Basic Network Training

BNT
v 2.0.1

Training Agenda

- Defining a Network
  - Reasons to Use a Network
  - Network Infrastructure
  - Network Types
- OSI Model
  - OSI Layers
- Ethernet
  - MAC Addresses
  - CSMA/CD
- Ethernet Conectivity
  - IEEE Standarts

Training Agenda

- Switching
  - Forwarding Methods
  - Vlan/ STP/ LACP/ PoE
- TCP/IP – IPv4
  - TCP/IP vs. OSI Model
  - IP Addressing
  - How Routers Work
  - IP Routing Protocols
  - NAT
  - DHCP
  - Multicast
- Introduction IPv6

Defining a Network

Basis

Definition of a LAN

- A **LAN** is a system of cabling, equipment and software which allows computers to share and exchange data electronically, using an agreed format (protocol), within a 'local' area.

- A LAN is a collection of *different* technologies, not just the cable that connects the computers. The network cards in the computers, the hubs and switches in the middle, and the software that the computers run, must all work together to create a functional network.

Types of Area Network

- A *LAN* is a *Local Area Network*.
  - LAN usually means "in the same building".

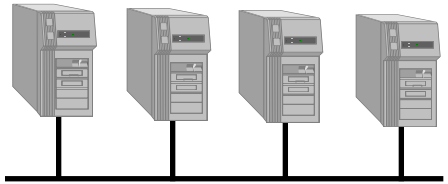
- MAN - Metropolitan Area Network
  - Interconnecting LANs and users within a city area, typically by dedicated fibre optics

- WAN - Wide Area Network
  - Interconnecting LANs and users over long distances, often on a public network

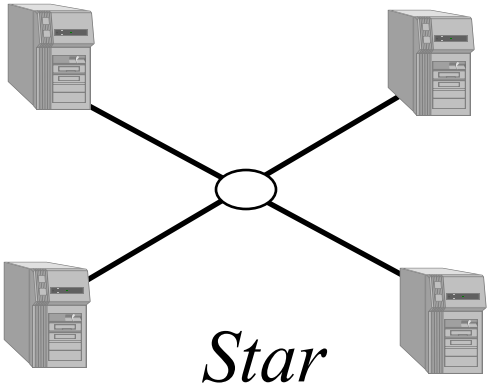
Why use a LAN?

- Users can share data
  - Saves time, makes work more efficient
- Connect different computers together
  - A LAN can be the common denominator
- Users can share resources (printers, storage)
  - Saves money on expensive capital equipment
  - Centralised administration
- E-mail, Internet and Multimedia
  - Reduces paper documents, better information

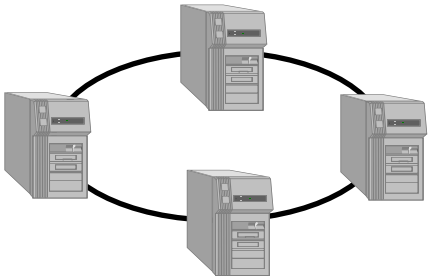
Network Wiring Topologies



Bus

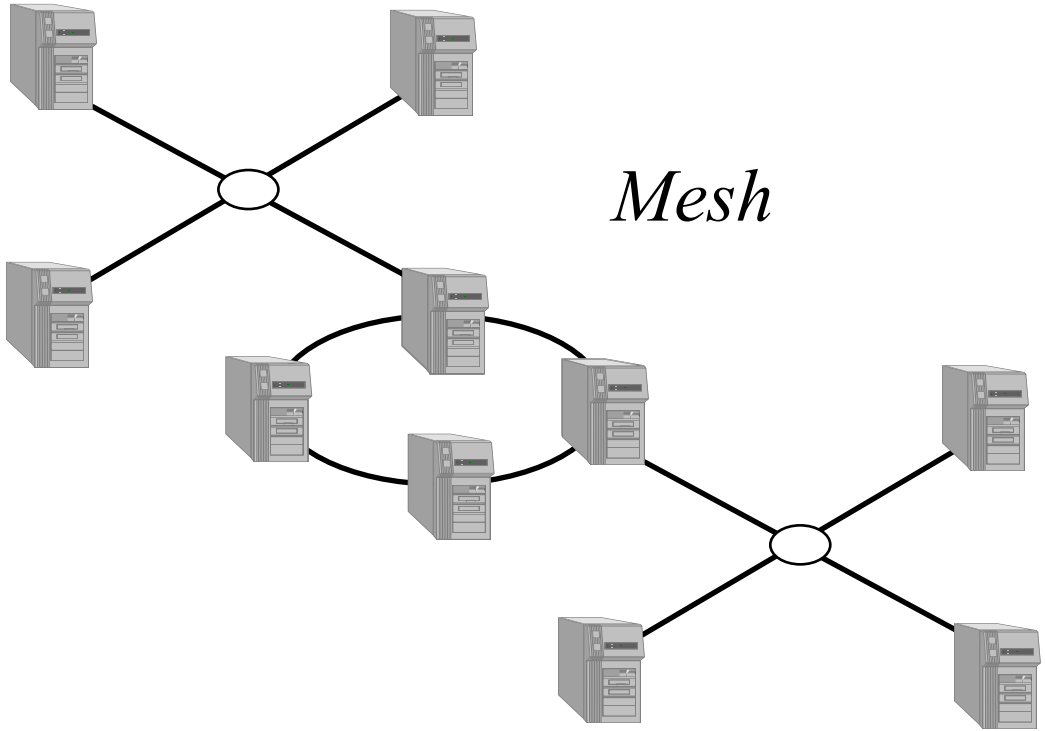


Star



Ring

Network Wiring Topologies

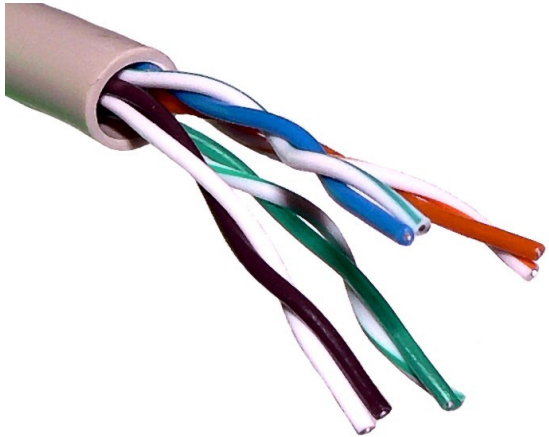


Ethernet Cable Options

The cable provides physical connection. Today two cable types are available.

Cooper

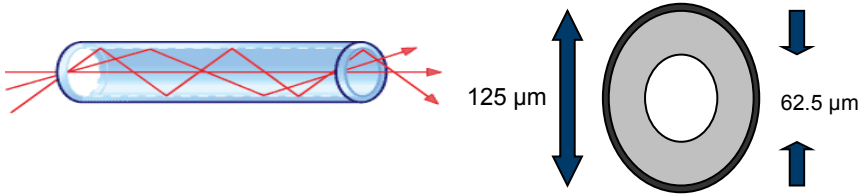
Twister Pair



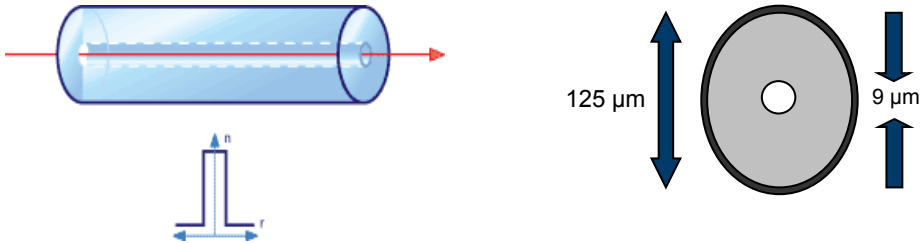
Fiber

Fiber

» Multimode fibre optics uses lower power LED transmitters, and is affordable.



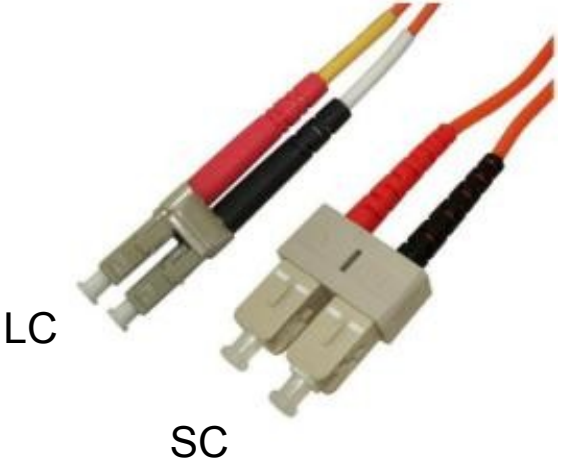
» Single-mode fibre optics uses laser transmitters for very long cable distances (up to 80 km), and can be very expensive by comparison.



Ethernet Cable Connector

Cooper Connectors

Fiber Connectors



Allied Telesis™

OSI Model

Open Systems Interconnection (OSI)

» The OSI reference model was created to help define how network processes function in general, including the various components of networks and transmission of data.

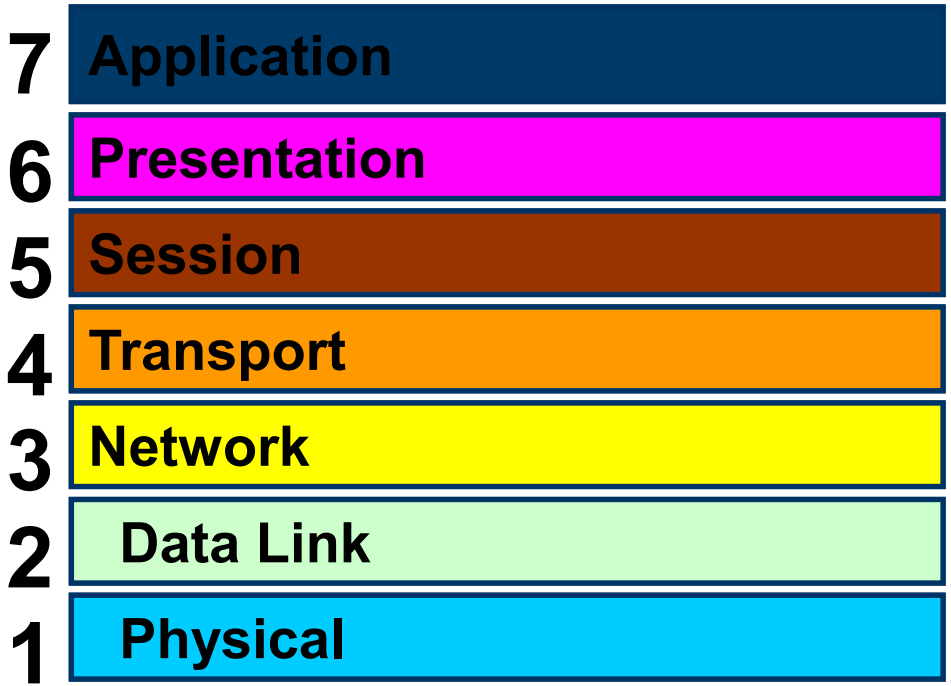
» As a result of this research, the ISO created a model that would help vendors create networks that would be compatible with, and operate with, other networks.

OSI Layers

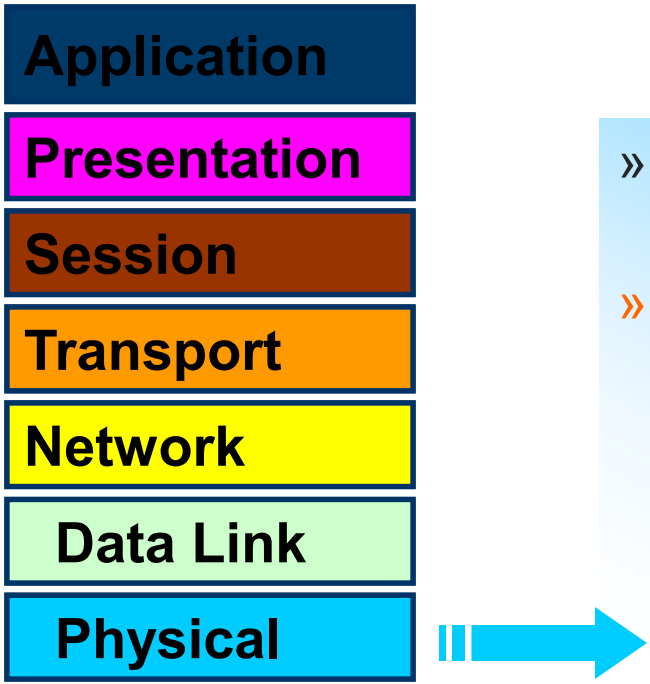
- The OSI reference model has seven layers, each illustrating a particular network function.
- The OSI reference model defines
  - the network functions that occur at each layer.
  - an understanding of how information travels throughout a network
  - how data travels from application programs through a network medium, to an application program located in another computer

ISO/OSI Reference Model

OSI: Open Systems Interconnection

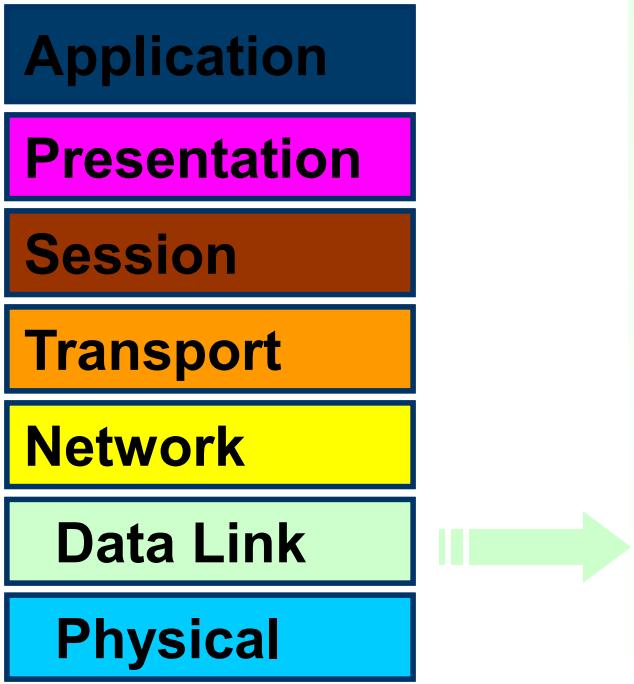


Layer 1: Physical



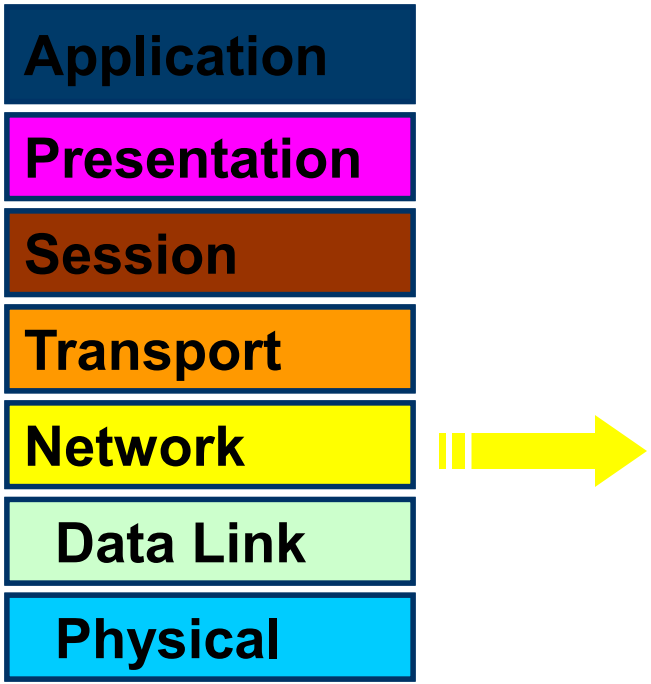
- Transmits binary sequences onto the channel
- This layer specifies
  - mechanical interfaces
  - voltages relative to 0 and 1
  - cable type, dimension, electrical characteristics and properties
  - type of connectors

Layer 2: Data Link



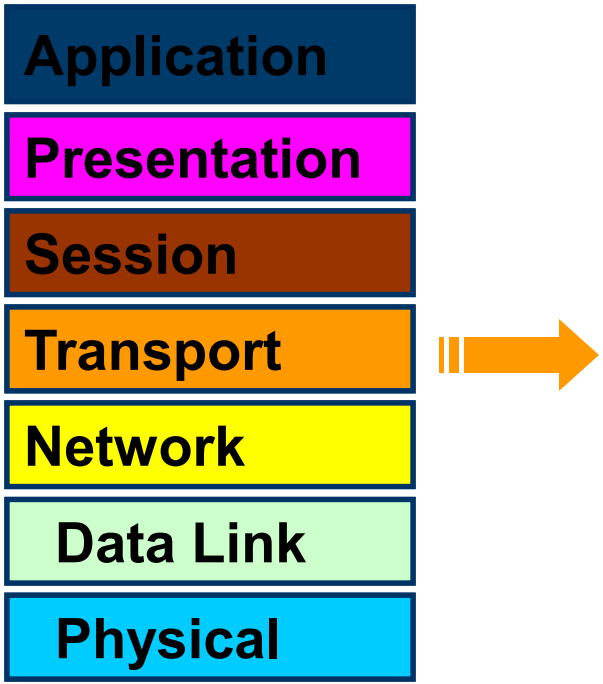
- To transmit frames in a secure way
- It accepts frames as input and transmits their octets in sequence (serial transmission)
- It verifies the presence of errors and adds Frame Check Sequence (FCS)
- It can manage error correction procedures implementing retransmission
- It manages addressing

Layer 3: Network



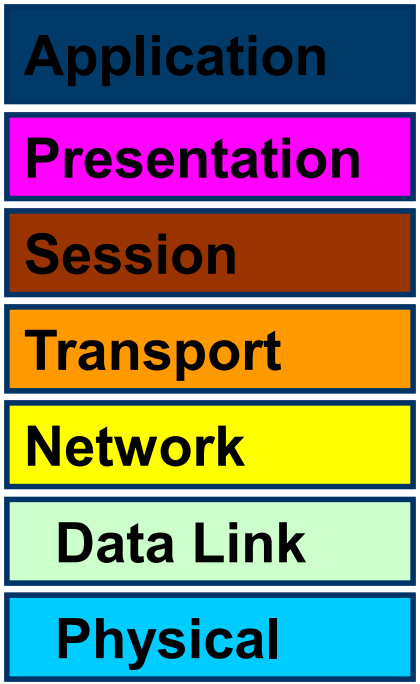
- Manages packet routing:
  - decides through which ISs a packet has to run in order to reach its destination
- Layer 3 uses routing tables to optimise network traffic
  - IS: Intermediate System

