Networker’s Handbook
(part 1)

PDS (Přenos dat, počítačové sítě a protokoly)

Vladimír Veselý, veselyv@fit.vutbr.cz

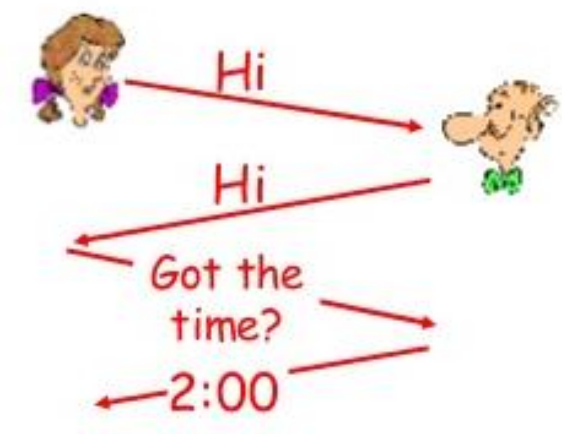
Agenda

- **Communication**
- **Network stack**
- **Active network devices**
  - modem, hub vs. switch, switch vs. router
- **Addressing**
  - MAC, IPv4, IPv6
- **Packet traversal**
- **Demonstrations**

Communication

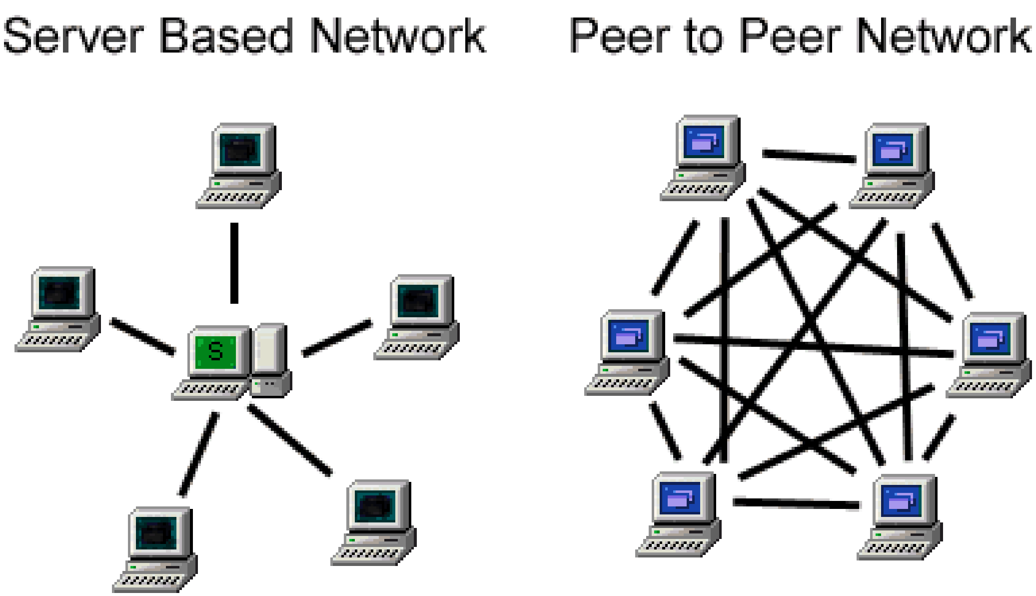
Protocol

- Defines syntax and semantics of exchanged messages
  - Order of exchange
  - Role of entities
  - Actions performed
- Analogy with human interaction
  - Greetings
  - “What time is it?”
- Network protocols
  - Machine vs. human
  - Text (mail, web, FTP) vs. Binary (Radius, Skype)

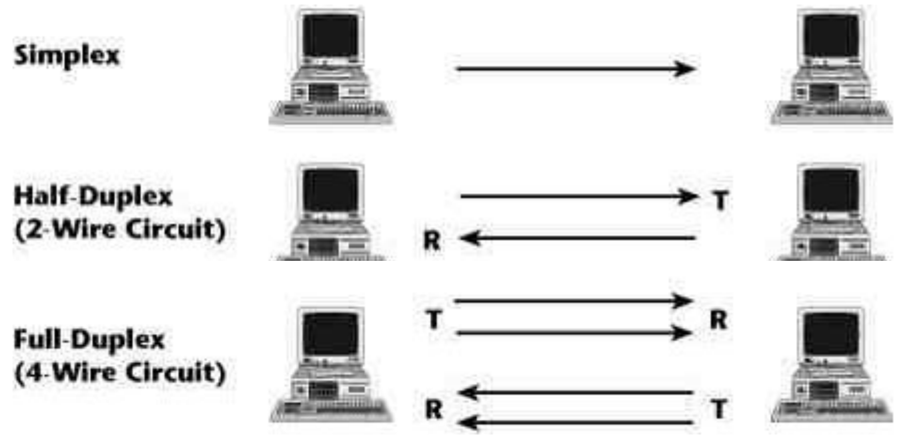


Communication Models

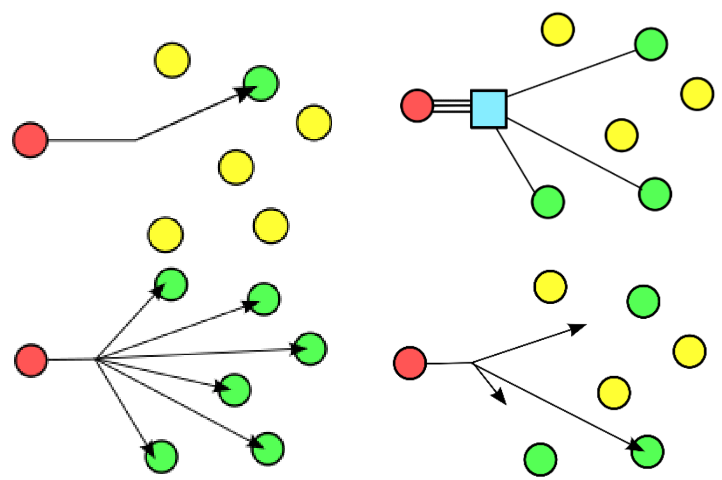
- **Client-server**
  - Client requests server for a service
  - E.g., web browser initiates communication with web server
- **Peer-to-peer**
  - Minimal server usage
  - E.g., BitTorrent, Gnutella



Transfer Types

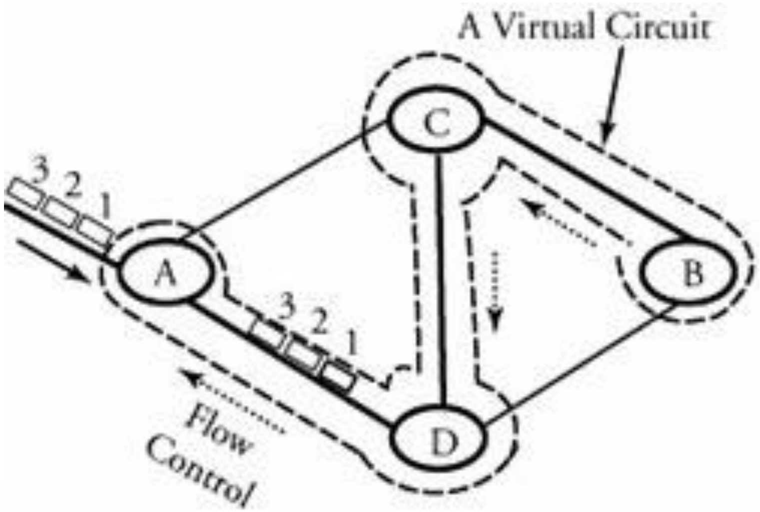


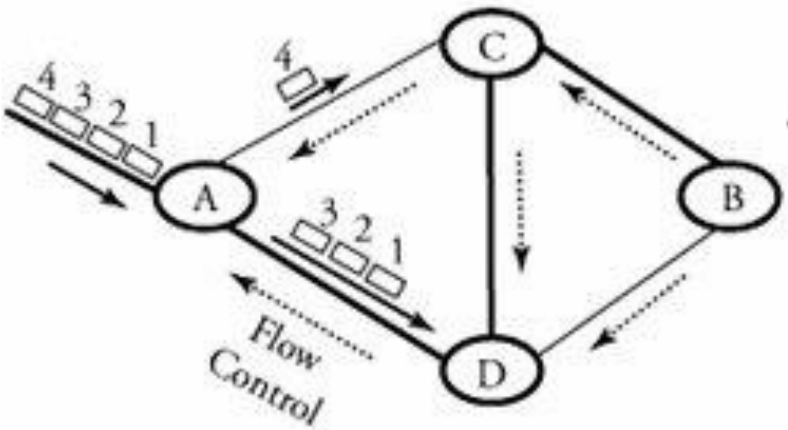
- Medium P.O.V.
  - **Simplex**
    - one direction only
  - **Half-duplex**
    - both directions but one direction simultaneously
  - **Full-duplex**
    - both directions simultaneously
- Entities P.O.V.
  - **Unicast** – one to one
  - **Broadcast** – one to all
  - **Multicast** – one to a group
  - **Anycast** – one to the closest



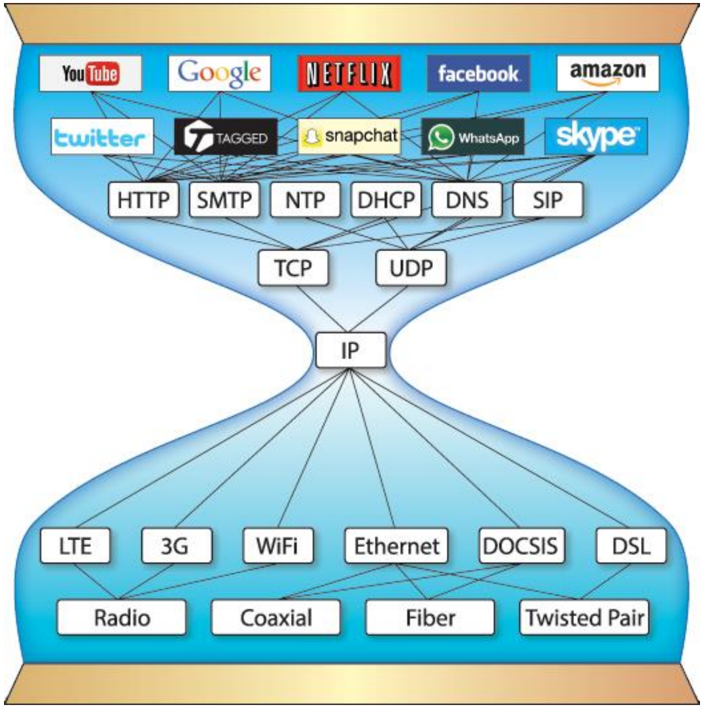
CO vs. CL

- **Connection-oriented**
  - Handshaking
  - Reliable data transfer
    - Acknowledgements
    - Flow control
    - Congestion control
  - E.g., TCP, SCTP
- **Connectionless**
  - Without initial synchronization of communicating parties
  - Unreliable data transfer
    - Best-effort delivery
  - E.g., UDP





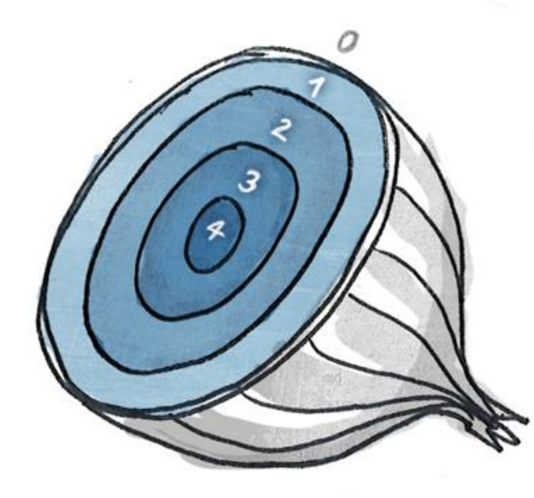
Network Stack



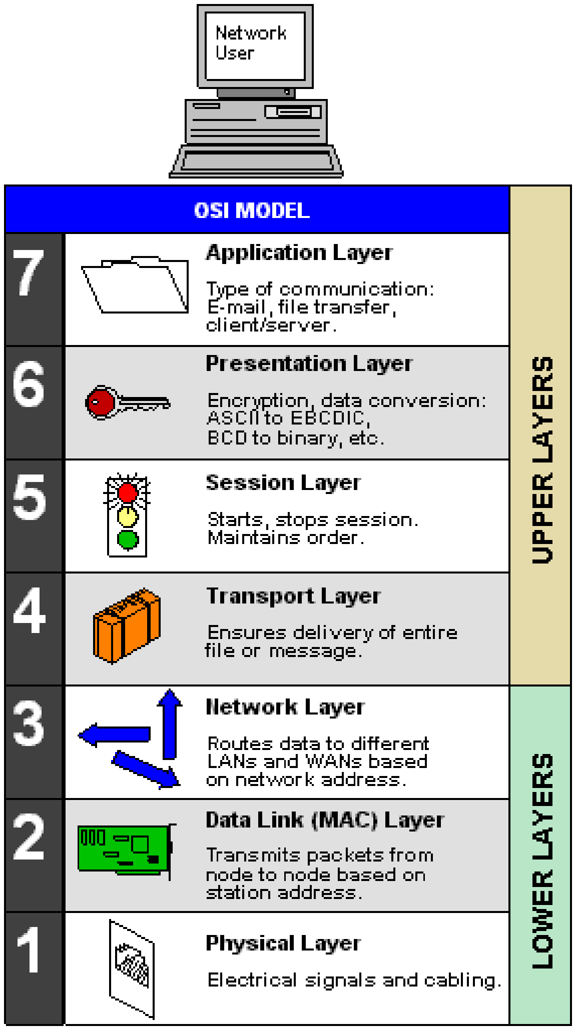
Layered Models

- Computer networks are complex systems
- Too many “parts”
  - End-systems
  - Routers and switches
  - Cable systems
  - Applications
  - Protocol
  - HW and SW
- Thus, division of scope into layers
- Referential layered models
  - ISO/OSI
  - TCP/IP

- Modular layers
  - Relationship between subsystems
  - Transparent change of layer due to the well-defined APIs
  - Extensible communication



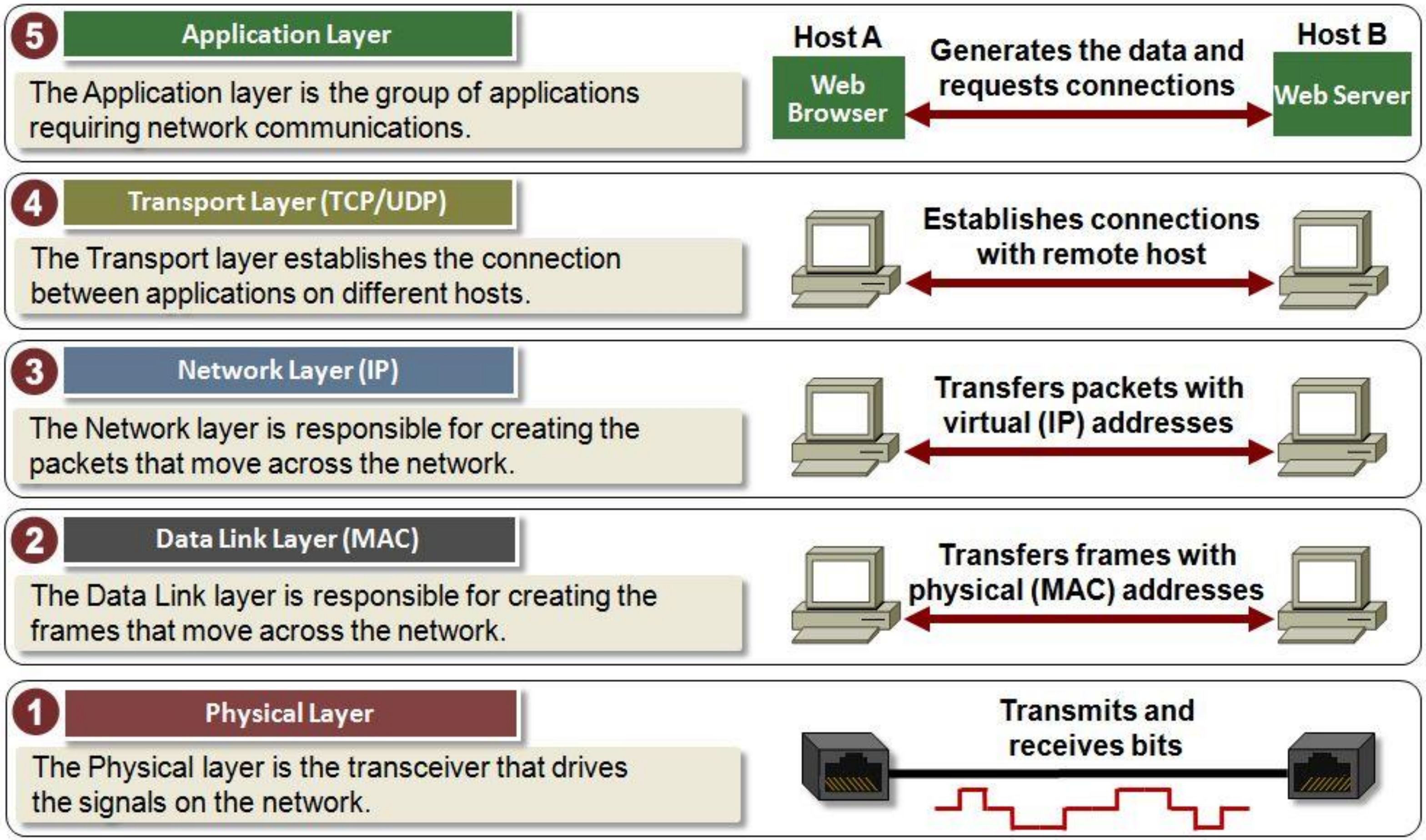
ISO/OSI



OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	**User Applications** SMTP	**GATEWAY** Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**	JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting PACKET FILTERING	**Routers** IP/IPX/ICMP		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch** **Bridge** **WAP** PPP/SLIP Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub**		

TCP/IP

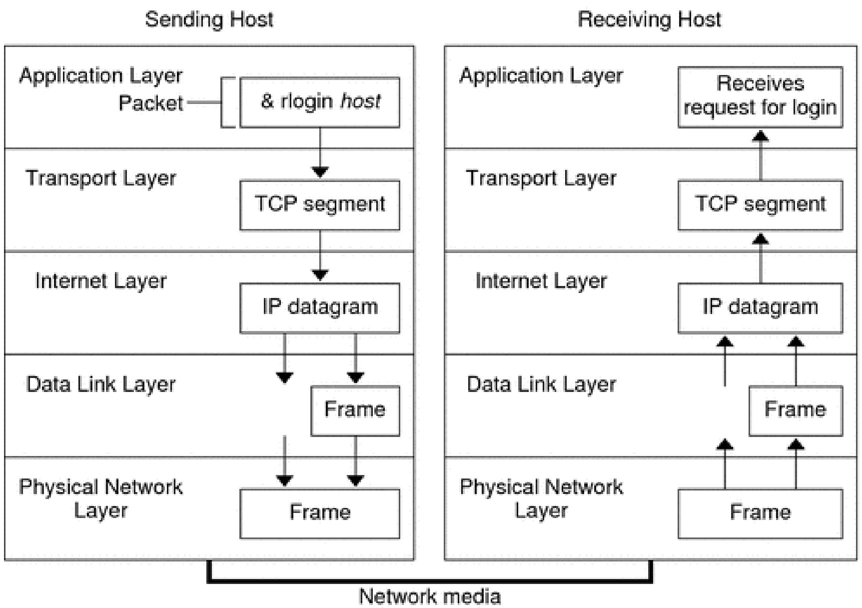


5 Application Layer
The Application layer is the group of applications requiring network communications.
Host A
Web Browser
Generates the data and requests connections
Host B
Web Server
4 Transport Layer (TCP/UDP)
The Transport layer establishes the connection between applications on different hosts.
Establishes connections with remote host
3 Network Layer (IP)
The Network layer is responsible for creating the packets that move across the network.
Transfers packets with virtual (IP) addresses
2 Data Link Layer (MAC)
The Data Link layer is responsible for creating the frames that move across the network.
Transfers frames with physical (MAC) addresses
1 Physical Layer
The Physical layer is the transceiver that drives the signals on the network.
Transmits and receives bits

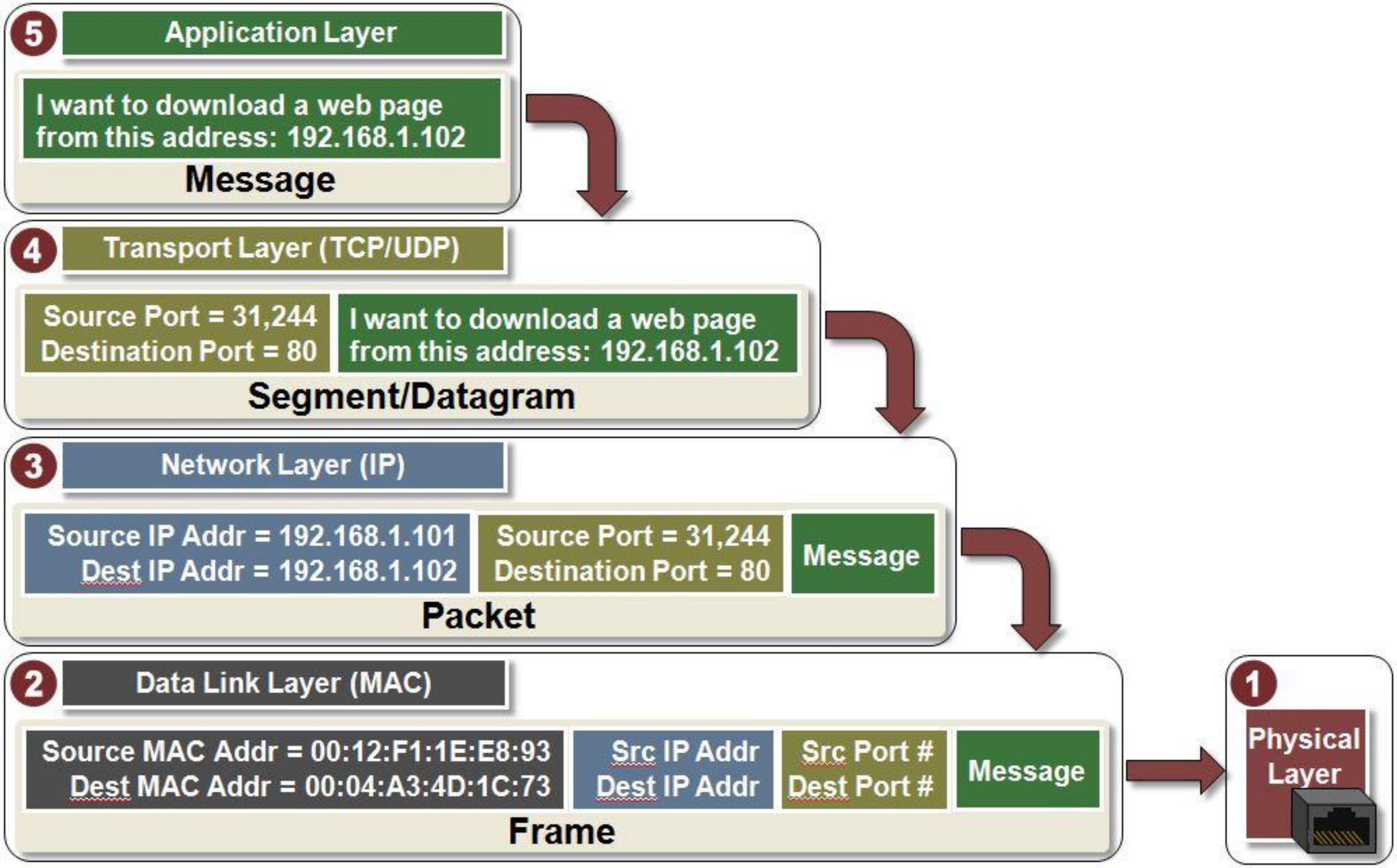
Protocol Data Units

- Unit of information processed by a given layer
- PDU consists of header + payload + (optionally) trailer
- As data traverses through layers
  - down: encapsulation occurs, header is appended
  - up: decapsulation occurs, header is stripped

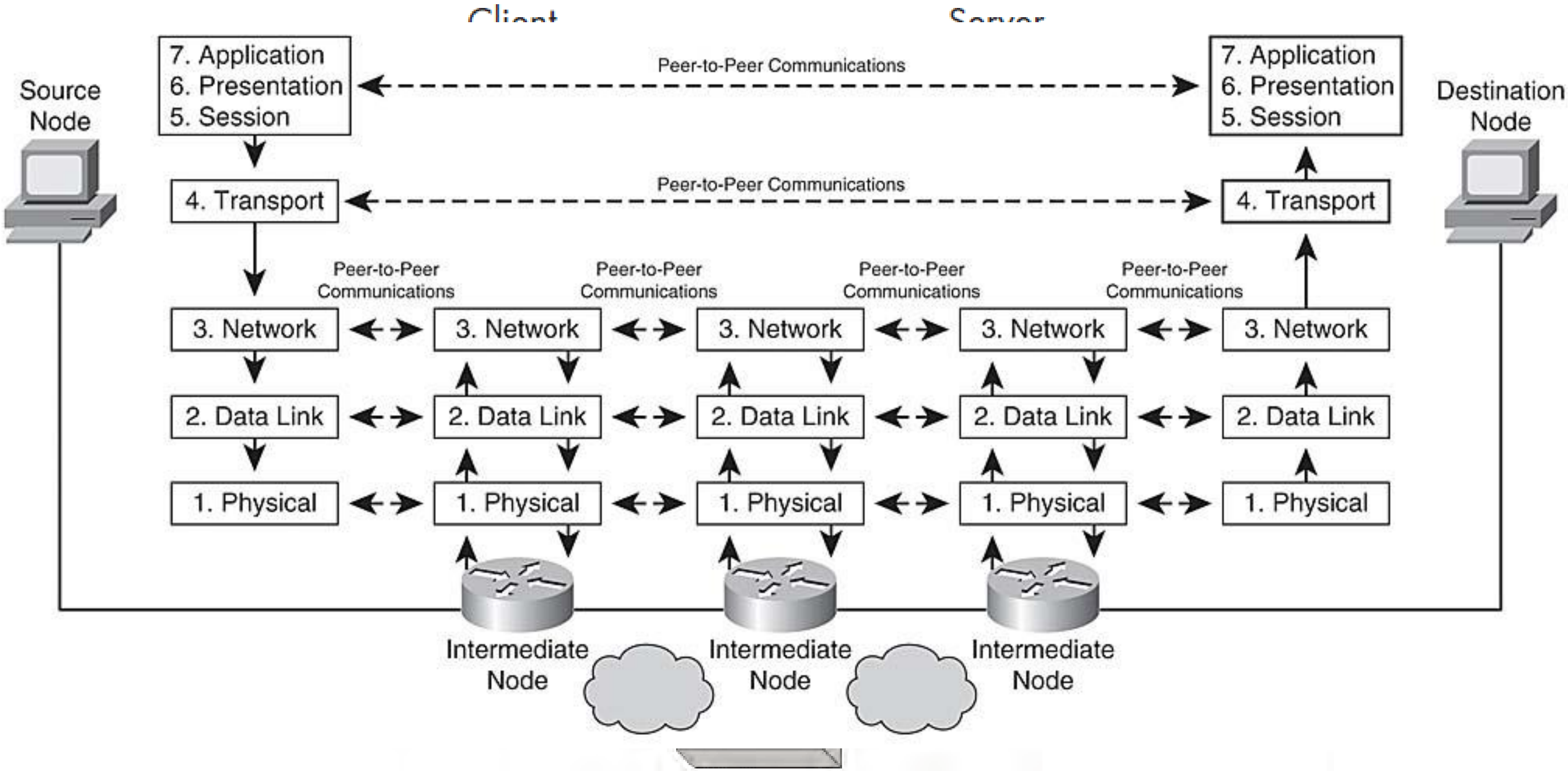
- PDU taxonomy
  - L7 PDU = application data
  - L4 PDU = **segments** (TCP)
    datagrams (UDP)
  - L3 PDU = **packets**
  - L2 PDU = **frames**
  - L1 PDU = bits



