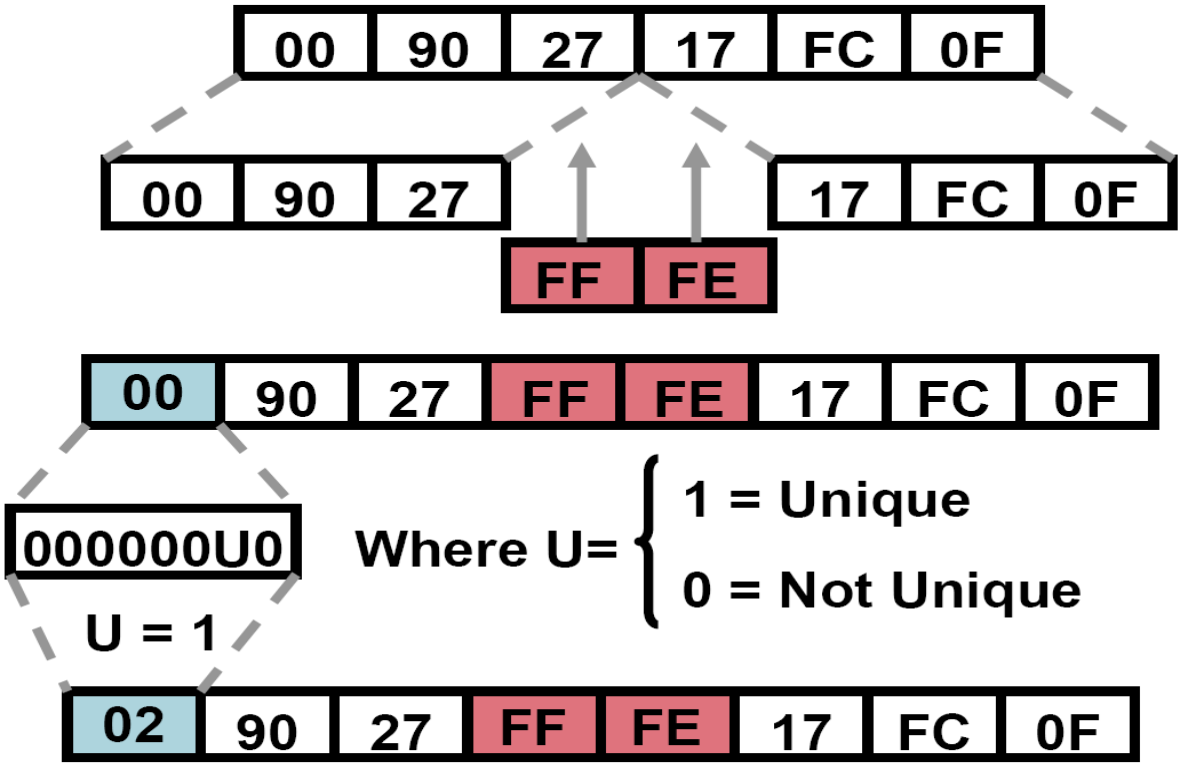
- LA, NLA and SLA used for hierarchical addressing
  - TLA - Top-Level Aggregation
  - RES – Reserved (must be zero)
  - NLA - Next-Level Aggregation Identifier
  - SLA - Site-Level Aggregation Identifier

IPv6 Interface Identifier

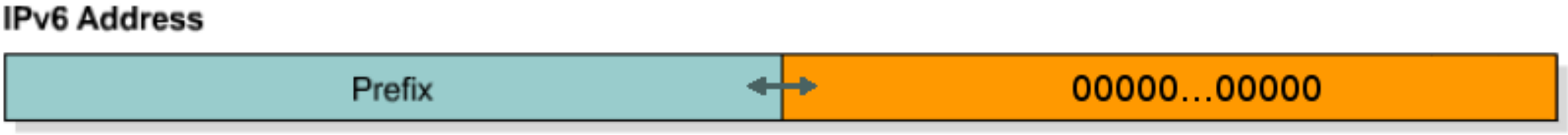
- Lowest-Order 64-Bit field of any address:
  - Auto-configured from a 64-bit EUI-64, or expanded from a 48-bit MAC address (e.g. Ethernet address)
  - Auto-generated pseudo-random number
  - Assigned via DHCP
  - Manually configured