Layer 4: Transport



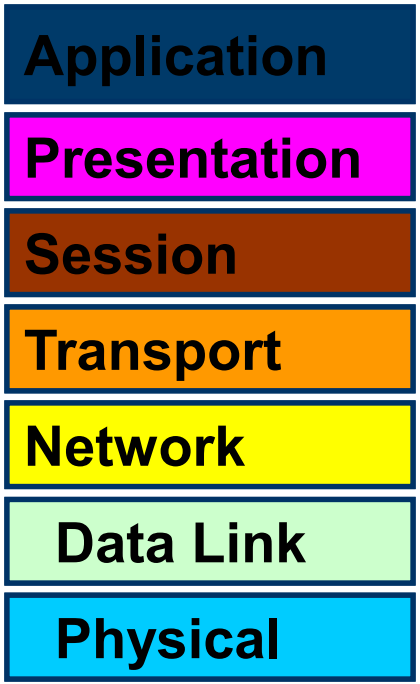
- Provides services to transfer data end-to-end
- Layer 4 can
  - fragment frames to adapt them to Layer 3 dimensions
  - find/correct errors
  - check data flow and congestion
- It is responsible for the reliability of data transmitted over the network

Layer 5: Session



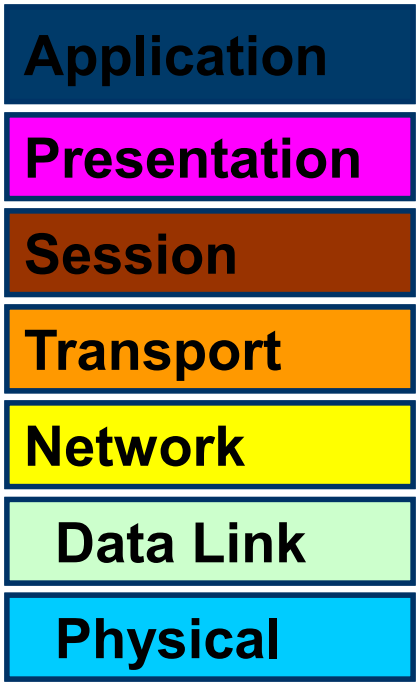
» It is responsible for establishing the dialogue and synchronising systems and data exchange

Layer 6: Presentation



- Defines data conversion
- It manages the syntax of information to be transferred
- It ensures that data is presented to applications in an understandable format, since information is represented in different ways on different machines - ASCII or EBCDIC

Layer 7: Application

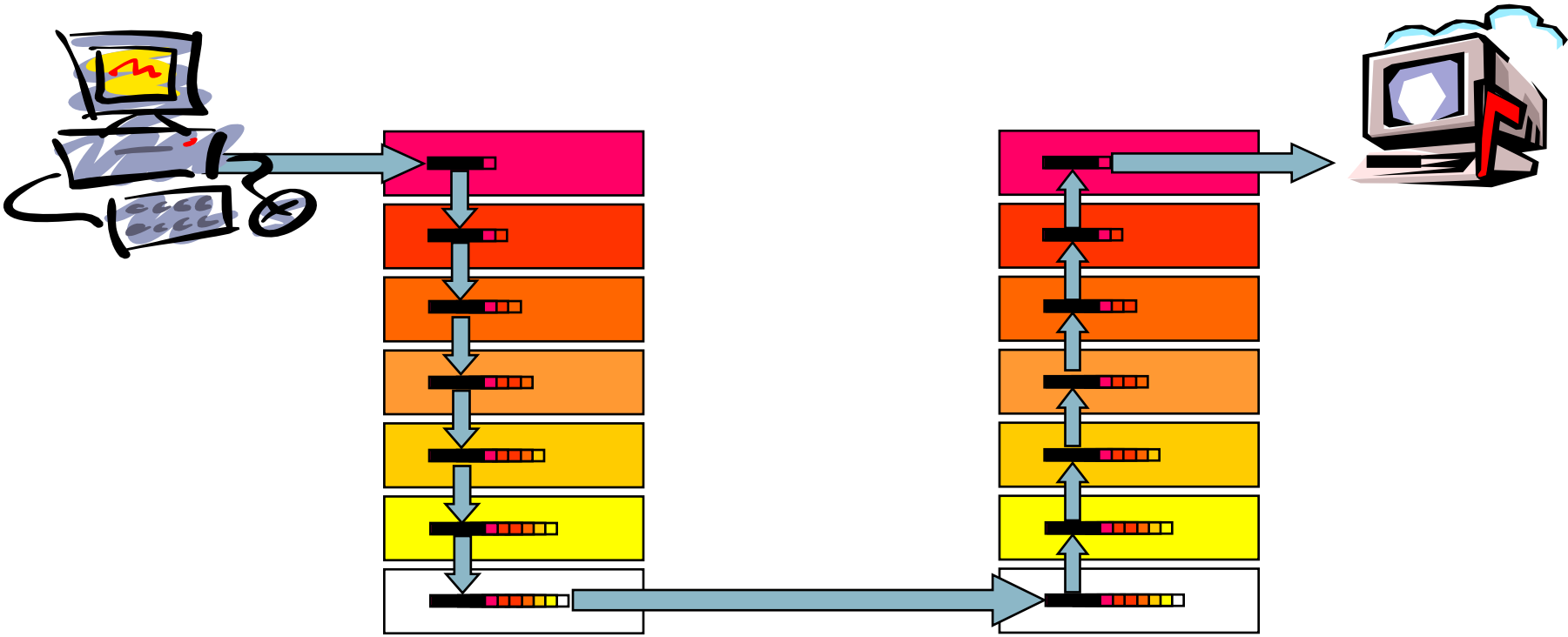


- It's the interface between applications on the system (software that belongs to the operating system or software necessary to use the network)
- Examples:
  - VT: Virtual Terminal, interactive link to a remote machine
  - FTAM: File Transfer and Access Management
  - X.400: Electronic mail
  - X.500: Directory Service

Data Conmunication

- All communications on a network originate at a source and are sent to a destination.
- A networking protocol using all or some of the layers listed in the OSI reference model move data between devices.
- A data frame is able to travel across a computer network because of the layers of the protocol.
- This method of passing data down the stack and adding headers and trailers is called encapsulation.

OSI Example



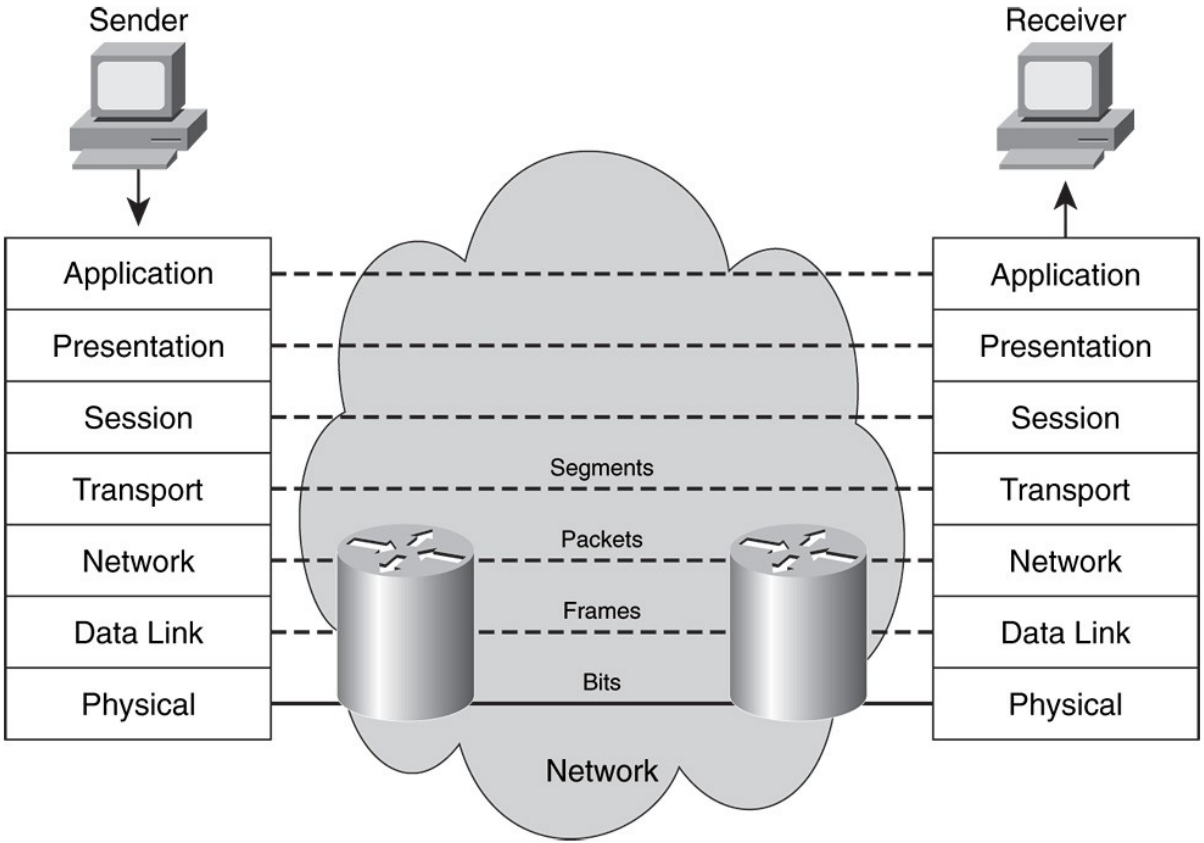
The network layer

- Provides a service to the transport layer, and the transport layer presents data to the internetwork subsystem.
- Moves the data through the internetwork by encapsulating the data and attaching a header to create a datagram.
- The header contains information required to complete the transfer, such as source and destination logical addresses.

The data link & Physical layers

- The data link layer Provides a service to the network layer by encapsulating the network layer datagram in a frame.
- The physical layer provides a service to the data link layer, encoding the data link frame into a pattern of 1s and 0s (bits) for transmission on the medium at Layer 1.
- Network devices work at the lower three layers.
  - Hubs are at Layer 1,
  - switches are at Layer 2,
  - and routers are at Layer 3.

Data Communications



Ethernet

The most common type of LAN

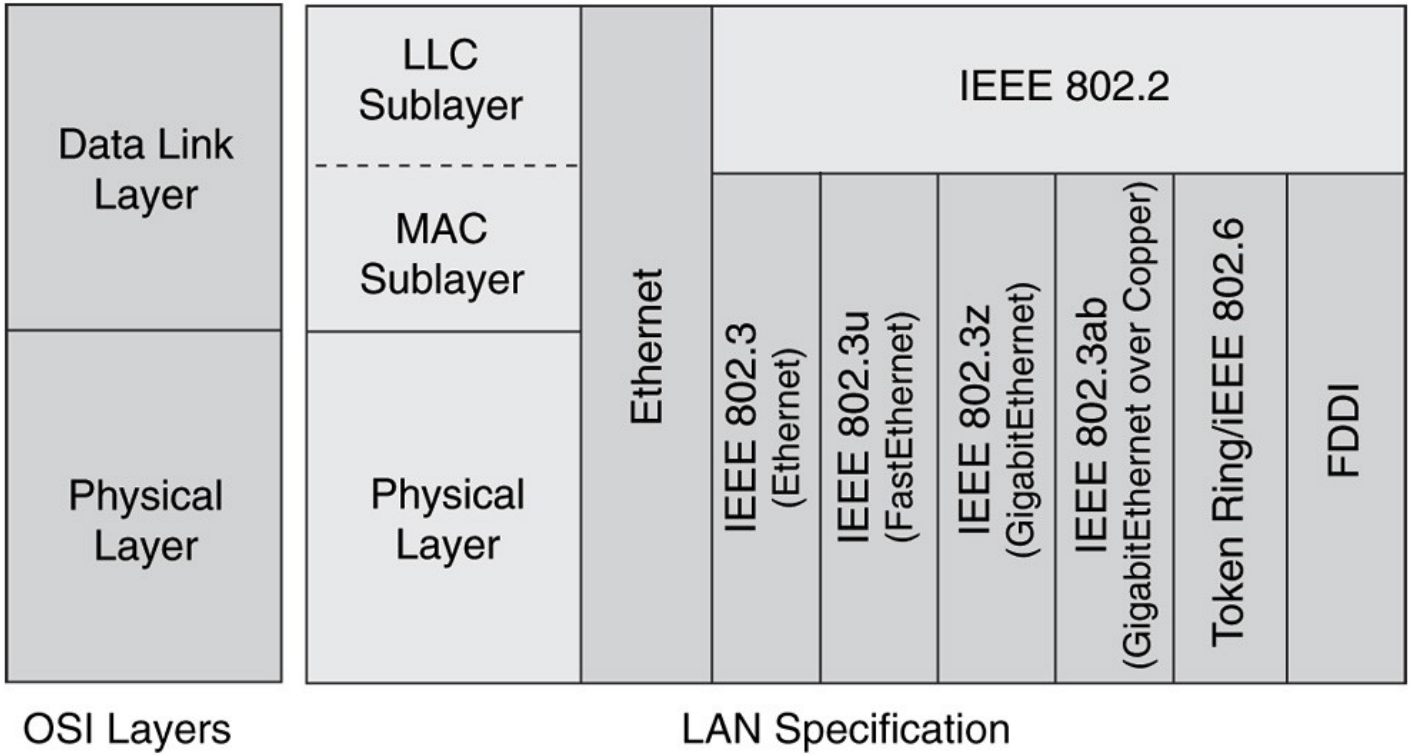
Ethernet

- IEEE Ethernet 802.3 and was based on the carrier sense multiple access with collision detection (CSMA/CD) process.

- Ethernet LAN standards specify cabling and signaling at both the physical and data link layers of the OSI reference model.

- Ethernet 802.3 specified
  - the physical layer (Layer 1)
  - the MAC portion of the data link layer (Layer 2).

Ethernet


Data Link Layer
Physical Layer
LLC Sublayer
MAC Sublayer
Physical Layer
Ethernet
IEEE 802.2
IEEE 802.3 (Ethernet)
IEEE 802.3u (FastEthernet)
IEEE 802.3z (GigabitEthernet)
IEEE 802.3ab (GigabitEthernet over Copper)
Token Ring/IEEE 802.6
FDDI
OSI Layers
LAN Specification

LLC Sublayer

- This layer participates in the encapsulation process.

- An LLC header tells the data link layer what to do with a packet when it receives a frame.
  - For example, a host receives a frame and then looks in the LLC header to understand that the packet is destined for the IP protocol at the network layer.

MAC Sublayer

- The MAC sublayer deals with physical media access.
- The IEEE 802.3 MAC specification defines MAC addresses (physical addresses), which uniquely identify multiple devices at the data link layer.
  - To participate on the network, each device must have a unique MAC address.
- The MAC sublayer maintains a table of MAC addresses of devices.

MAC Address

- A MAC address is a set of six bytes normally written in hexadecimal
  - example “00-C0-BA-00-8C-6A” or “00:C0:BA:00:8C:6A”

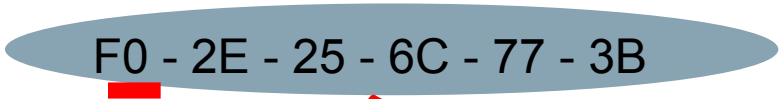
- The MAC address is usually programmed into hardware, and is assumed to be completely unique.
  - Each manufacturer of network equipment has a special code (called Organisationally Unique Identifier, or OUI) which is used in their MAC addresses.
  - Allied Telesis for example has the following ranges of addresses (besides others) assigned to it:

    00-A0-D2-xx-xx-xx

    00-09-41-xx-xx-xx

- MAC addresses belong to Layer 2 and are not the IP addresses

MAC Address



48 Bits (6 Octets)

Sequence of bits on the Ethernet

0000 1111 0111 0100 1010 0100 0011 0110 1110 1110 1101 1100

The first bit of the data link address distinguishes multicast addresses from individual addresses

0 - individual address

1 - group address or multicast address, a broadcast address is a special multicast address consisting entirely of 1´s and addresses all stations on an Ethernet

Ethernet Rules: CSMA/CD

» Ethernet signals are transmitted to every station connected to the LAN, using a special set of rules to determine which station can "talk" at any particular time.

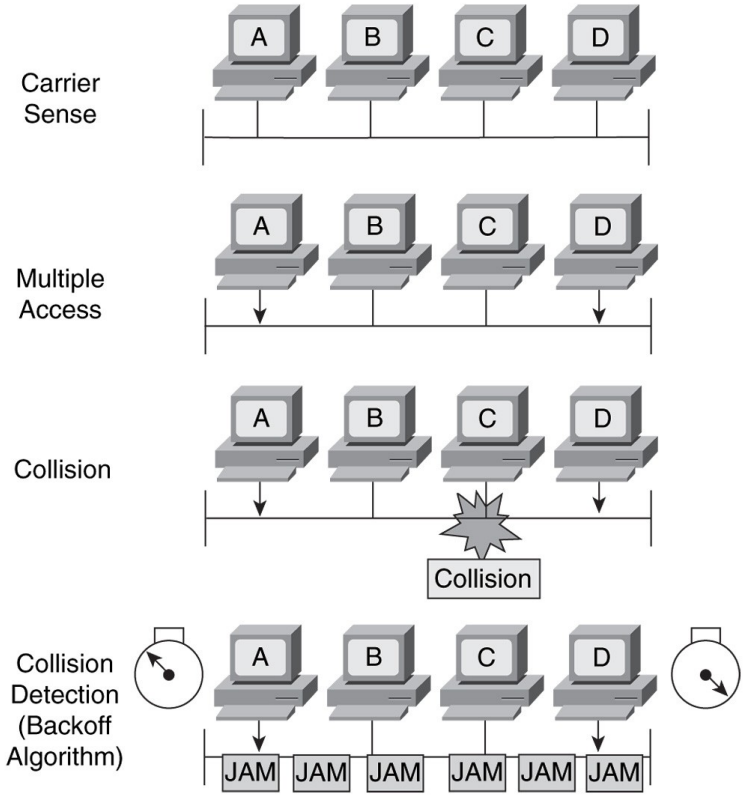
» Ethernet LANs manage the signals on a network by CSMA/CD, which is an important aspect of Ethernet.