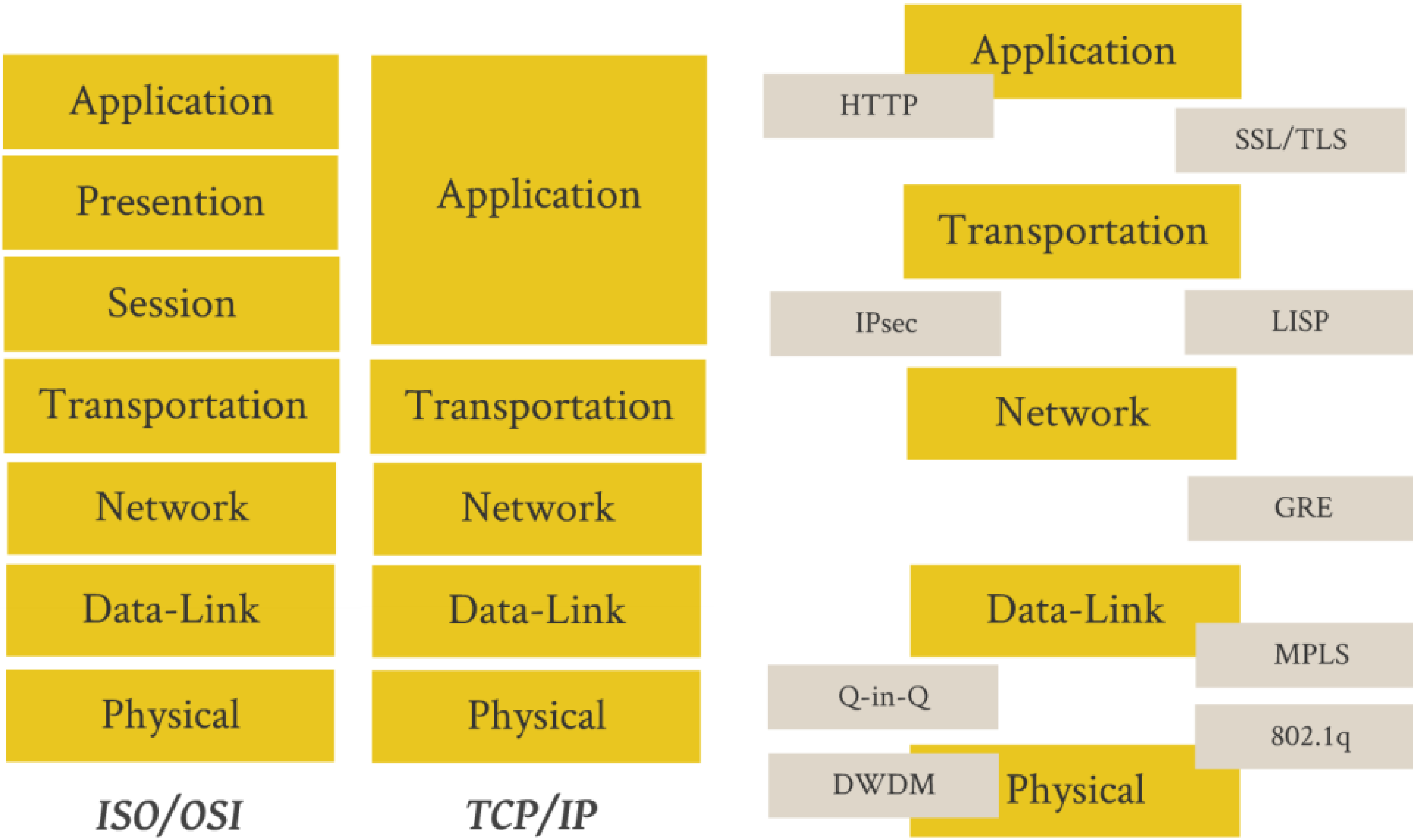
En/De-capsulation



En/De-capsulation



Rebutal

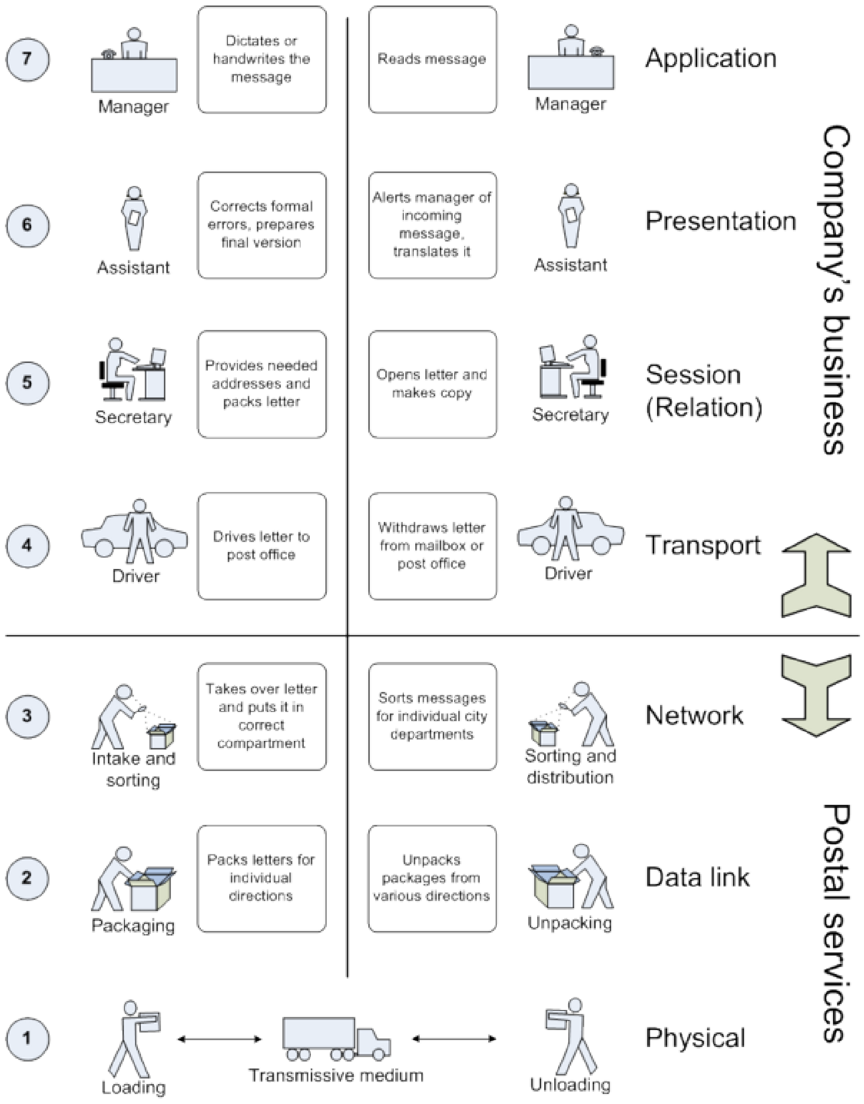


Application
Presention
Session
Transportation
Network
Data-Link
Physical
ISO/OSI
Application
Transportation
Network
Data-Link
Physical
TCP/IP
Application
HTTP
SSL/TLS
Transportation
IPsec
LISP
Network
GRE
Data-Link
MPLS
Q-in-Q
802.1q
DWDM
Physical

Devices

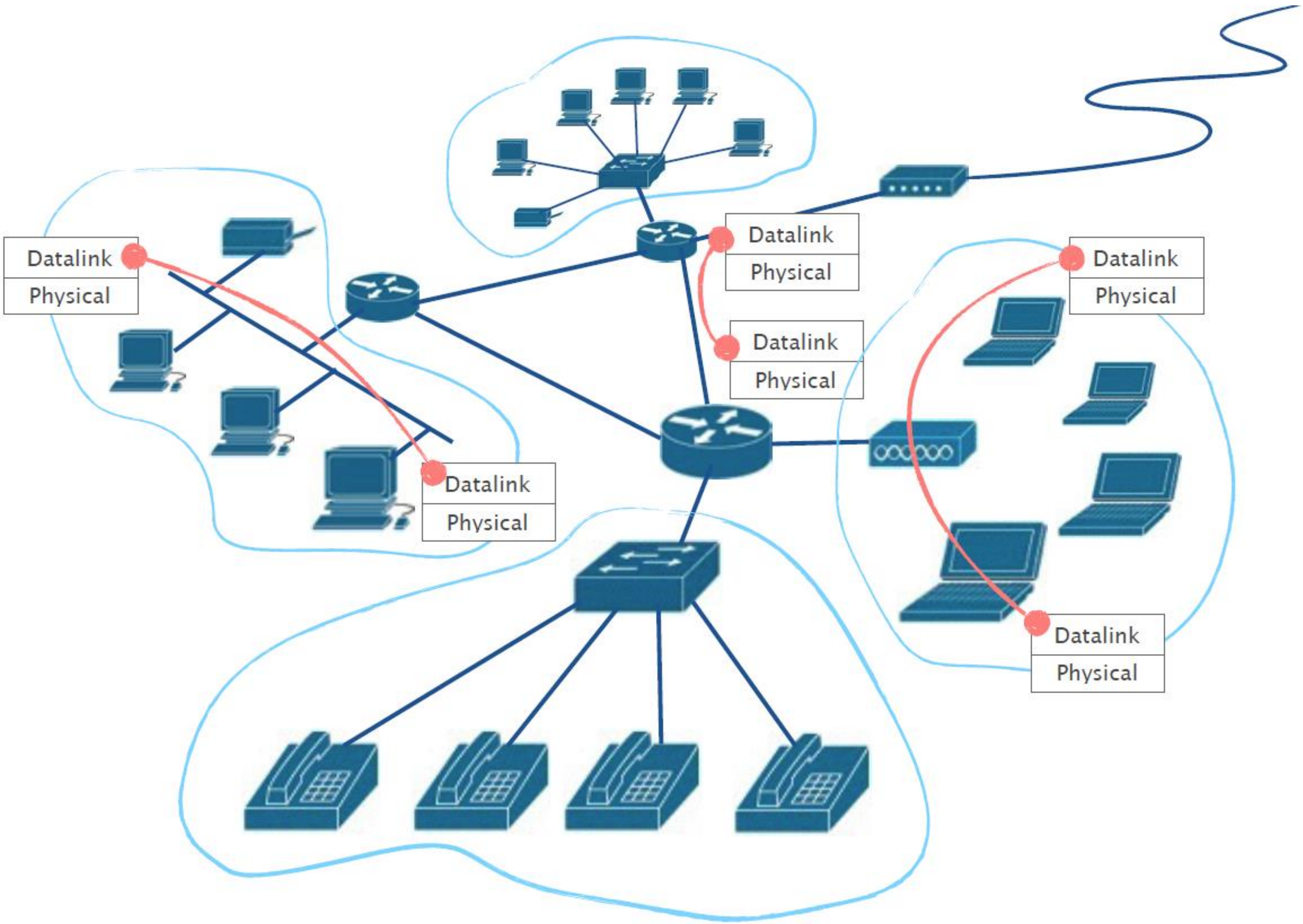
Layer Analogy

- Layer 2
  - hop-by-hop
  - local
- Layer 3
  - end-to-end
  - remote



RM – OSI and letter communication parallel

Data-Link Layer

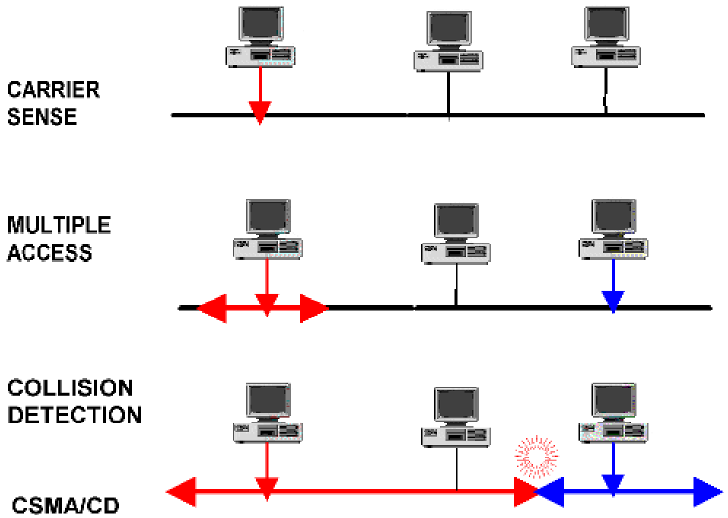


L2 Responsibilities

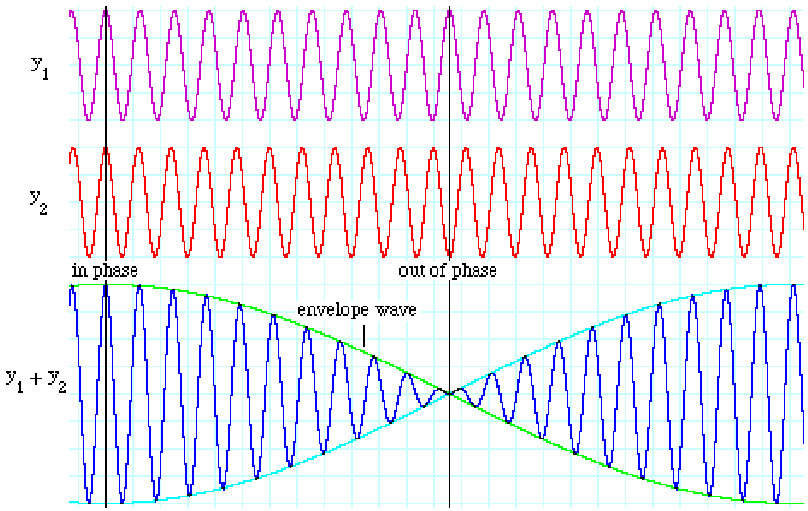
- **Media Access Control**
  - controlling how devices in a network gain access to medium and permission to transmit it
- **Link-Layer Control**
  - identifying Network layer protocols and then encapsulating them and controls error checking and frame synchronization
- IEEE 802.*
  - 802.3 Ethernet
  - 802.11 WiFi
  - 802.15.1 Bluetooth

Collision

- Shared medium allows only exclusive access



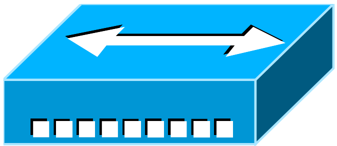
- If multiple nodes sends data, **collision** occurs



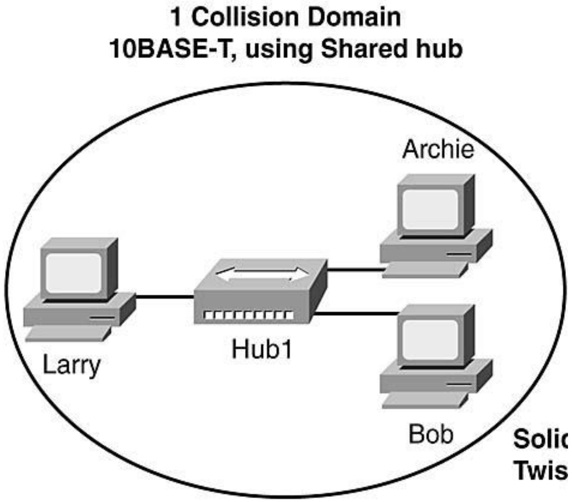
Modem

- L1.5 device
- Translates one data-link technology onto another
  - Usually Ethernet onto something else
  - Telephone, CATV, DSL

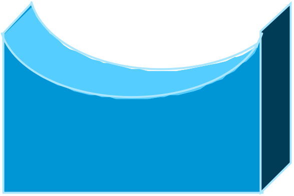
Hub, Repeater



- L1 devices
  - Hub is multiport repeater
- Regenerate electromagnetic signal
- Extend range of shared medium and network itself
- Extend **collision domain** (network segment when communicating devices may experience collision) and broadcast domain
- Hierarchical topologies
- Only same speed segments



Switch, Bridge

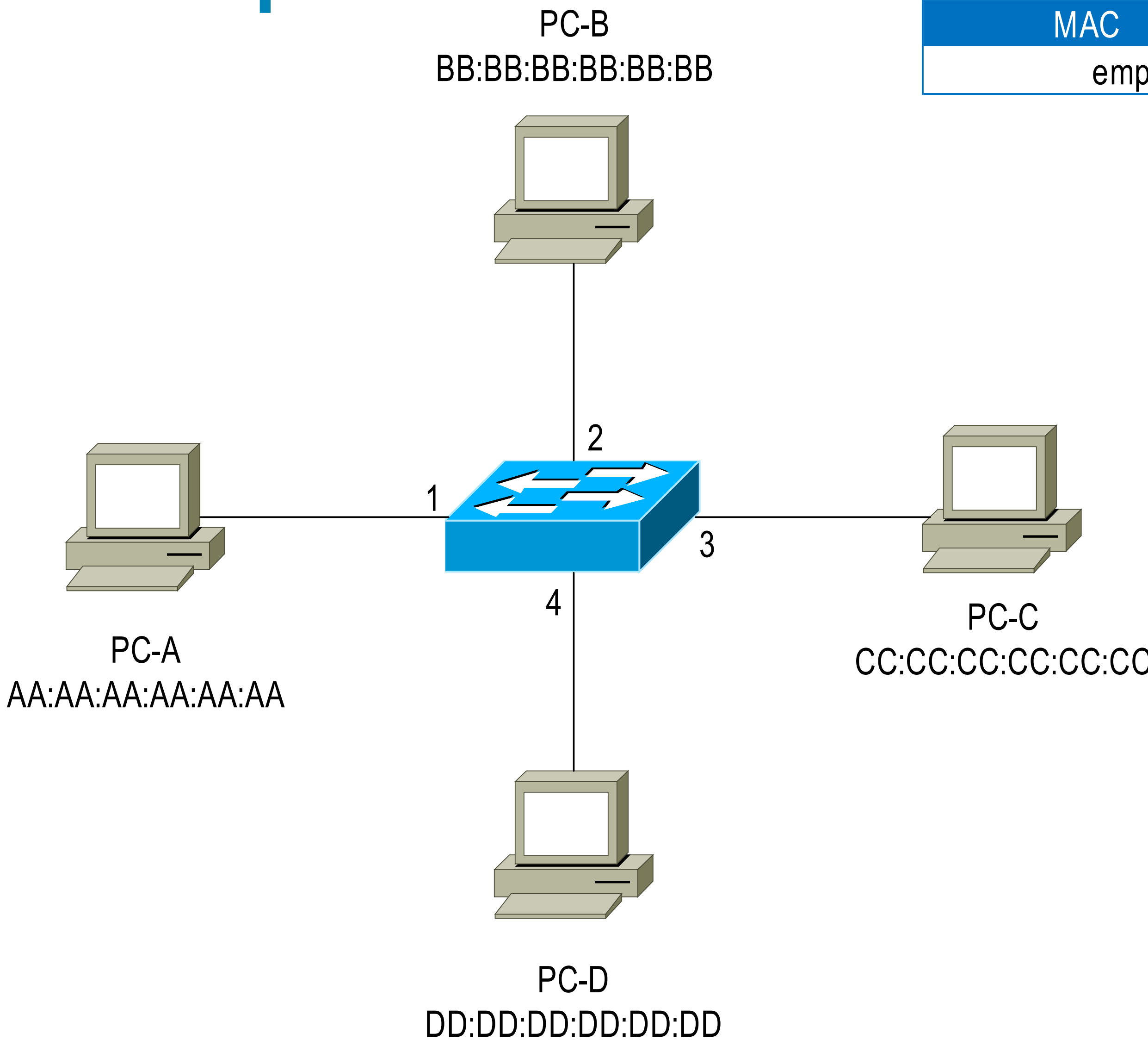


- L2 devices
  - Switch is multiport bridge
- CAM table
  - Association between port and MAC address
  - CAM populated upon receiving frame
  - Frame forwarding to destination based on CAM, otherwise flooding
- Limit collision domain
  - Ideally only full-duplex point-to-point segments
- Extend **broadcast domain** (network segment within the reach of broadcast communication)

Switch Example PC-A ⇨ PC-C

CAM Table

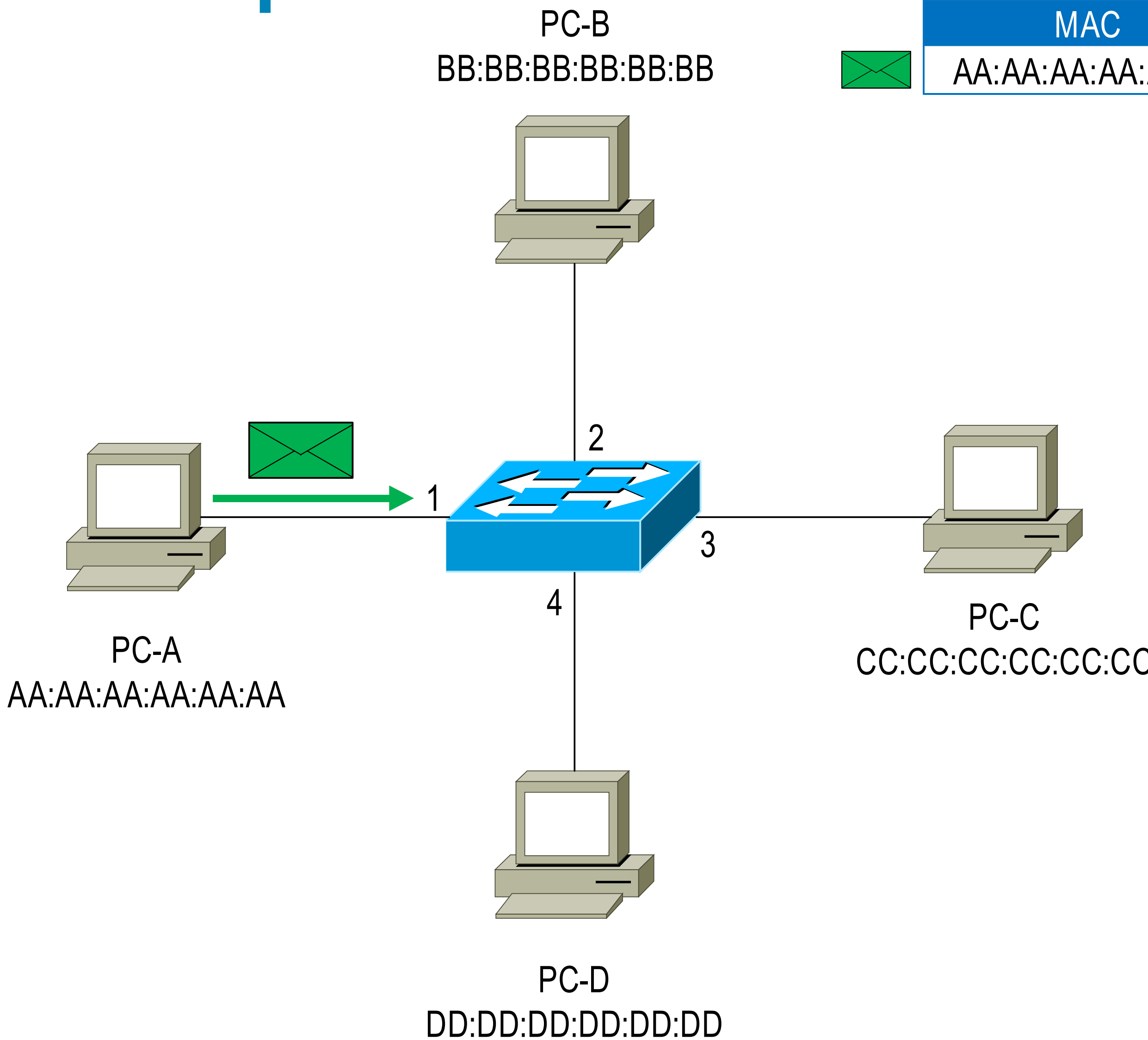
MAC	Port
empty	



Switch Example PC-A ⇨ PC-C

CAM Table

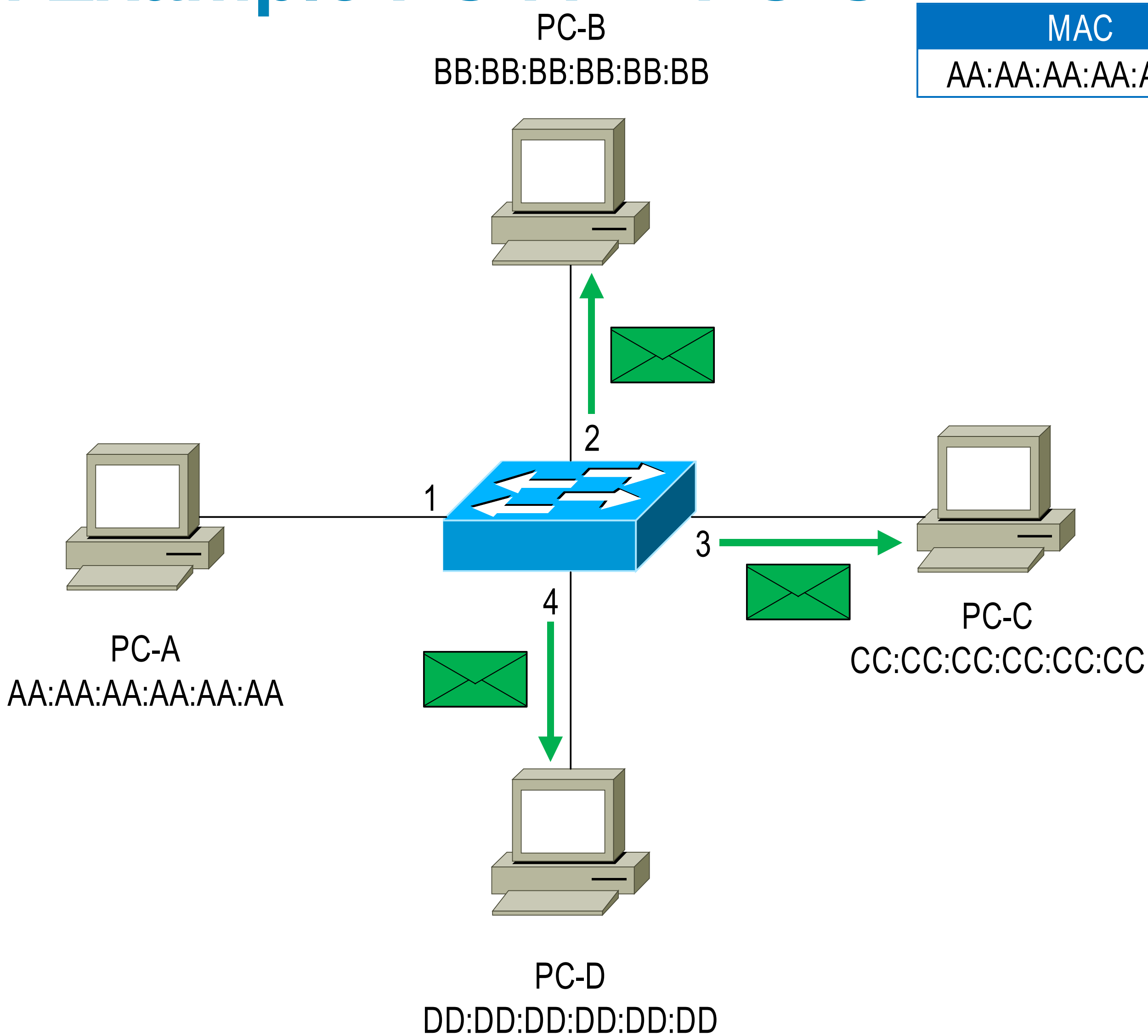
MAC	Port
AA:AA:AA:AA:AA:AA	1



Switch Example PC-A ⇨ PC-C

CAM Table

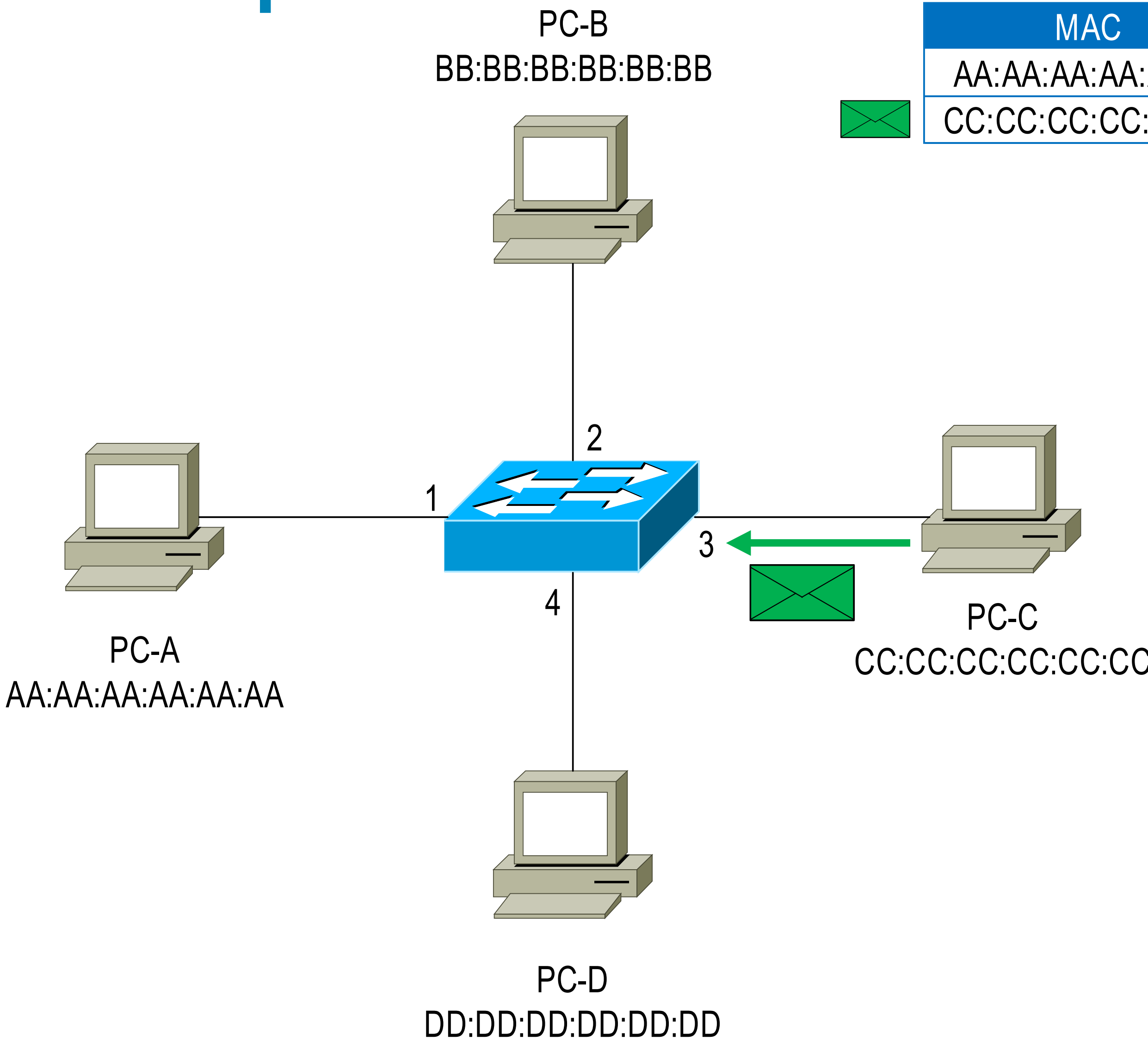
MAC	Port
AA:AA:AA:AA:AA:AA	1



Switch Example PC-A ⇦ PC-C

CAM Table

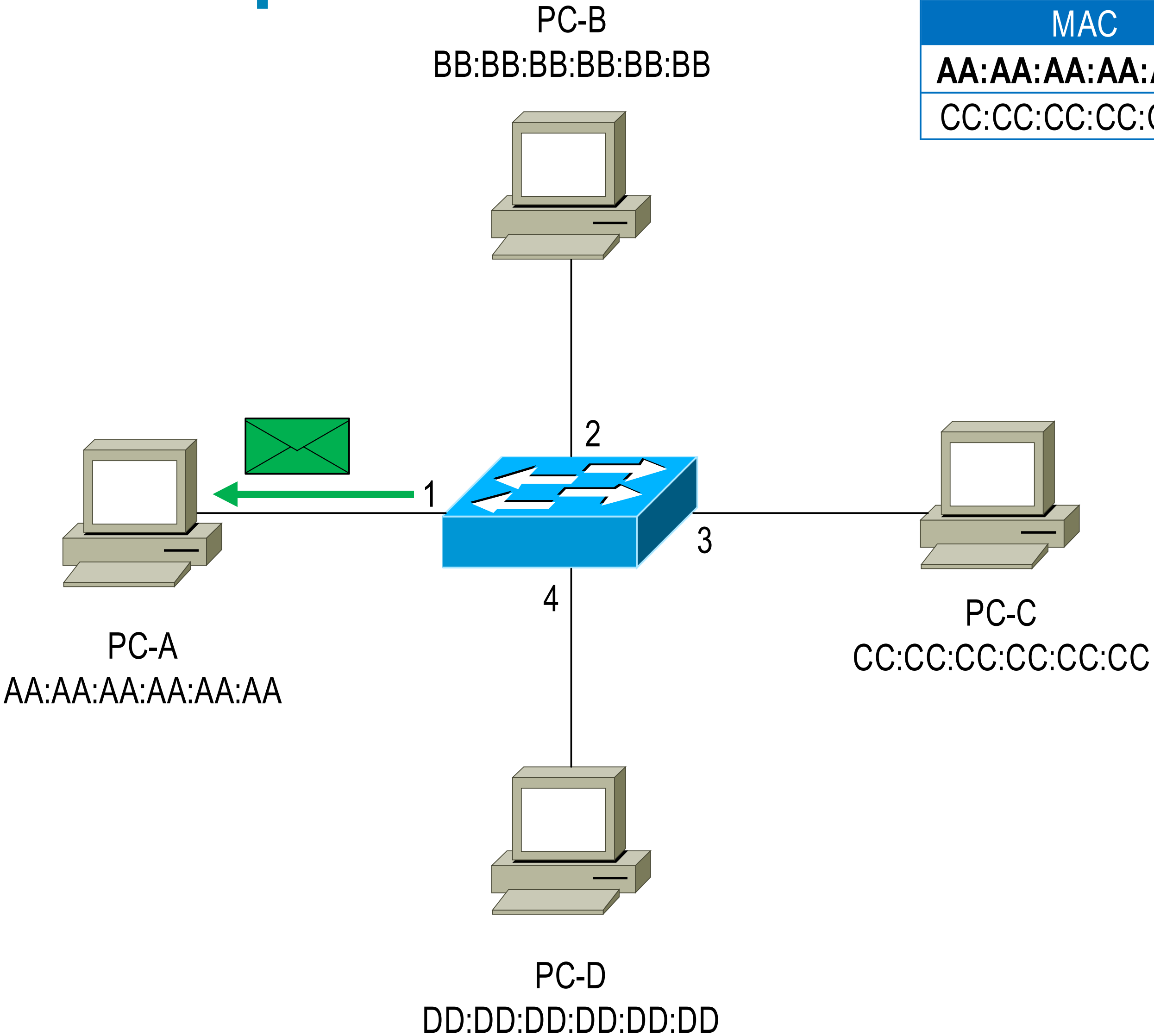
MAC	Port
AA:AA:AA:AA:AA:AA	1
CC:CC:CC:CC:CC:CC	3