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

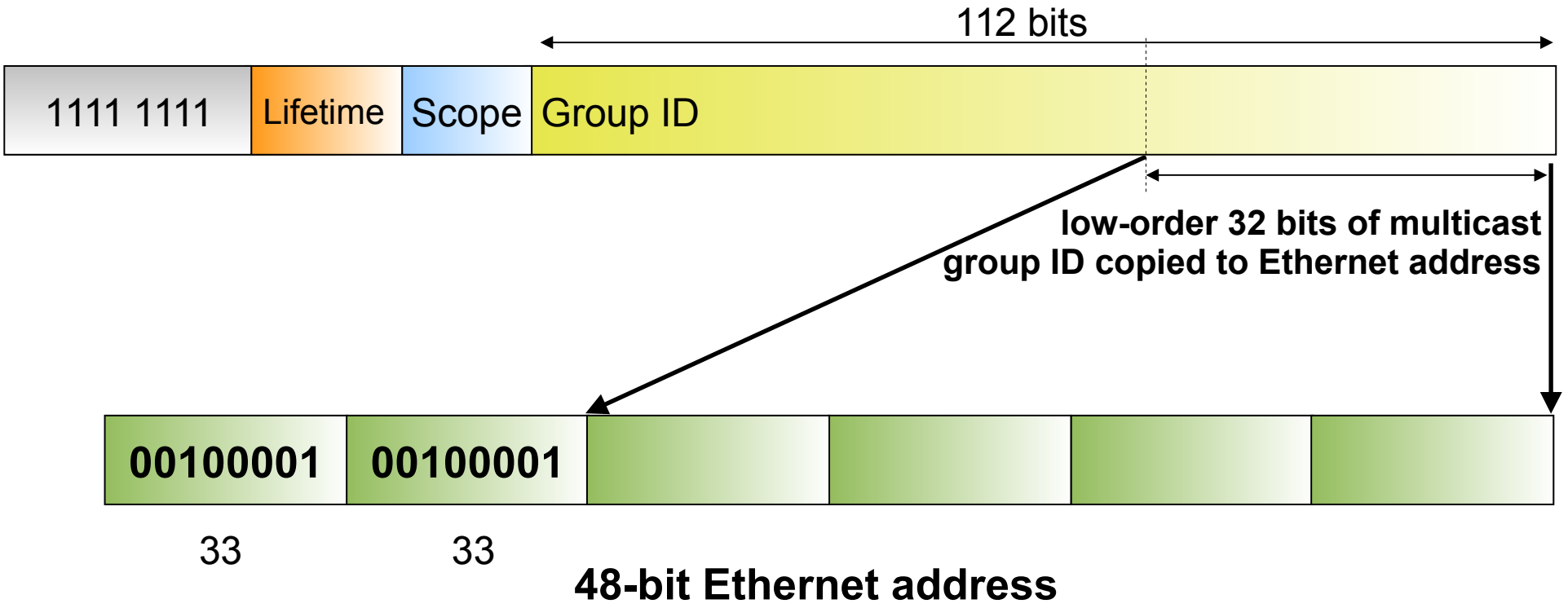
8-bit	4-bit	4-bit	112-bit
1111 1111	Lifetime	Scope	Group-ID

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.

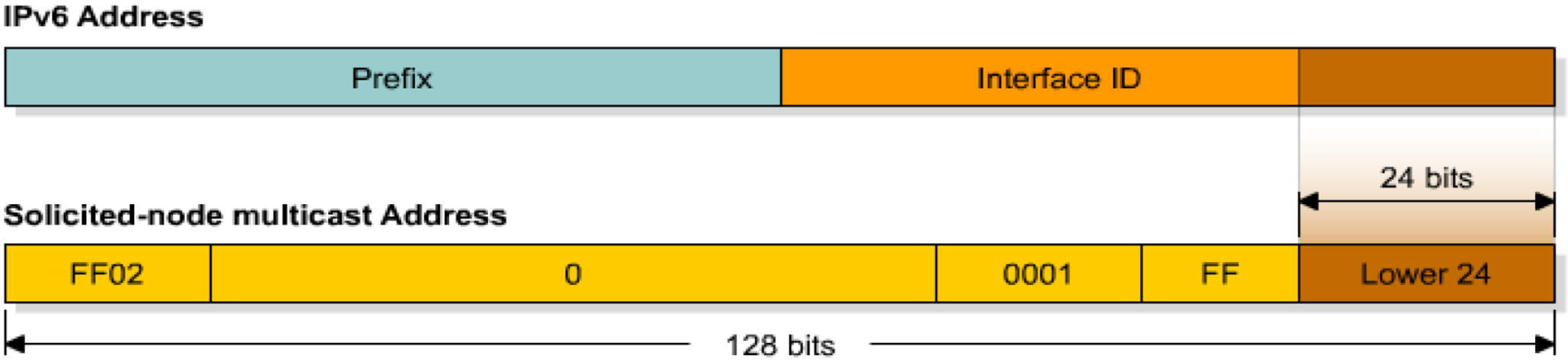
Mapping a IPv6 Multicast Address to Ethernet Address



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

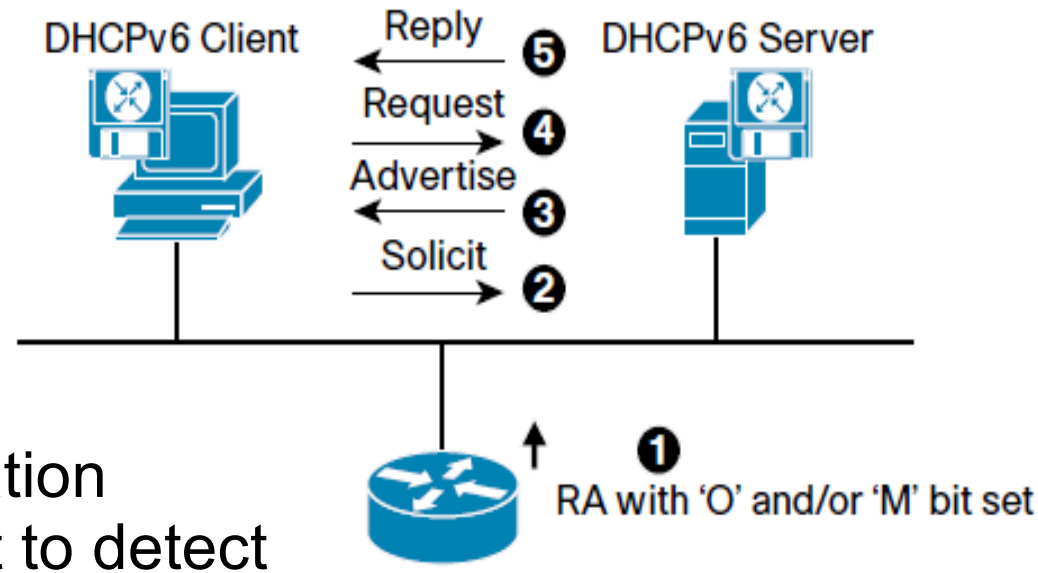
- Redirect is used by a router to signal the reroute of a packet to a better router