CSMA/CD

- Carrier Sense Multiple Access / Collision Detection

- It follows different steps in order to allow communication without collisions in a shared channel:
  - listening before talking
  - listening while talking
  - back-off

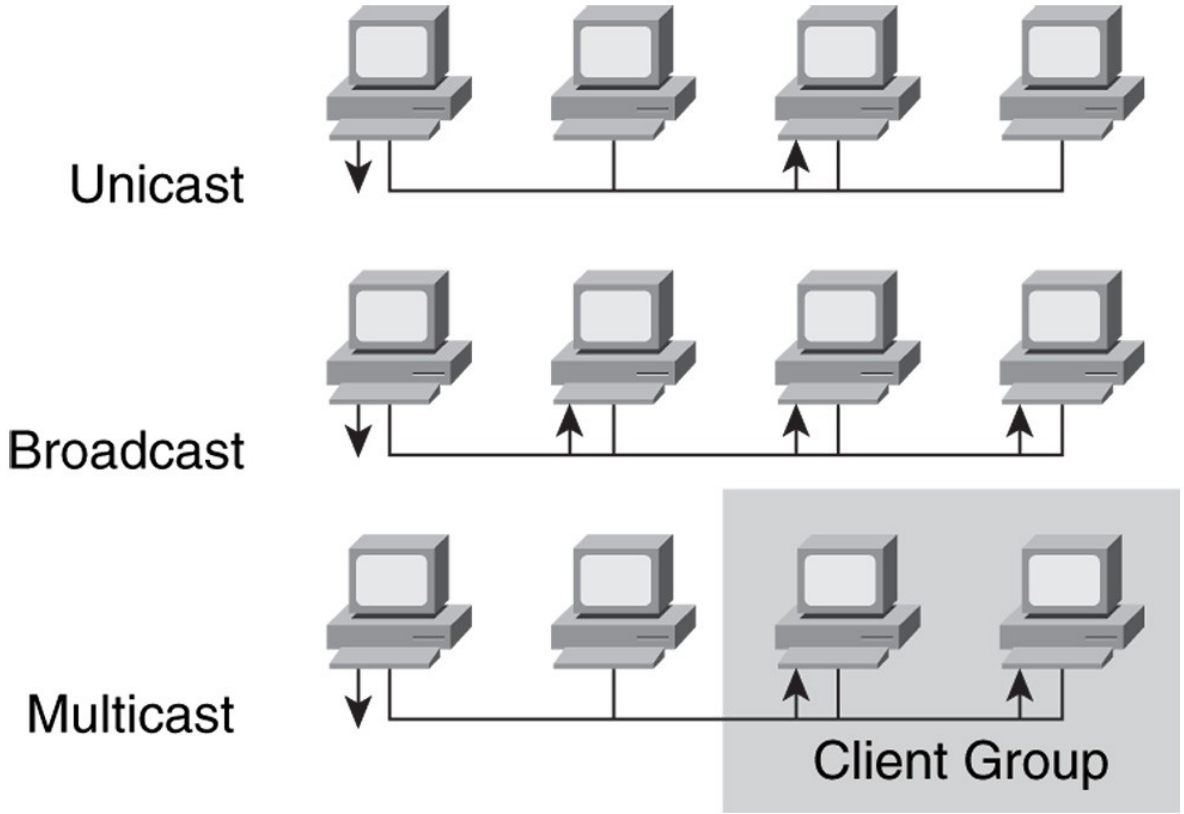
CSMA/CD


Carrier Sense
A
B
C
D
Multiple Access
A
B
C
D
Collision
A
B
C
D
Collision
Collision Detection (Backoff Algorithm)
A
B
C
D
JAM
JAM
JAM
JAM
JAM
JAM

Ethernet Frame Addressing

- Communications in a network occur in three ways:
  - unicast,
  - broadcast,
  - and multicast.
- Ethernet frames are addressed accordingly

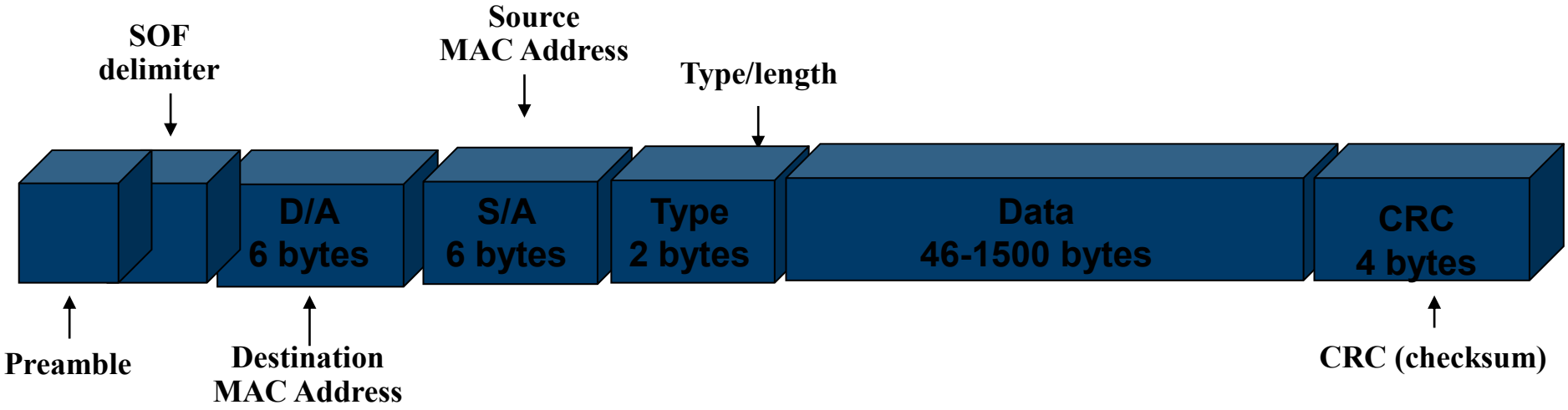
Ethernet Frame Addressing



How Data is Transferred

- All data is transferred in '*packets*'
- A packet of data has addressing details at the start, and error checking data at the end. This is known as a '*frame*'
- Moving data in small pieces gives everyone an equal chance to get their data through
- Smaller packets are more likely to be delivered without errors

The Ethernet Frame



Preamble allows timing alignment

Start Of Frame delimiter indicates start of frame

CRC (Cyclic Redundancy Check) is a checksum to ensure the frame was received OK

Total frame length varies from 64 to 1,518 bytes (after SOF delimiter)

Allied Telesis™

Ethernet

Conectivity

Ethernet Technologies

- 10 Mbit/s Ethernet
  - One of the oldest network technologies, and still popular
- Fast Ethernet (100 Mbit/s)
  - Upgrade route from 10 Mbit/s, providing higher performance
- Gigabit Ethernet (1000 Mbit/s)
  - The Actual generation for servers and backbones, providing very high throughput.
- Ten Gigabit Ethernet (10000 Mbit/s)
  - The next generation for servers and backbones, providing very high throughput

100 Mbit/s Ethernet

IEEE 802.3u – 100Mb/s

- CSMA / CD - Carrier Sense Multiple Access / Collision Detection
- The Ethernet frame is the same
- Cat 5 o Cat5e Twister Pair can be used with a maximum of 100 meters on each link

Auto-Negotiation

- Auto-Negotiation automatically adjusts the speed and duplex of the attached network devices to the highest matching speed/mode.

- Auto-negotiation only works with UTP/STP networks. No fiber optic or coaxial

Auto-Negotiation Parallel Detection

- The Parallel Detection function is used in the situation where only one partner in the link is capable of Auto-Negotiation.
  - Only detects and sets signaling speed, either 10Mbps, 100Mbps or 1000Mbps
  - Cannot detect or set duplex mode
  - Resulting connections will be half duplex

Fast link pulse

» When two auto-negotiating devices are connected in a network, both devices send out a series of signals called fast link pulses (FLPs).

- These link pulses tell the other device what they are capable of.
- Both devices will then auto-negotiate the highest common denominator or speed/duplex setting for those devices.

Auto-Negotiation Priorities

- The priority level (highest to lowest) for Auto-Negotiation are:
  - 1000BASETX Full Duplex
  - 100BASET2 Full Duplex
  - 100BASET2 Half Duplex
  - 100BASETX Full Duplex
  - 100BASET4 Half duplex
  - 100BASETX Half Duplex
  - 10BASET Full Duplex
  - 10BASET Half Duplex

100BASE-X Technologies: TX

- 100BASE-TX
  - Uses two twisted pairs
  - Must have Category 5 cable to run on
  - Max distance 100m
  - Full or Half duplex possible

100BASE-X Technologies: FX

- 100BASE-FX
  - Uses two 62.5/125 or 50/125 multimode fibres
  - Operates at 1300nm (10BASE-FL operates at 850nm)
  - Full duplex is possible but *no* auto-negotiation
  - The maximum link length depends on the configuration of the network

100Base-FX - Cable Distances

- 100Base-FX Multi-Mode
  - Half-duplex: 412 meters max
  - Full-duplex: 2000 meters max
- 100Base-FX Single-Mode
  - Half-duplex: 412 meters max
  - Full-duplex: 15 kilometers max

1000 Mbit/s Ethernet

Gigabit Ethernet

- The initial standard for gigabit Ethernet was produced by the IEEE in 1998 as IEEE 802.3z, and required optical fiber. 802.3z is commonly referred to as 1000BASE-X.

- IEEE 802.3ab, ratified in 1999, defines gigabit Ethernet transmission over UTP Cat5,Cat5e or Cat6 cabling and became known as 1000BASE-T.

- IEEE 802.3ah, ratified in 2004 added two more gigabit fiber standards, 1000BASE-LX10 and 1000BASE-BX10.

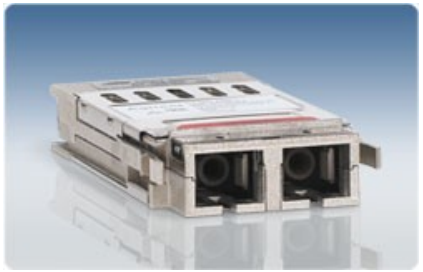
1000BaseX Cable Options

Standard	Media	Range
1000BaseLX-10	Single Mode Fibre	10km
1000BaseLX	Multi-Mode Fibre	550m
1000BaseSX	Multi-Mode	220-500m
1000BaseT	UTP	100m

1000BaseX Media

» The basic media carrier for 1000Base are the GBIC and SFP modules. GBICs and SFP are a media independent devices. Provide plug in options for SX or LX fibre

– GBIC use SC connector



– SFP use LC connector

10000 Mbit/s Ethernet

10 Gigabit Ethernet

- Being standardised in IEEE 802.3ae due in 2002
- Defines only Full-Duplex point to point links
- Half-Duplex operation, hubs and CSMA/CD do not exist in 10GbE.
- High-performance backbone technology

10 Gigabit Ethernet

» The 10 gigabit Ethernet standard encompasses a number of different physical layer (PHY) standards, such as those based on SFP+, XFP or XENPAK. SFP+ has become the most popular

SFP+

XFP

10 Gigabit Ethernet Over fiber

- 10GBASE-SR ("short range") is a port type for multi-mode fiber and uses 850 nm lasers.
  - Over 62.5 micron multi-mode fiber cabling it has a maximum range of 26 m, over 62.5 micron OM1 it has a range of 33 m, over 50 micron OM2 a range of 82 m, over OM3 300 m and over OM4 400 m

- 10GBASE-LR ("long reach") is a port type for single-mode fiber and uses 1310 nm lasers.
  - 10GBASE-LR has a specified reach of 10 km

10 Gigabit Ethernet Over Copper

» 10GBASE-CX4 was the first 10G copper standard published by 802.3 (as 802.3ak-2004).
  – It is specified to work up to a distance of 15 m.

» SFP+ Direct Attach o SFP+Cu. It uses a passive twin-ax cable assembly and connects directly into an SFP+ slot.
  – It has a range of 7 m
  – It is low power, low cost and low latency

10 Gigabit Ethernet Over Copper

- 10GBASE-T, or IEEE 802.3an-2006, is a standard released in 2006 to provide 10 Gbit/s connections over UTP cables with RJ45 connector
  - distances up to 100 meters.
  - 10GBASE-T cable infrastructure can also be used for 1000BASE-T allowing a gradual upgrade from 1000BASE-T using autonegotiation to select which speed to use.
  - 10GBASE-T has latency in the range 2 to 4 microseconds compared to 1 to 12 microseconds on 1000BASE-T.

Allied Telesis™

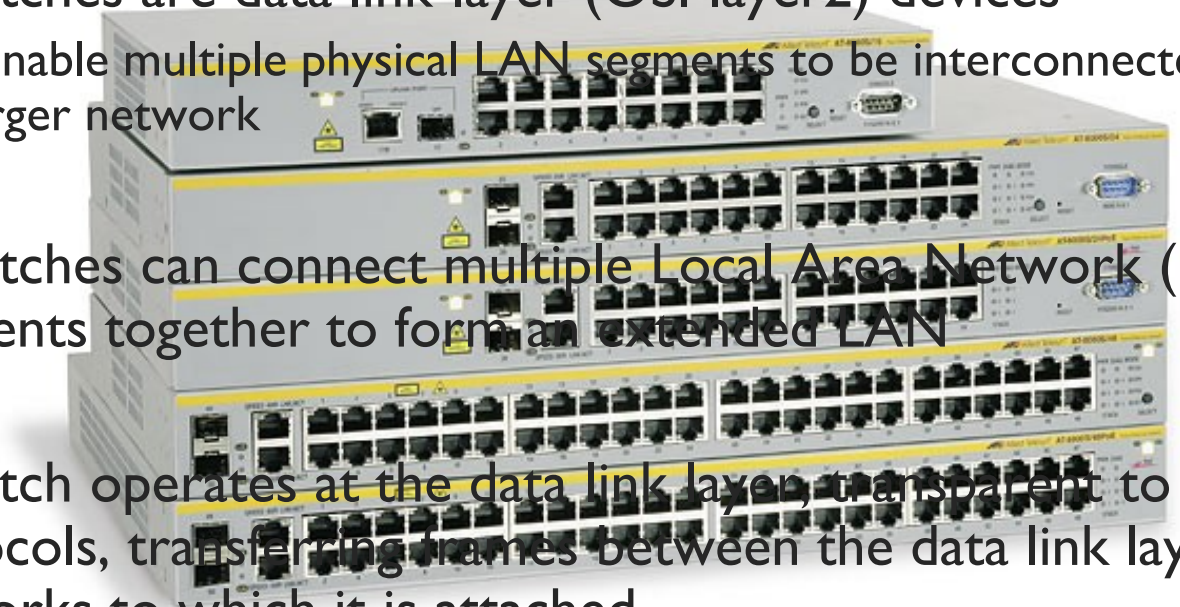
Switching

Forwanding Data

What a switch is…

» Switches are data link-layer (OSI layer2) devices

–enable multiple physical LAN segments to be interconnected into a single larger network



» Switches can connect multiple Local Area Network (LAN) segments together to form an extended LAN

» Switch operates at the data link layer, transparent to higher layer protocols, transferring frames between the data link layers of the networks to which it is attached

What a switch is…

» Switch can examine and discard or admit frames according to their VLAN tag fields

» Switch can also examine the address fields of the frames and forward the frames based on knowledge of which network contains the station with an address matching the frame's destination address

» Switch can act as an intelligent filtering device, redirecting or blocking the movement of frames between networks

Use of switches

» Increase the physical extent and the maximum number of stations on a LAN

» Connect LANs which have a common L2 protocol but different media (fibre with copper or 100M with 1000M)

» Achieve multiple connections within and between LANs

» Improve bandwidth usage by not transmitting all packets to all ports

» Filter traffic

» Achieve QoS (Quality of Service)

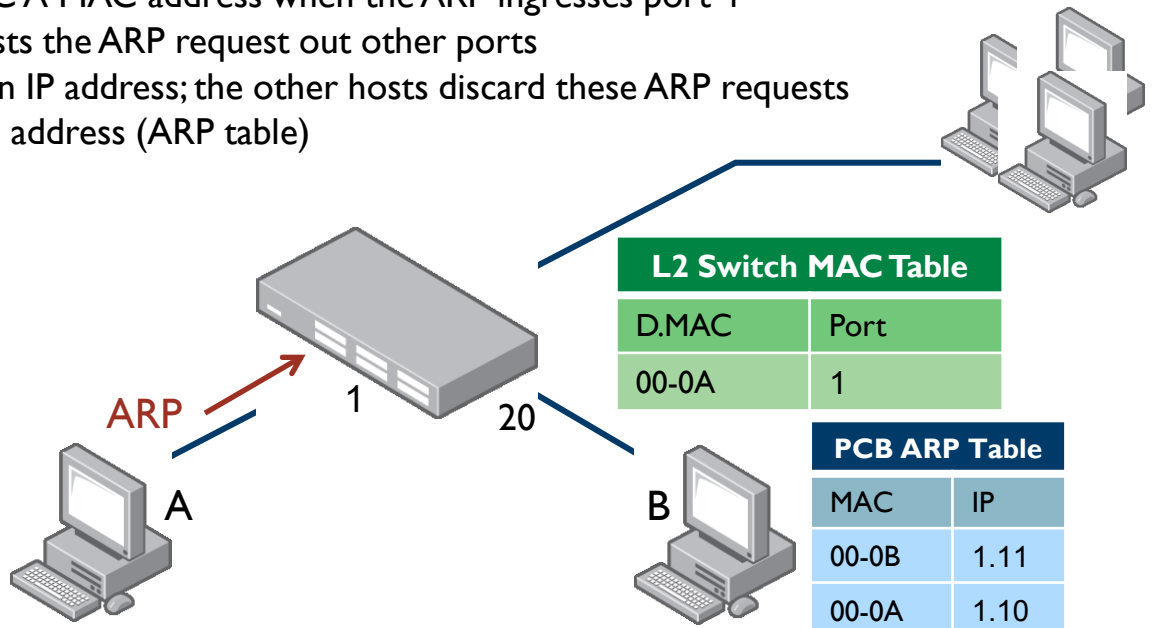
How a switch Works

Address Learning (Example when IPv4 is the L3 protocol)

- PC A needs to know PC B's MAC address (IP is known)
- An ARP packet is generated by PC A (Broadcast)
- The L2 switch learns PC A MAC address when the ARP ingresses port 1
- The L2 switch broadcasts the ARP request out other ports
- PC B recognizes its own IP address; the other hosts discard these ARP requests
- PC B learns PC A MAC address (ARP table)

ARP Packet	
D.MAC	S.MAC
FF-FF	00-0A
D.IP	S.IP
1.11	1.10

PCB ARP Table	
MAC	IP
00-0A	1.10



L2 Switch MAC Table	
D.MAC	Port
00-0A	1

PCB ARP Table	
MAC	IP
00-0B	1.11
00-0A	1.10

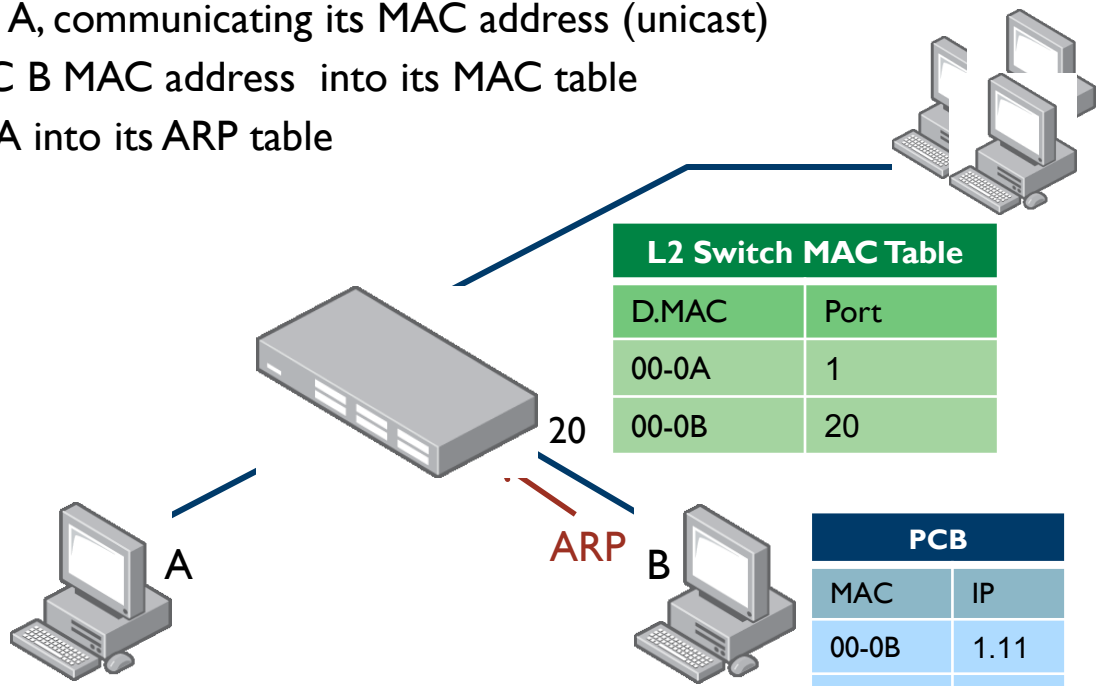
How a switch Works

Address Learning (Example when IPv4 is the L3 protocol)