Switch Example PC-A ⇦ PC-C

CAM Table

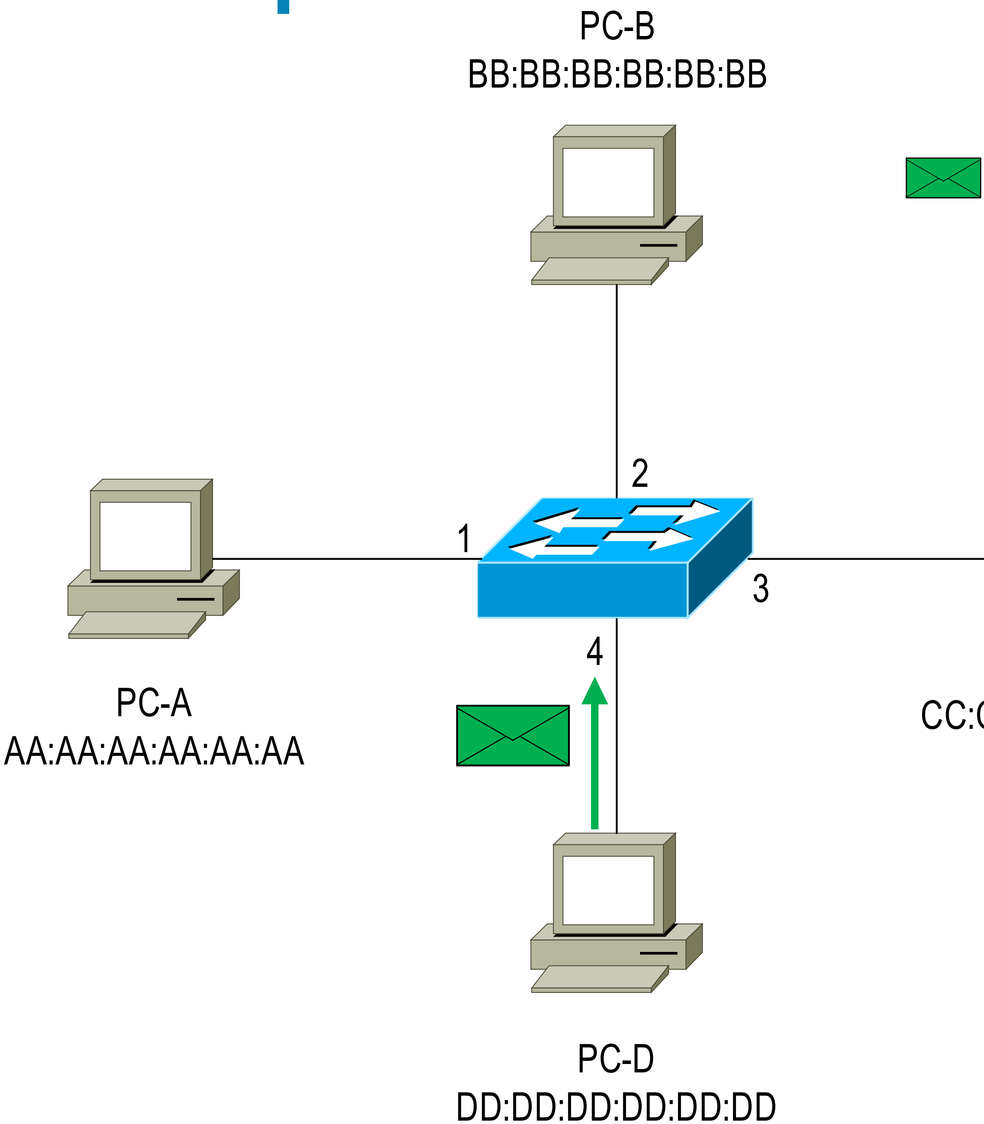
MAC	Port
AA:AA:AA:AA:AA:AA	**1**
CC:CC:CC:CC:CC:CC	3



Switch Example PC-D ⇨ PC-C

CAM Table

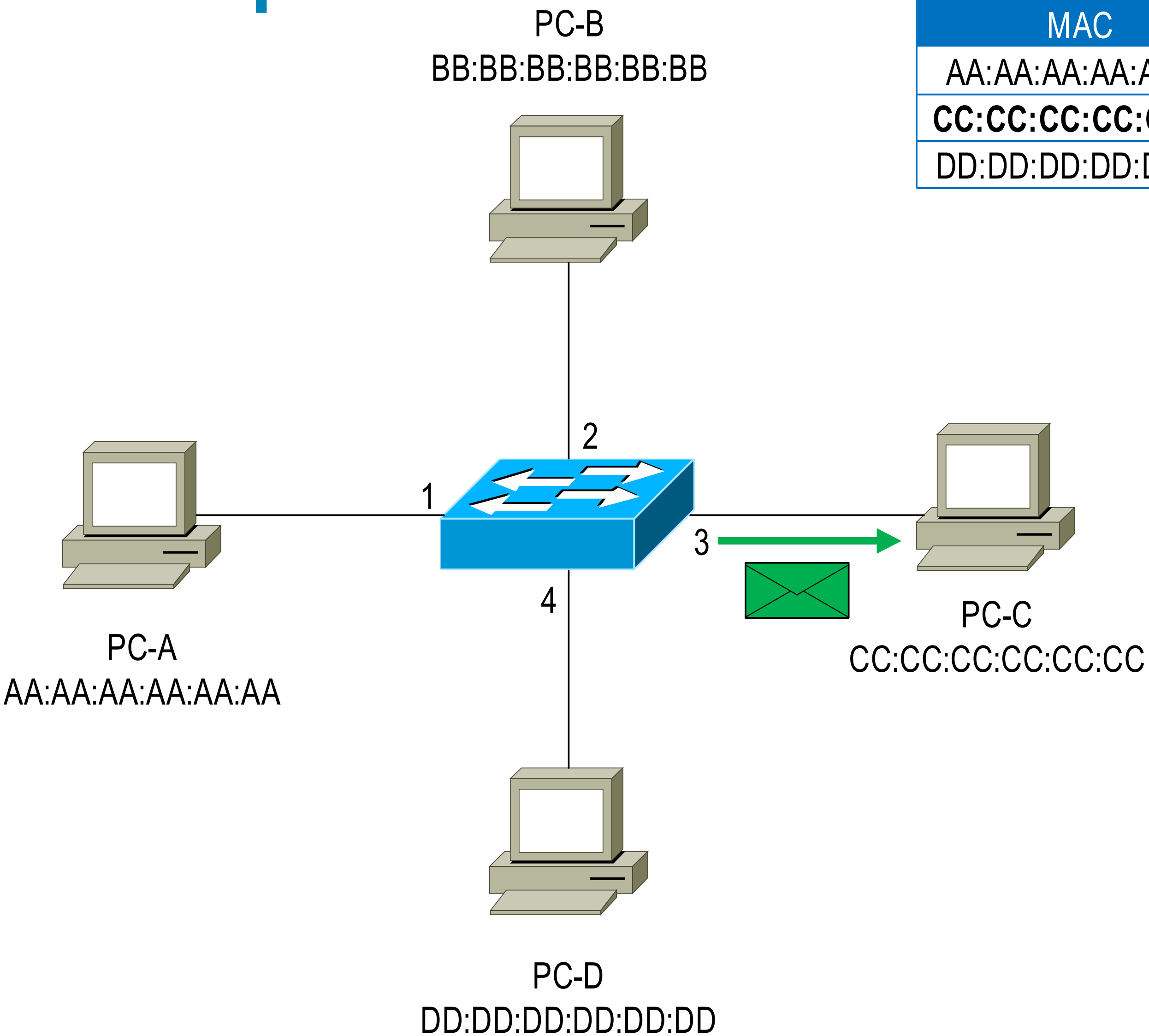
MAC	Port
AA:AA:AA:AA:AA:AA	1
CC:CC:CC:CC:CC:CC	3
DD:DD:DD:DD:DD:DD	4



Switch Example PC-D ⇨ PC-C

CAM Table

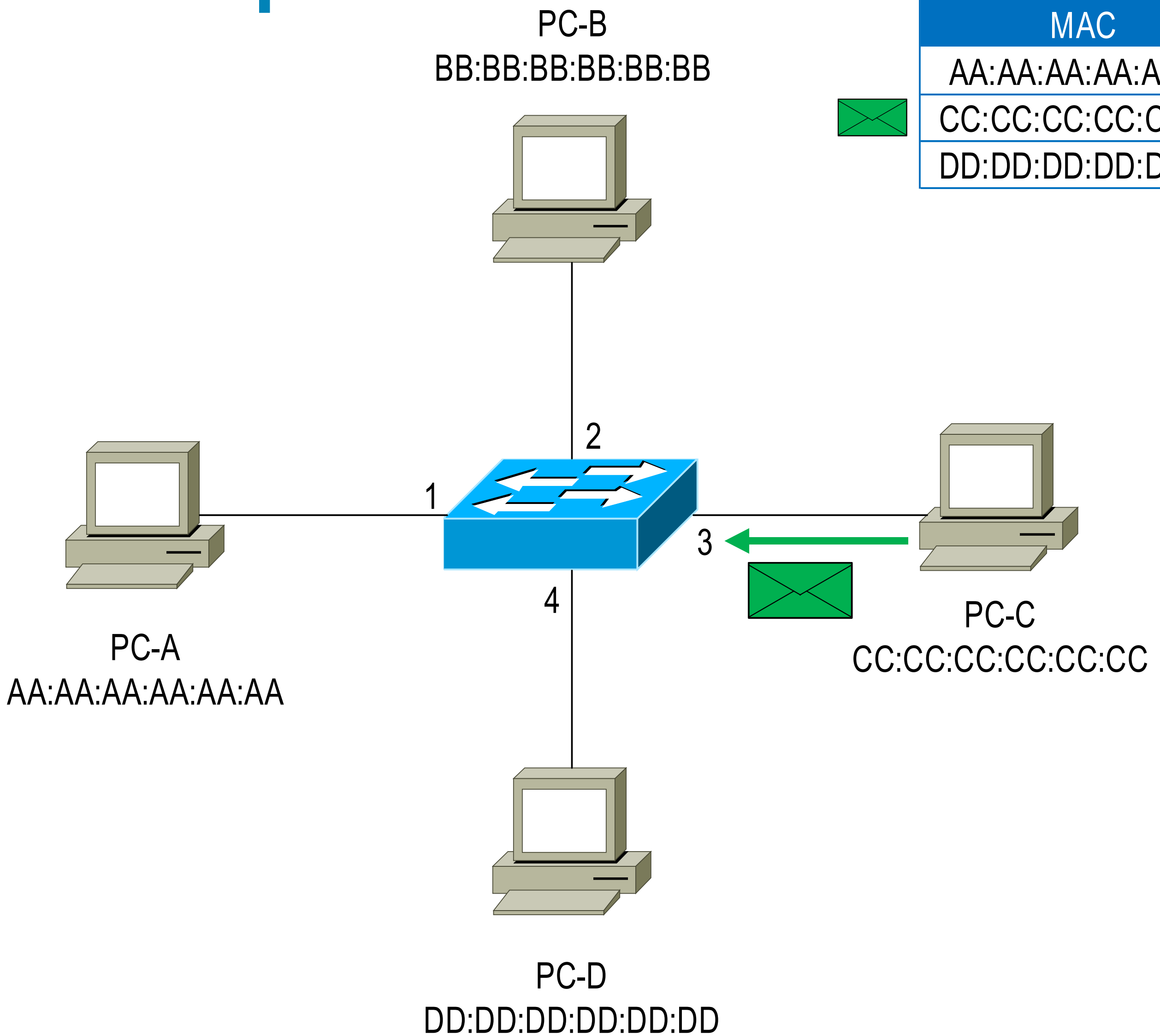
MAC	Port
AA:AA:AA:AA:AA:AA	1
CC:CC:CC:CC:CC:CC	**3**
DD:DD:DD:DD:DD:DD	4



Switch Example PC-D ⇦ PC-C

CAM Table

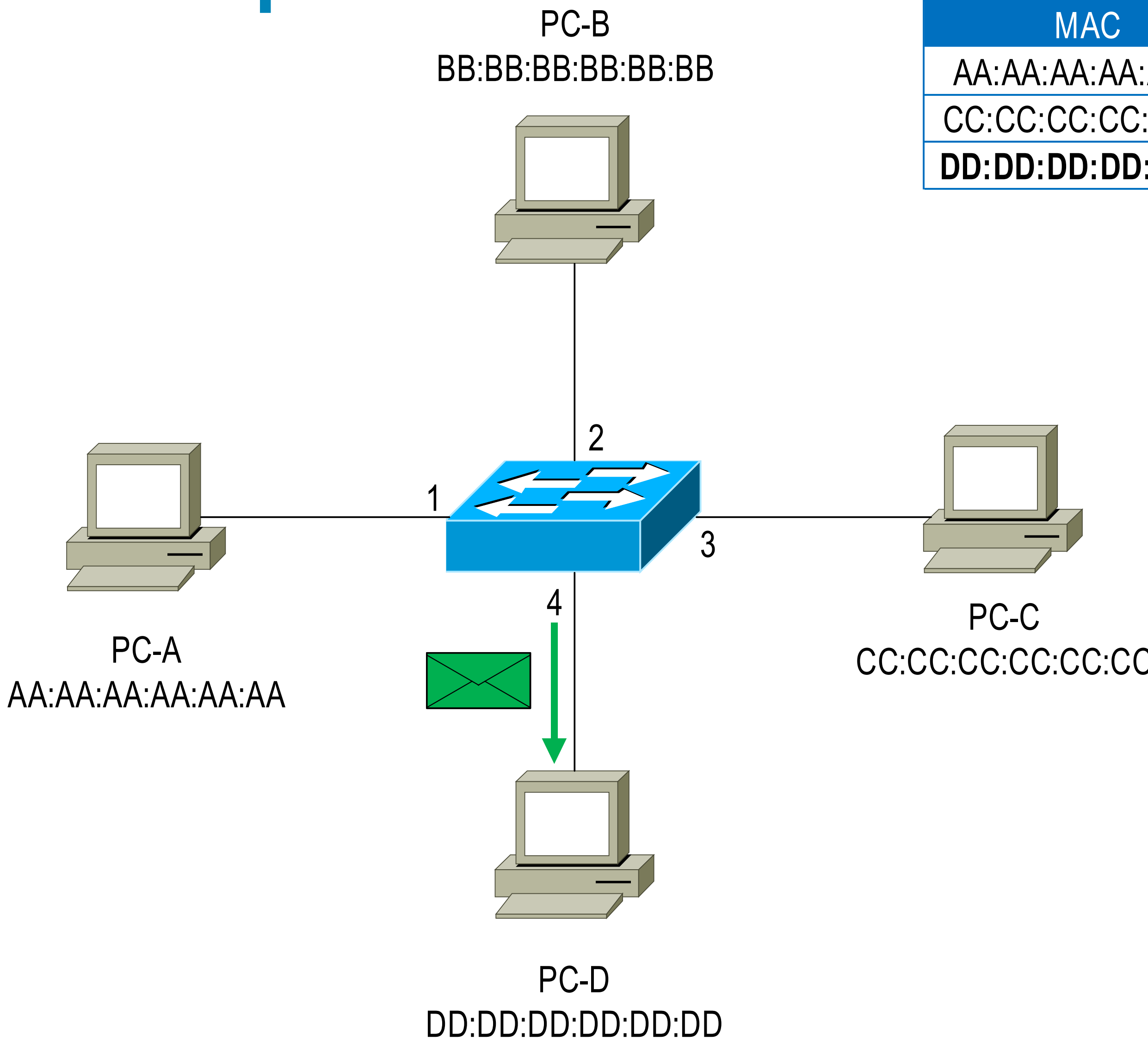
MAC	Port
AA:AA:AA:AA:AA:AA	1
CC:CC:CC:CC:CC:CC	3
DD:DD:DD:DD:DD:DD	4



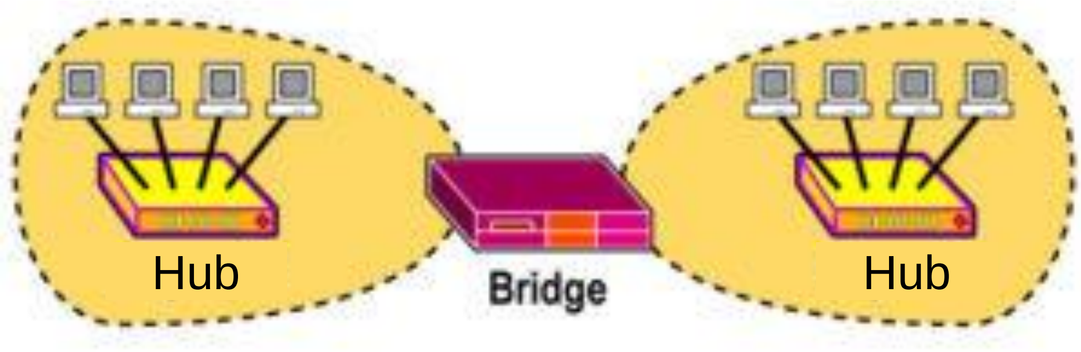
Switch Example PC-D ⇦ PC-C

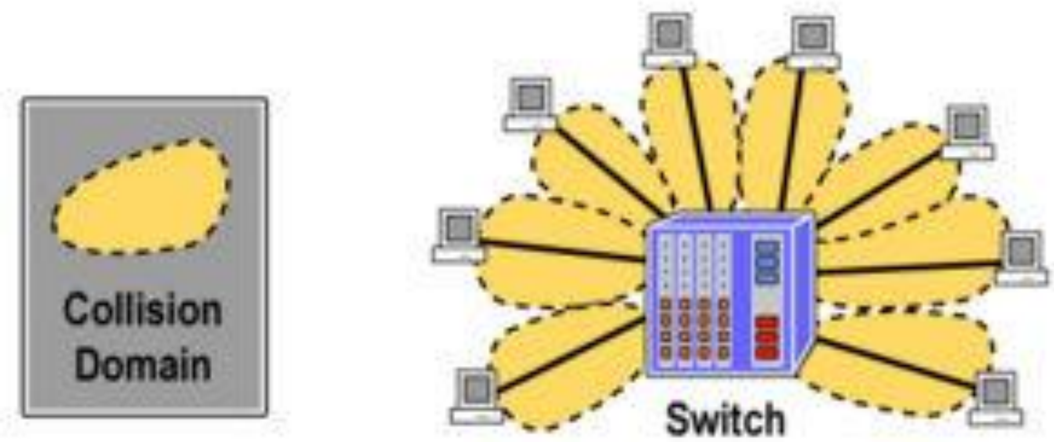
CAM Table

MAC	Port
AA:AA:AA:AA:AA:AA	1
CC:CC:CC:CC:CC:CC	3
DD:DD:DD:DD:DD:DD	**4**

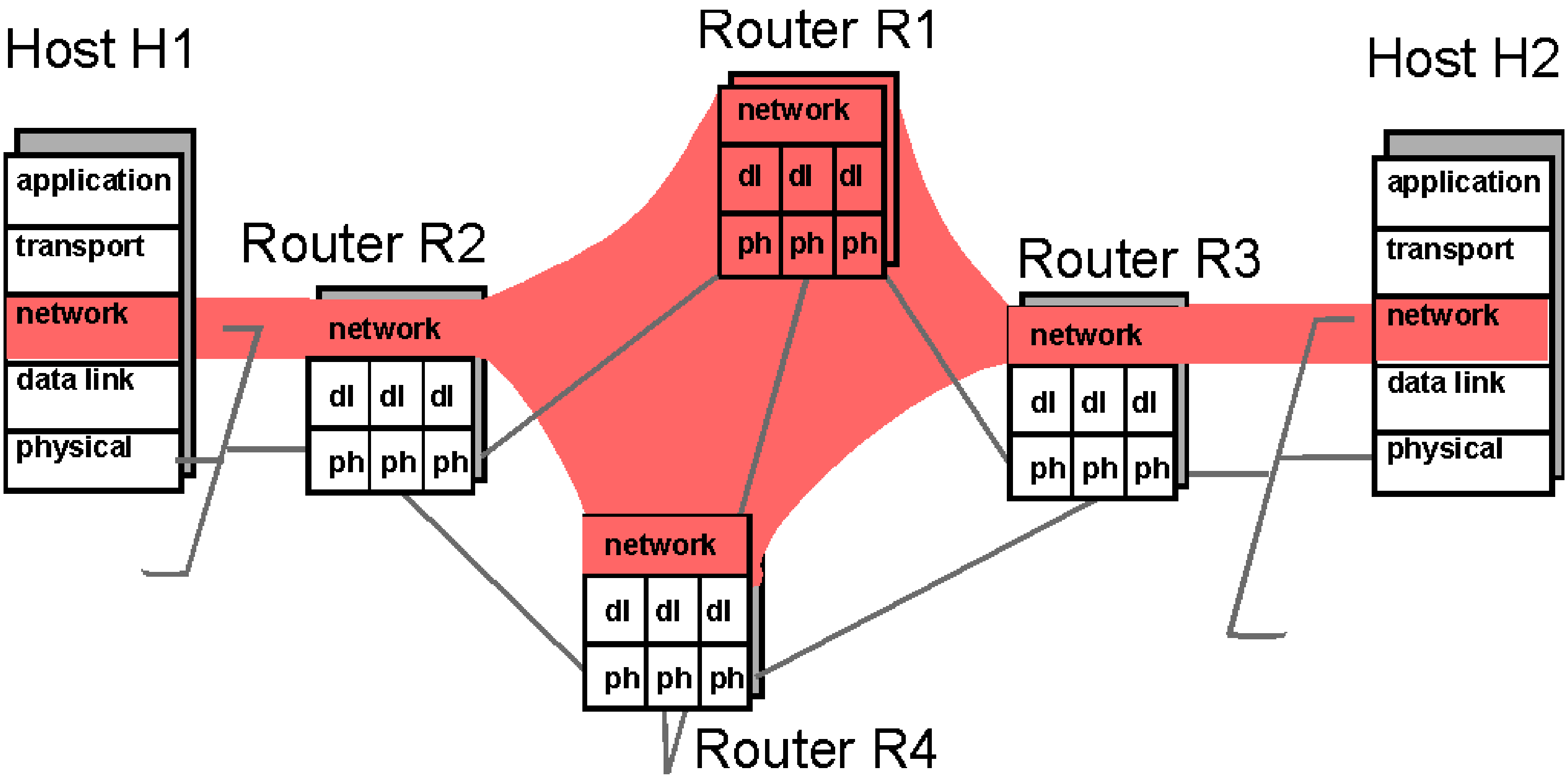


Collision Domain





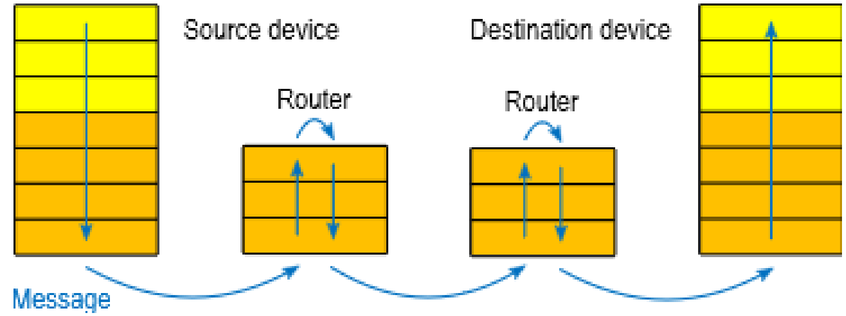
Network-Layer



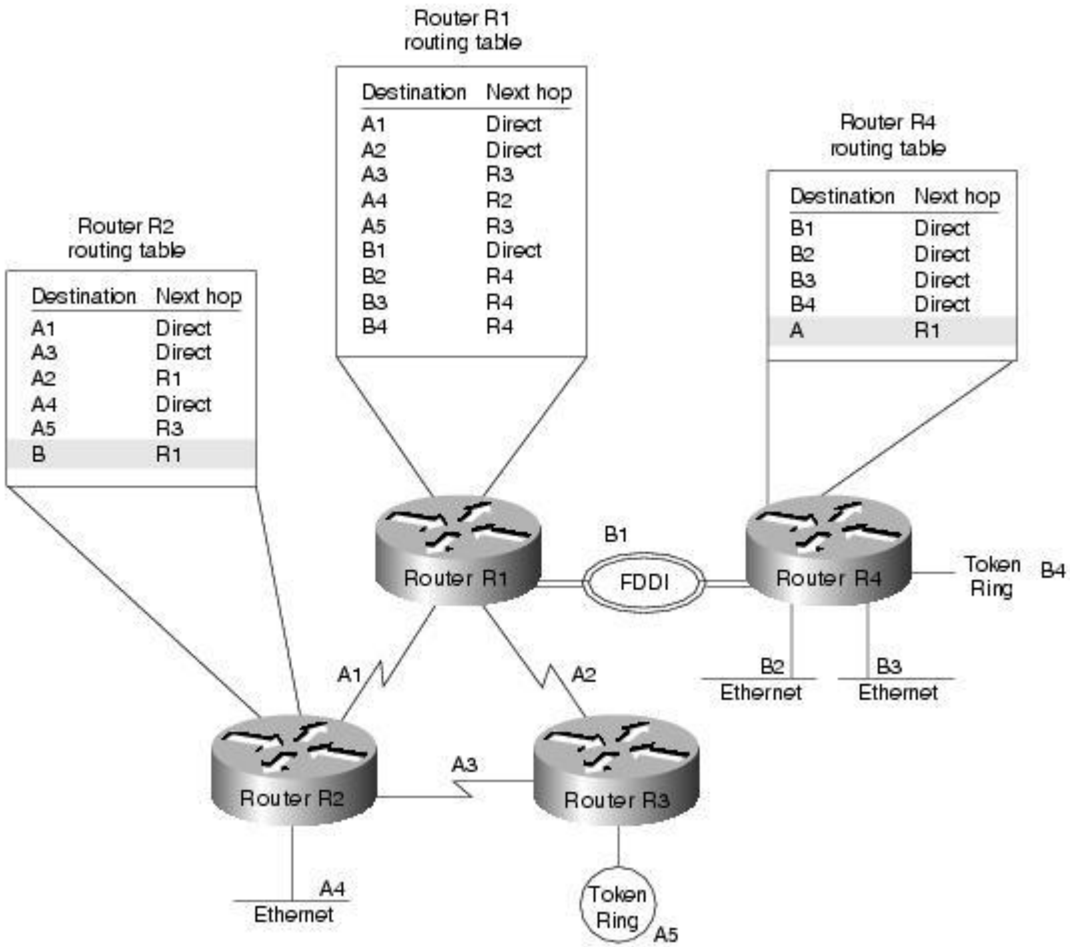
L3 Responsibilities

- **Routing**
  - Next-hop address and outgoing interface is chosen for each incoming packet – determine packet’s **route**
- **Packet forwarding**
  - Dispatching of packet from ingress interface towards egress interface
- **Fragmentation**
  - If the message is too large to be transmitted from one node to another on the data link layer, the network may implement message delivery by splitting the message into several fragments
- **Delivery feedback**
  - Optional notification about delivery errors