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



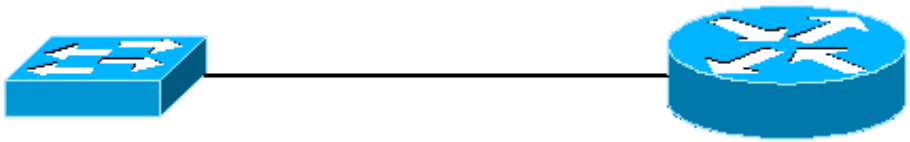
- Basic DHCPv6 concept is similar to DHCP for IPv4.
- If a client wishes to receive configuration parameters, it will send out a request to detect available DHCPv6 servers.
  - This done through the "Solicit" and "Advertise" messages.
  - Well known DHCPv6 Multicast addresses are used for this process.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



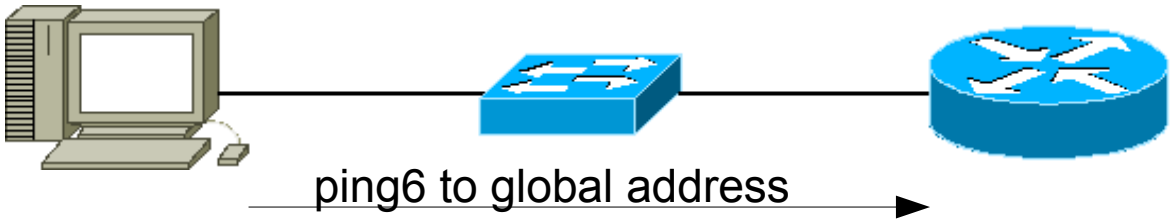
Multicast (all MLDv2-capable routers) ff02::16	**MLDv2 Report Message** (Multicast all routers)	**Null address ::**
Multicast (all MLDv2-capable routers) ff02::16	**MLDv2 Report Message** (Multicast solicited-node address)	**Null address ::**
Multicast solicited-node address ff02::1:ff+(address's last 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**→ **Multicast solicited-node address**
(Target's IPv6 address) **ff02::1:ff+(address's last 24 bits)**

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

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

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

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

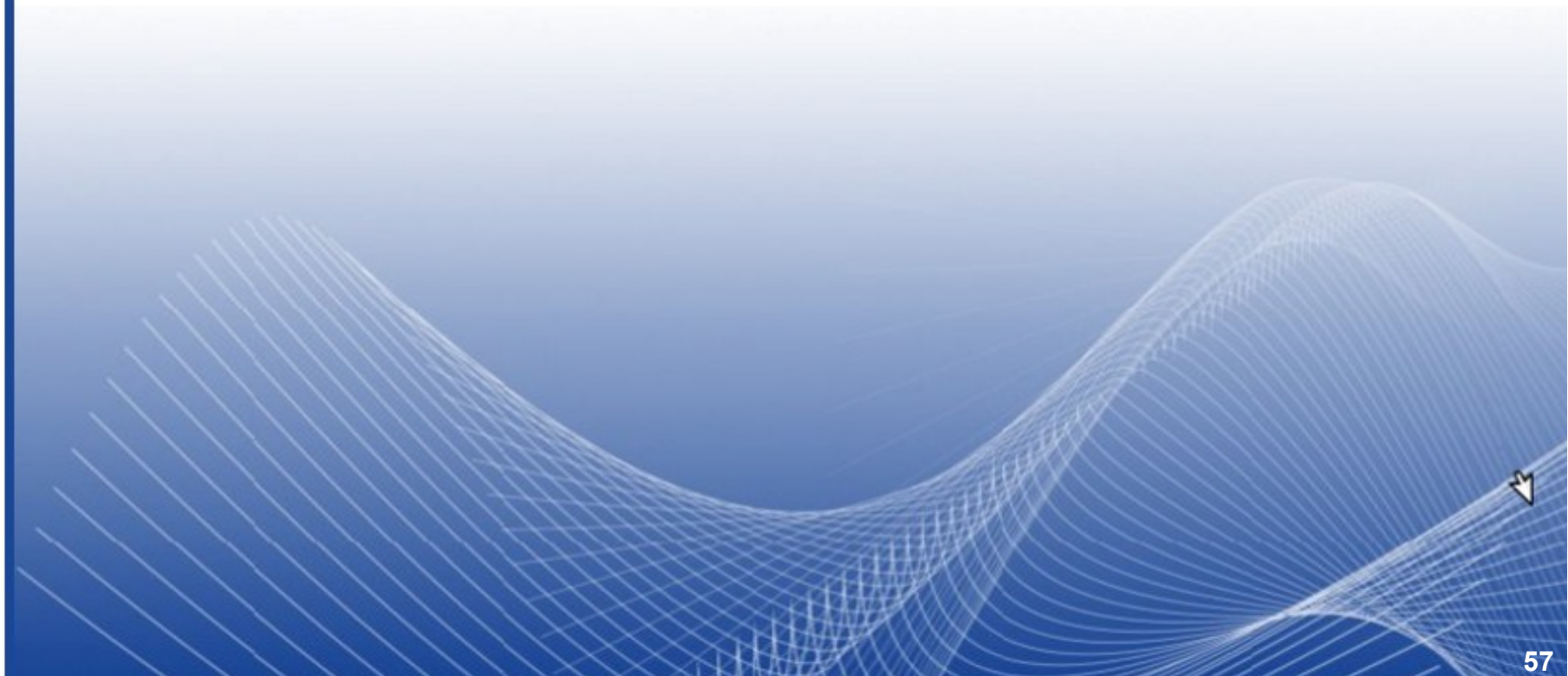
Global/link-local address ←— **Global/link-local address**