- PC B answers to PC A, communicating its MAC address (unicast)
- The switch learns PC B MAC address into its MAC table
- A learns PC B MACA into its ARP table

ARP Packet	
D.MAC	S.MAC
00-0A	00-0B
D.IP	S.IP
1.10	1.11

PCA	
MAC	IP
00-0A	1.10
00-0B	1.11



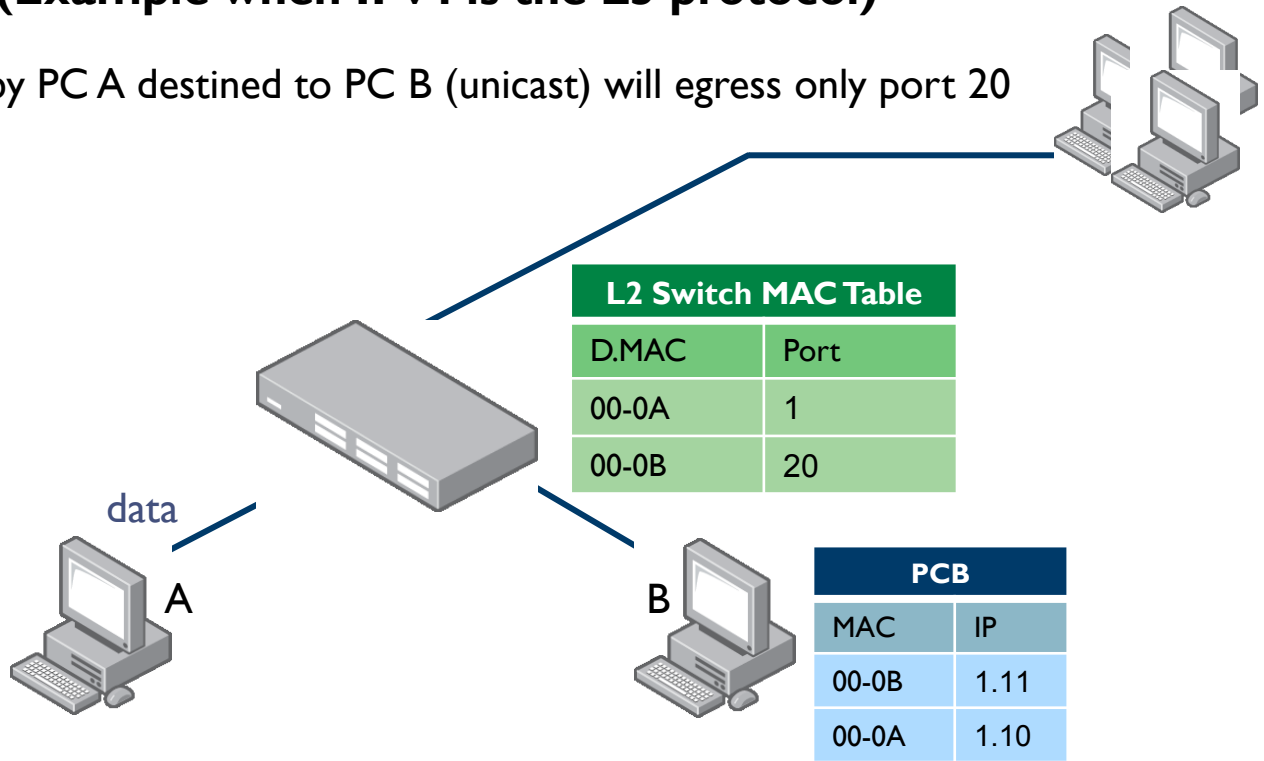
L2 Switch MAC Table	
D.MAC	Port
00-0A	1
00-0B	20

PCB	
MAC	IP
00-0B	1.11
00-0A	1.10

How a switch Works

Address Learning (Example when IPv4 is the L3 protocol)

» Traffic is generated by PC A destined to PC B (unicast) will egress only port 20



Data Packets	
D.MAC	S.MAC
00-0B	00-0A
D.IP	S.IP
1.11	1.10

PCA	
MAC	IP
00-0A	1.10
00-0B	1.11

L2 Switch MAC Table	
D.MAC	Port
00-0A	1
00-0B	20

PCB	
MAC	IP
00-0B	1.11
00-0A	1.10

How a switch Works

» When a switch is first powered up, its Forwarding Database (FDB) is empty.

» The switch cannot possibly know in advance all the MAC addresses in use in the network, and which VLANs all those MAC addresses reside in. So, it needs to **learn** all the MAC-address/VLAN combinations as packets start to flow through it.

Switching Techniques

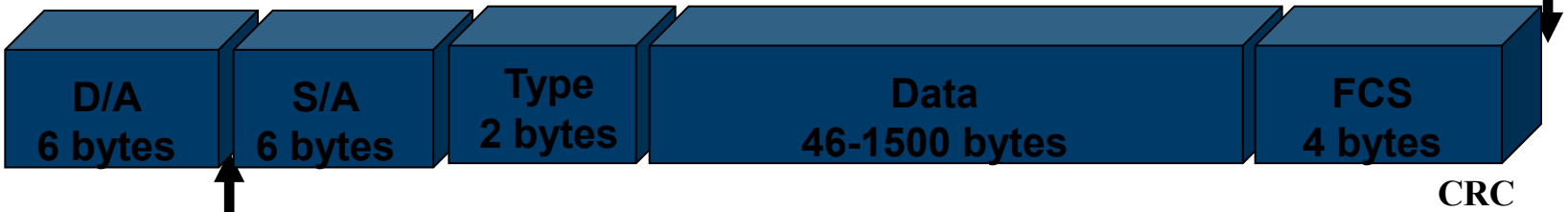
- Store-and-Forward
  - An entire frame must be received before it is forwarded. This means that the latency through the switch is relative to the frame size - the larger the frame size, the longer the delay through the switch

- Cut-Through
  - Allows the switch to begin forwarding the frame when enough of the frame is received to make a forwarding decision. This reduces the latency through the switch

Switching Techniques

Store and forward switching

Whole frame buffered in memory, then sent



Cut-through switching

Forwarding started just after the destination MAC address arrives

L2 Switching Features

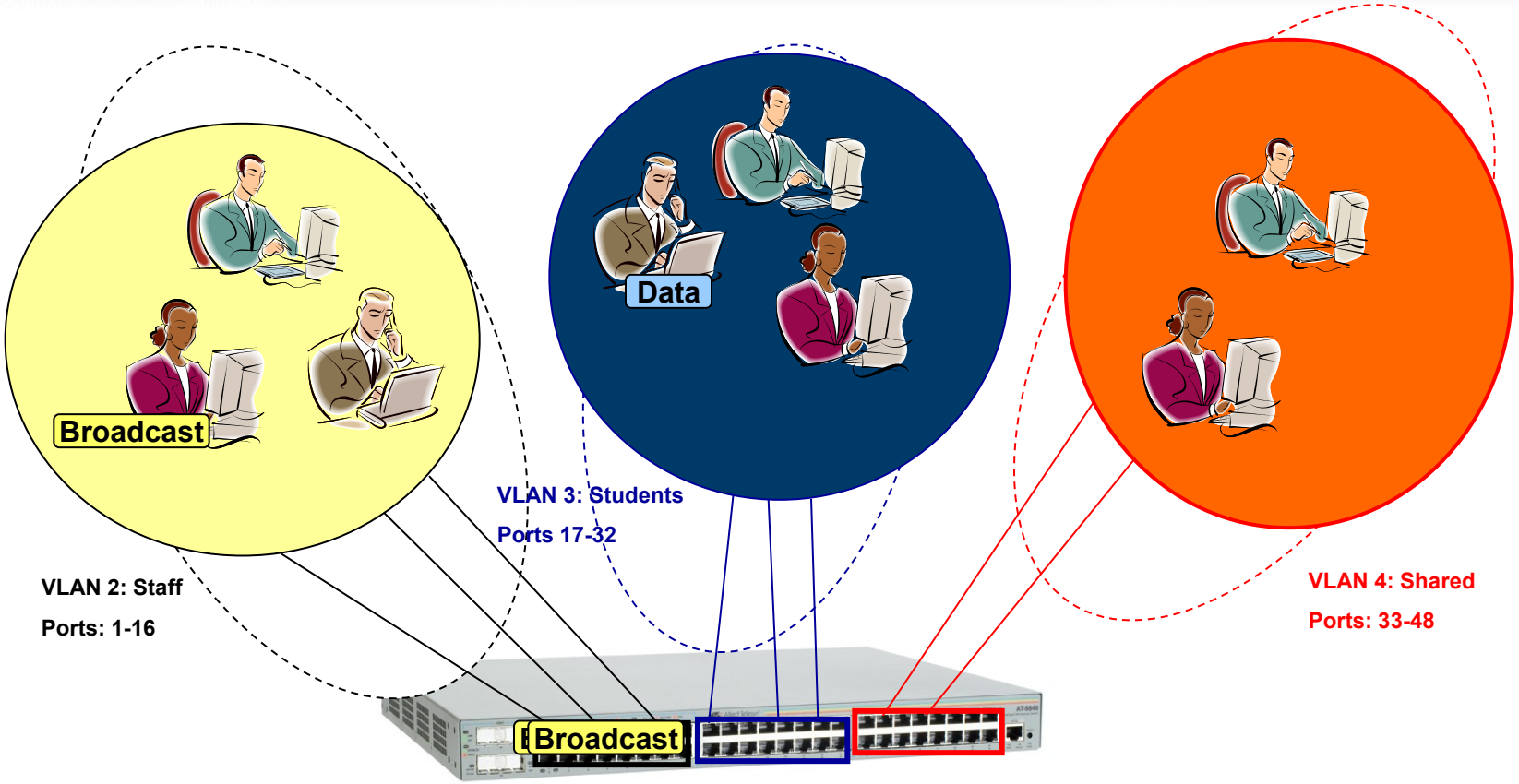
Vlan, STP, LACP, PoE

Vlan

Vlan

- Virtual Local Area Networks (VLANs) are a logical grouping of network users and resources connected to defined ports on the switch.
- VLAN features allow the network to be segmented by software management, improving network performance and security
- A Virtual LAN is a software-defined broadcast domain

Vlan

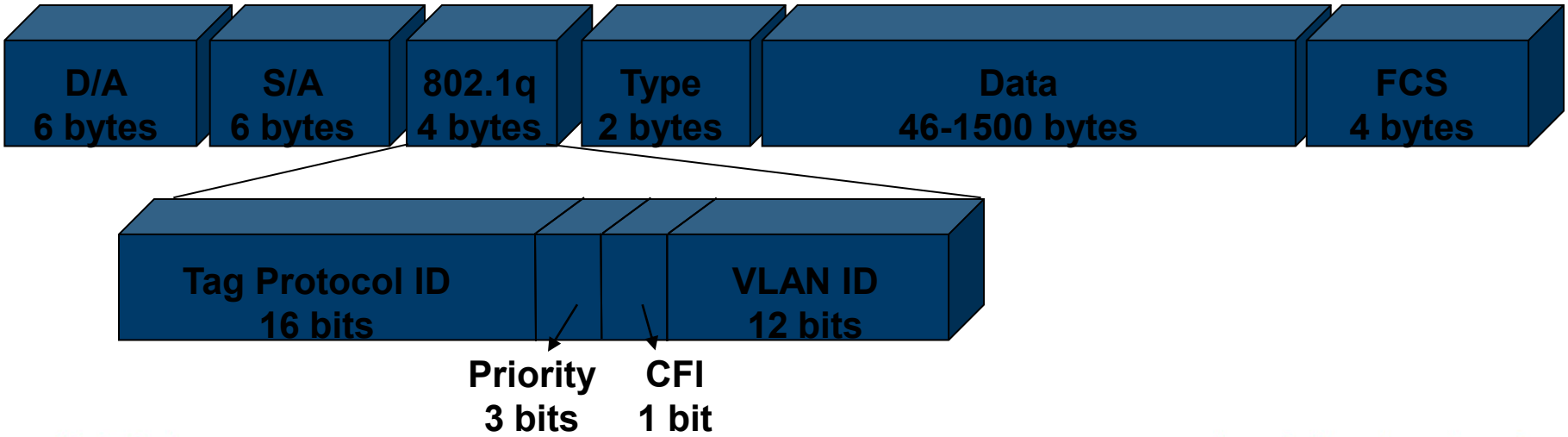

Broadcast
Data
VLAN 3: Students
Ports 17-32
VLAN 2: Staff
Ports: 1-16
VLAN 4: Shared
Ports: 33-48
Broadcast

Vlan advantages

- Further improve LAN performance, as broadcast traffic is limited to LAN segments serving members of the VLAN to which the sender belongs
- Provide security, frames are only forwarded to those stations belonging to the sender's VLAN, and not to stations in other VLANs on the same physical LAN.
- Reduce the cost of moving or adding stations to function or security based LANs, as this generally requires only a change in the VLAN configuration

Vlan 802.1q and Cos 802.1p

- To accommodate Vlan identification within an Ethernet frame, a 4-byte 802.1q Tag is added to the frame
- This increases the maximum Ethernet frame size to 1522 bytes



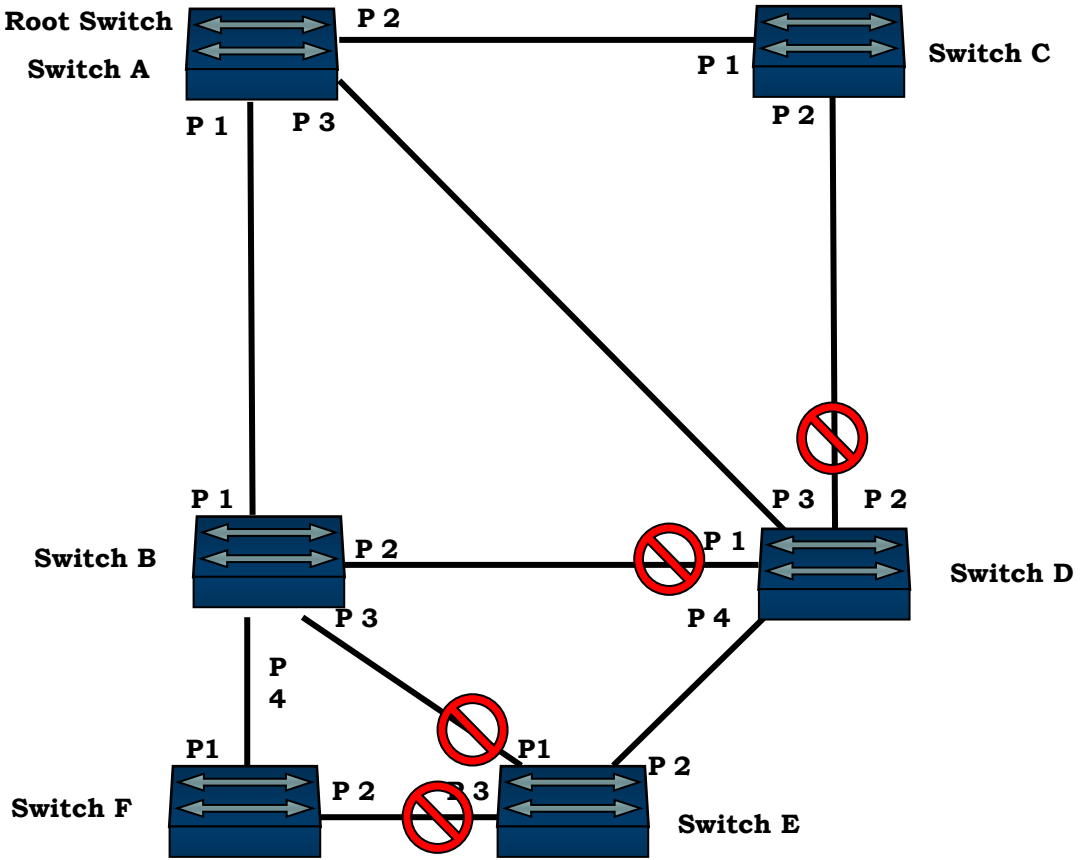
STP

Spanning Tree Protocol

» Spanning Tree Protocol was developed to prevent routing loops in a network. If a router, bridge, or switch has more than one path to the same destination, a routing problem could occur.