Routing



Source device
Destination device
Router
Router
Message



Router R1
routing table
Destination Next hop
A1 Direct
A2 Direct
A3 R3
A4 R2
A5 R3
B1 Direct
B2 R4
B3 R4
B4 R4
Router R4
routing table
Destination Next hop
B1 Direct
B2 Direct
B3 Direct
B4 Direct
A R1
Router R2
routing table
Destination Next hop
A1 Direct
A3 Direct
A2 R1
A4 Direct
A5 R3
B R1
Router R1
B1
FDDI
Router R4
Token Ring
B4
B2
Ethernet
B3
Ethernet
A1
A2
A3
Router R2
Router R3
A4
Ethernet
Token Ring
A5

MTU

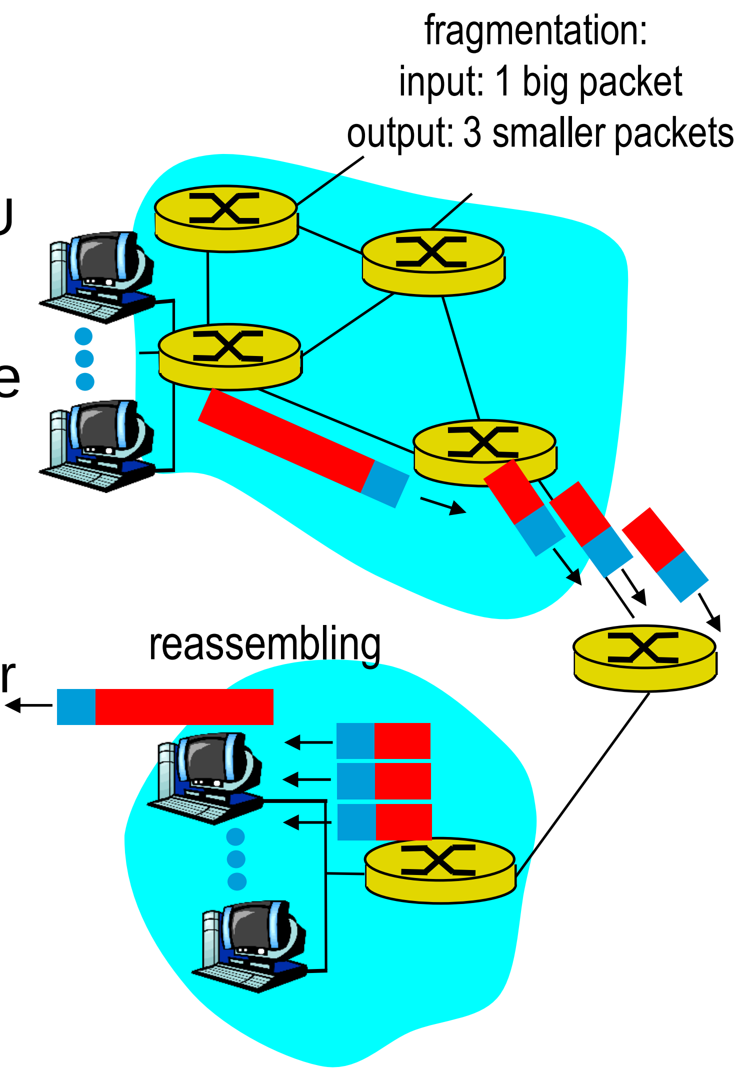
- **Maximum Transmission Unit (MTU)**
  - Largest PDU size for a given technology
  - Depends on L2 technology but influences also L3 and L4 retrospectively

Media	Maximum Transmission Unit (bytes)
Internet IPv4 Path MTU	At least 68[4]
Internet IPv6 Path MTU	At least 1280[6]
Ethernet v2	1500[8]
Ethernet with LLC[9] and SNAP,[9] PPPoE[10]	1492[11]
Ethernet Jumbo Frames	1501 - 9198[12]
PPPoE over Ethernet v2	1492[14]
PPPoE over Ethernet Jumbo Frames	1493 - 9190[15]
WLAN (802.11)	7981[16]
Token Ring (802.5)	4464
FDDI	4352[5]

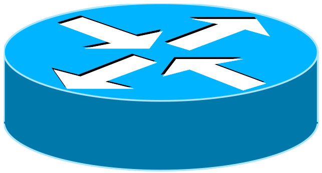
- **Minimum allowed datagram size**
  - All nodes must be prepared and willing to accept this large PDU
  - 576 B for IPv4, 1280 B for IPv6

Fragmentation

- Physical constraints of L2 limit MTU size
  - Different links may have different MTU sizes
- IF link enroute has MTU < packet size THEN router fragments IP packet
  - Reassemblong is performed by destination
  - Special ICMP message indicates error in reassembling or timeout when waiting for fragments
- Path MTU discovery
  - RFC 1191, 2923

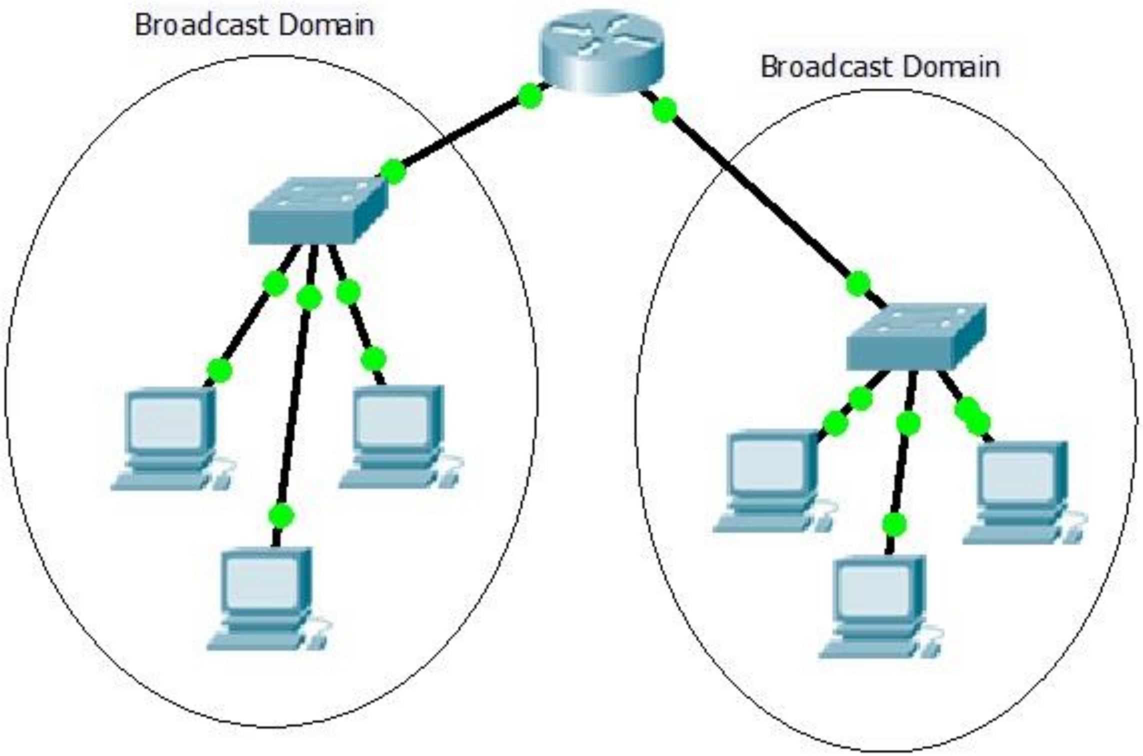


Router

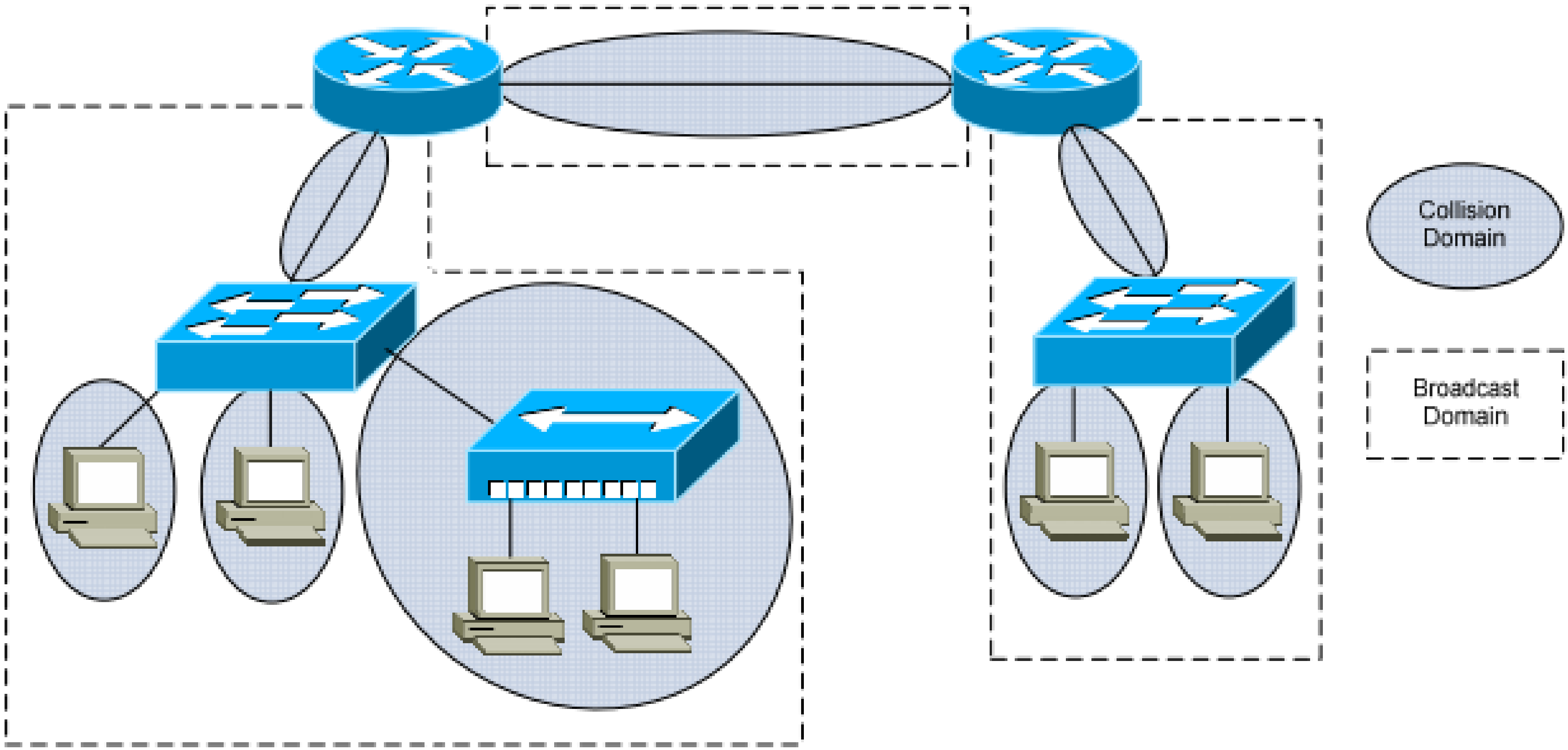


- L3 device
- Limits **broadcast domain** (segment of network within the reach of broadcast communication)
- Maintains independent routing table
- Performs routing decisions
  - Employs **longest-prefix match** on destination address

Broadcast Domain



Collision and Broadcast Domains



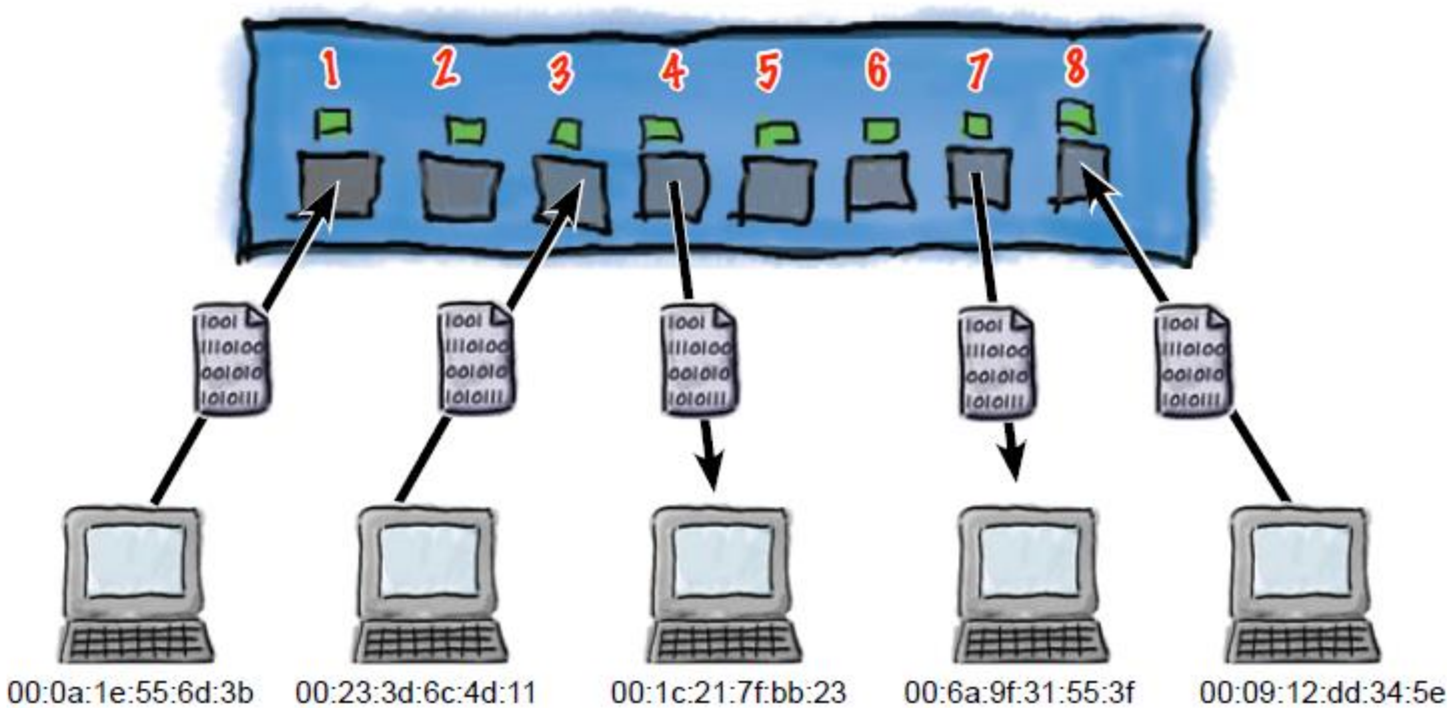
Addressing

Ethernet

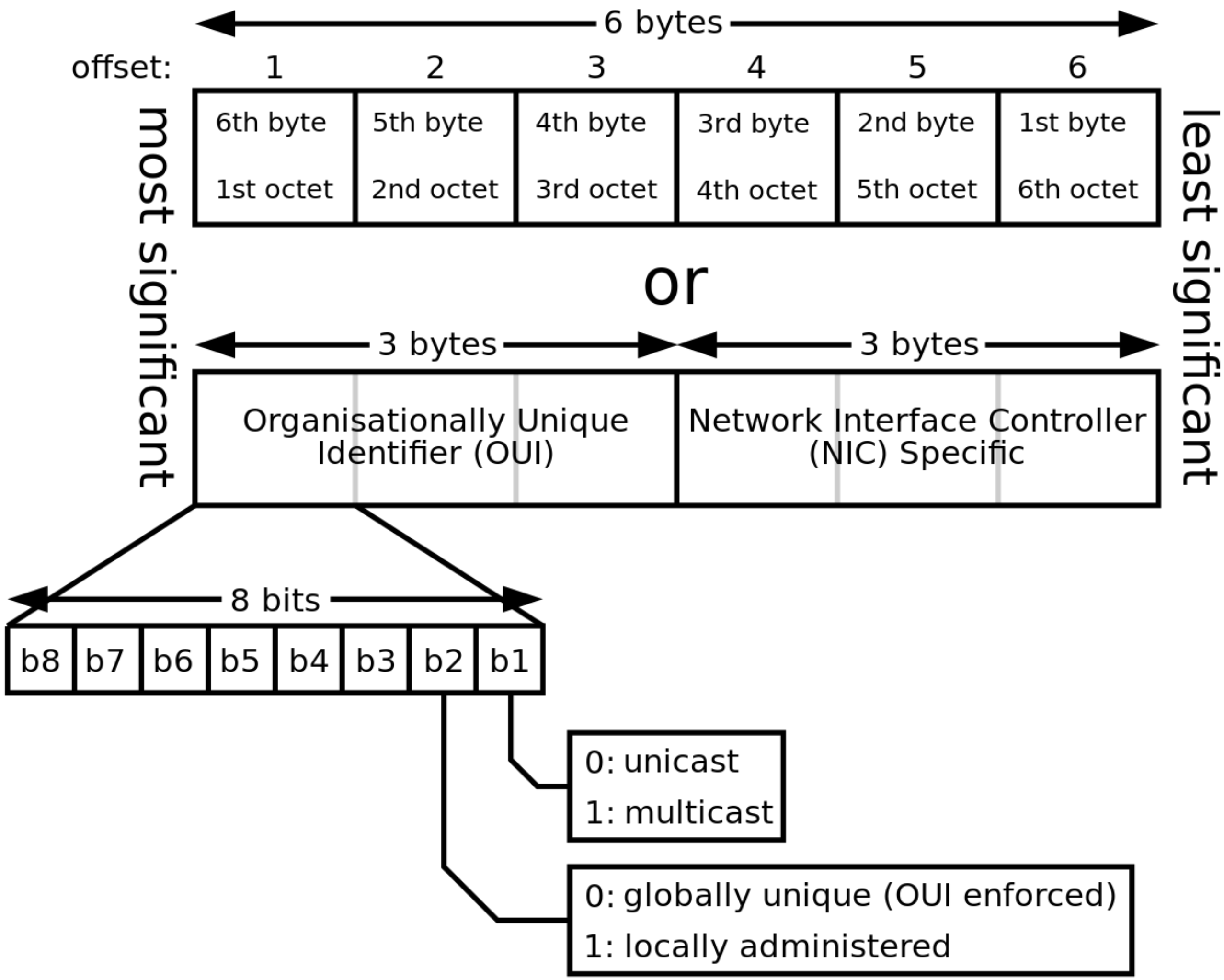
- Shared medium
- Speed
  - 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps, 40 Gbps, 100 Gbps
  - Autonegotiation
- **Duplexness**
  - Both half-duplex (CDMA/CS) and full-duplex
  - Auto-MDIX
- Cable systems – metallic (coax, twisted pair), optical
- Unreliable connectionless communication
- Power over Ethernet (PoE)

Ethernet Addressing

- 48-bits long **MAC address** burned to ROM of NIC
  - Each address should be unique (at least on the segment)
  - Flat address space assigned by IEEE



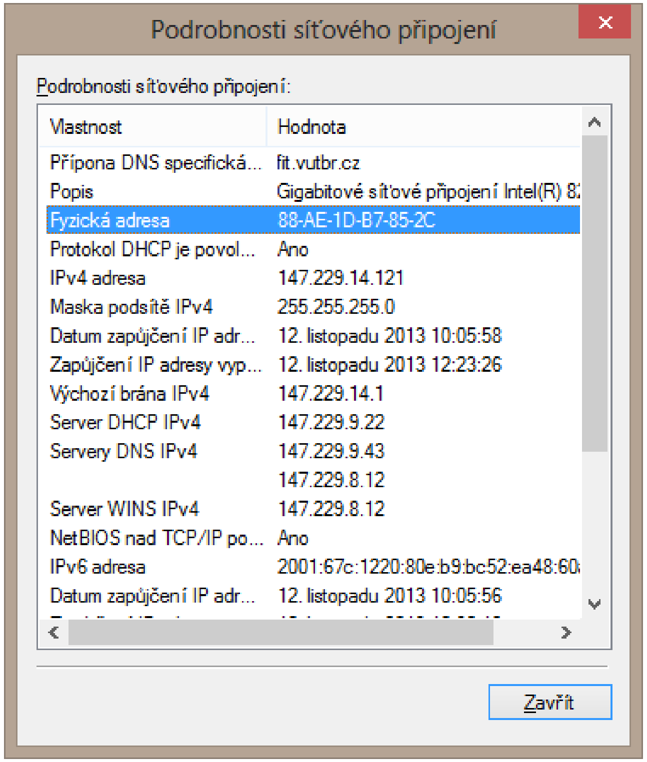
MAC Syntax



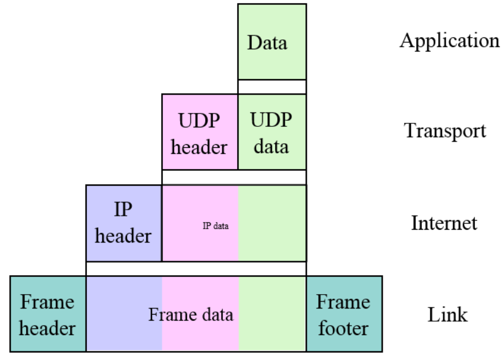
6 bytes
offset:
1
2
3
4
5
6
6th byte
1st octet
5th byte
2nd octet
4th byte
3rd octet
3rd byte
4th octet
2nd byte
5th octet
1st byte
6th octet
most significant
least significant
or
3 bytes
3 bytes
Organisationally Unique Identifier (OUI)
Network Interface Controller (NIC) Specific
8 bits
b8
b7
b6
b5
b4
b3
b2
b1
0: unicast
1: multicast
0: globally unique (OUI enforced)
1: locally administered

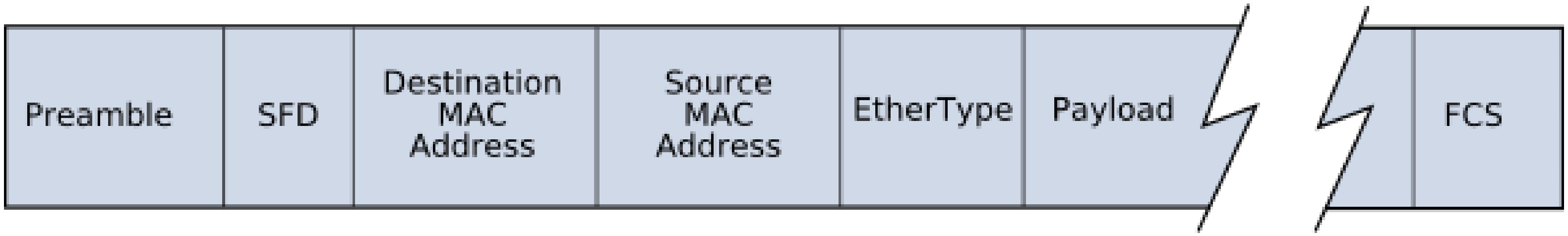
How to determine MAC address?

- Windows: `ipconfig /all`
- Linux: `ifconfig` or `ip a`
- http://www.wireshark.org/tools/oui-lookup.html



Ethernet Header





Ethernet

Field length, in bytes	7	1	6	6	2	46-1500	4
	Preamble	SOF	Destination address	Source address	Type	Data	FCS

IEEE 802.3

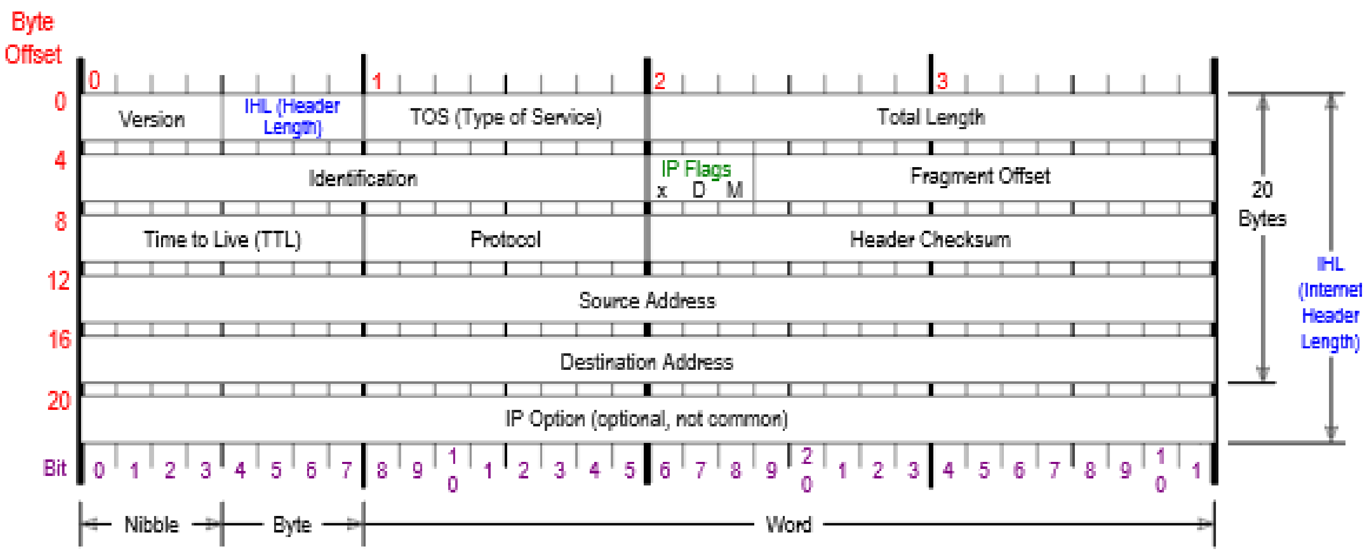
Field length, in bytes	7	1	6	6	2	46-1500	4
	Preamble	SOF	Destination address	Source address	Length	802.2 header and data	FCS

SOF = Start-of-frame delimiter
FCS = Frame check sequence

IPv4

- RFC 791 in 1981
- Connectionless
- IP packets exchanged on network layer
- No QoS (best-effort delivery)
  - QoS supported added later
    - IntServ
    - DiffServ

IPv4 Header



Version

Version of IP protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmentet, fragment size (Total Length) must me a multiple of 8 bytes.

IP Flags

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

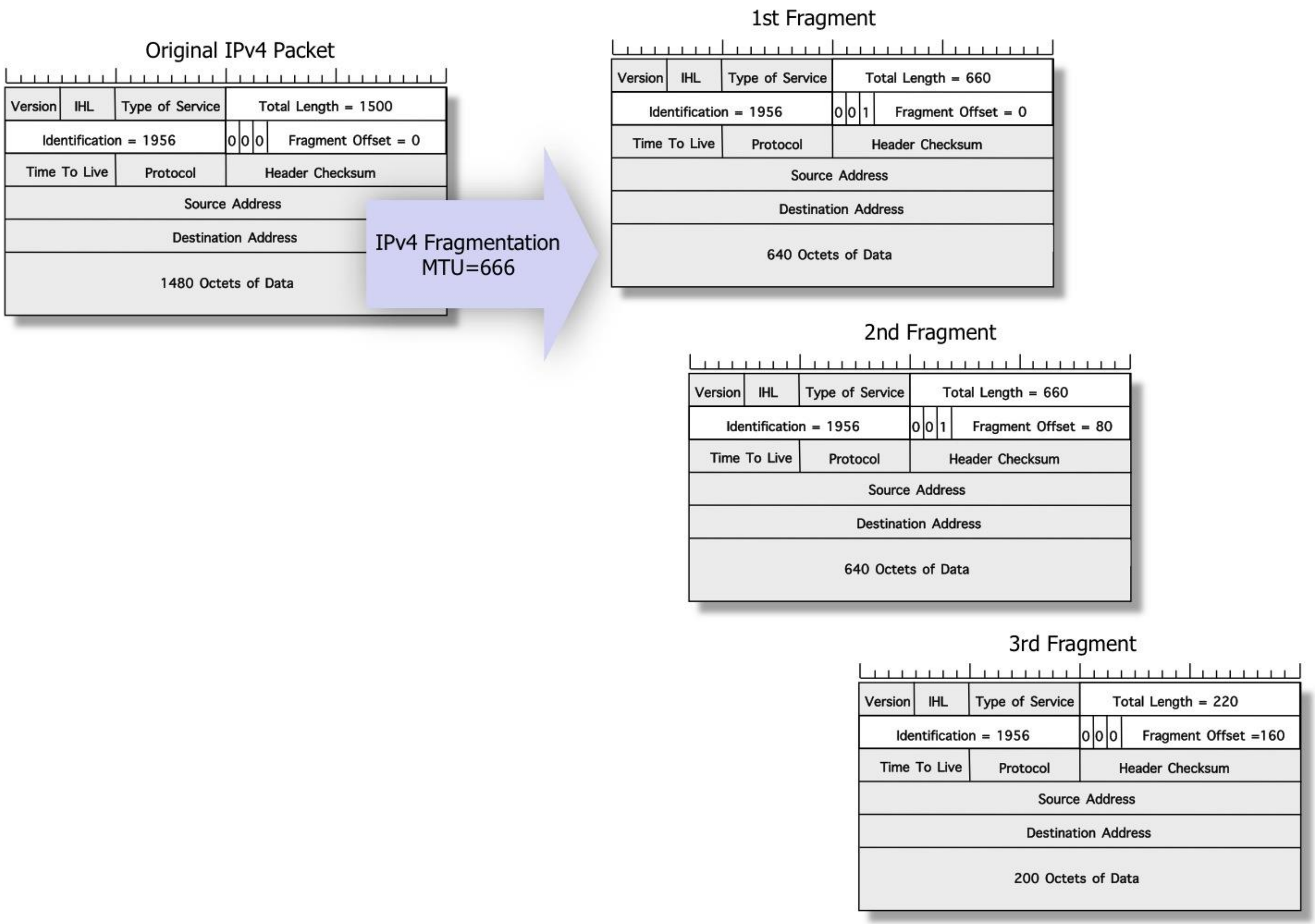
Header Checksum

Checksum of entire IP header.