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

IP Addresses Allocation Planning



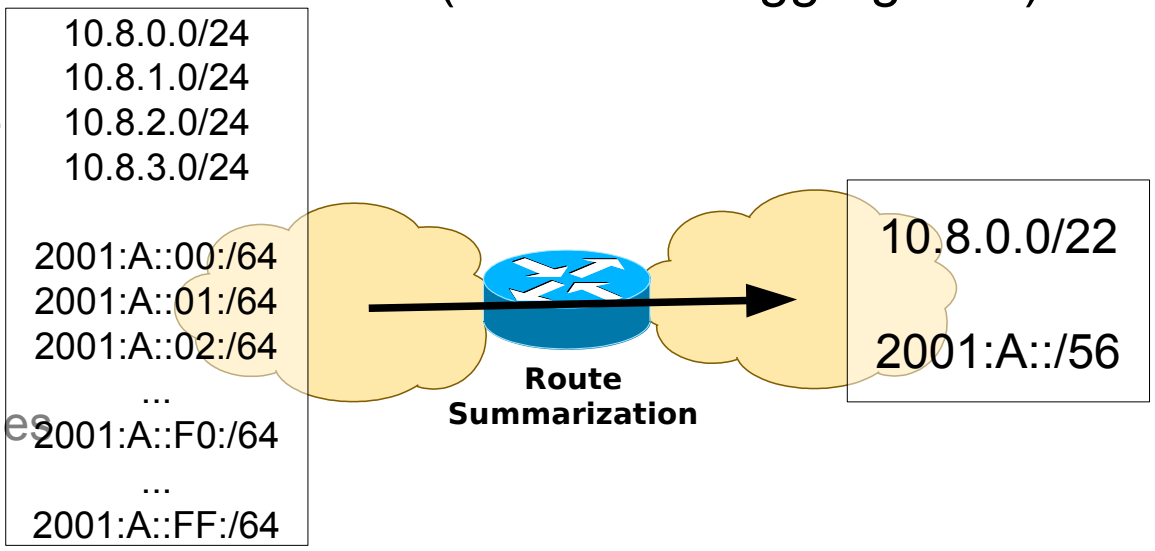
Physical vs. Logical Networks

- 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.

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

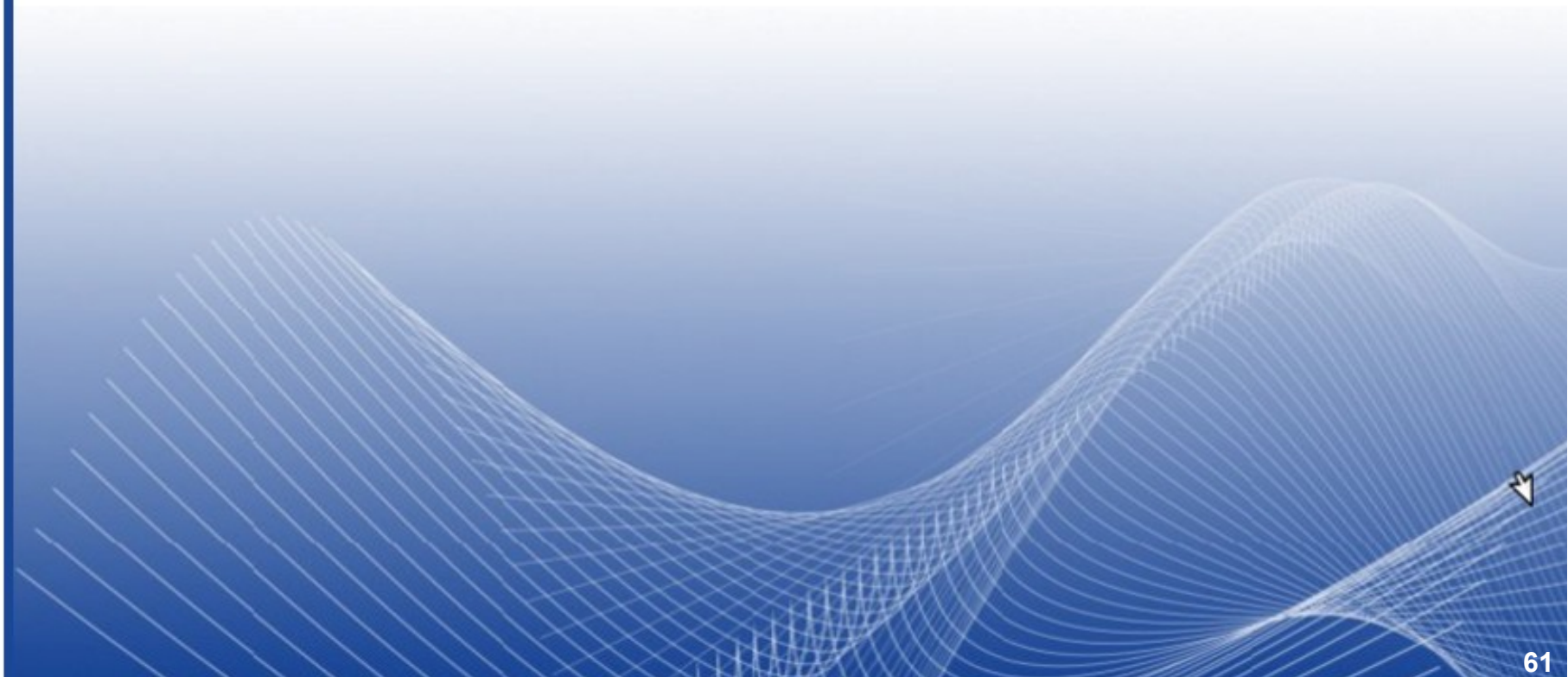
- Allocate address blocks that allow route summarization (addresses aggregation) for “similar” (sub)networks
  - Important in scaling any routing protocol.
    - Simpler configurations, reduces routing tables (and routes databases) sizes, number/size of exchanged packets, faster convergence.
  - Efficient and easily managed address rules for quality of service (QoS) and security purposes.