» The Spanning Tree Protocol automatically disables redundant paths in a network to avoid loops, and enables them when a fault in the network means they are needed to keep traffic flowing

Spanning Tree Protocol



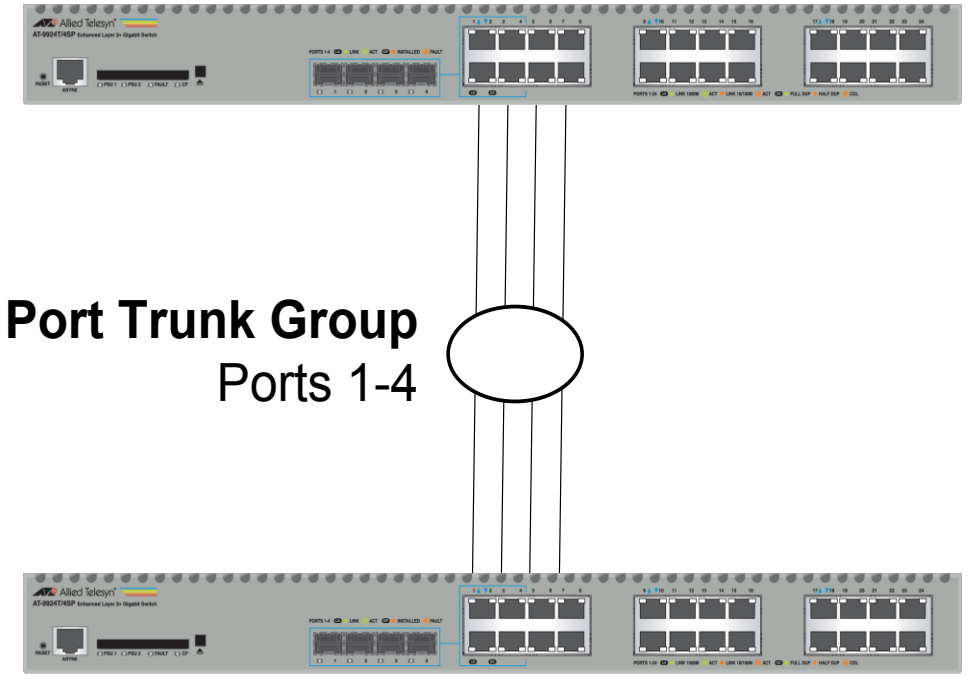
Port Aggregation

Port Trunking or link Aggregation

- Ability to support multiple, point-to-point, parallel active links between switches or between a switch and a server
- Link Aggregation allows a number of ports to be configured to join together to make a single logical connection providing:
  - Higher Bandwidth
  - Redundancy
  - Load Sharing
- A trunk group may not include Ethernet ports and Gigabit ports or Copper and Fiber ports

Port Trunking or link Aggregation

Port Trunking



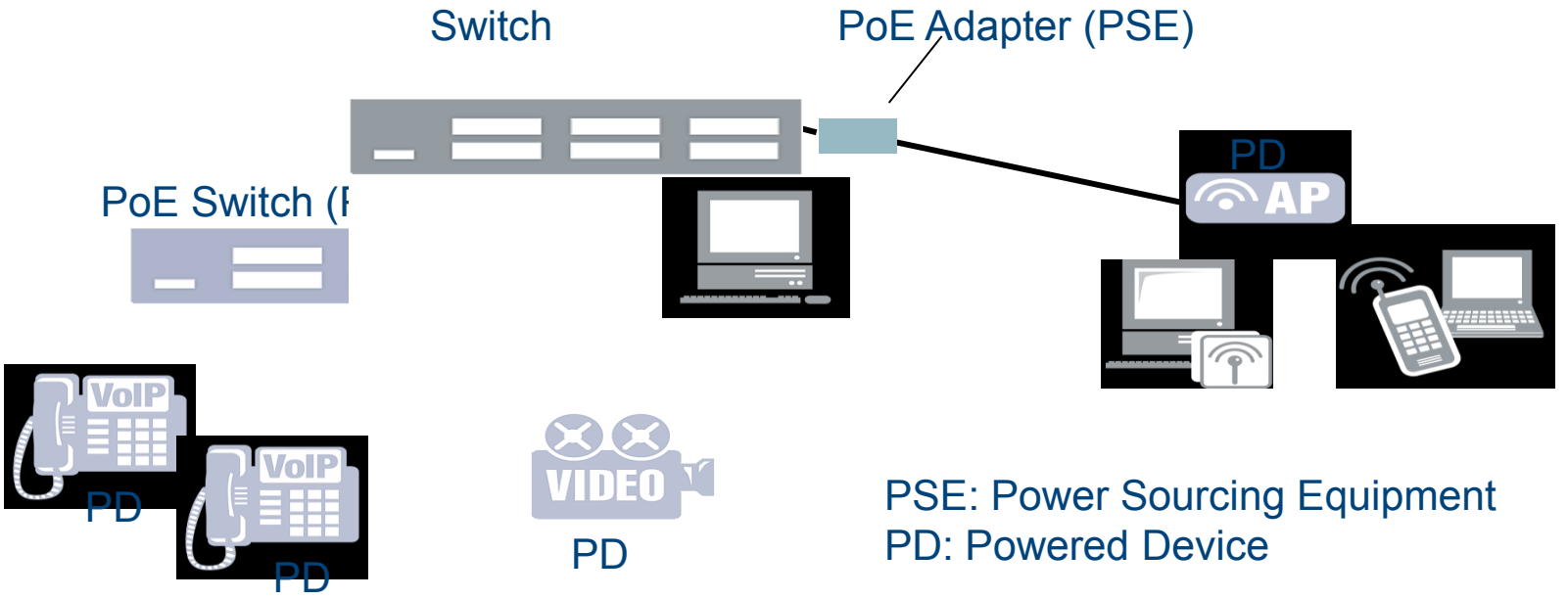
Power Over Ethernet

PoE

Power over Ethernet (PoE)

- Power over Ethernet (PoE) is a technology allowing devices such as IP telephones to receive power over existing LAN cabling
- Power is supplied to network devices over the same cabling used to carry network traffic
- Devices that require power are called Powered Devices (PDs)
- Devices that provide power to PDs are called Power Sourcing Equipment (PSE)

Power over Ethernet (PoE)



Advantages of PoE

- A single cable between switch and Powered Device (PD)
- No separate power installation/ connection needed for PD's
- Device placement is not limited to nearby power sources
- PD's can be easily moved to wherever there is LAN cabling
- Safer - no mains voltages anywhere
- A UPS can guarantee power to devices during mains failure
- Devices can be shut down or reset remotely
- Little configuration or management required

Delivered Power

- The IEEE 802.3af standard supports delivery of up to 15.4 watts per port

- The IEEE 802.3at standard supports delivery of up to 30 watts per port

Power Classes

» The power classes outlined by IEEE 802.3af/at are:

Class	Power usage
0	0.44 W to 30W (default)
1	0.44 W to 3.84 W
2	3.84 W to 6.49 W
3	6.49 W to 12.95 W
4	30w

TCP / IP

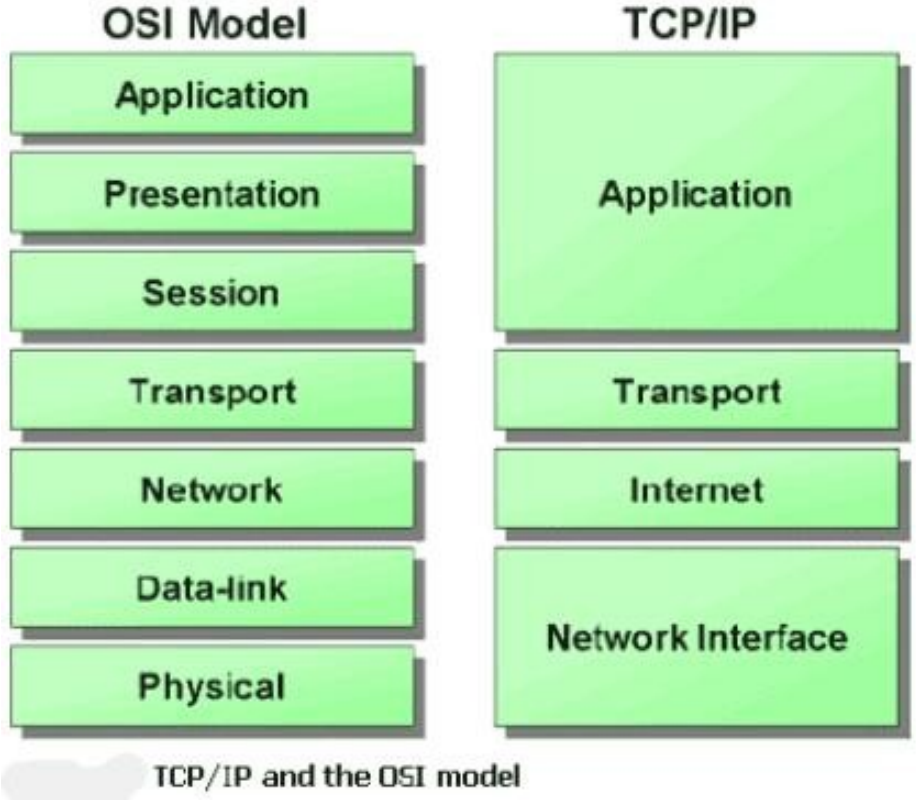
IPv4

Introduction to TCP/IP

- TCP/IP began as a non-commercial project in the 1970s. It was a military project of the U.S. Defence Advanced Research Projects Agency (DARPA)
- The TCP/IP suite is a layered model similar to the OSI reference model.
- Its name is actually a combination of two individual protocols, Transmission Control Protocol (TCP) and Internet Protocol (IP).
  - It is divided into layers, each of which performs specific functions in the data communication process.

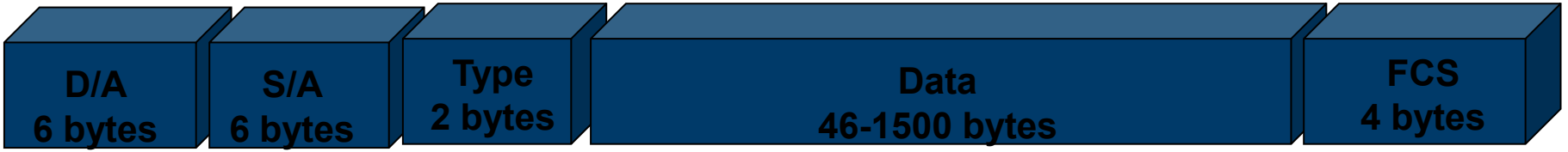
Introduction to TCP/IP

» To understand TCP/IP, it is useful to compare its layers with the OSI Reference Model

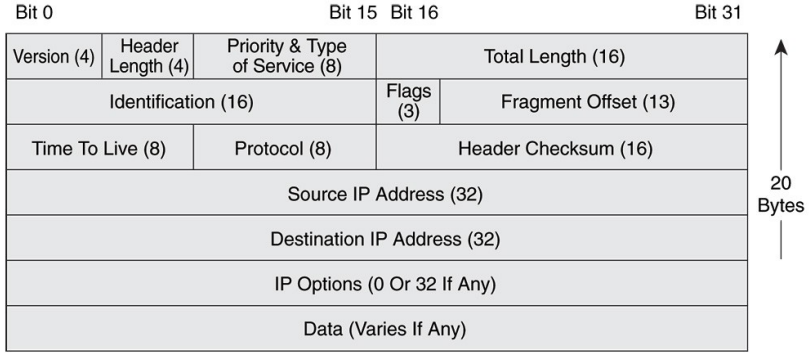


TCP/IP and the OSI model

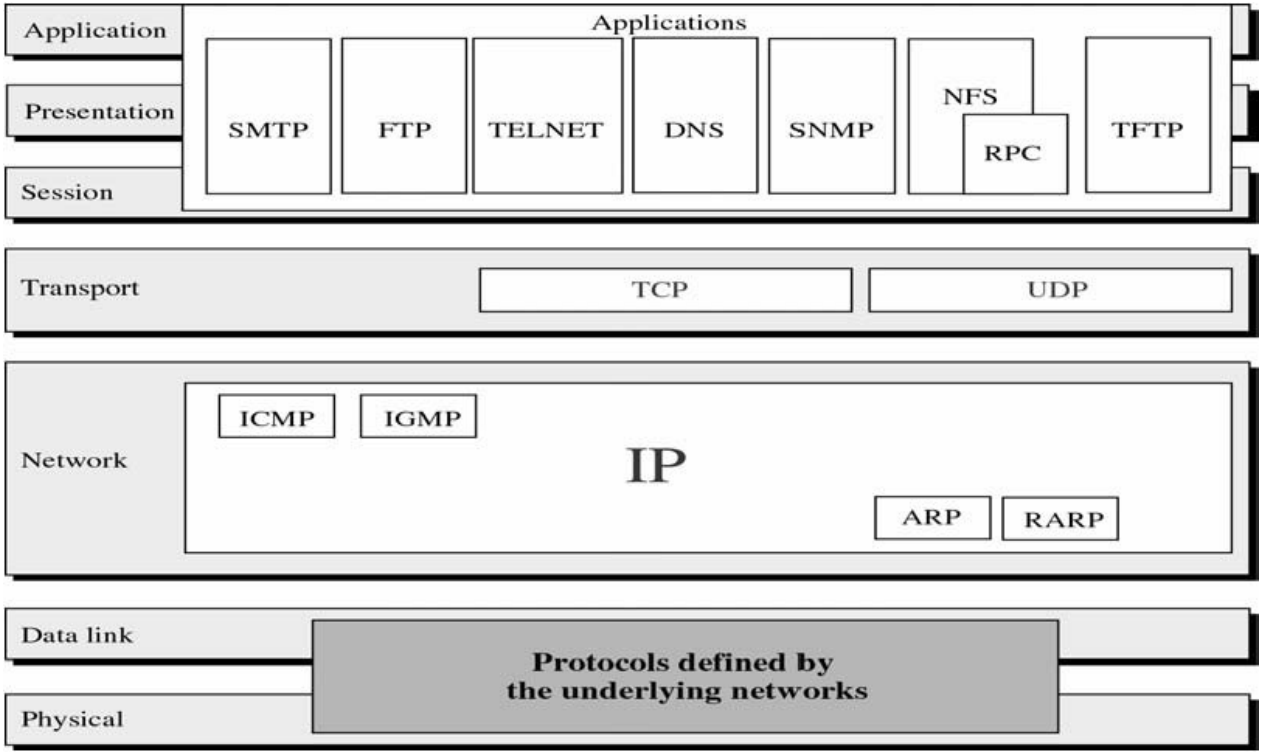
Ethernet Frame: IP Header



CRC



TCP/IP Elements



Transport Layer - L4

» TCP and UDP are two alternative transport protocols
  – TCP: flow control end-to-end
  – UDP: simple transport, not a reliable protocol

» They can operate simultaneously with many applications using port numbers

TCP/UDP Ports

- In a TCP or UDP packet, the port number defines which application in the upper layer will receive the packet
- Ports are the medium through which client applications address a server application
  - E.g., an FTP client connecting to an FTP server must use
    - the IP address of the remote host
    - the TCP port number associated to the FTP server

Well Known Ports TCP/UDP Ports

Service	Port	TCP	UDP
FTP	21	X	
Telnet	23	X	
SMTP	25	X	
TFTP	69		X
HTTP	80	X	
POP	110	X	
NTP	119	X	
SNMP	161		X

TCP

- Used by applications that need reliable transmission of information (e.g. Telnet, FTP, SMTP, etc.)

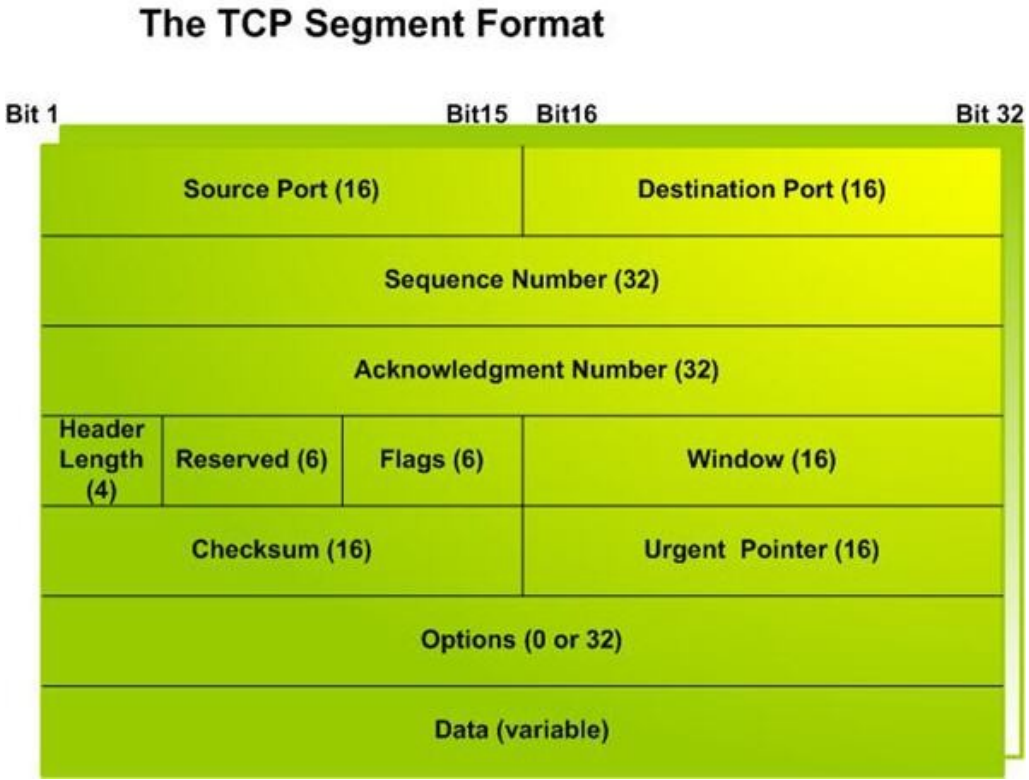
- TCP functions include
  - Error Checking
  - Flow control
  - State check and synchronisation check

- TCP assures packet delivery, UDP does not!

TCP

- A virtual circuit is established between the TCP layers of two communicating nodes
- This virtual circuit is associated to a transport protocol providing for
  - full-duplex communication
  - an acknowledge mechanism
  - flow control
- TCP needs more bandwidth and CPU resources than UDP

TCP Packet



- Source and destination ports identify the end points of the virtual connection
- Sequence number is the serial number of the transmitted packet, used to check if any packet has been lost
- Acknowledgement number indicates the next frame number that the receiver is waiting to receive

UDP

- UDP adds two functions to IP
  - information multiplexing between applications
  - checksums to verify data integrity

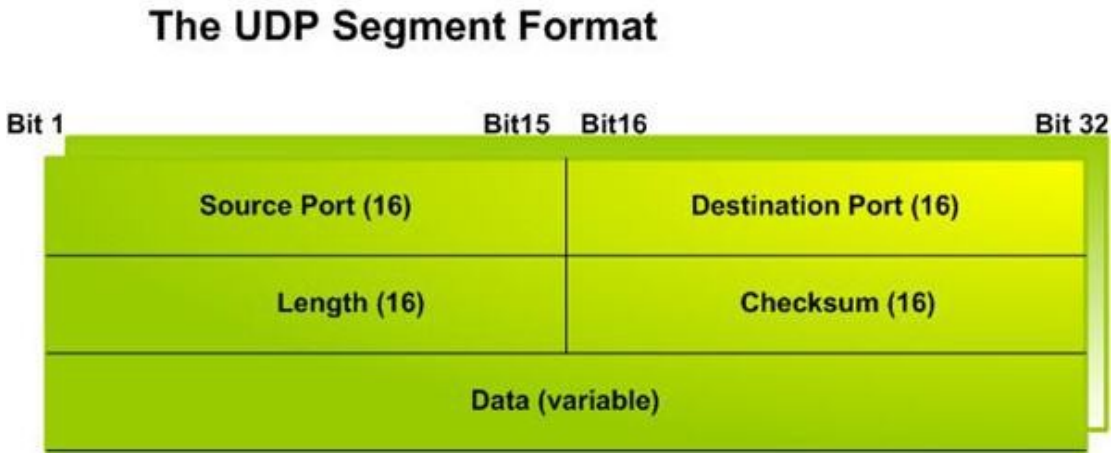
- UDP doesn't provide flow control mechanisms
  - it cannot adapt dynamically to traffic flow changes
  - it doesn't provide retransmission after errors; retransmission must be managed by the application
  - it is suitable for multimedia applications
- Error checking
  - it checks the packet integrity, but cannot correct errors

UDP

- The main applications that use UDP are
  - NFS (Network File System)
  - SNMP (Simple Network Management Protocol)
  - Multimedia streaming (multicast traffic)

- Useful when
  - the application encapsulates all data in a single packet
  - it is not important that all packets arrive to destination
  - the application itself manages retransmission