RFC 791

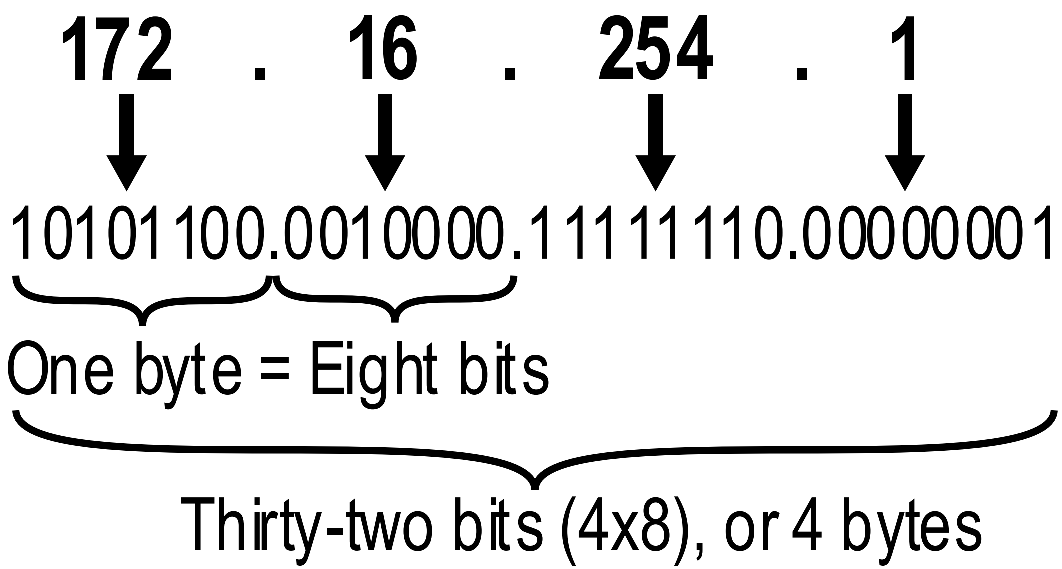
Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

IPv4 Fragmentation



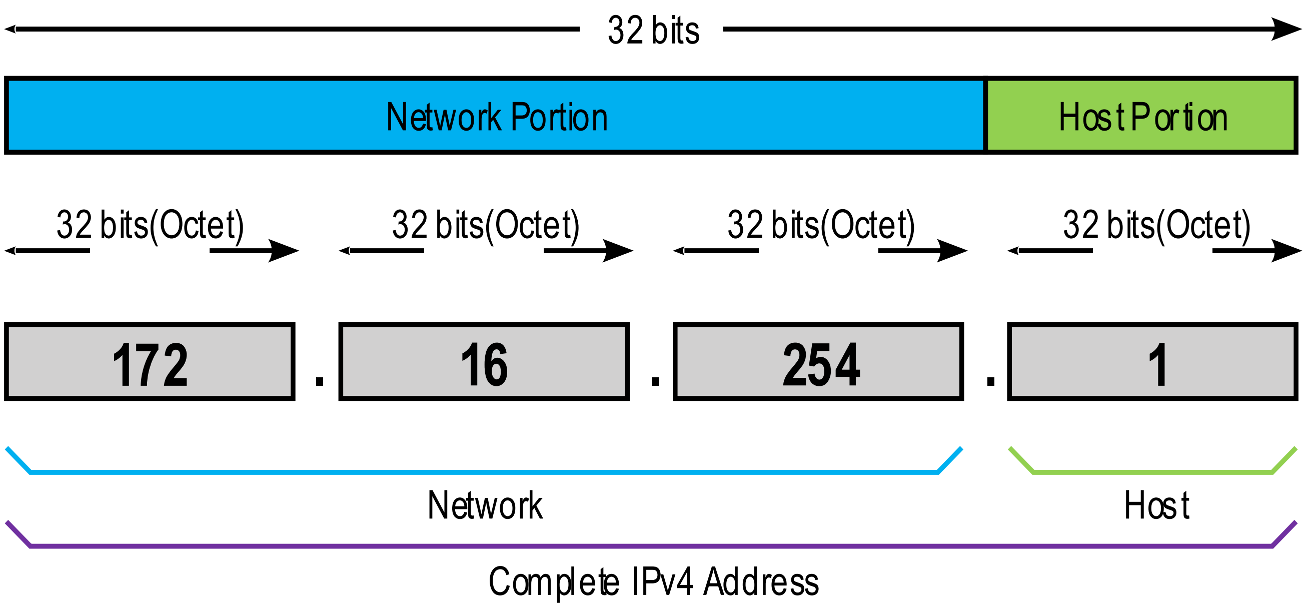
IPv4 Address

- IPv4 address is always 32-bits long
  - IPv4 address identifies NIC
  - binary vs. dotted-decimal form (e.g., 147.229.176.14)
  - $2^{32} - 2$ addresses available (first 0.0.0.0 and last 255.255.255.255 are reserved)



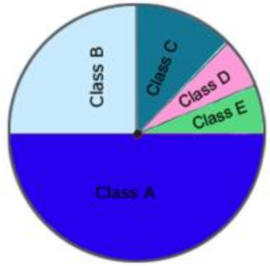
IPv4 Addressing

- Address consists of two parts:
  network identification (NetId) + host identification (HostId)
  - E.g., 147.229.0.0 as NetId and 0.0.176.14 as HostId



- *Where is the border between NetId and HostId?*
  - Classful addressing vs. Classless addressing

Classful



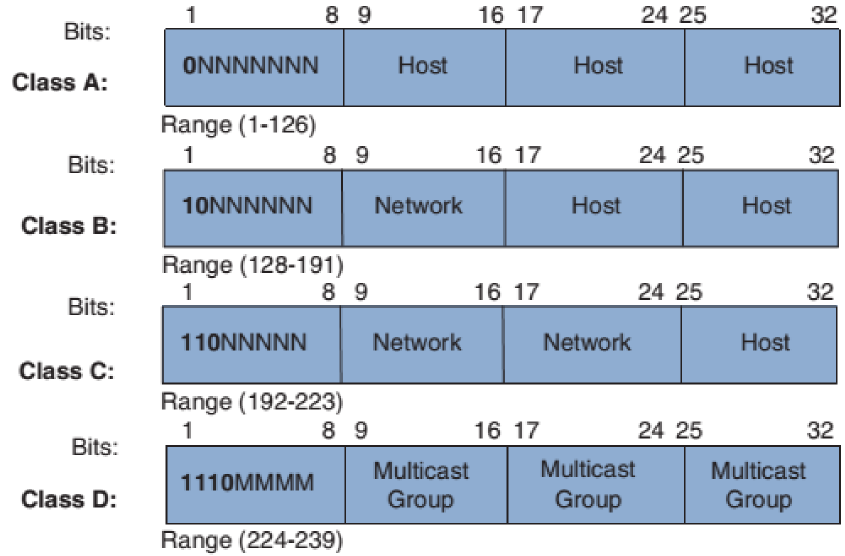
Class A: 2^{31} = 2,147,483,648 addresses, 50%

Class B: 2^{30} = 1,073,741,824 addresses, 25%

Class C: 2^{29} = 536,870,912 addresses, 12.5%

Class D: 2^{28} = 268,435,456 addresses, 6.25%

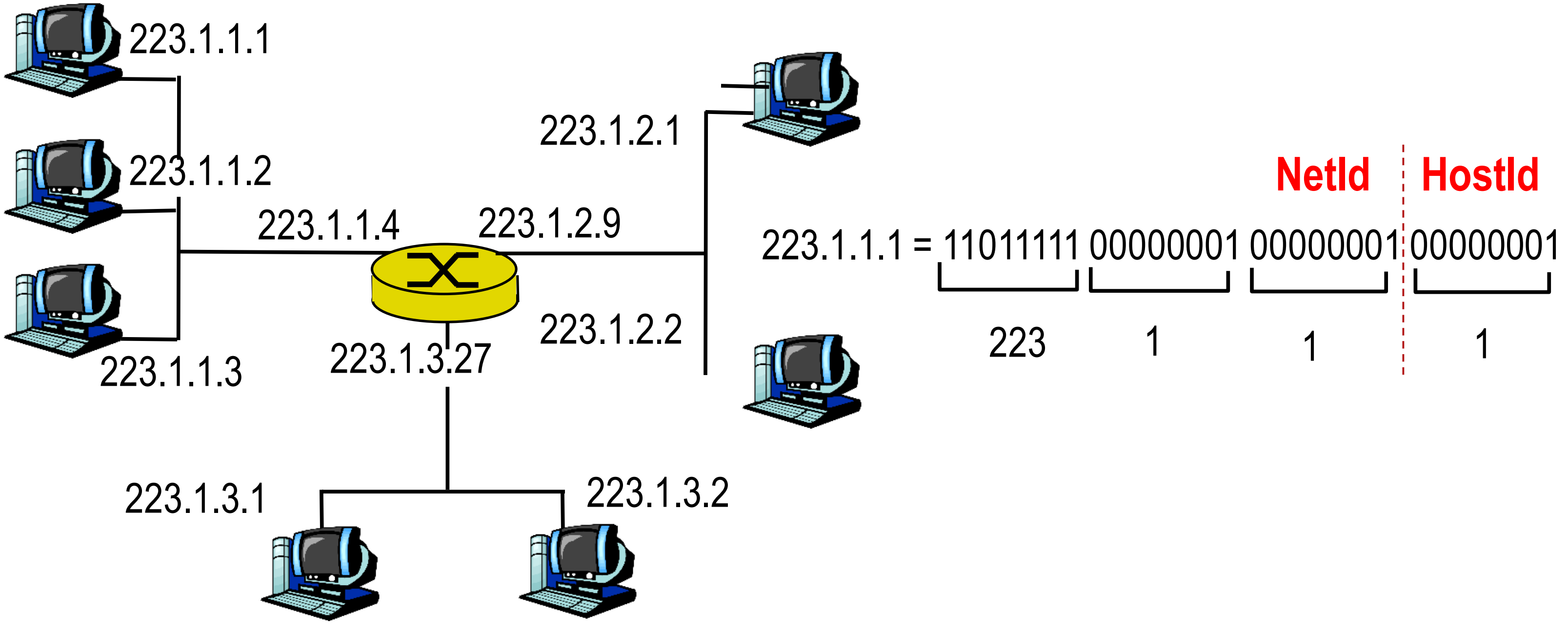
Class E: 2^{28} = 268,435,456 addresses, 6.25%



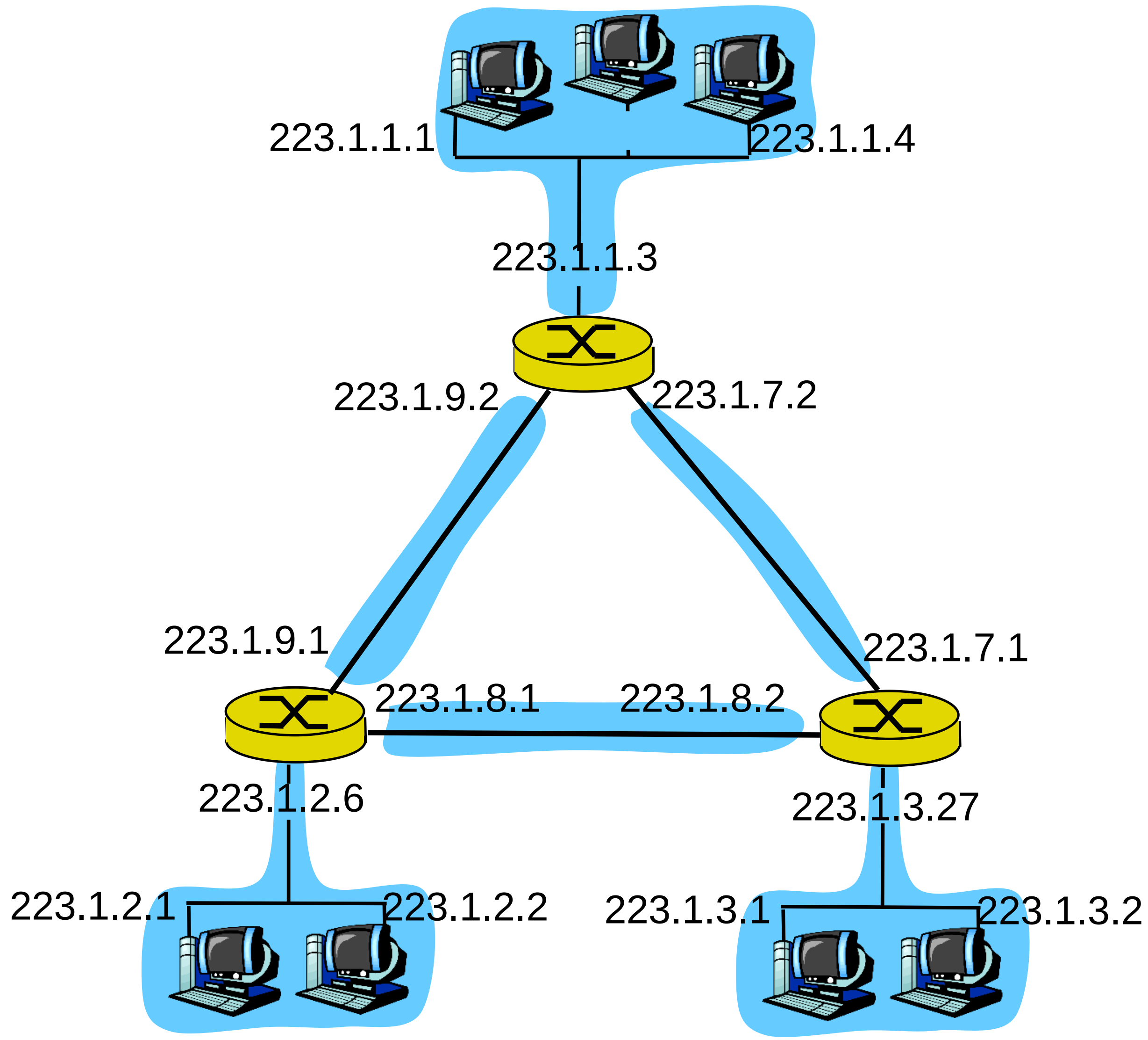
Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Total addresses in class	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	2,147,483,648 (2^{31})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	1,073,741,824 (2^{30})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	536,870,912 (2^{29})	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	268,435,456 (2^{28})	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	268,435,456 (2^{28})	240.0.0.0	255.255.255.255

Motivation behind NetId

- Each NIC has single IPv4 address
  - Host has usually one NIC
  - Router has usually two or more NICs
- *Is destination of packet in the same LAN or in another?*
  - Either local (within LAN using ARP) or remote (using default gateway)
  - Compare source and destination node's NetId
  - Nodes with the same NetId are within the same LAN



Class C Networks Example



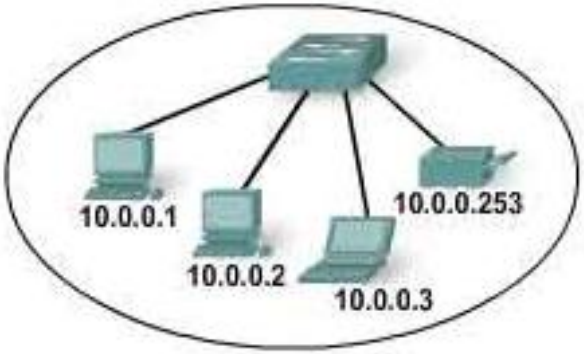
Special IPv4 Addresses

- IPv4Address := {NetId, HostId}
  - {NetId, all 0s} a.k.a. **network address**
    - address of a given network (cannot be assigned to NIC)
  - {NetId, all 1s}
    - **(Directed) broadcast address**
    - If packet is sent to this destination address then it is broadcasted to all nodes with the same NetId
  - {NetId, other}
    - Unicast address that may be assigned to node's NIC

- According to communication type
  - Unicast = most of Class A, B and C addresses
  - Broadcast = some of Class A, B and C addresses
  - Multicast = all Class D addresses

Special IPv4 Addresses

	Network			Host
Network Address	10	0	0	0
	00001010	00000000	00000000	00000000
Broadcast Address	10	0	0	255
	00001010	00000000	00000000	11111111
Host Address	10	0	0	1
	00001010	00000000	00000000	00000001



Classless

- Subnet mask
  - 32-bit long stream of consecutive 1s (NetId part) and 0s (HostId part)
  - *Address without mask does not make any sense!*

IP Address	192	168	48	247
Subnet Mask (binary)	1111 1111	1111 1111	1111 1111	0000 0000
Subnet Mask (dotted decimal)	255.	255.	255.	0

192.168.48.247

Network ID Host ID

- **Subnetting**
  - RFC 917, 950 in 1980s
  - Networks within class may have different subnet mask thus dividing one network into smaller portions of the same size
- **Variable Length Subnet Mask (VLSM)**
  - RFC 1009 in 1987
  - VLSM is extending network prefix (adding bits to NetId)
- **Classless Interdomain Routing (CIDR)**
  - RFC 1918 in 1996
  - Elimination of classes
  - CIDR aggregates addresses (reducing bits in NetId)

Subnet Mask Table

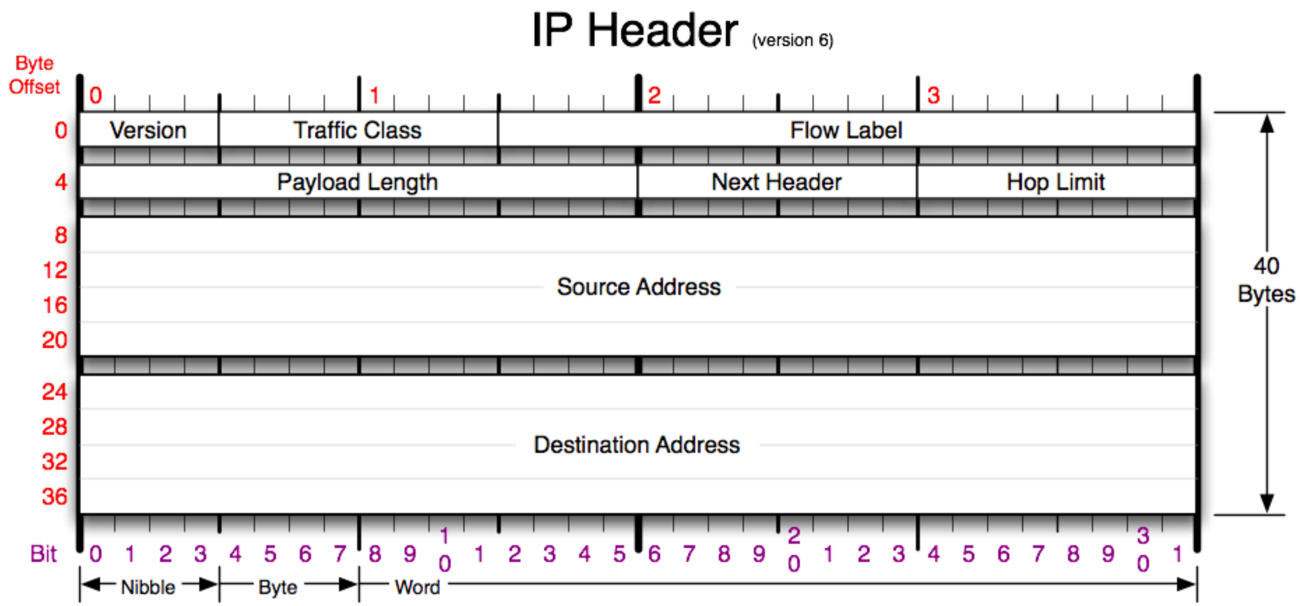
Class A Network (/8–/30) · Class B Network (/16–/30) · Class C Network (/24–/30)

			Subnets			Hosts		
/	Netmask	Block Size	Class A	Class B	Class C	Class A	Class B	Class C
8	255.0.0.0	256	1			16777214		
9	255.128.0.0	128	2			8388606		
10	255.192.0.0	64	4			4194302		
11	255.224.0.0	32	8			2097150		
12	255.240.0.0	16	16			1048574		
13	255.248.0.0	8	32			524286		
14	255.252.0.0	4	64			262142		
15	255.254.0.0	2	128			131070		
16	255.255.0.0	256	256	1		65534	65534	
17	255.255.128.0	128	512	2		32766	32766	
18	255.255.192.0	64	1024	4		16382	16382	
19	255.255.224.0	32	2048	8		8190	8190	
20	255.255.240.0	16	4096	16		4094	4094	
21	255.255.248.0	8	8192	32		2046	2046	
22	255.255.252.0	4	16384	64		1022	1022	
23	255.255.254.0	2	32768	128		510	510	
24	255.255.255.0	256	65536	256	1	254	254	254
25	255.255.255.128	128	131072	512	2	126	126	126
26	255.255.255.192	64	262144	1024	4	62	62	62
27	255.255.255.224	32	524288	2048	8	30	30	30
28	255.255.255.240	16	1048576	4096	16	14	14	14
29	255.255.255.248	8	2097152	8192	32	6	6	6
30	255.255.255.252	4	4194304	16384	64	2	2	2

IPv6

- Fragmentation done only on end-points
- Increased IPv6 MTU to 1280 B
- Path MTU Discovery for IPv6 (RFC 1981)
  - Leverages ICMPv6 packet too big to discover appropriate MTU
- 40 B long fixed length of the basic IPv4 header
  - Header processing does not require checksum recalculation
  - Extension headers carry optional information
- Broadcast communication not supported
  - Substituted with multicast address

IPv6 Header



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 6 structure only.

Traffic Class

8 bit traffic class field.

Flow Label

20 bit flow label.

Payload Length

16-bit unsigned integer. Length of the IPv6 payload, i.e., the rest of the packet following this IPv6 header, in octets. Any extension headers are considered part of the payload.

Source Address

128-bit address of the originator of the packet.

Next Header

8-bit selector. Identifies the type of header immediately following the IPv6 header. Uses the same values as the IPv4 Protocol field.

Destination Address

128-bit address of the intended recipient of the packet (possibly not the ultimate recipient, if a Routing header is present).

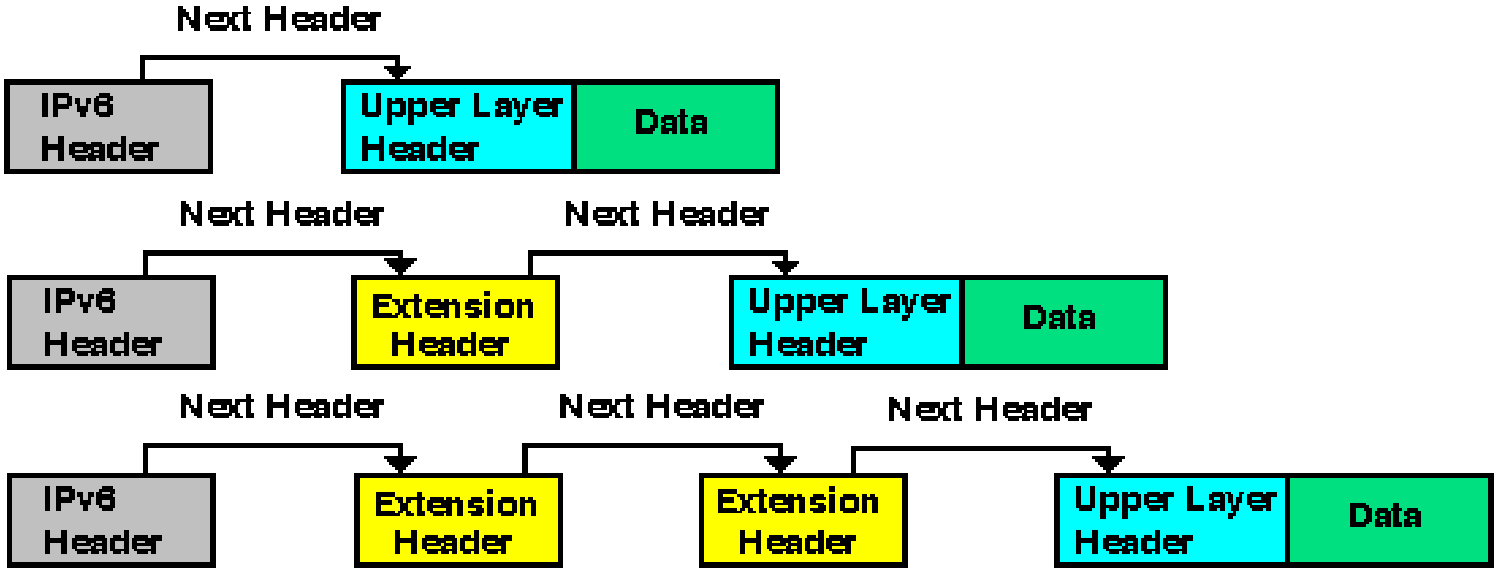
Hop Limit

8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero.

RFC 2460

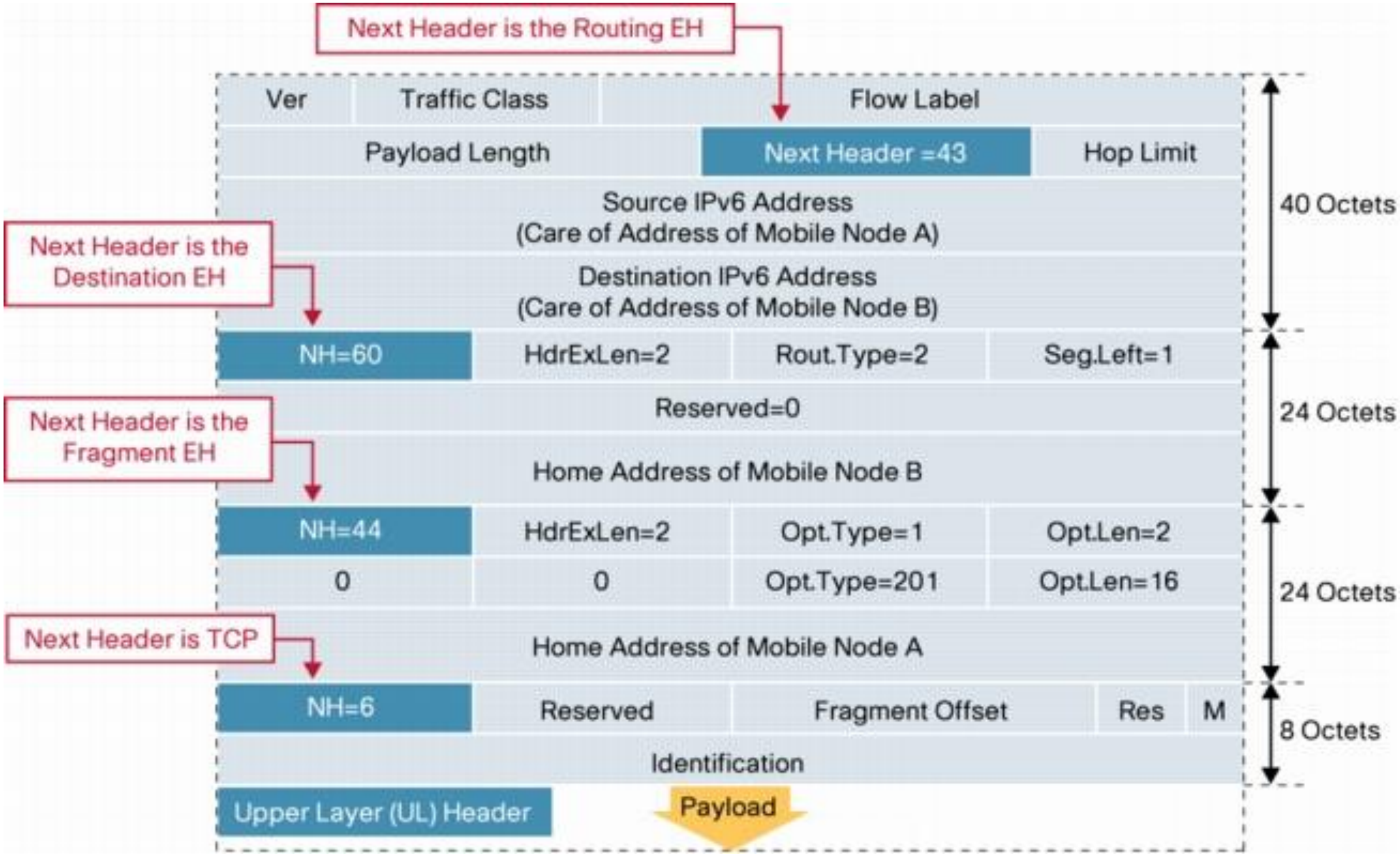
Please refer to RFC 2460 for the complete Internet Protocol version 6 (IPv6) Specification.