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:
    - Use network 10.0.0.0/8
      - 2nd byte for rack/switch number, 3rd byte for VLANs, and the 4th byte for hosts.
      - 10.rack_number.VLAN.host /24
- IPv6 address allocation
  - Available addresses are not an issue.
  - Usage of summarization must be considered.
- 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.

IPv4/IPv6 Transition Mechanisms



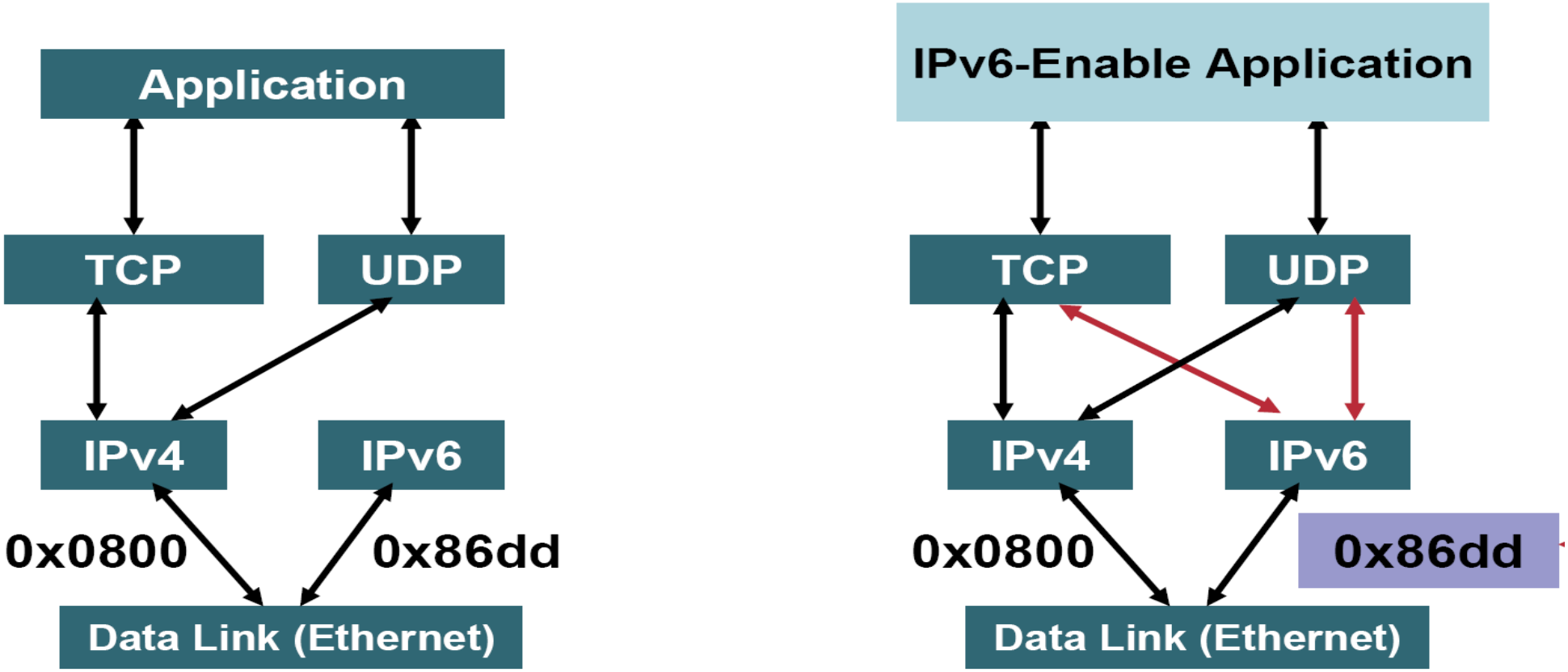
IPv6 Deployment Techniques (1)

- Deploying IPv6 using dual-stack backbones
  - IPv4 and IPv6 applications coexist in a dual IP layer routing backbone
  - All routers in the network need to be upgraded to be dual-stack
- IPv6 over IPv4 tunnels
  - Manually configured
  - Generic routing encapsulation (GRE)
  - Semiautomatic tunnel mechanisms
  - Fully automatic tunnel mechanisms (IPv4-compatible and 6to4)

IPv6 Deployment Techniques (2)

- Translation Mechanisms
  - Network Address Translation-Protocol Translation (NAT-PT)
  - TCP-UDP Relay
  - Bump-in-the-Stack (BIS)
  - SOCKS-Based Gateway
  - ...
- Deploying IPv6 over dedicated data links
  - Using the same Layer 2 infrastructure as for IPv4
  - Using separate Frame Relay or ATM PVCs, separate optical links, or Wave Division Multiplexing (WDM)
- Deploying IPv6 over MPLS backbones