UDP Packet

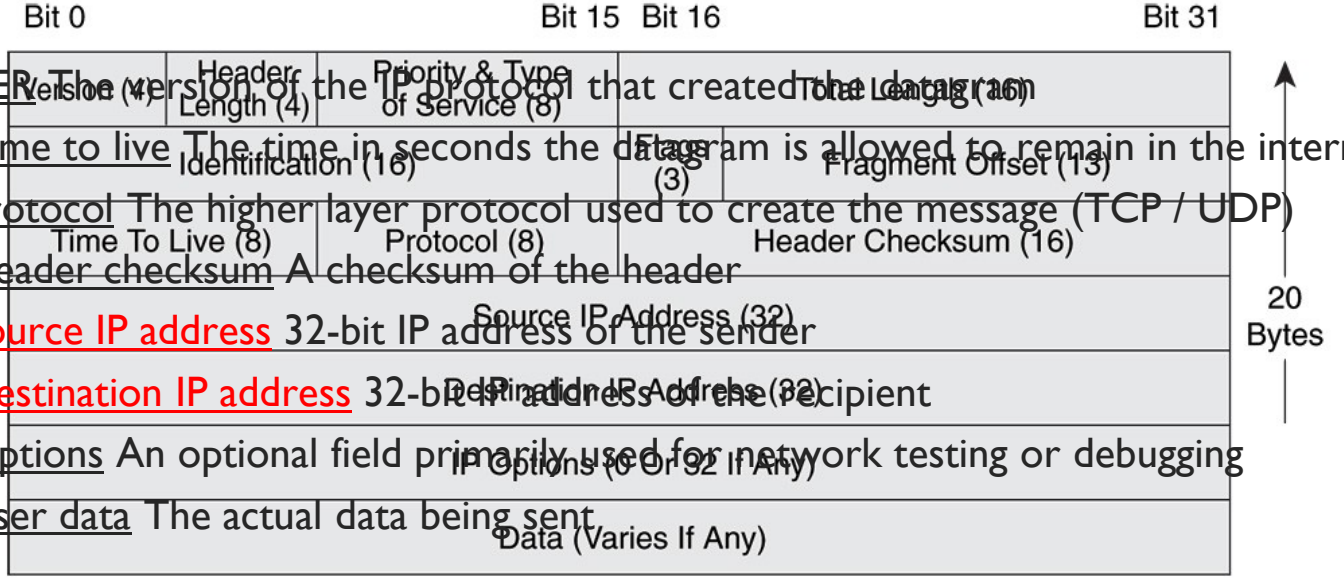


- Source and destination ports identify the end points of the virtual connection
- Checksum and UDP source are optional and can be set to 0

Network Layer - IP Protocol

- It receives data from transport layer and encapsulates them in packets
- It routes these packets on the subnet, possibly breaking them into fragments
- At the destination
  - pastes (if necessary) the fragments in packets
  - takes out the transport layer data from these packets
  - sends the data to the transport layer in the order in which they arrived (which could be different from the order in which they were sent)

IP Datagram



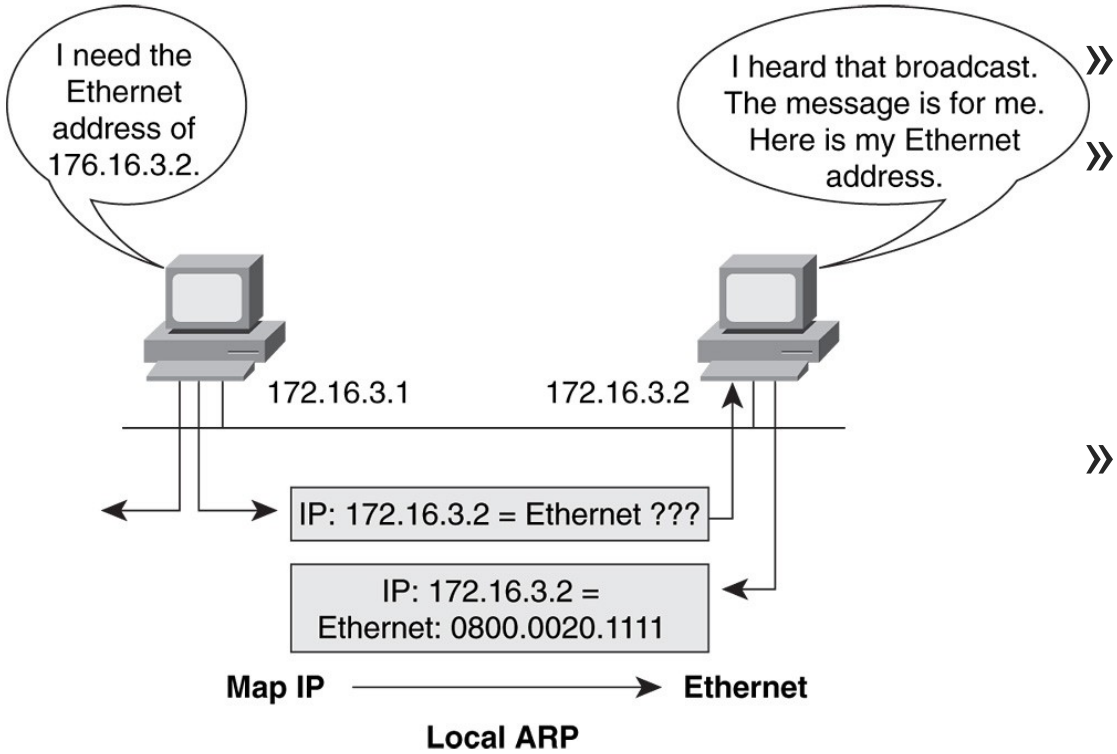
- VER The version of the IP protocol that created the datagram
- Time to live The time in seconds the datagram is allowed to remain in the internet system
- Protocol The higher layer protocol used to create the message (TCP / UDP)
- Header checksum A checksum of the header
- Source IP address 32-bit IP address of the sender
- Destination IP address 32-bit IP address of the recipient
- Options An optional field primarily used for network testing or debugging
- User data The actual data being sent

- IP is the network layer for TCP/IP and it is a simple datagram protocol

Control Protocols

- Some protocols are designed to provide control on IP subnets
  - ARP
  - RARP
  - ICMP (ping)

ARP - Address Resolution Protocol



- ARP works at Layer 2
- For IP on Ethernet, the logical (IP) address needs to be bound to MAC address of its destination.
- Each IP device on a network segment maintains an ARP table in its memory.

ARP - Address Resolution Protocol

- The ARP table maintains a correlation between each IP address and its corresponding MAC address.
- The ARP table, or ARP cache, keeps a record of recent bindings of IP addresses to MAC addresses.
- The ARP table is created and maintained dynamically, adding and changing address relationships as they are used on the local host. The entries in an ARP table usually expire after a period of time, by default 300 seconds; however, when the local host wants to transmit data again, the entry in the ARP table is regenerated through the ARP process.

RARP - Reverse ARP

- It is used to discover the IP address of a host starting from its physical address (data link address)

- Useful when it is necessary to connect stations without a hard disk; during the boot operation they load from a server the image of the binary code of the operating system

Internet Control Message Protocol

- ICMP is used to verify the state of the network
  - Echo request and echo reply

- Used to report wrong behaviours
  - Ping
  - Destination Unreachable
  - Time Exceeded for a datagram
  - Parameter Problem on a datagram

Allied Telesis™

TCP / IP

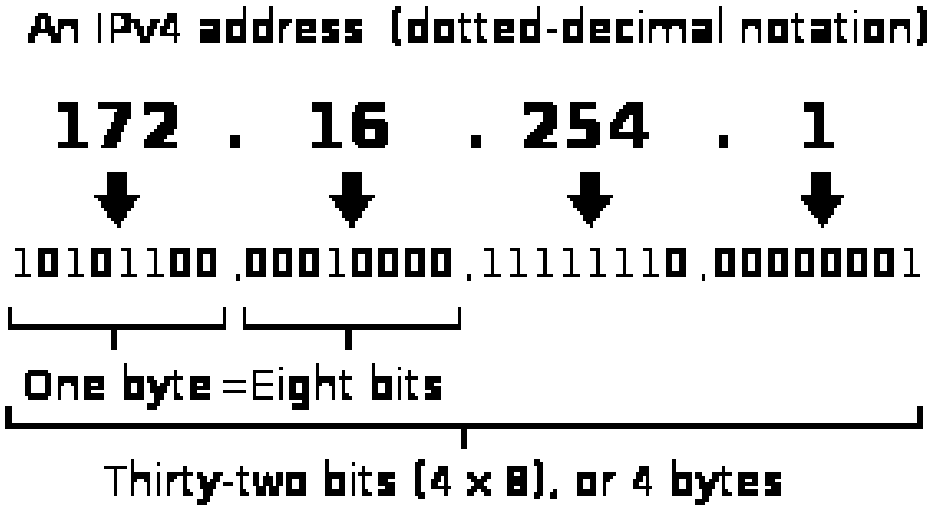
IPv4 Addressing

IPv4 Addressing

- IP addresses are 4 octet (32 bit) numbers that identify both
  - network address, i.e. the number assigned to the IP network; a network is made of a single communication channel connected to the hosts (for example a LAN or a point to point line between two routers)
  - host address, i.e. the number that identifies a specific host

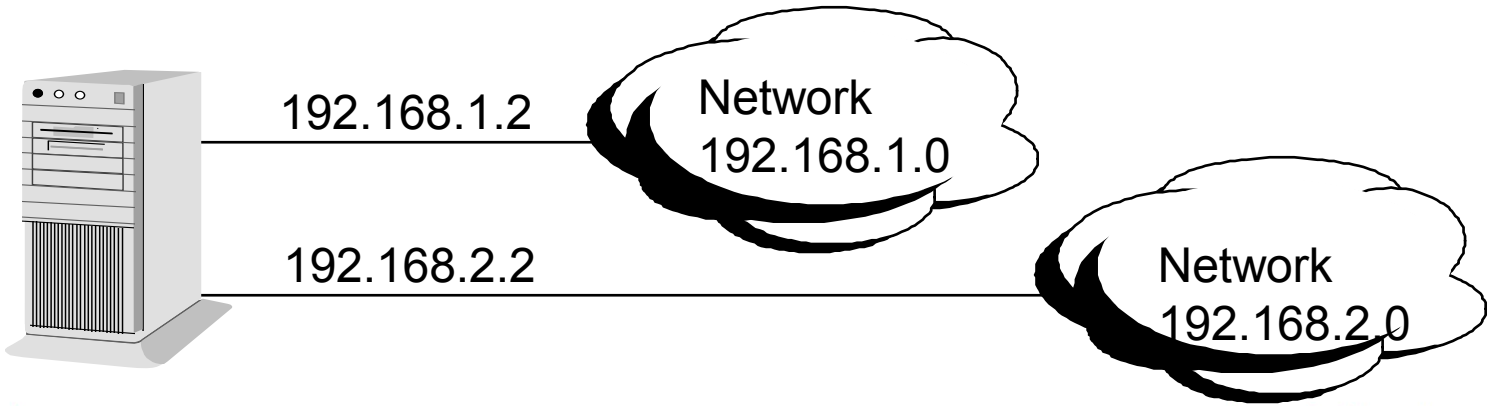
IP Addressing

» IP addresses are represented in dotted decimal notation: each byte is expressed in decimal notation and they are separated by a dot



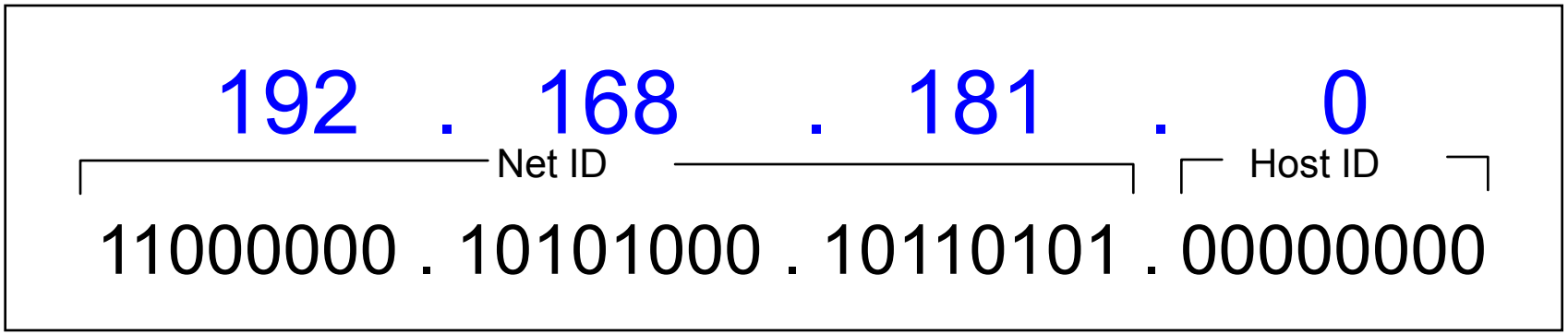
IPv4 Addressing

» Since IP numbers encode both a network and a host address, they do not specify an individual machine, but a connection to a network

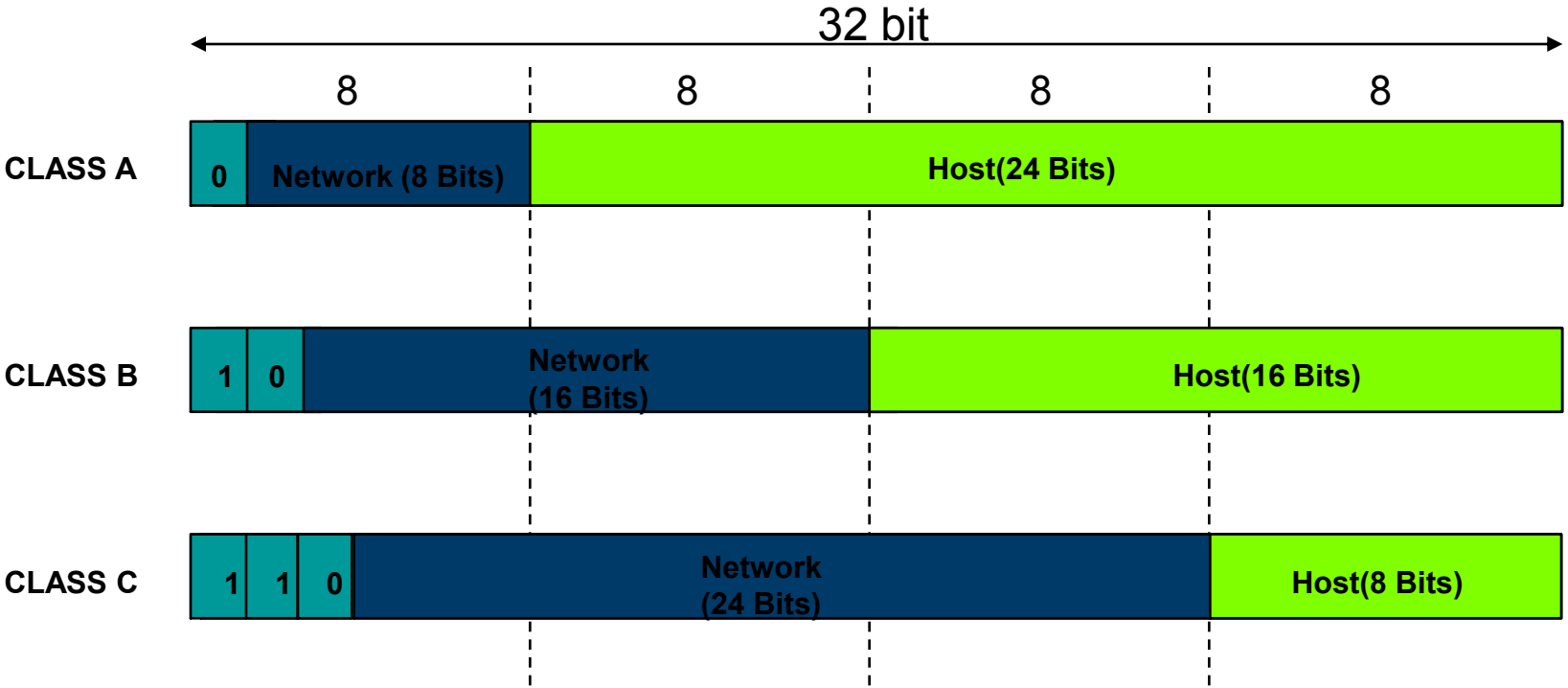


Network Addresses

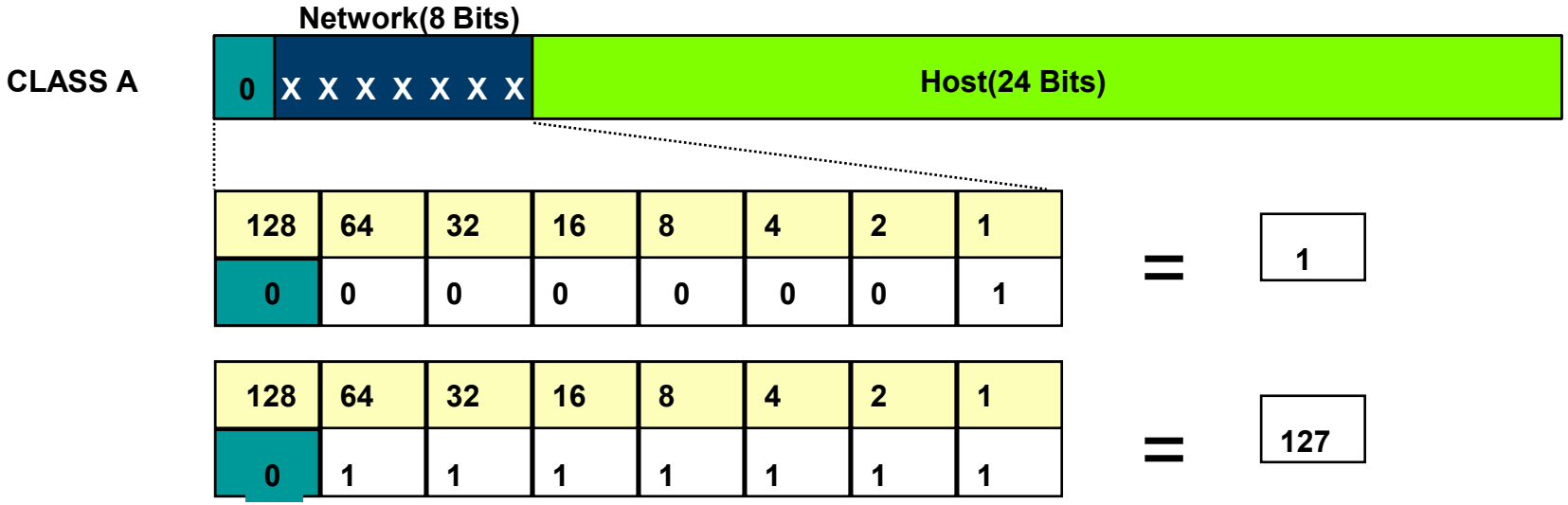
- Internet addresses can be used to refer to networks as well as to individual hosts
- By convention, a network address has a host ID with all bits set to zero