Extension Headers



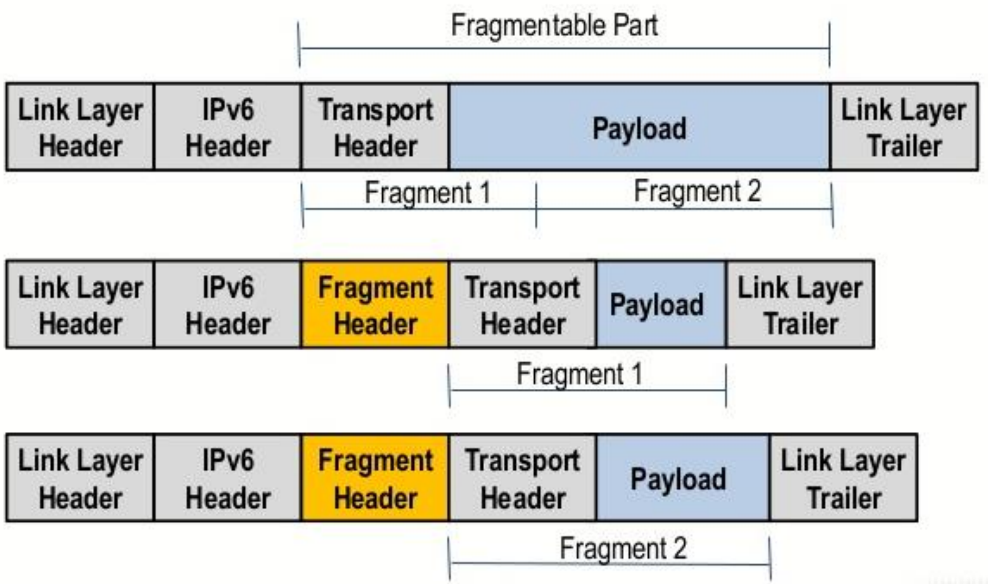
- Append themselves after the basic IPv6 header
  - Types
    - Hop-by-hop (Next header=0), Destination options (Next header=60), Routing (Next header=43), Fragment (Next header=44)
    - Authentication (AH) (Next header=51), Encapsulating Security Payload (ESP) (Next header=50)
    - No next header (Next header=59)
    - TCP/IP protocols (TCP=6; UDP=17; OSPF=89)
- Each extension header contains type of the next header, length and data

Extension Header Example



IPv6 Fragmentation

- Minimum link MTU for IPv6 is 1280B (vs. 68B for IPv4).
  - On links with MTU < 1280, link-specific fragmentation and reassembly must be used
  - IPv6 routers do not implement packet fragmentation
  - `IF` fragmentation is necessary `THEN` end node does it
- Implementations are expected to perform **path MTU discovery (PMTUD)** to send packets bigger than 1280
  - Destination is checked periodically every 10 minutes
- A hop-by-hop option supports transmission of **jumbograms** with up to 2^{32} octets of payload



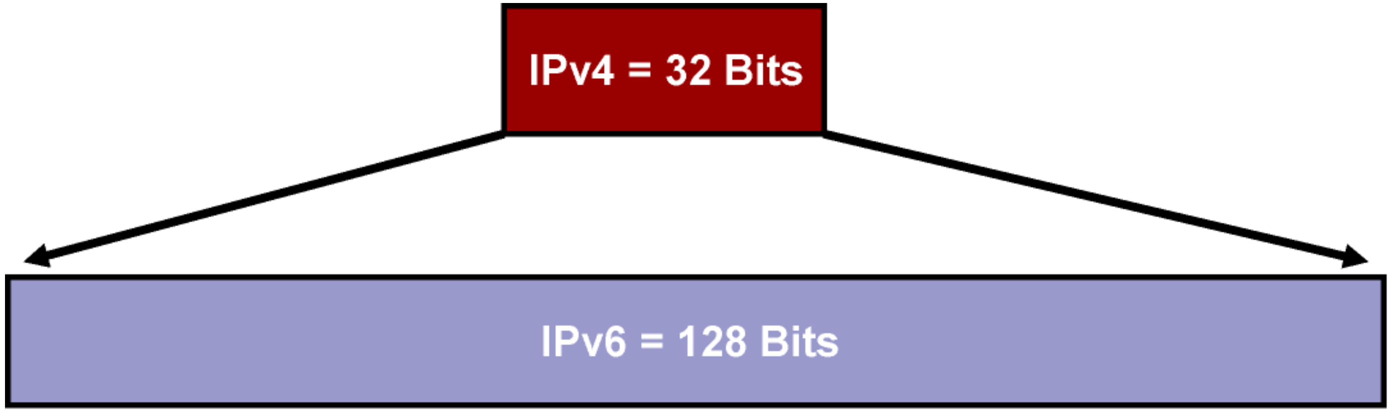
Larger Address Space

IPv4

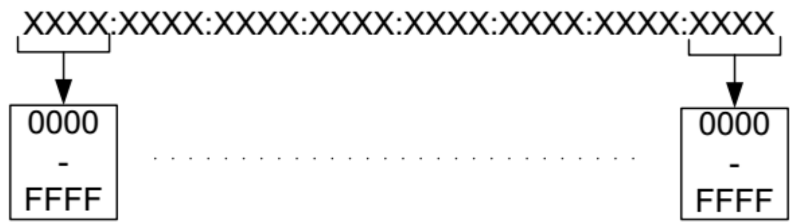
- 32 bits or 4 bytes long
  - 4,200,000,000 possible addressable nodes

IPv6

- 128 bits or 16 bytes: four times the bits of IPv4
  - 3.4 * 10^{38} possible addressable nodes
  - 340,282,366,920,938,463,374,607,432,768,211,456
  - 5 * 10^{28} addresses per person



IPv6 Address



- $x:x:x:x:x:x:x:x$, where x is a 16-bit hexadecimal field
- Leading zeros in a field are optional:
  - 2031:0:130f:0:0:9c0:876a:130b
- Only once per address successive fields of 0 can be represented as ::

2031:0000:130f:0000:0000:09c0:876a:130b

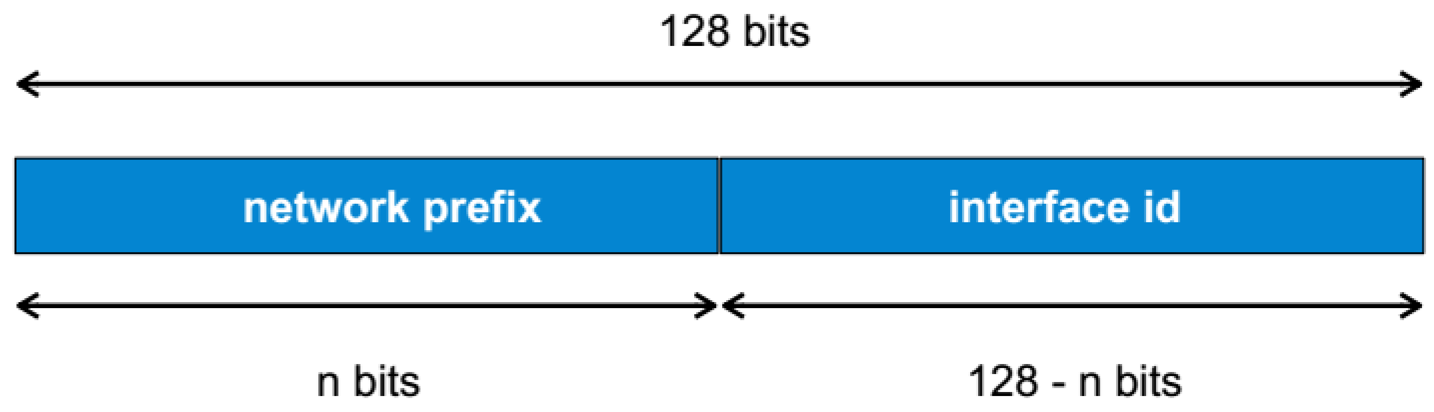
2031:0:130f::9c0:876a:130b

ff01:0:0:0:0:0:0:1 >>> ff01::1

0:0:0:0:0:0:0:1 >>> ::1

0:0:0:0:0:0:0:0 >>> ::

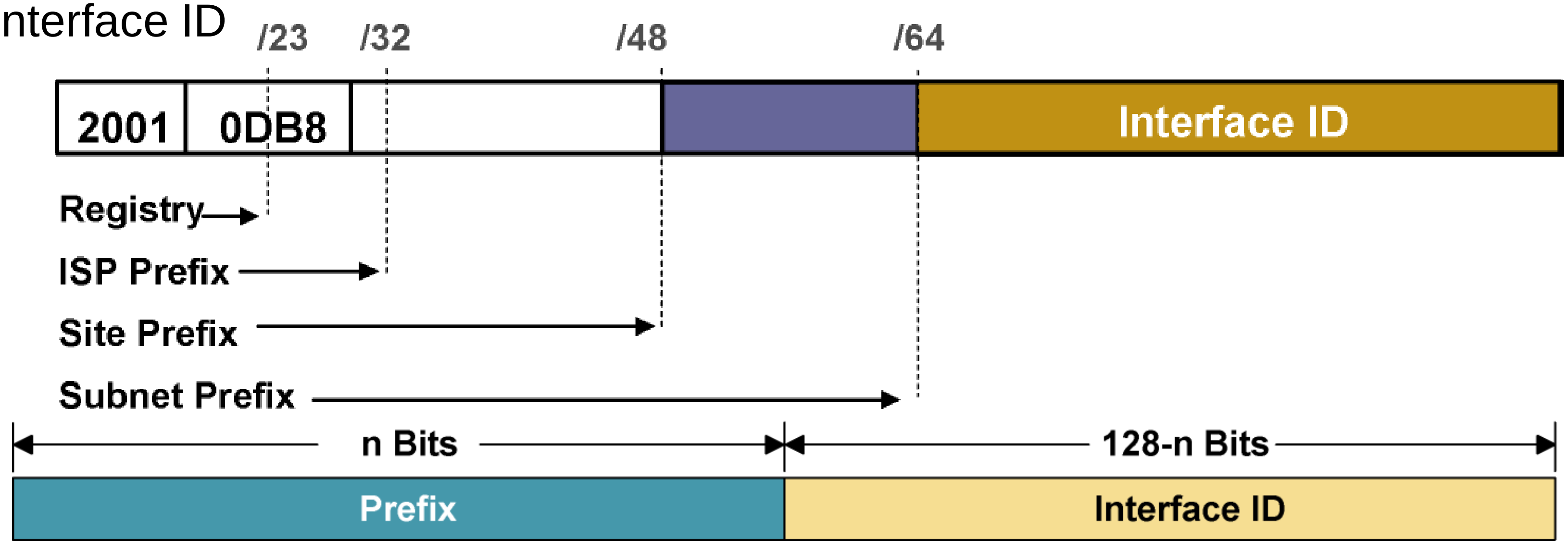
Addressed Overview



- As described in RFC 4291:
  - **::/128** Not specified address
  - **::0/0** Default-gateway
  - **::1/128** Loopback
  - **ff00::/8** Multicast
  - **fe80::/10** Link-Local Unicast
  - **fc00::/7** Unique Local Unicast, RFC 4193
  - **::A.B.C.D** IPv4-compatible addresses (not recommended)
  - **::ffff:A.B.C.D** IPv4-mapped address
  - All others Global Unicast

Global Unicast and Anycast

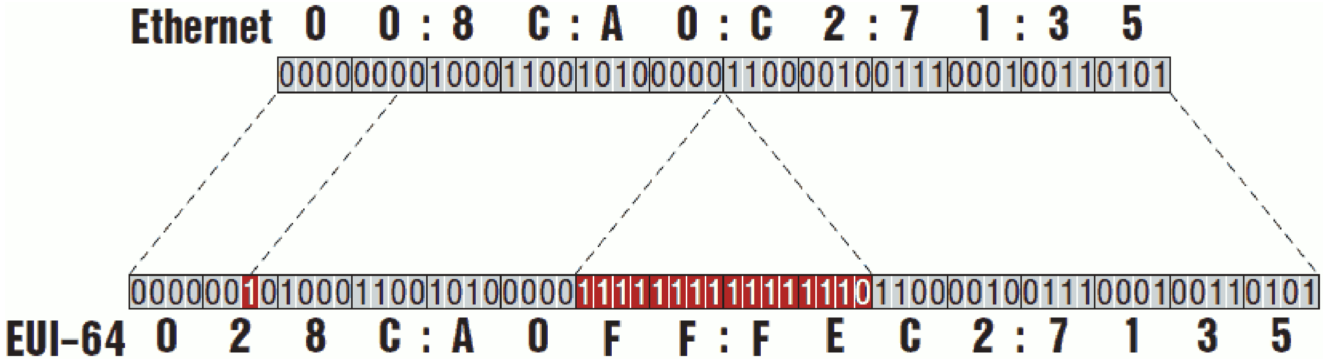
- Global Unicast and Anycast addresses have the same format
- **Global Unicast address**
  - Global Routing Prefix (Registry + ISP pref + site pref)
    - Global Unicast address with network prefix /48 is usually assigned
    - Allows reasonable aggregation
  - Subnet ID (a.k.a. Subnet prefix)
  - Interface ID



- An IPv6 **anycast address** is a global unicast address that is assigned to more than one interface

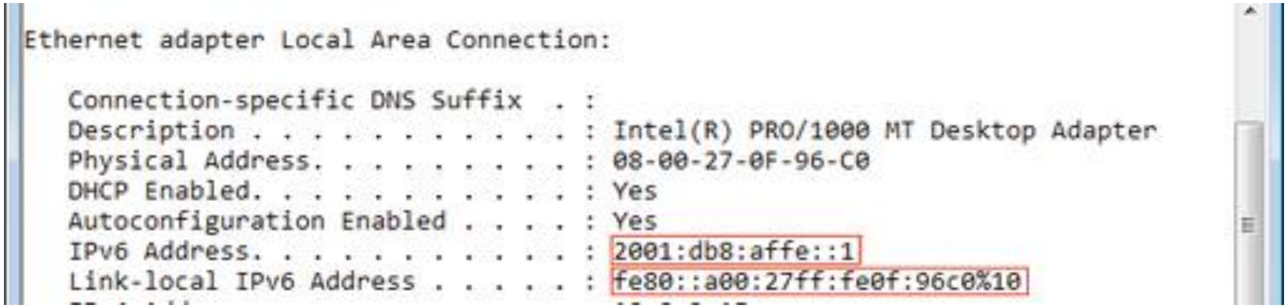
EUI-64 Interface ID

- Cisco uses the extended universal identifier EUI-64 format to do stateless autoconfiguration (SLAAC)
  - Modified EUI-64 is 64bits long and is used as Interface ID
- Modified EUI-64 expands the 48-bit MAC to 64 bits by:
  1. Inserting two bytes FF:FE between OUI and S/N
  2. The universal/local bit is inverted

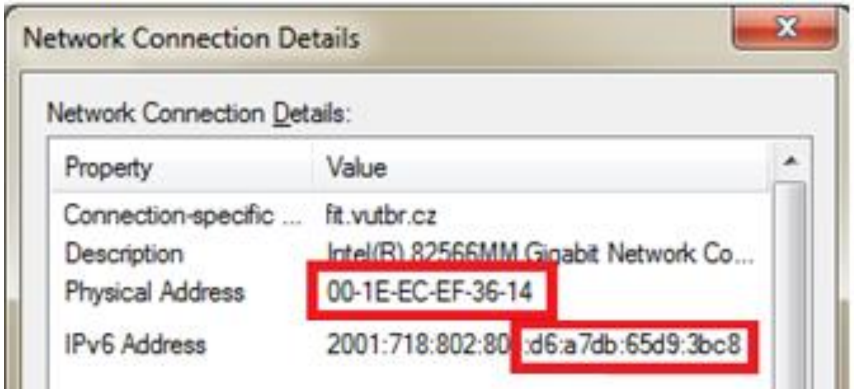


Interface ID Example

- Interface ID could be generated using
  - EUI-64

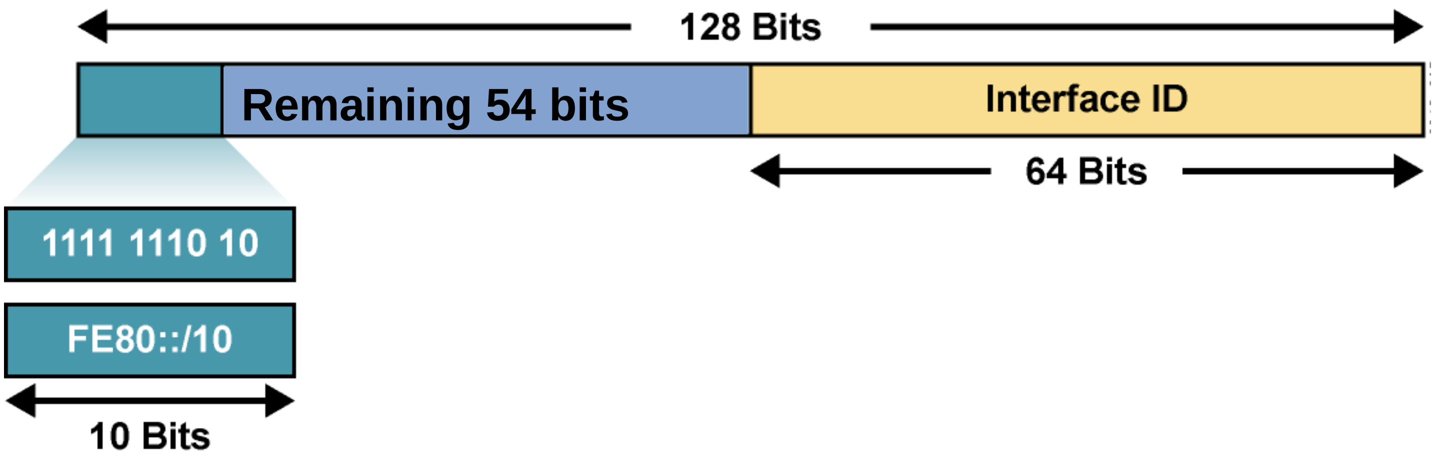


  - Privacy Extension



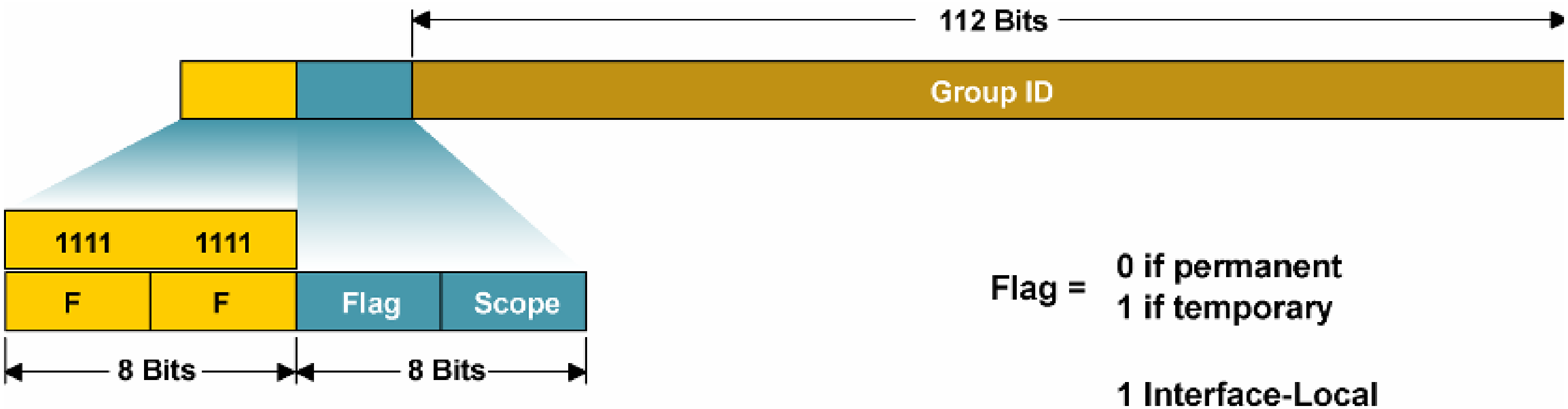
  - CGA

Link-Local Address



- **Link-local address** has specific FE80::/10, random 54 bits (usually zero) and Interface ID in EUI-64 format or created by Privacy extensions
- Mandatory address for communication between two IPv6 devices
- Automatically assigned by router as soon as IPv6 is enabled
- Also used for next-hop calculation in routing protocols
- Unique and valid only in one broadcast domain
- Remaining 54 bits could be zero or any manual configured value

IPv6 Multicast Addresses



Flag = 0 if permanent
1 if temporary

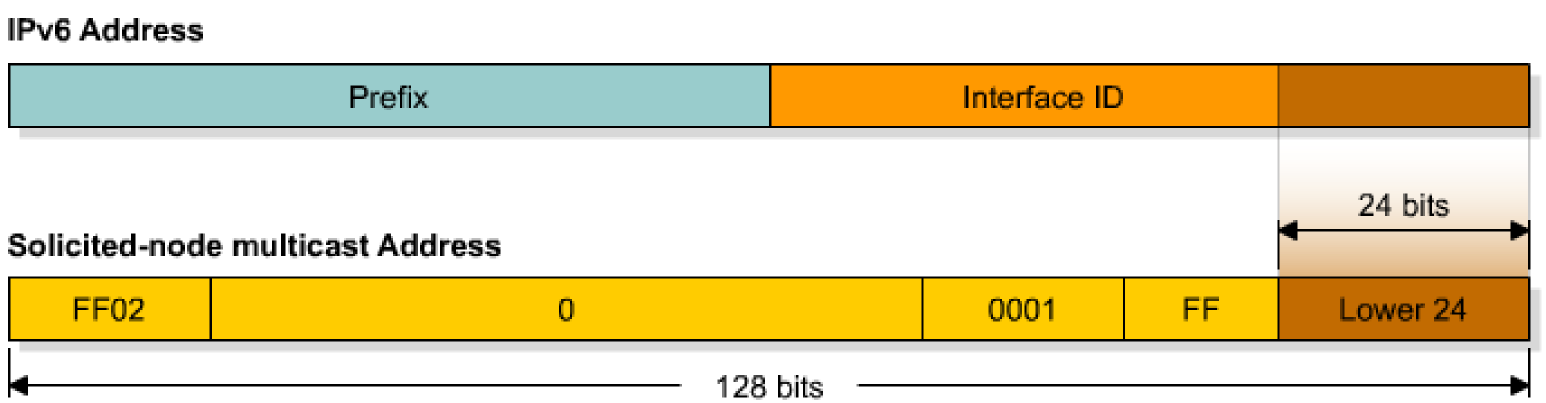
Scope = 1 Interface-Local
2 Link-Local
3 Subnet-Local
4 Admin-Local
5 Site-Local
8 Organization
E Global

- **Multicast address** is frequently used
  - Replaces broadcast
  - Has prefix FF00::/8

	Meaning
FF02::1	All nodes
FF02::2	All routers
FF02::9	All RIP routers
FF02::1:FFXX:XXXX	Solicited-node

Solicited-Node Multicast Address

- **Solicited-node multicast address** consists of prefix FF02::1:FF:/104 + lower 24 bits corresponding unicast or anycast address of the node
- Used by ICMPv6
  - ICMPv6 is encapsulated in IPv6 packet, Solicited-Node address is used as destination IPv6 address
- Address with link-local scope

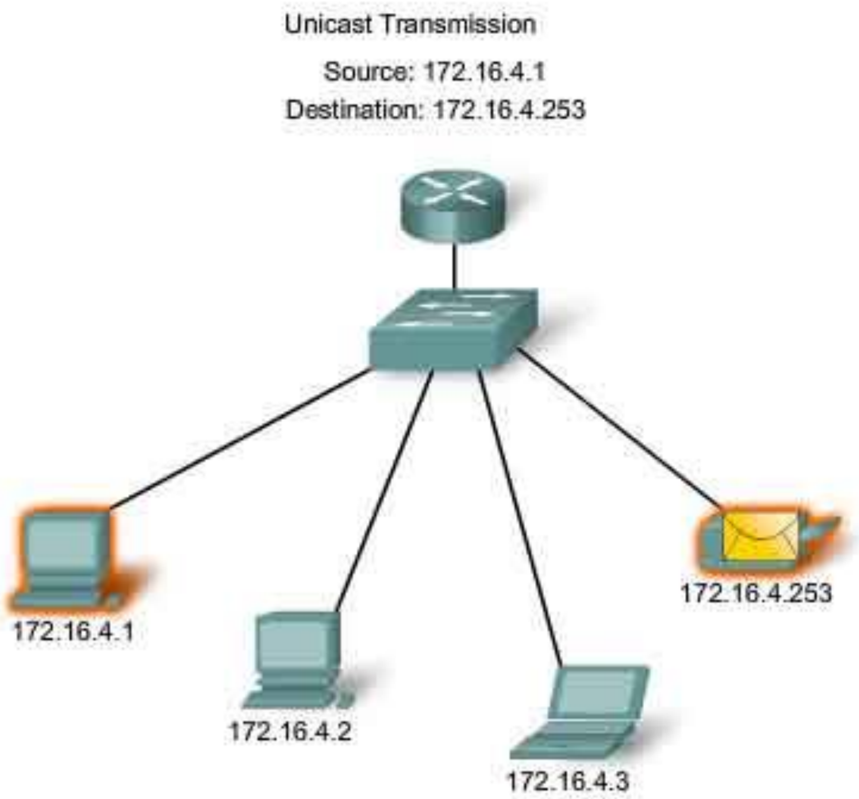


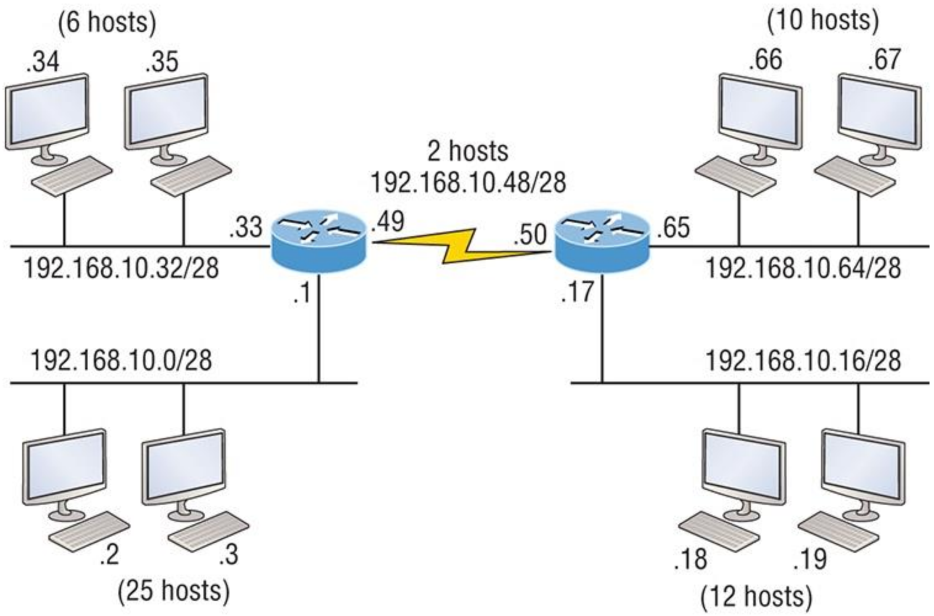
Packet Traversal

Terms

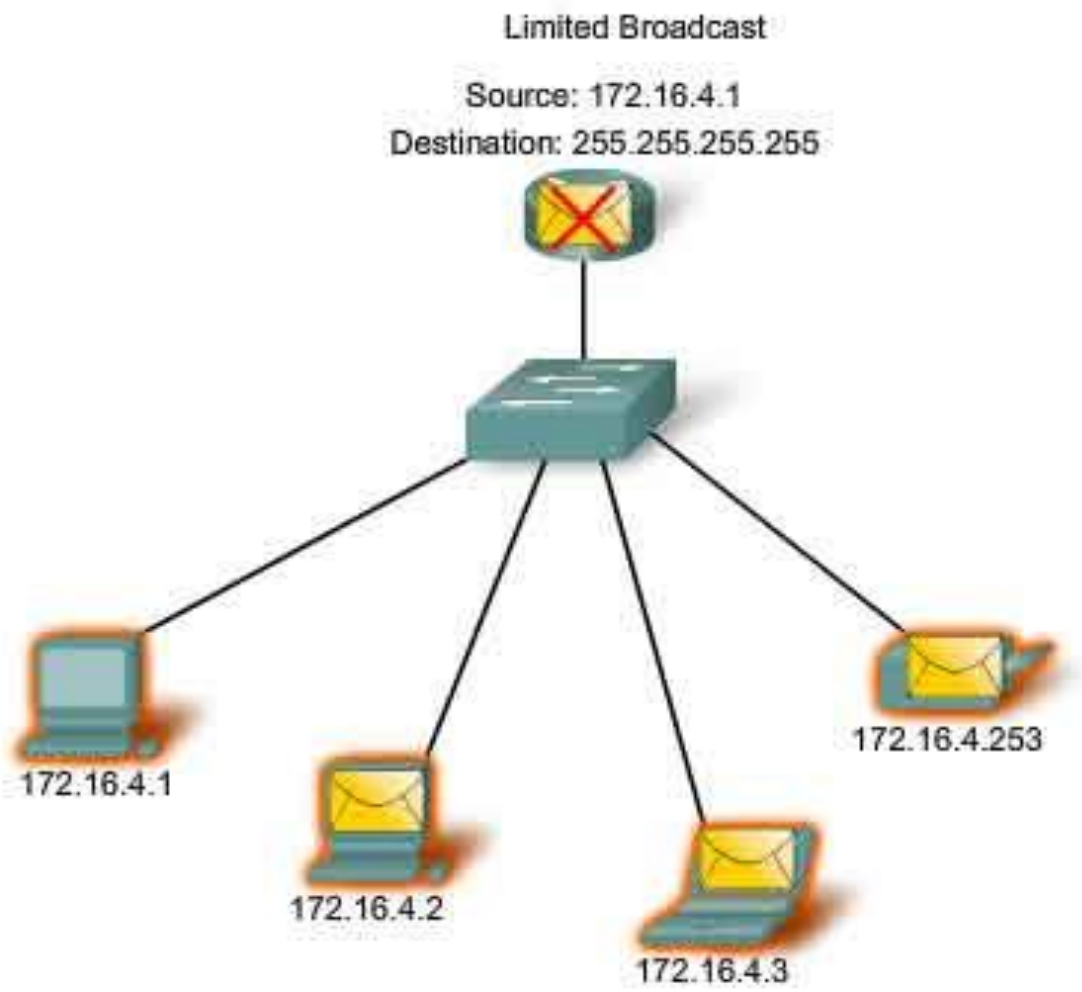
- Adjacent devices
  - on the same line/wire
  - on the same link
- Hop-by-hop
  - one TTL/hop away
- End-to-end
  - endpoints $\{0, n\}$ hops away