Dual Stack



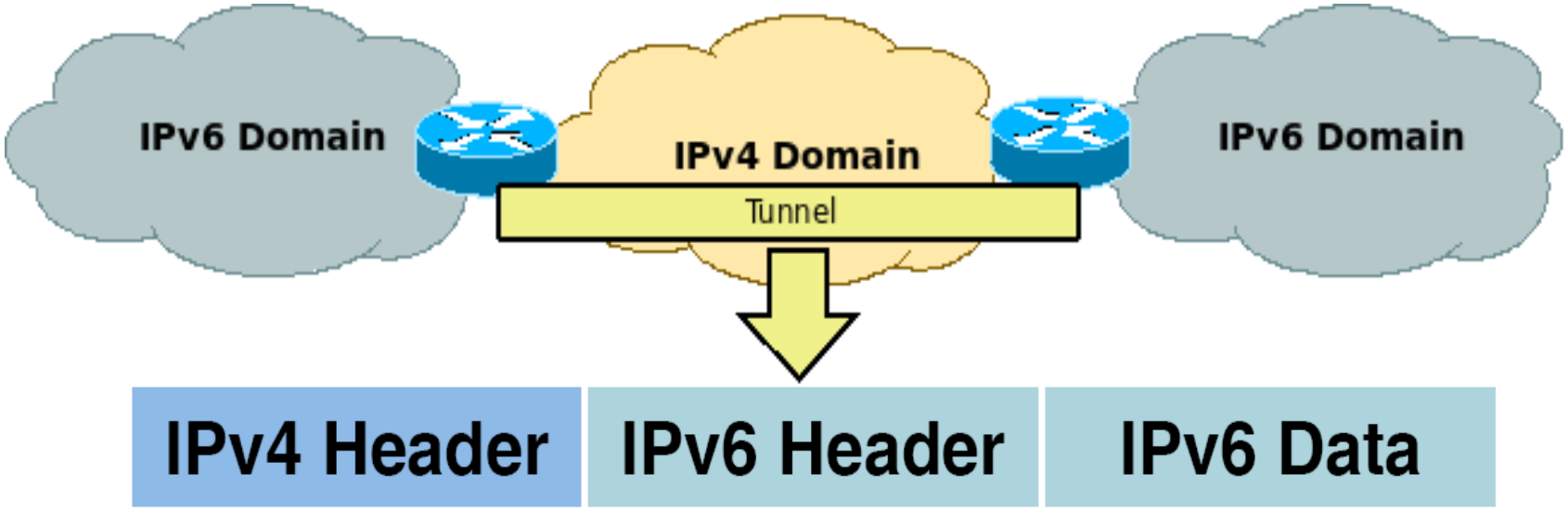
- Applications may talk to both
- Choice of the IP version is based on DNS responses and application preferences

Overlay Tunneling

- Manual
  - IPv6 Manually Configured IPv6 over IPv4
  - IPv6 over IPv4 GRE Tunnel
- Semi-automatic mechanisms
  - Tunnel Broker
  - Teredo
  - Dual Stack Transition Mechanism (DSTM)
- Automatic mechanisms
  - Automatic IPv4 Compatible Tunnel (deprecated)
  - 6to4 Tunnel
  - ISATAP Tunnels

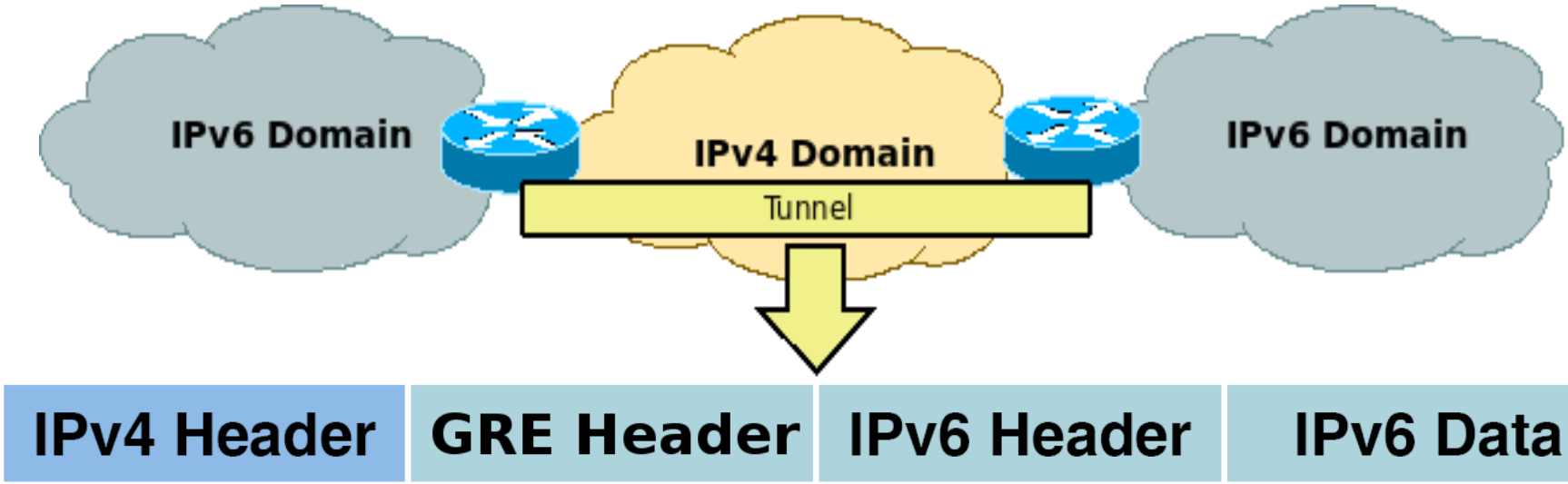
IPv6 Manually Configured

- Permanent link between two IPv6 domains over an IPv4 backbone
- Primary use is for stable connections that require regular secure communication between
  - Two edge routers, end system and an edge router, or for connection to remote IPv6 networks
- Tunnel between two points
- Complex management