IANA Primary IP Address Classes



CLASS A



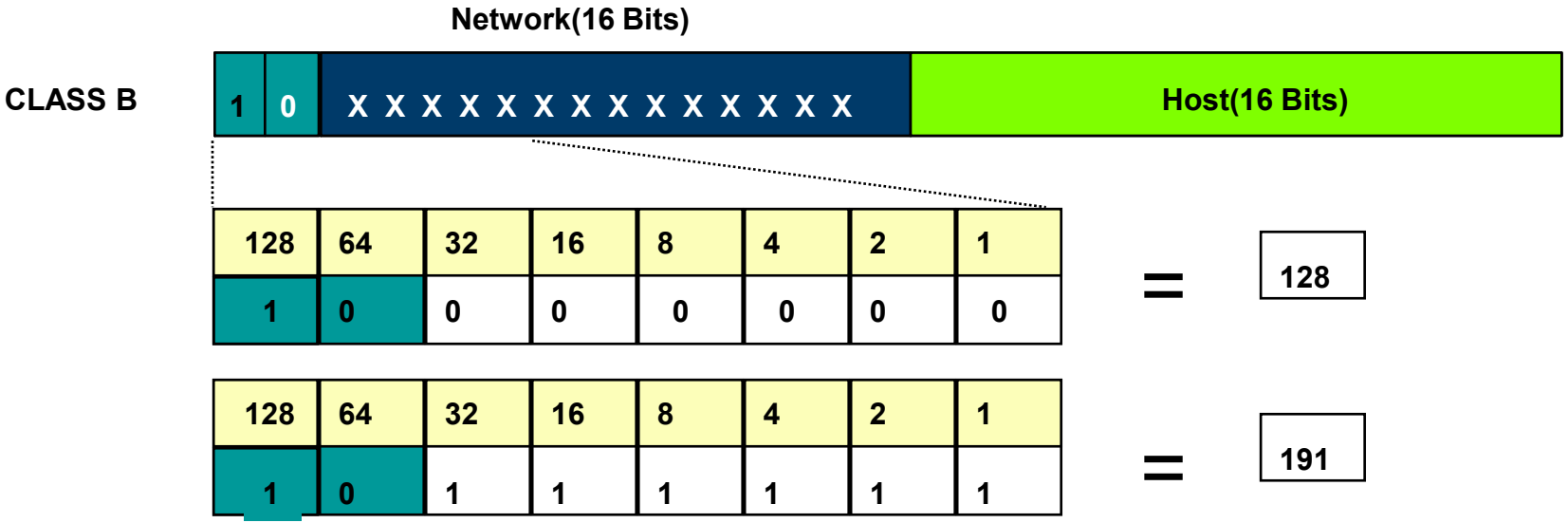
- Class A first byte range: 1-127
- First bit of network field fixed to 0

Class A Addresses

- With class A addresses, the Most Significant Bit (MSB) is reserved and must be zero, this results in the following range of network addresses
  - networks 1 – 126
  - network 127 is reserved for Loopbacks

- There are 126 usable networks
- Each with 16,777,216 (2^{24}) hosts

CLASS B



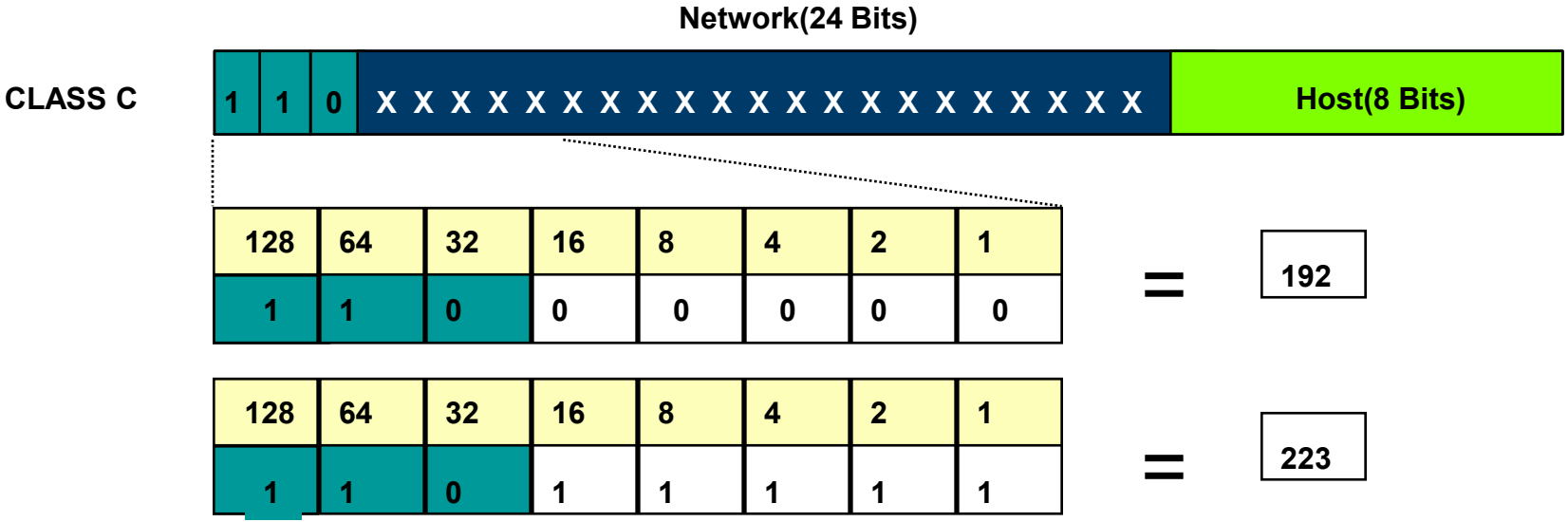
- Class B first byte range: 128-191
- First two bits of network field fixed to 1|0

Class B Addresses

- With class B addresses the two Most Significant Bits (MSB) are reserved (1 0), this results in the following range of network addresses
  - networks 128 – 191

- There are 16,384 (2^6 x 2^8) usable networks
- Each with 65,536 (2^{16}) hosts

CLASS C



- Class C address range: 192-223
- First three bits of network field fixed to 1|1|0

Class C Addresses

- With class C addresses the 3 Most Significant Bits (MSB) are reserved (1 1 0), this results in the following range of network addresses
  - networks 192 – 223

- There are 2,097,152 (2^5 x 2^8 x 2^8) usable networks
- Each with 256 (2^8) hosts

IANA IPv4 Classes

	8 bits	8 bits	8 bits	8 bits
Class A	Network	Host	Host	Host
Class B	Network	Network	Host	Host
Class C	Network	Network	Network	Host
Class D	Multicast			
Class E	Reserved			

Class	**Address range (High octet)**	**Mask**
Class A	0 - 127	255.0.0.0
Class B	128 – 191	255.255.0.0
Class C	192 - 223	255.255.255.0

Special IPv4 Addresses: Loopback and Private Addresses

- Local loopback subnet within each host: address 127.0.0.1 / 8

- Private addresses are needed due to shortage of public addresses
- Private addresses, which should never be declared in a public network
- Access to private addresses from the public network is typically via NAT (Network address translation)

Address Class	Reserved address space
Class A	10.0.0.0 through 10.255.255.255
Class B	172.16.0.0 through 172.31.255.255
Class C	192.168.0.0 through 192.168.255.255

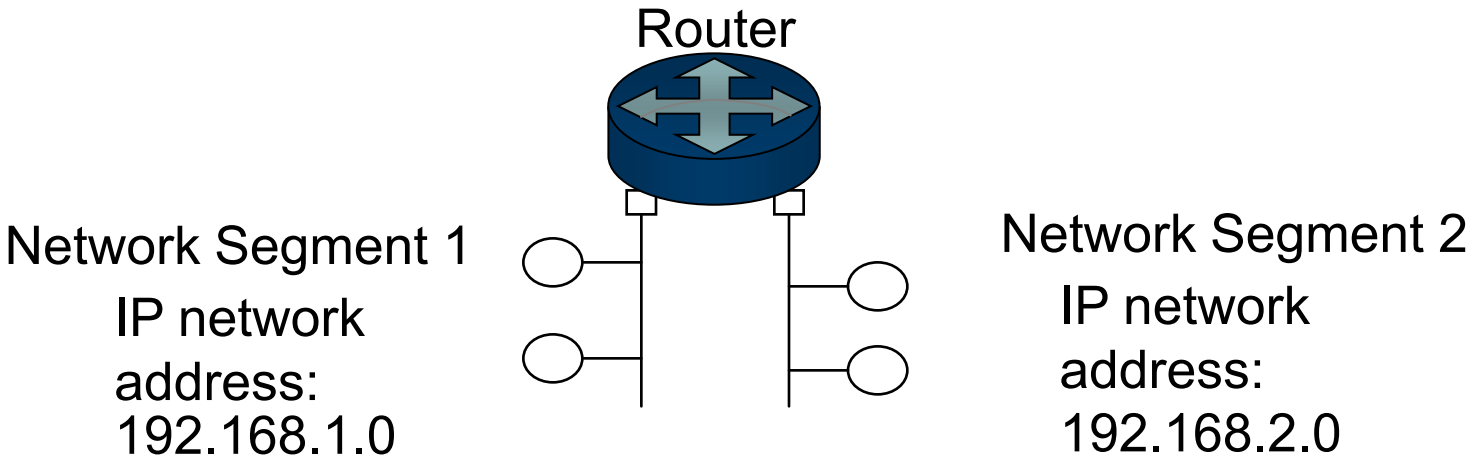
Network Addresses

» In order to establish simple communication, hosts must have the same network addresses

» If hosts have different network addresses, then we must use a router to connect two network segments

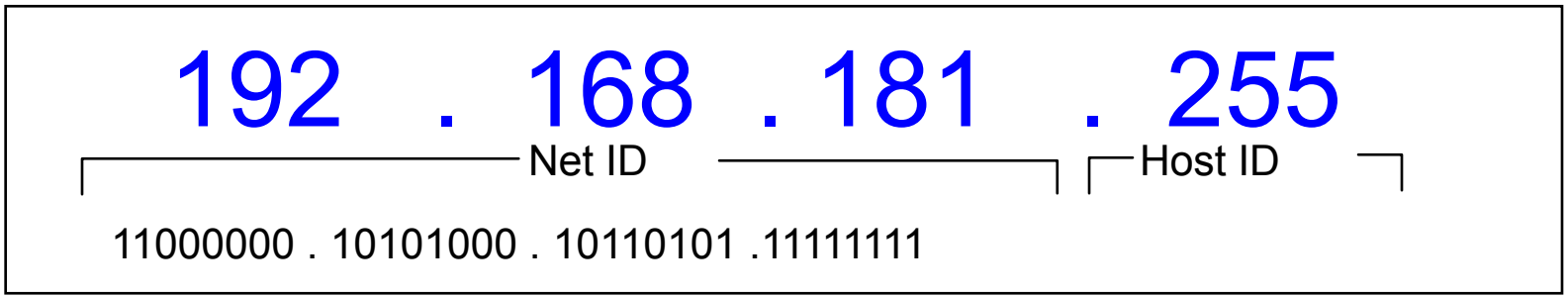
Network Addresses

» A router can connect only IP network segments that have different network addresses



Broadcast Addresses

- The broadcast address is used to send a message to all users on the network
- By convention, a broadcast address has a host ID with all bits set to one



IP Subnet Masks

- Routing is based on the Net ID portion of IP addresses and routers need to extract this portion quickly for efficient routing
- To do this, a subnet mask is used
- The subnet mask acts as an indicator of the network portion of an IP address

IP Subnet Masks

- The subnet mask uses bits set to 1 to indicate the network portion of the address and bits set to 0 to indicate the host portion

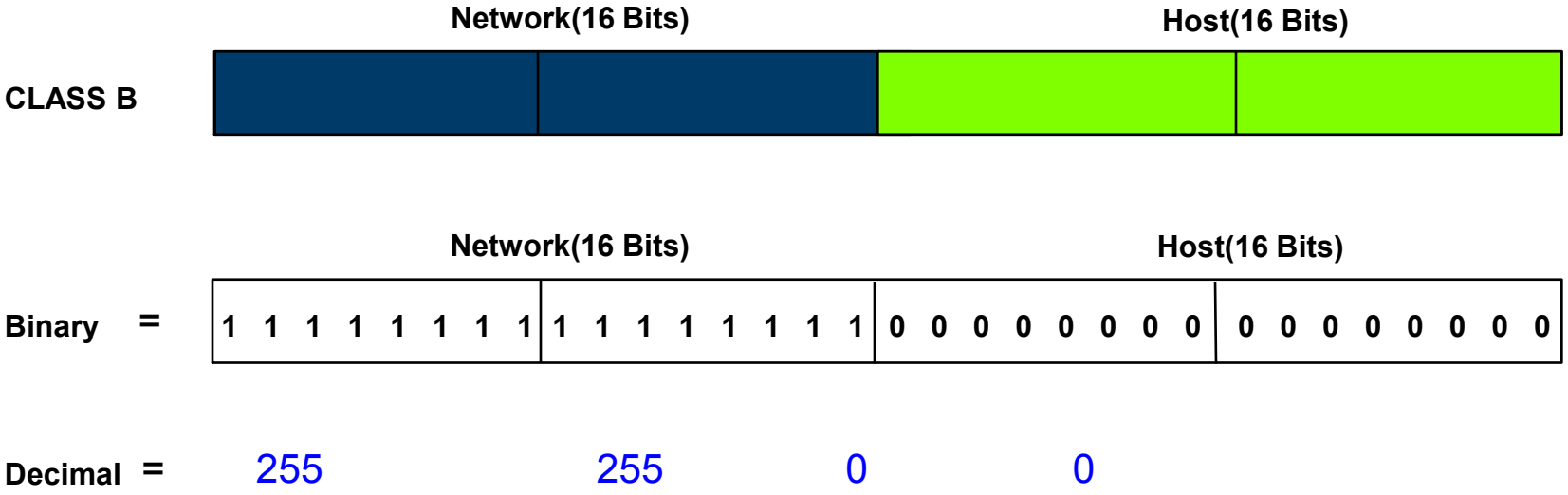
- The mask is written in dotted decimal notation

Class A Default Subnet Mask

	Network(8 Bits)								Host(24 Bits)								Host(24 Bits)							
Binary =	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Decimal =	255								0								0							

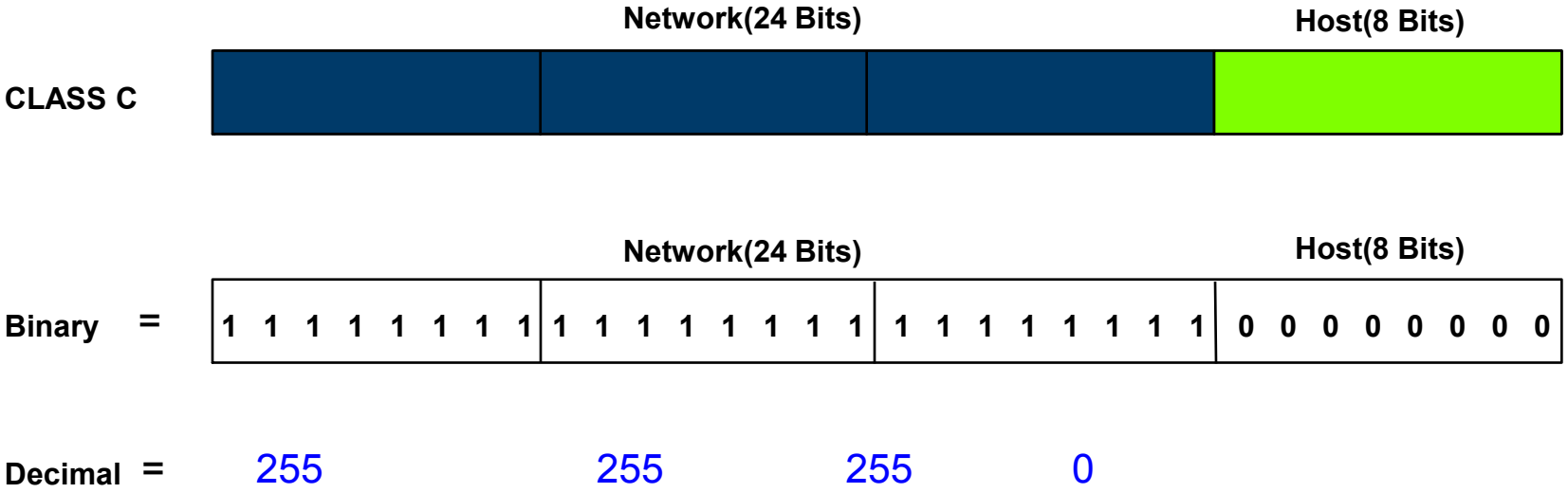
In a Class A, the first 8 bits are reserved by default as networking bits and the remaining 24 bits are host bits

Class B Default Subnet Mask



In a Class B, the first 16 bits are reserved by default as networking bits and the remaining 16 bits are host bits

Class C Default Subnet Mask



In a Class C, the first 24 bits are reserved by default as networking bits and the remaining 8 bits are host bits

TCP / IP

IP Addressing: Subneting

Subnetting

- In order to reduce the number of used networks on the public Internet, every network can be divided into subnets, each one containing its own hosts
- There is no need to communicate this outside a private network
- The original network address can be seen as a couple of numbers: subnet number and host number

Subnetting

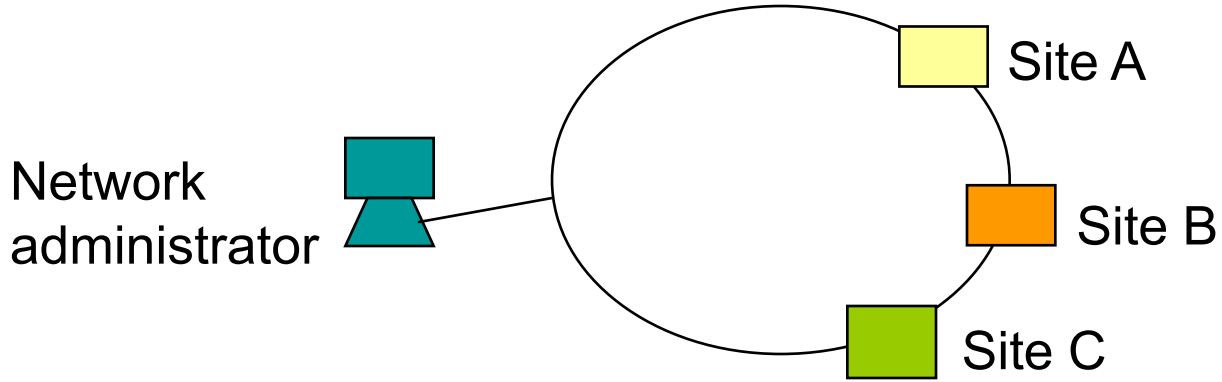
- It is possible to obtain many subnets containing few hosts or few subnets with many hosts

- Subnet masks are used to determine which bits in the IP address are networking bits and which are host bits

- The convention is that networking bits are represented by 1 and host bits are represented by 0

Subnetting Example

- Consider a company with many production sites
- There is a LAN in every site with a different network address
- The central site must administrate the whole private network