IPv4/v6 Unicast

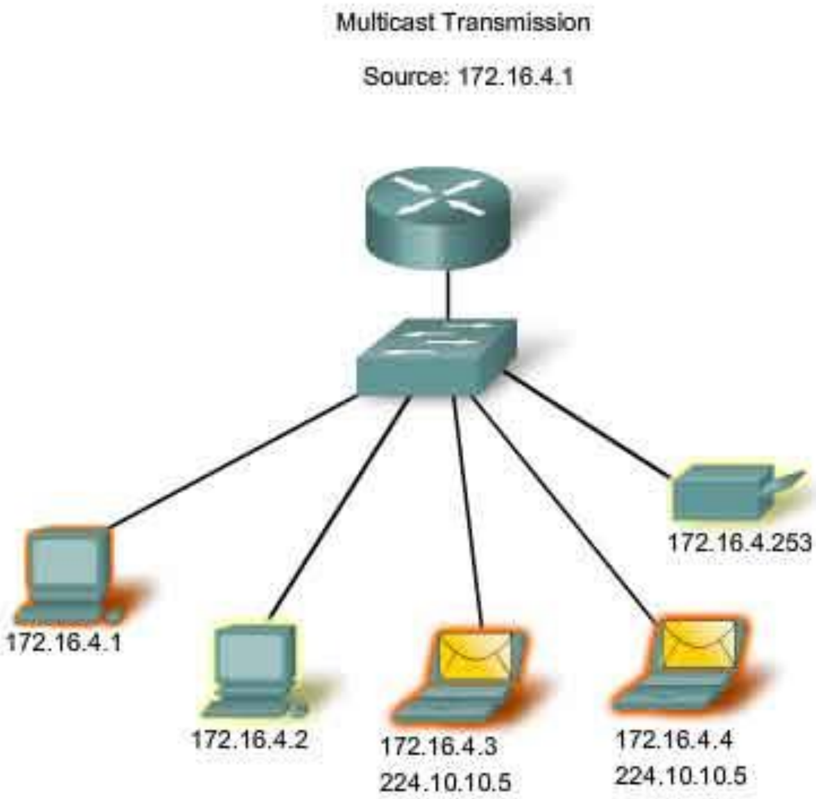


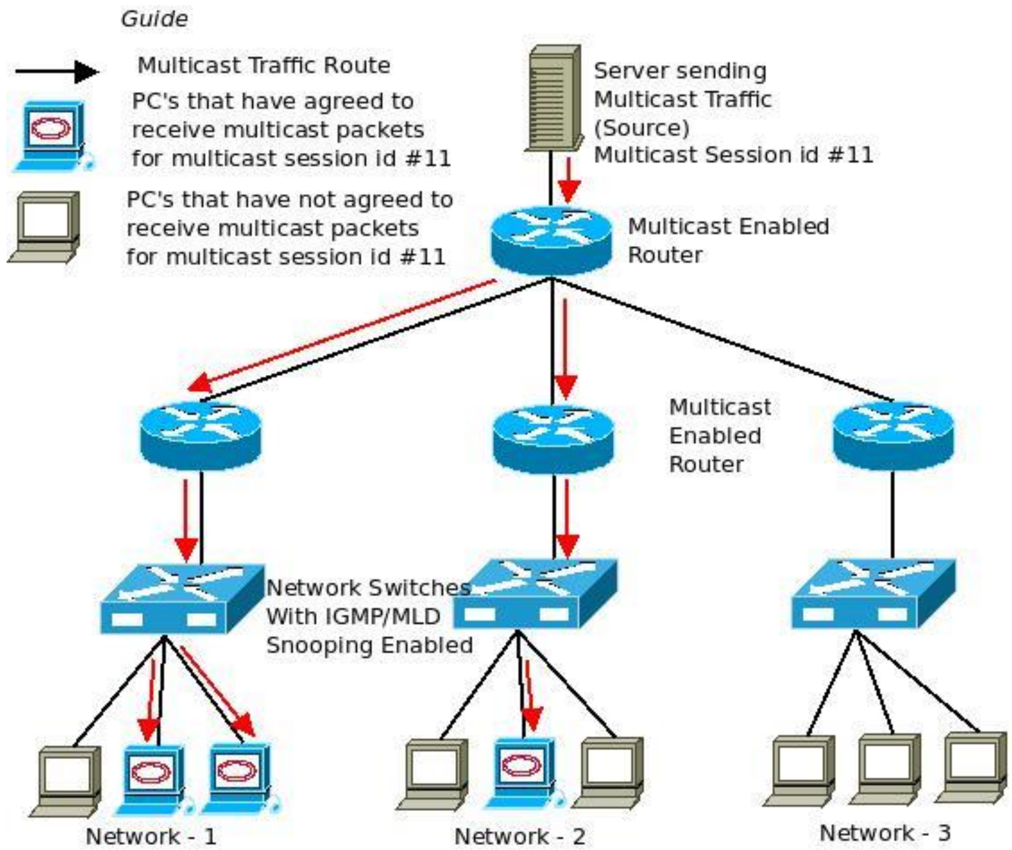


IPv4 Broadcast

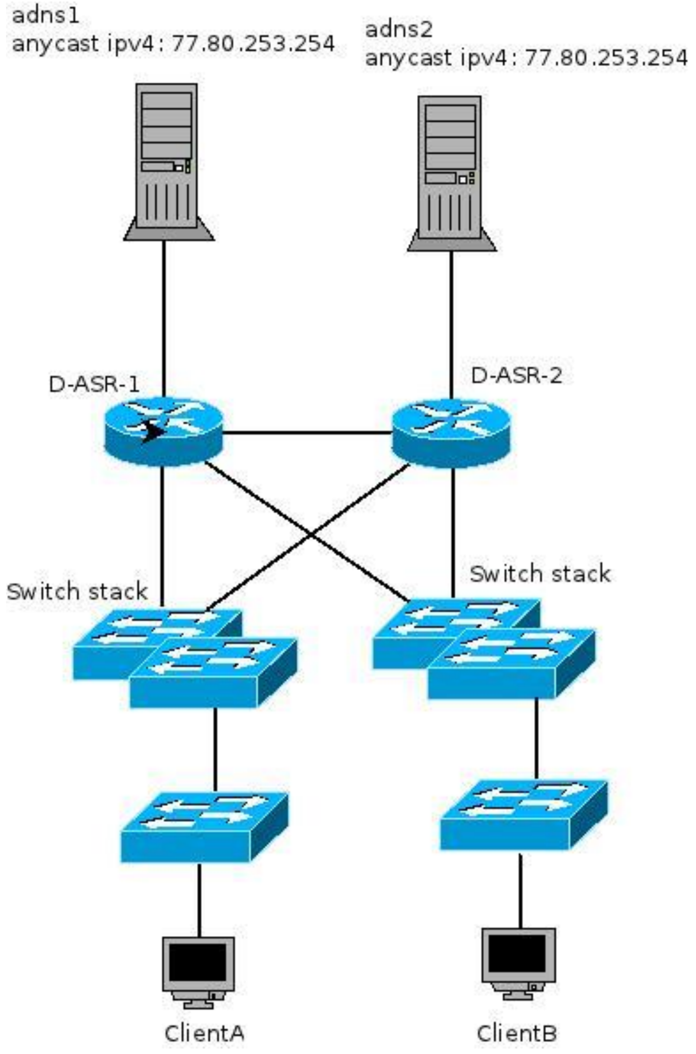


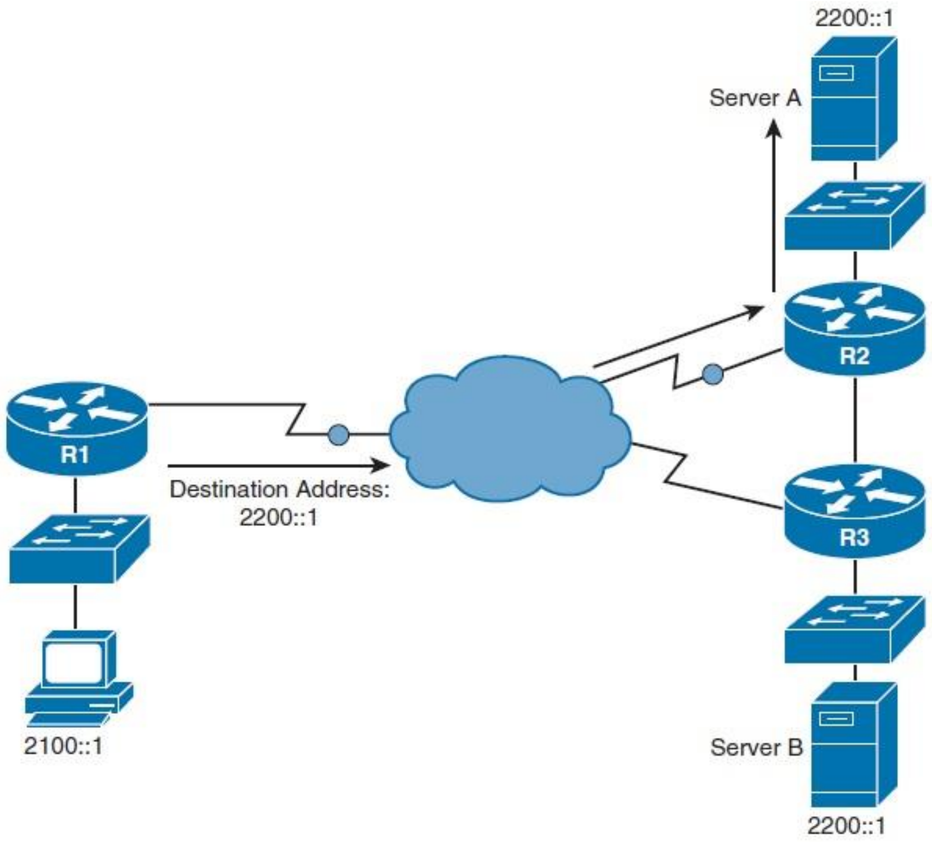
IPv4/v6 Multicast



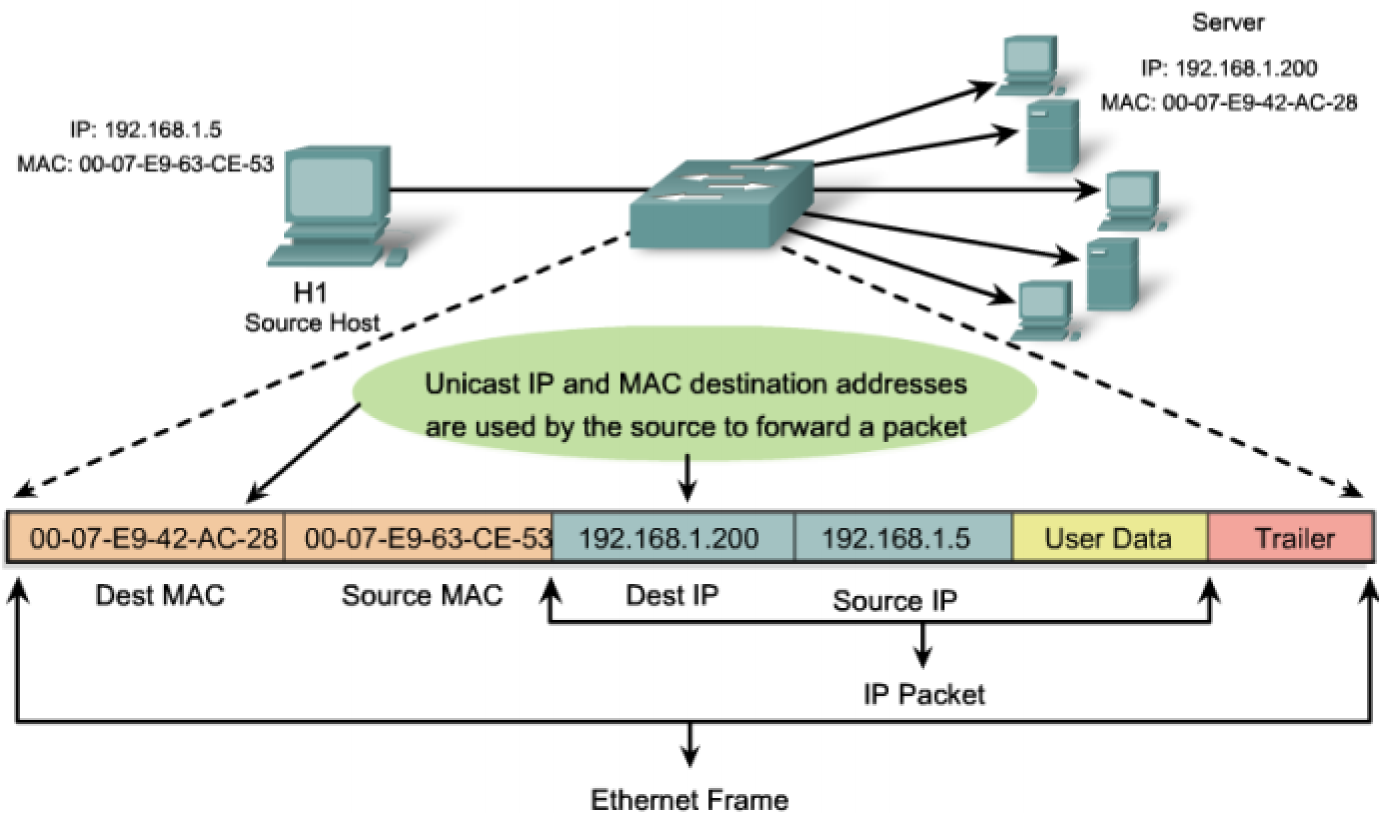


IPv4/6 Anycast

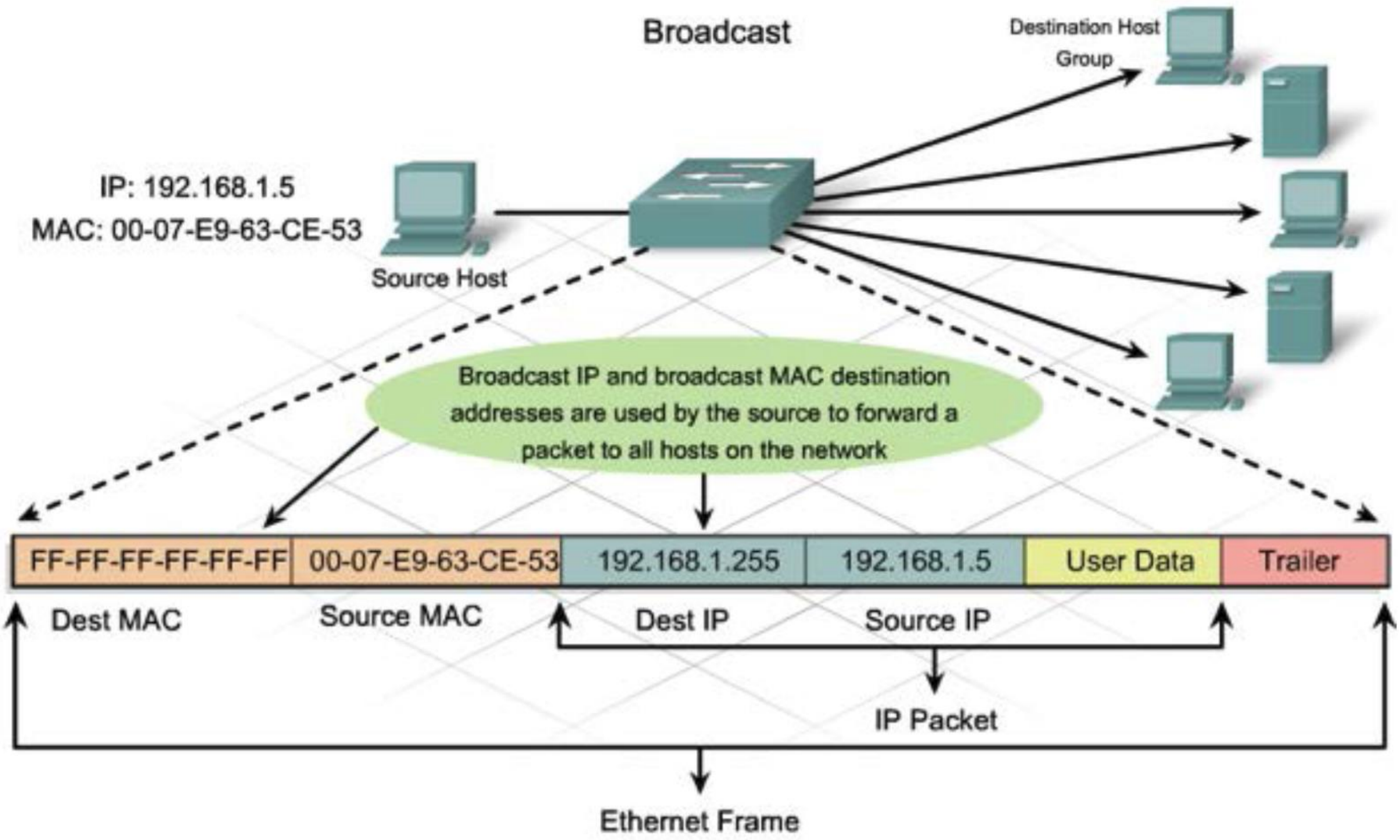




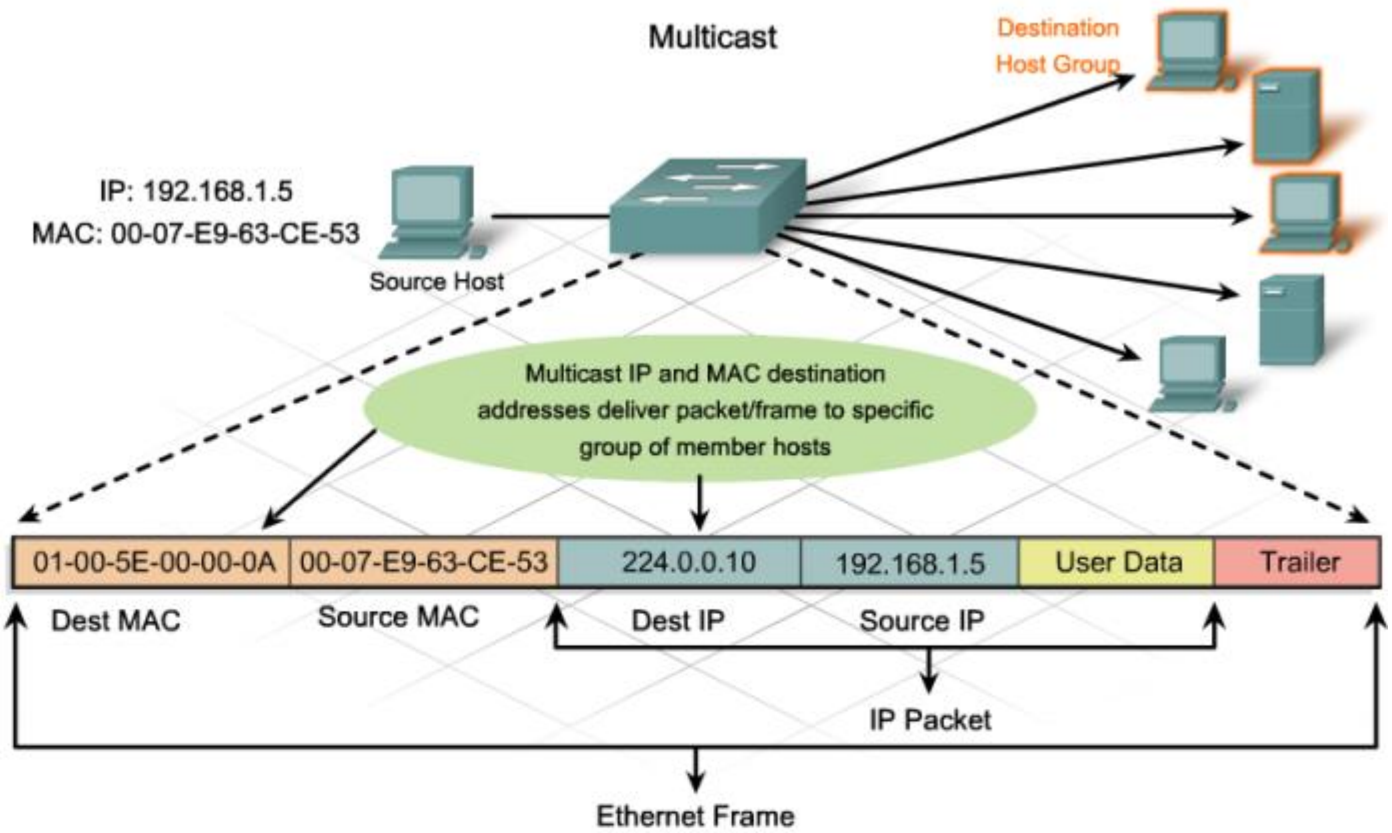
Ethernet Unicast



Ethernet Broadcast



Ethernet Multicast



Layer 2 – Layer 3 Binding

- *Host knows.*
  - IP address assigned by administrator
- *Host does not know.*
  - MAC address assigned by manufacturer

- Glue between Layer 2 and Layer 3 addresses
  - ARP is for IPv4 to Ethernet MAC resolution
  - ND is for IPv6 to Ethernet MAC resolution

- When PDU are being encapsulated, host can’t leave destination MAC address field blank.
- Each IP-to-MAC binding stored in local cache

Address Resolution Protocol

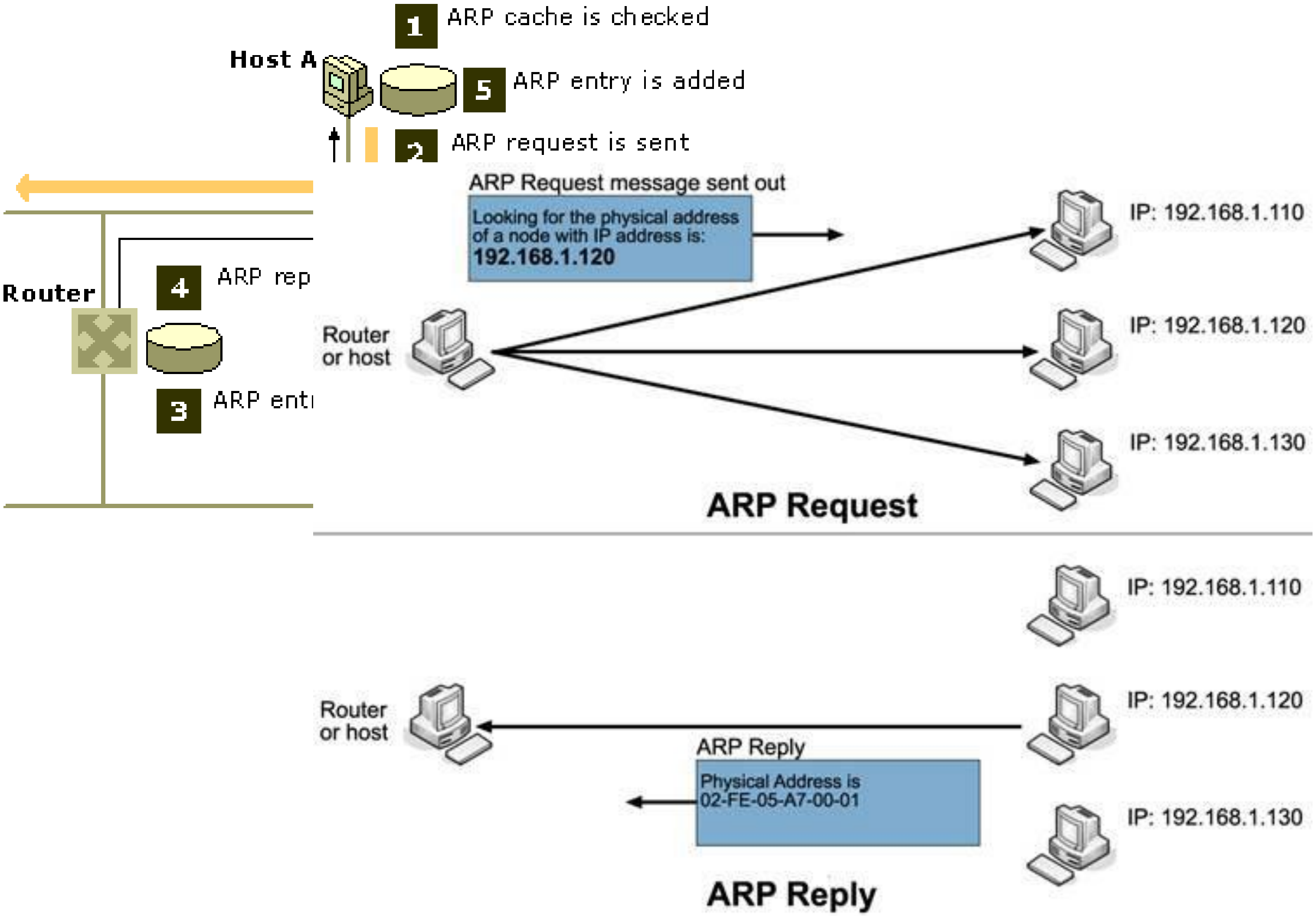
- RFC826
- Whenever IPv4-to-MAC binding is missing, ARP exchange occurs
- Layer 2.5 protocol
  - Encapsulated directly into Ethernet frame
- Simple request-response protocol
  - Although, ARP allows unsolicited responses

- *TCP/IPv4 stack cannot work without ARP!*

ARP Header

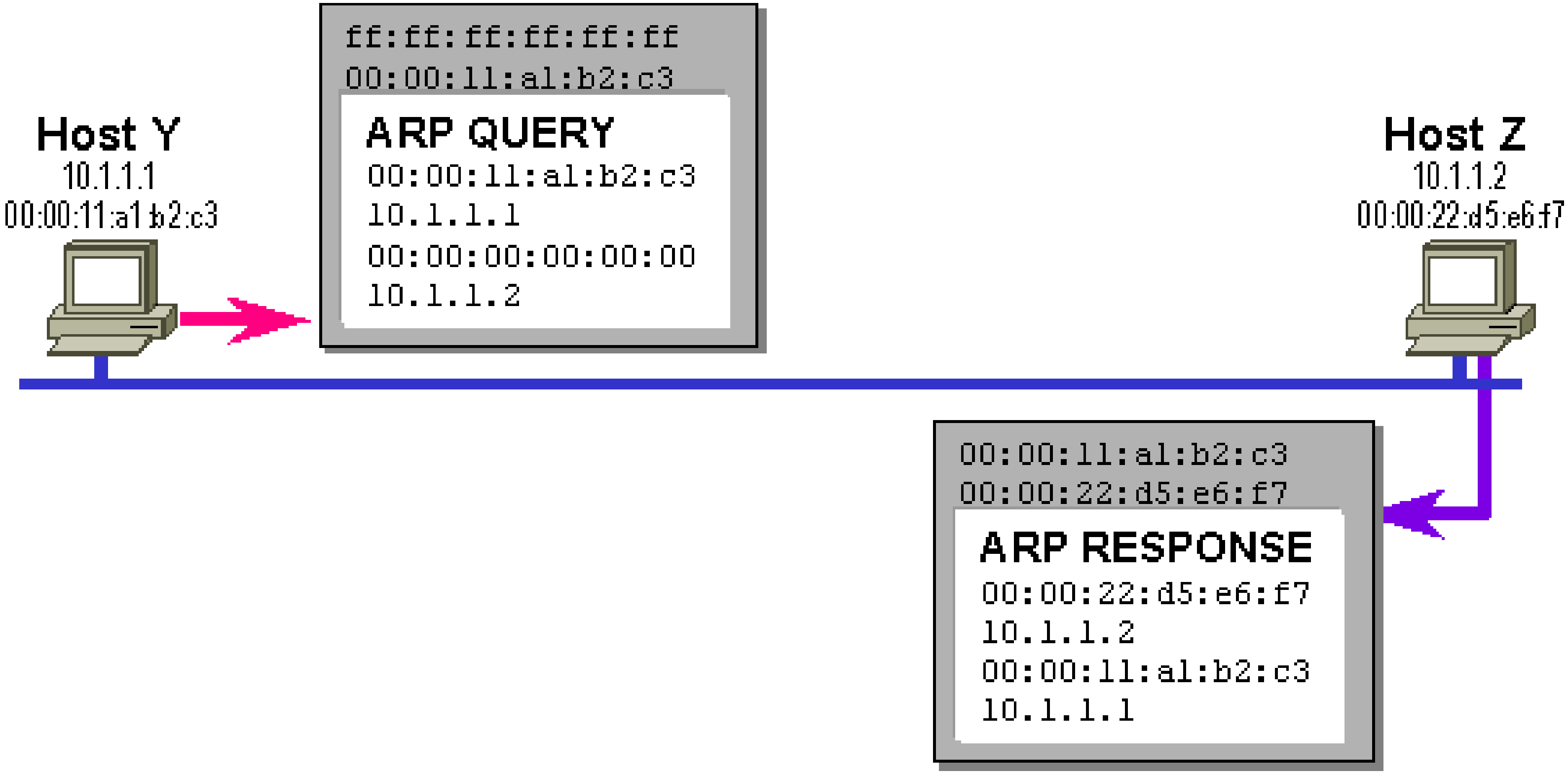
8 bits	8 bits	8 bits	8 bits
Hardware Type (2bytes)		Protocol Type (2bytes)	
Hardware Add Length (1byte)	Protocol Add Length (1byte)	Operation (2bytes)	
Sender Hardware Address (6bytes)			
		Sender IP Address (4bytes)	
		Target Hardware Address (6bytes)	
Target IP Address (4bytes)			

ARP Concept Exchange



ARP Real Exchange

- Request is broadcasted
- Sender is stored in the receivers cache
- Response is unicasted



ARP Cache

- Windows/Linux: `arp -a`
- Linux: `ip neighbor`

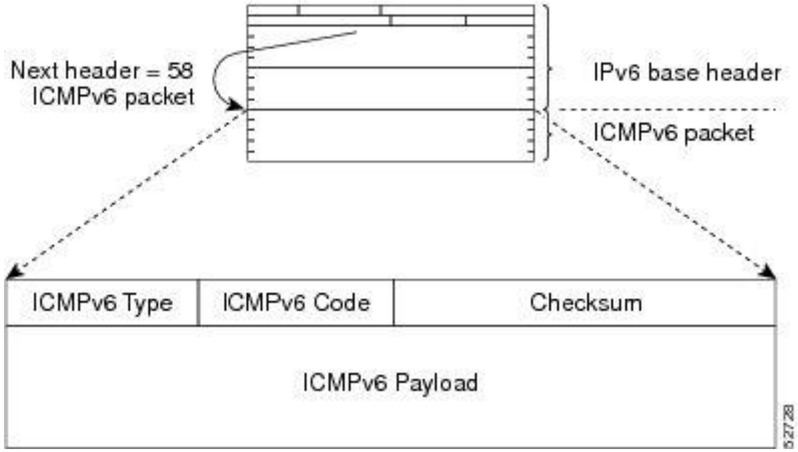
C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. Všechna práva vyhrazena.