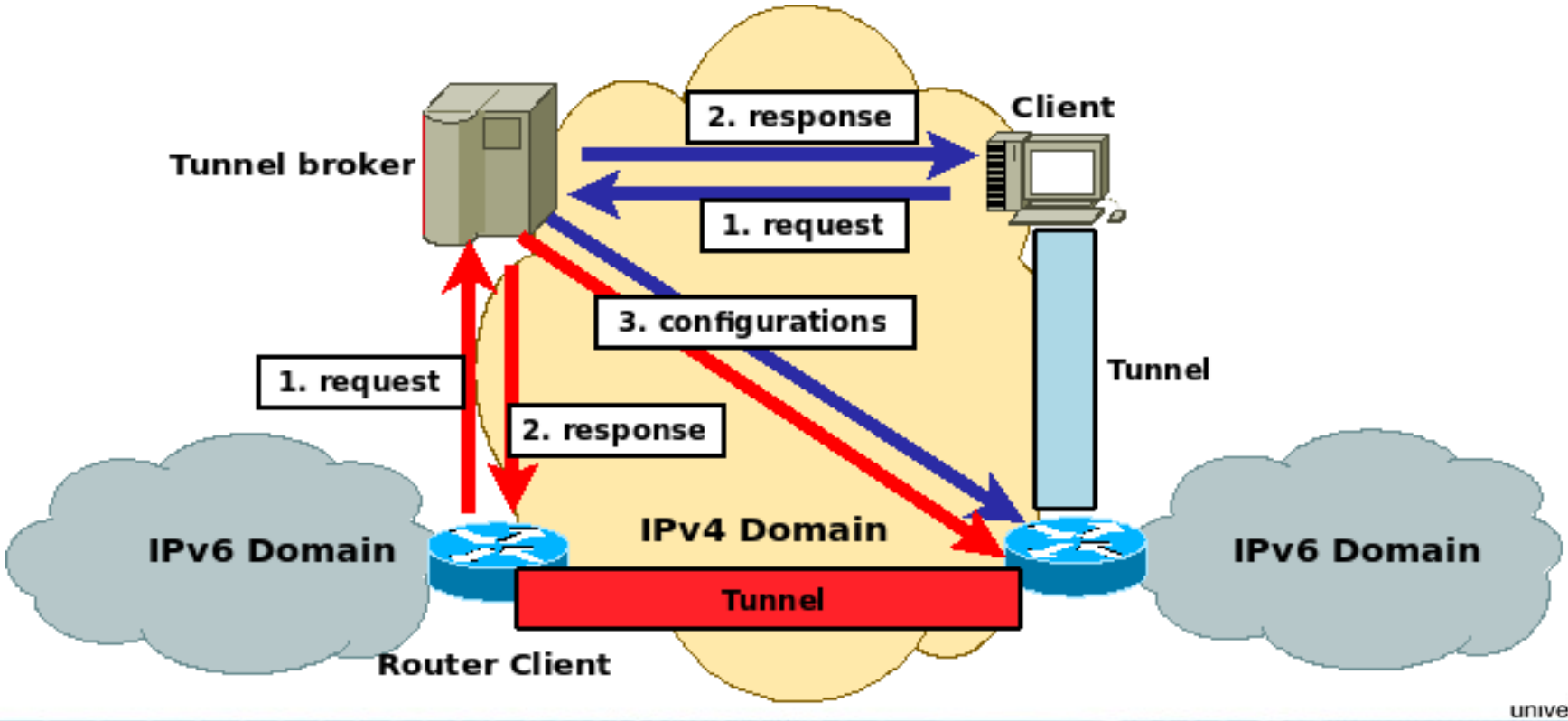
IPv6 over IPv4 GRE Tunnel

- Uses the standard GRE tunneling technique
  - GRE – Generic Route Encapsulation
- Also must be manually configured
- Primary use is for stable connections that require regular stable communications
- IPv4 over IPv6 also possible



Tunnel Broker

- A tunnel broker service allows IPv6 applications on dual-stack systems access to an IPv6 backbone
- Automatically manages tunnel requests and configuration
- Potential security implications
  - Broker is a single point of failure
- Most common implementation: Teredo.



Automatic IPv4 Compatible Tunnel

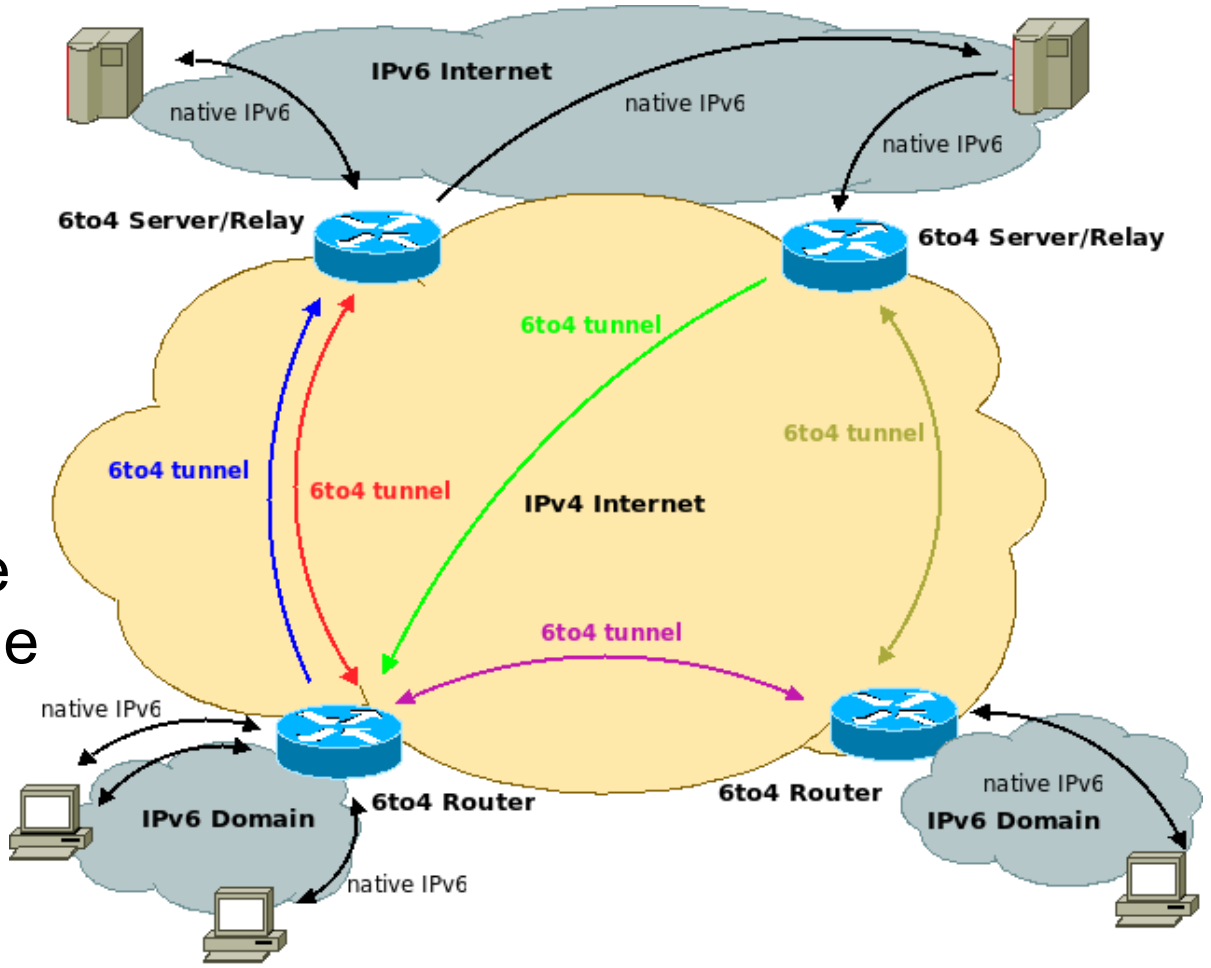
- IPv4 tunnel end-point address is embedded within the destination IPv6 address
- An automatic IPv4-compatible tunnel can be configured between edge routers or between an edge router and an end system.
- Systems must be dual-stack
- Communication only with other IPv4-compatible sites
- This tunneling technique is currently deprecated