C:\Users\Mordeth>arp -a

Interface: 147.229.14.121 --- 0xc
  Internet Address      Physical Address      Type
  147.229.14.1          00-04-96-1d-4e-30     dynamic
  147.229.14.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

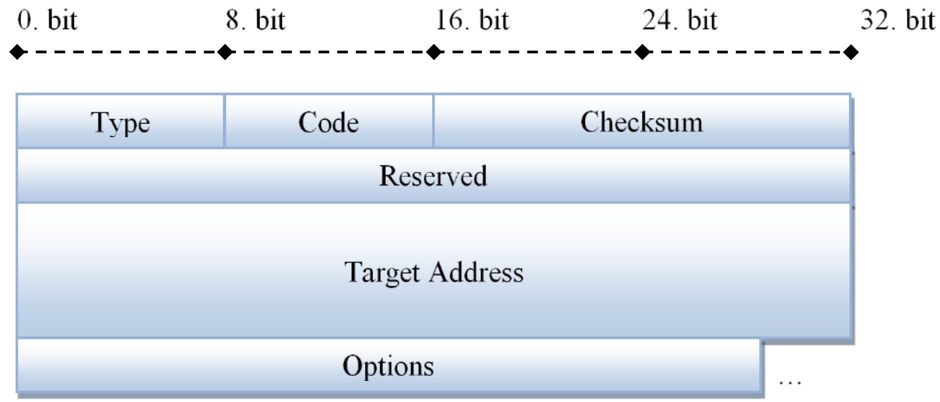
Neighbor Discovery Protocol

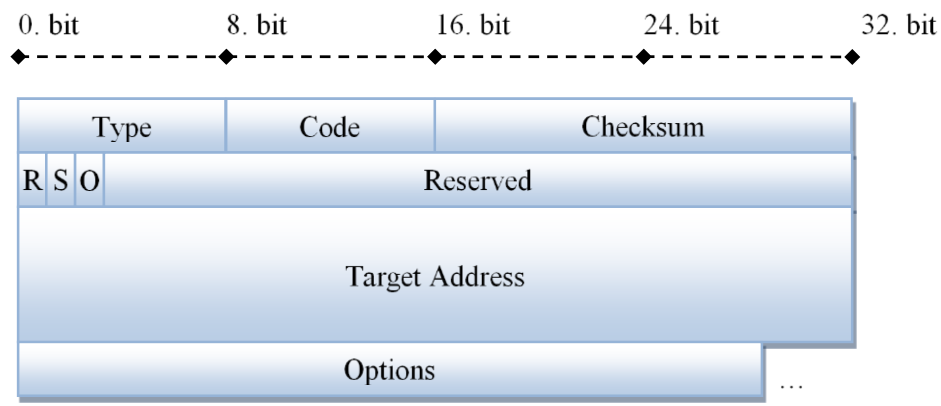
- RFC4861
- ND is versatile protocol
  - Duplicit address detection
  - IPv6-to-MAC resolution
  - Router-advertisements
- Layer 3 protocol
  - A part of ICMPv6
- *Once again, you cannot operate IPv6 without ND*

NDP Header

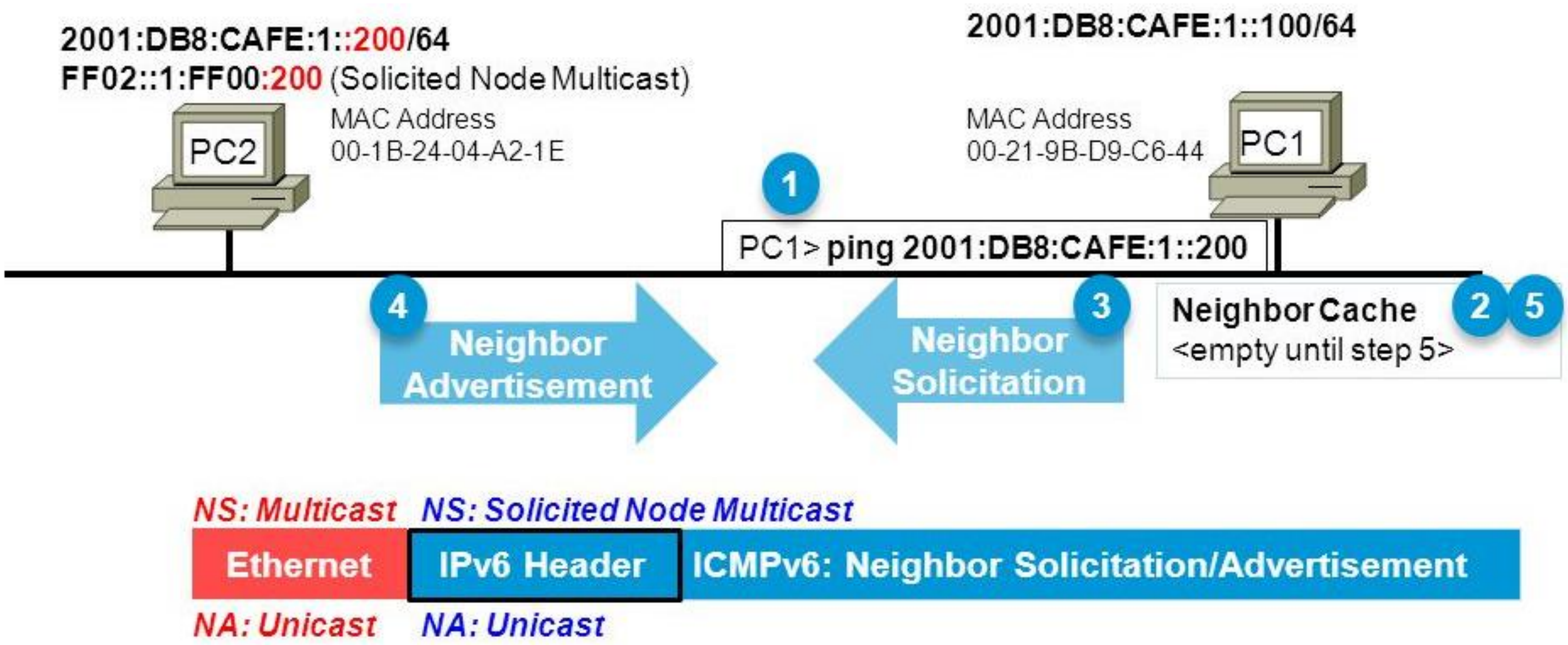


Type	Meaning
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem
128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group Membership Reduction
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect
138	Router Renumbering

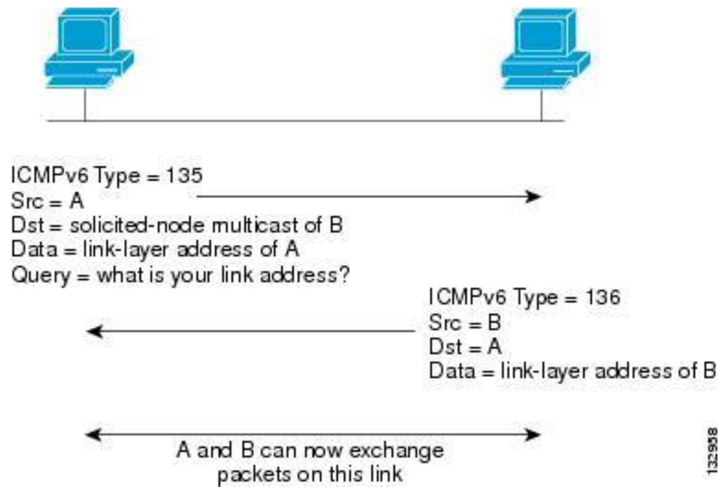


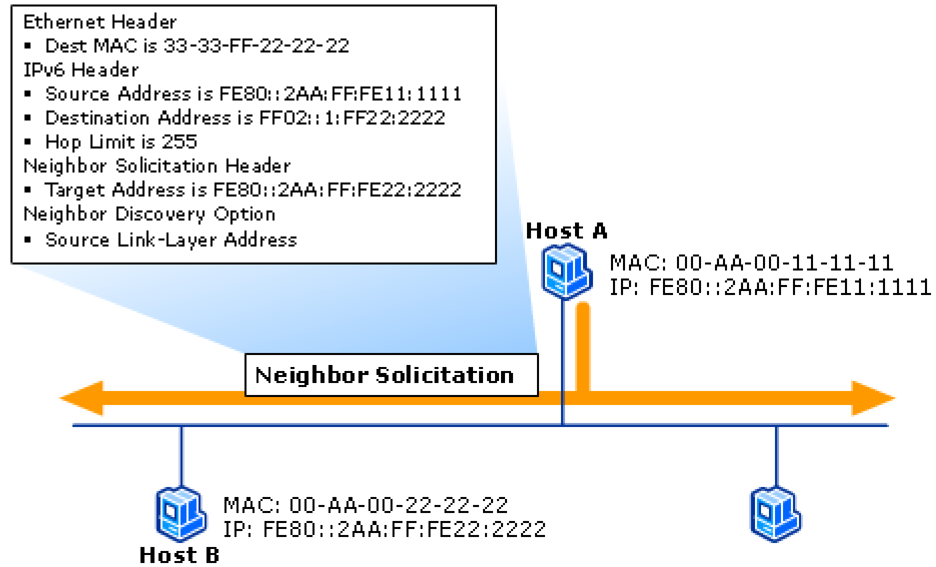


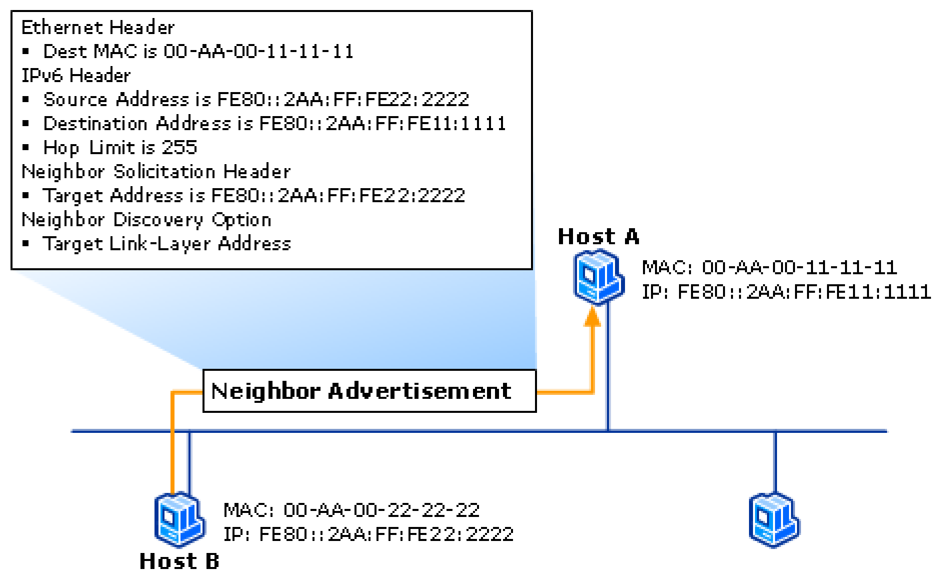
NDP Conceptual Exchange



NDP Real Exchange

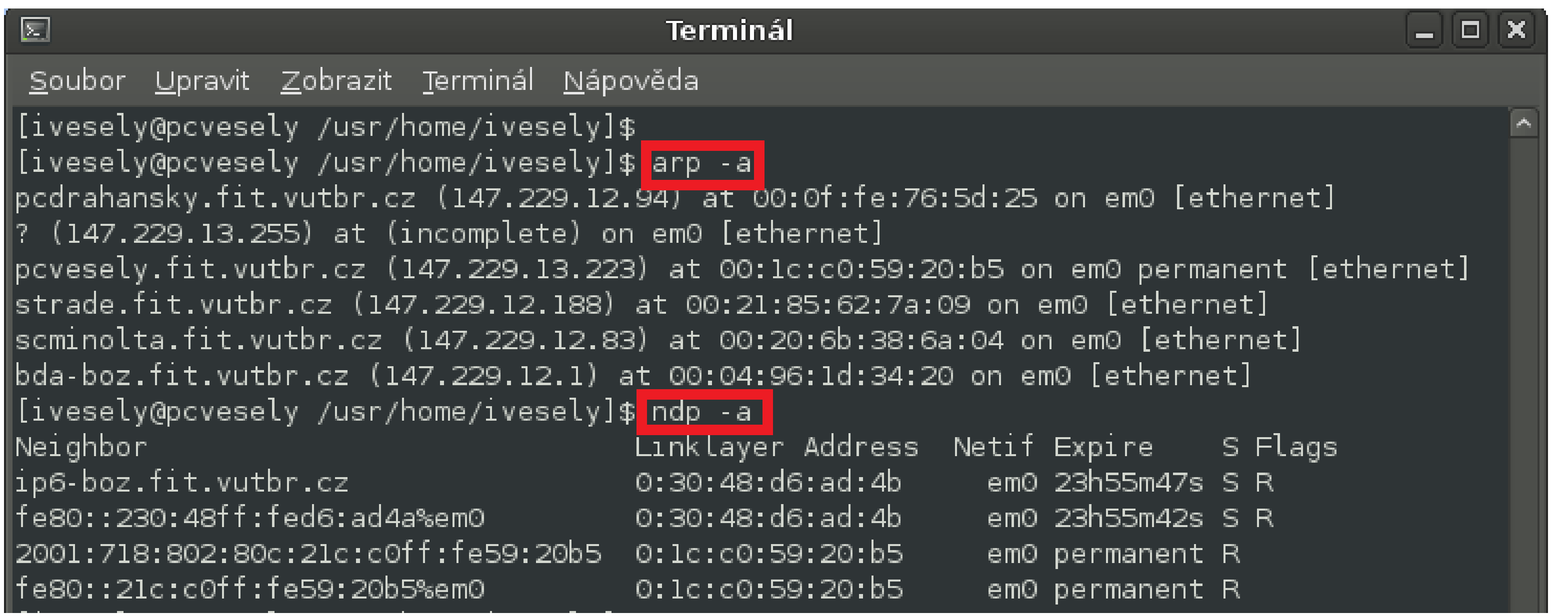






NDP Cache

- Unix: `ndp -a`
- Windows: `netsh interface ipv6 show neighbors`
- Linux: `ip neighbor`



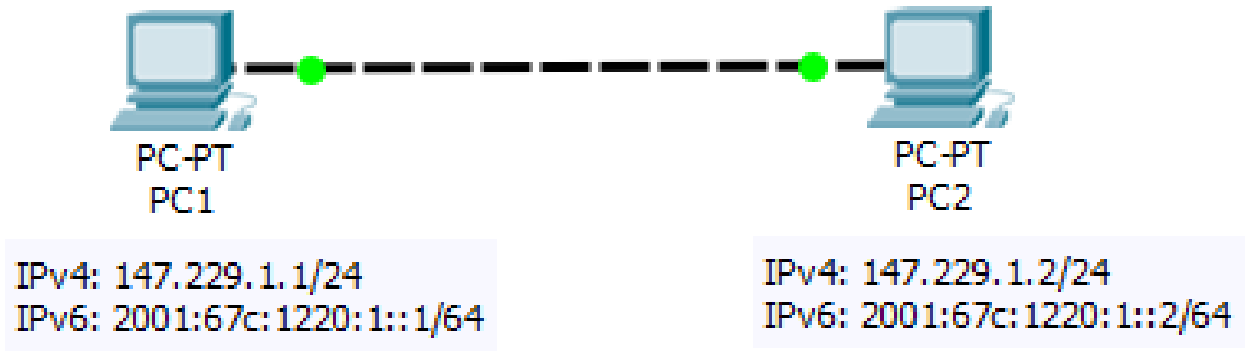
Demonstration

PacketTracer

- Network simulator with appealing GUI
- Developed for Cisco NetAcad but free of charge
- https://www.netacad.com/courses/packet-tracer-download/

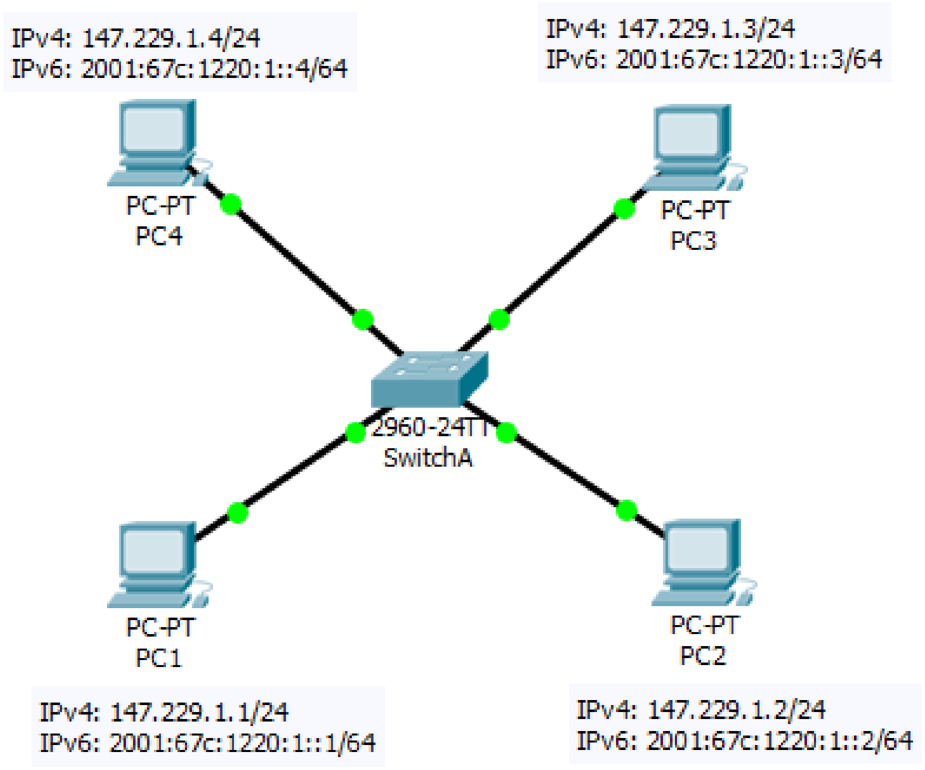
Between directly connected hosts

- Communication within LAN
- Usually crossover UTP Ethernet cable

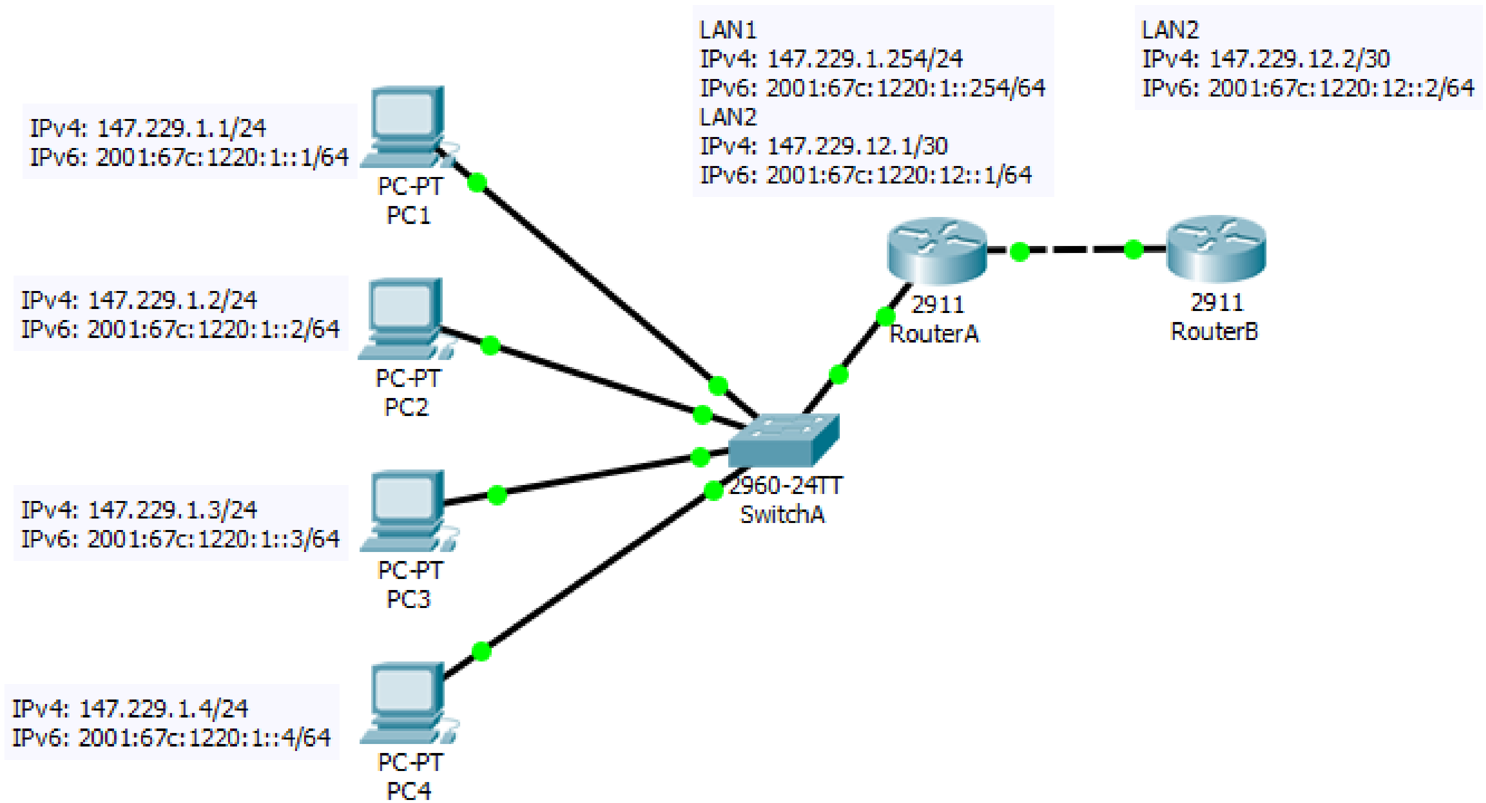


Between hosts in the same LAN

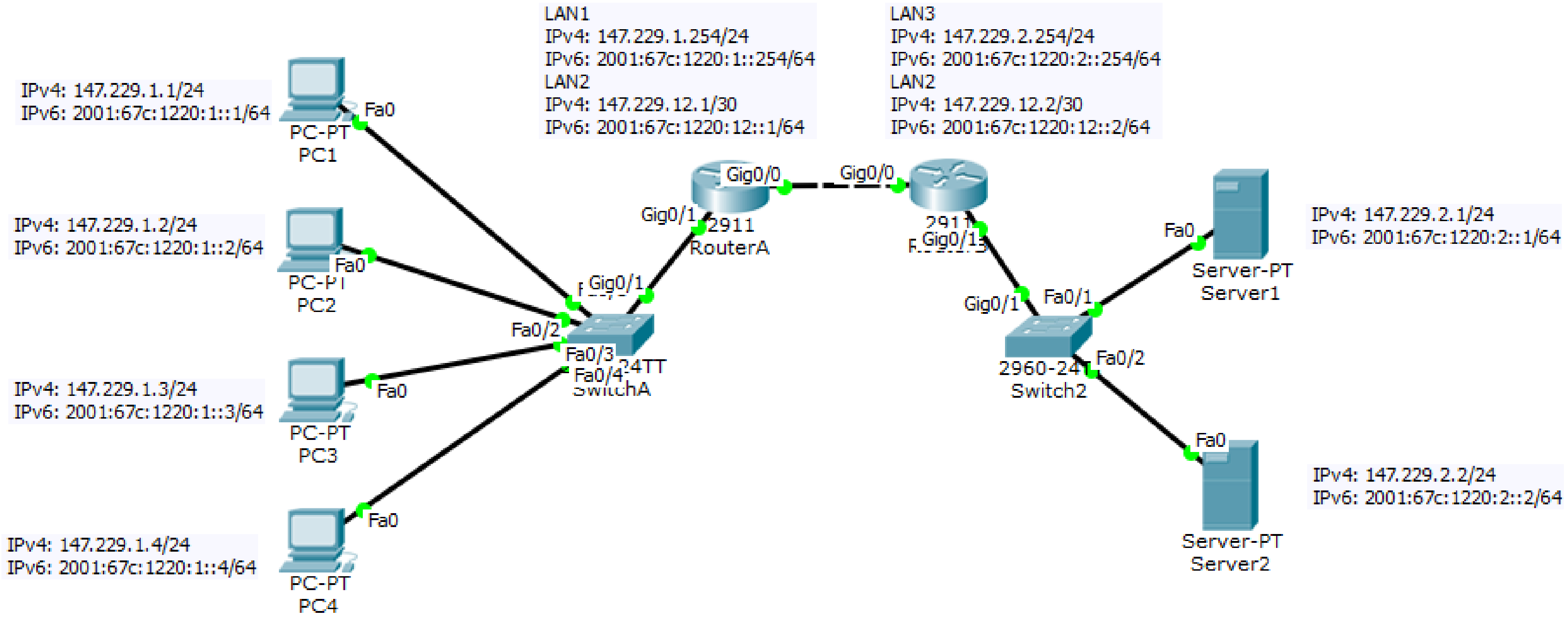
- H-S, S-R = straigth
- others = cross-over



Between two directly connected LANs



Accross the Internet



Self-Check

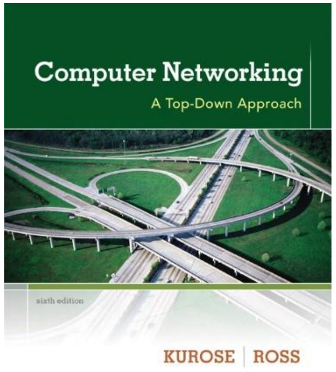
Questions

- Describe IP fragmentation!
- Explain operation of switch with CAM!
- Describe IPv6 Extension headers!
- What is the difference between unicast, multicast, broadcast and anycast? Which of them are present in IPv4 and IPv6?
- What is routing and what is switching?
- Describe ARP and ND L3-to-L2 resolution process!
- Inform about various Internet layered models!
- What is collision domain? Identify it on network diagram.
- What is broadcast domain? Identify it on network diagram.
- Explain IPv4 subnetting on example!
- Compare hub and switch? What is modem?
- How do you recognize IPv6 link-local address? What is the purpose of link-local addresses?

References

What to read next?

- Kurose, J.F., Ross K.W.: Computer Networking, A Top-Down Approach Featuring the Internet (6th edition). Addison-Wesley, 2012.



- "IPV6 (TŘETÍ VYDÁNÍ)", Pavel Satrapa, https://knihy.nic.cz/

- Microsoft, How IPv6 works, https://technet.microsoft.com/en-us/library/cc781672(v=ws.10).aspx