Automatic 6to4 Tunnels

- IPv4 tunnel end-point address is embedded within the destination IPv6 address
  - Automatic 6to4 tunnel allows isolated IPv6 domains to connect over an IPv4 network
  - Unlike the manually configured tunnels are not point-to-point, they are multipoint tunnels
  - 6to4 host/router needs to have a globally addressable IPv4 address
  - Cannot be located behind a NAT box
  - Unless the NAT box supports protocol 41 packets forwarding
  - Address format is:

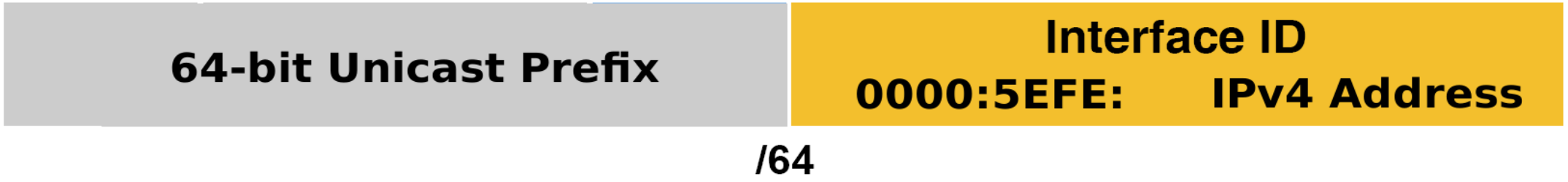
6to4 Relay Routers

- 6to4 router
  - Connects 6to4 hosts from a IPv6 domain and
    - Other 6to4 routers
    - The IPv6 Internet through a 6to4 relay router
- 6to4 relay router
  - Connects 6to4 routers on the IPv4 Internet and hosts on the IPv6 Internet.



ISATAP Tunnels

- Intra-site Automatic Tunnel Address Protocol
- Point-to-multipoint tunnels that can be used to connect systems within a site
- Used to tunnel IPv4 within as administrative domain to create a virtual IPv6 network over a IPv4 network
- Scalable approach for incremental deployment
- Encode IPv4 Address in IPv6 Address within the interface ID



Translation Mechanisms (1)

- Stateless IP/ICMP Translator (SIIT) Model
  - General mechanism that translates IPv4 headers into IPv6 headers or vice versa
- NAT-PT and NAPT-PT
  - NAT-PT translates an IPv4 packet into a semantically equivalent IPv6 datagram or vice versa
    - Translates only between IPv4 and IPv6 addresses
  - NATPT-PT perform network addresses plus port translation plus packet translation
  - DNS Application Level Gateway (DNS-ALG) performs a translation between the IPv4 and IPv6 DNS records (A and AAAA records)
  - IETF is currently deprecating NAT-PT
- Bump-In-the-Stack (BIS)
  - Translation at OS protocol stack in each host
  - Is a translation interface between IPv4 applications and the underlying IPv6 network
  - Three extra layers (name resolver extension, address mapper, and translator) are added to the IPv4 protocol stack
  - The BIS mechanism may be useful during initial stages of IPv4 transition to IPv6 when IPv4 applications remain unmodified within IPv6 domains

Translation Mechanisms (2)

- Bump-In-The-API (BIA)
  - Very similar to BIS
  - Instead of translating between IPv4 and IPv6 headers, BIA inserts an API translator between the socket API and the TCP/IP modules of the host stack
- SOCKS-Based IPv6/IPv4 Gateway
  - Based on SOCKSv5 permits communication between IPv4-only and IPv6-only hosts
  - When a client wants to connect to an application server
    - Sets up a connection to a well known, preconfigured proxy server using a special proxy protocol
    - Informs the proxy about the IP address and the port number of the application server it wants to communicate with
    - The proxy server is now responsible to set up a connection to the application server
    - After establishing the connection, the proxy relays packet between the client and application server hiding the actual connection

Translation Mechanisms (3)

- Transport Relay Translator (TRT)
  - Enables IPv6-only hosts to exchange traffic with IPv4-only hosts
  - No modification on hosts is required
  - IPv6 host uses a DNS-ALG to resolve its DNS queries
    - Will receive an IPv6 address specially constructed from the IPv4 address
    - Consists of a special network prefix associated with the transport relay and a host ID (the lower 64 bits) that embeds the IPv4 address of the remote host