Subnetting Example

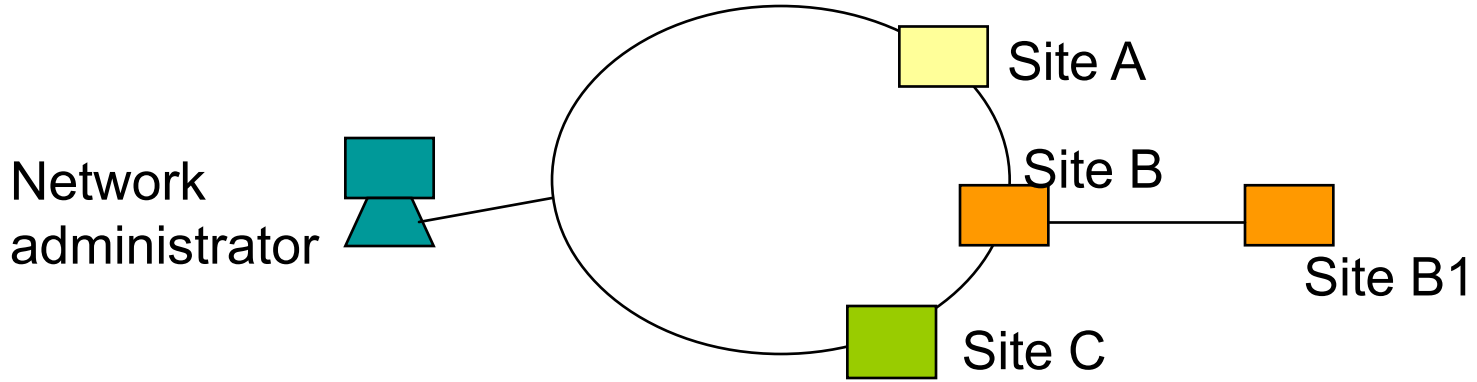
- If site B decides to open a new site (site B1), then the network administrator must give it a new network IP address
- If there are many new sites being opened, the work for the network administrator will become too big
- It is useful to connect the new site to the network in site B instead of the main network

Subnetting Example

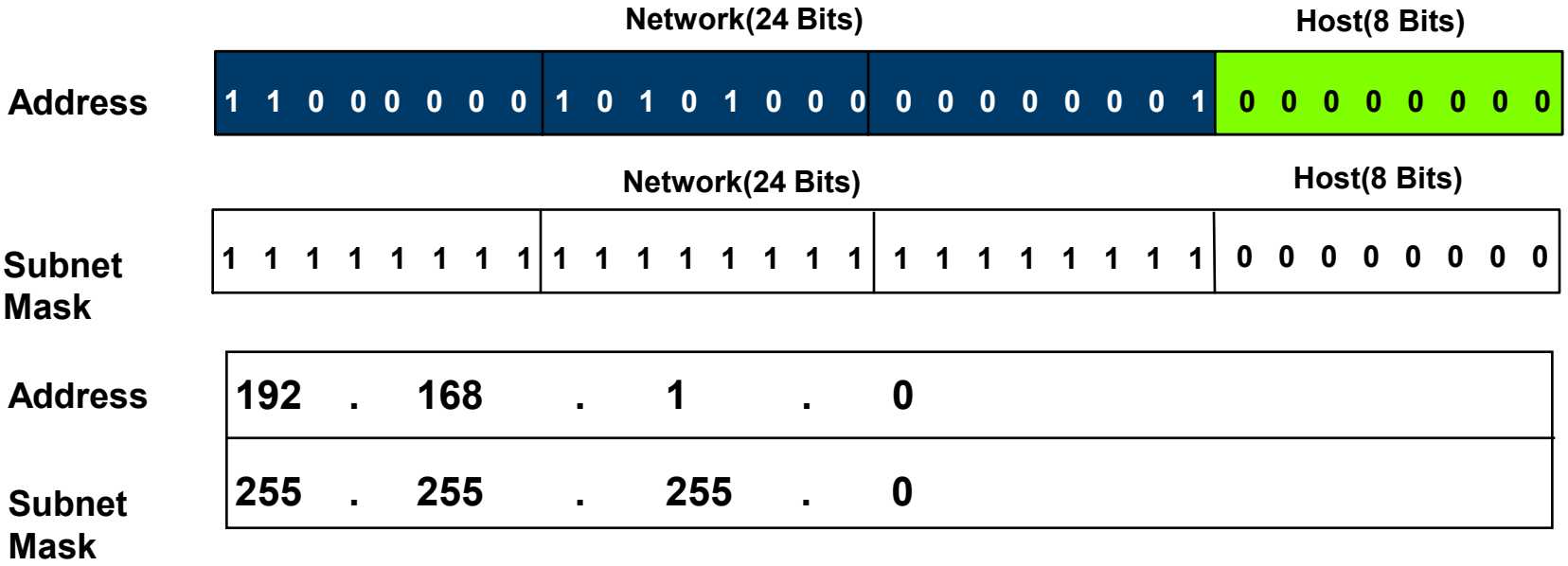
- To do this, site B will use subnetting
- All other stations will not know anything about this change; it is a private operation
- There is no need to add a new IP network address

Subnetting Example

» To create the subnet for site B1, both B and B1 must change their subnet mask number in order to obtain at least two subnets from the original network



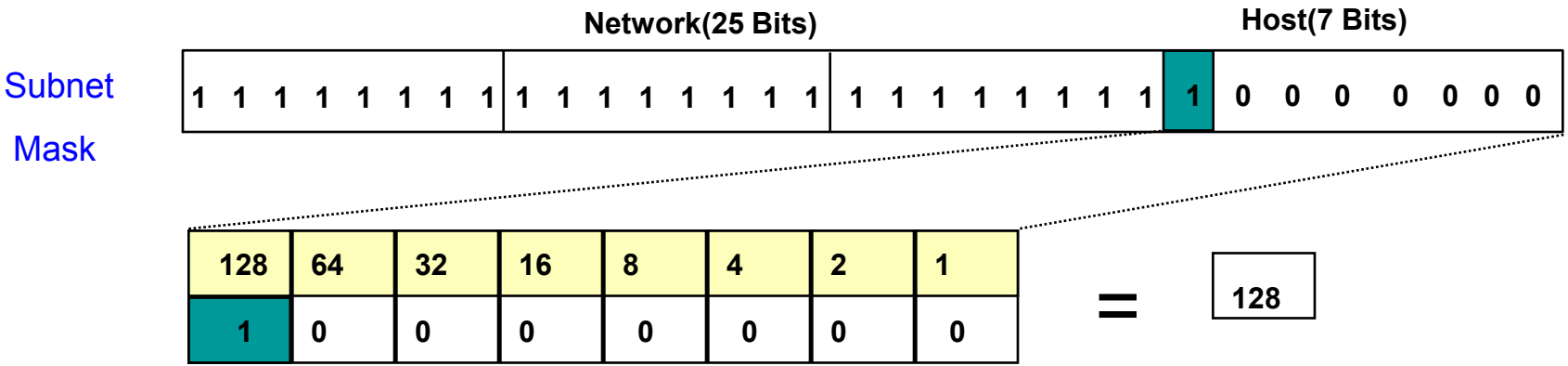
Class C Address



Here you can see a class C address with its default mask

Two Logical Networks

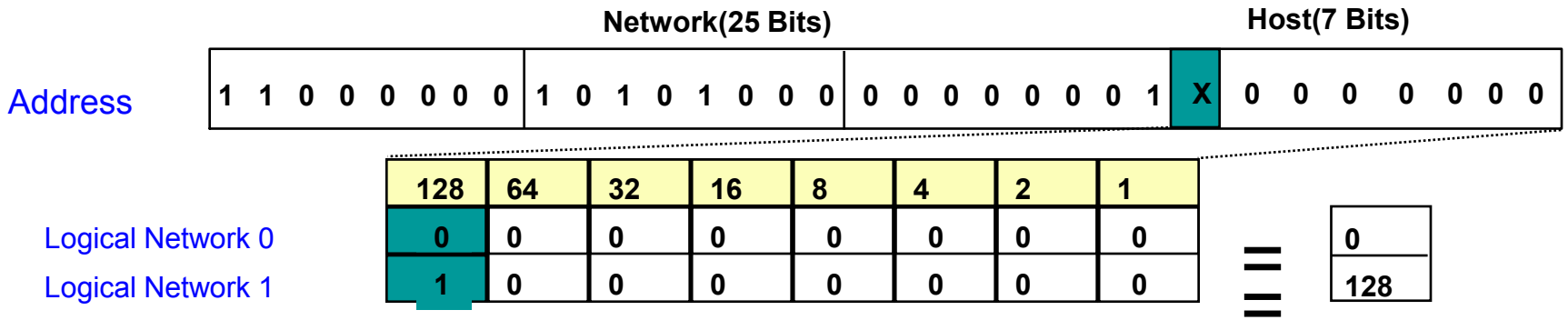
Address	192 . 168 . 1 . 0
Subnet Mask	255 . 255 . 255 . 128



If you want to obtain two logical networks from a class C address, you must modify the subnet mask to 255.255.255.128

Two Logical Networks

Address	192 . 168 . 1 . 0
Subnet Mask	255 . 255 . 255 . 128



Subnet 0 address: 192.168.1.0

Subnet 1 address: 192.168.1.128

Two Logical Networks

» In the previous example, the most significant bit of the last octet has been designated as a networking bit, which will effectively subdivide the Class C network into two logical networks, each being able to support 126 hosts and a broadcast address

Two Logical Networks

Original Addressing

192.168.1.0

255.255.255.0

Logical network 0 - 255.255.255.128

Network address 192.168.1.0

First Host address 192.168.1.1

Last Host address 192.168.1.126

Broadcast address 92.168.1.127

Logical network 1 - 255.255.255.128

Network address 192.168.1.128

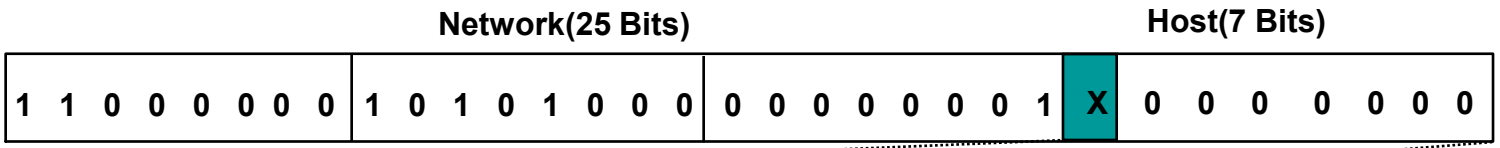
First Host address 192.168.1.129

Last Host address 192.168.1.254

Broadcast address 92.168.1.255

Two Logical Networks

Address	**192 . 168 . 1 . 0**
Subnet Mask	**255 . 255 . 255 . 128**

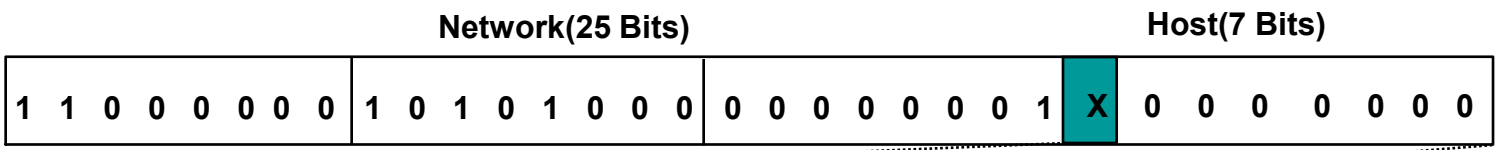


	128	64	32	16	8	4	2	1		
Logical Network 0	0	0	0	0	0	0	0	0	=	0
First Host	0	0	0	0	0	0	0	1	=	1
Last Host	0	1	1	1	1	1	1	0	=	126

For the hosts on subnet 0 you can use the range of addresses from .1 to .126

Two Logical Networks

Address	192 . 168 . 1 . 128
Subnet Mask	255 . 255 . 255 . 128



	128	64	32	16	8	4	2	1		
Logical Network 1	1	0	0	0	0	0	0	0	=	128
First Host	1	0	0	0	0	0	0	1	=	129
Last Host	1	1	1	1	1	1	1	0	=	254

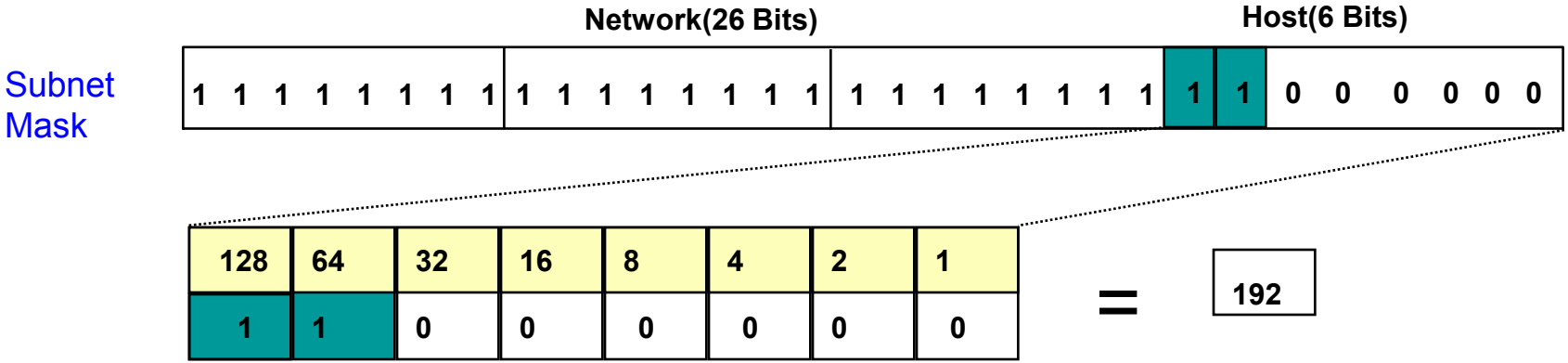
For the hosts on subnet 1 you can use the range of addresses from .129 to .254

Summary: Two Logical Networks

- If you must divide a Class C address into two networks, set the subnet mask to 255.255.255.128
- Logical network addresses
  - subnet 0 address is 192.168.1.0
  - subnet 1 address is 192.168.1.128
- Address Ranges
  - subnet 0 range is from .1 to .126
    - broadcast is .127
  - subnet 1 range is from .129 to .254
    - broadcast is .255

Four Logical Networks

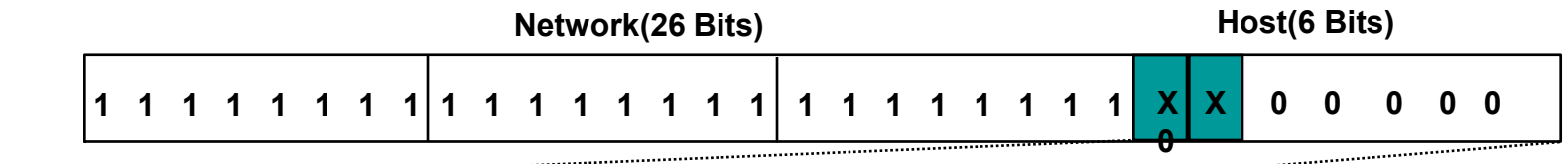
Address	192	.	168	.	1	.	0				
Subnet Mask	255	.	255	.	255	.	192				



If you want to obtain four logical networks from a class C address, you must modify the subnet mask to 255.255.255.192

Four Logical Networks

Address	192 . 168 . 1 . 0
Subnet Mask	255 . 255 . 255 . 192



	128	64	32	16	8	4	2	1	
Logical Network 0	0	0	0	0	0	0	0	0	0
Logical Network 1	0	1	0	0	0	0	0	0	64
Logical Network 2	1	0	0	0	0	0	0	0	128
Logical Network 3	1	1	0	0	0	0	0	0	192

Four Logical Networks

» In the previous example, the two most significant bits of the last octet have been designated as a networking bits which, will effectively subdivide the Class C network into four logical networks, each supporting 62 hosts and a broadcast address

Four Logical Networks

Original Addressing

192.168.1.0

255.255.255.0

Logical network 0 - 255.255.255.192

Network address 192.168.1.0
First Host address 192.168.1.1
Last Host address 192.168.1.62
Broadcast address 192.168.1.63

Logical network 1 - 255.255.255.192

Network address 192.168.1.64
First Host address 192.168.1.65
Last Host address 192.168.1.126
Broadcast address 192.168.1.127

Logical network 2 - 255.255.255.192

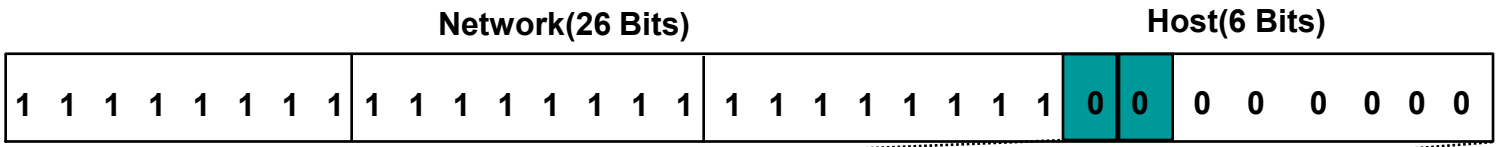
Network address 192.168.1.128
First Host address 192.168.1.129
Last Host address 192.168.1.190
Broadcast address 192.168.1.191

Logical network 3 - 255.255.255.192

Network address 192.168.1.192
First Host address 192.168.1.193
Last Host address 192.168.1.254
Broadcast address 192.168.1.255

Four Logical Networks

Address	192 . 168 . 1 . 0
Subnet Mask	255 . 255 . 255 . 192

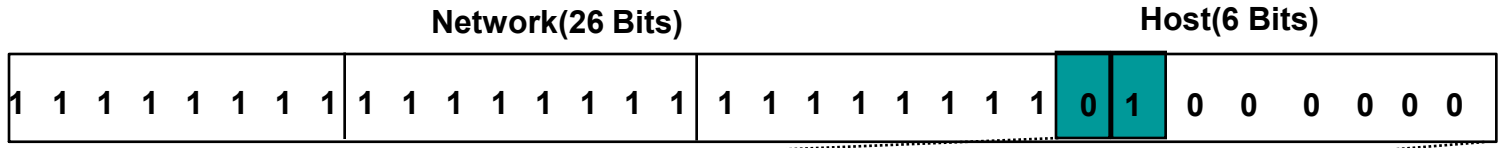


	128	64	32	16	8	4	2	1		
Logical Network 0	0	0	0	0	0	0	0	0	=	0
First Host	0	0	0	0	0	0	0	1	=	1
Last Host	0	0	1	1	1	1	1	0	=	62

For the hosts on subnet 0 you can use the range of addresses from .0 to .62; broadcast address 192.168.1.63

Four Logical Networks

Address	192 . 168 . 1 . 64
Subnet Mask	255 . 255 . 255 . 192

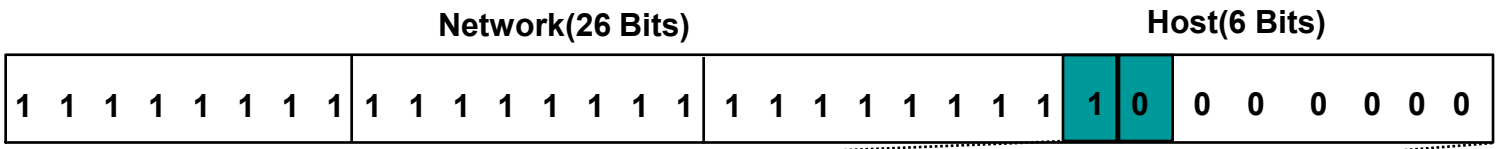


	128	64	32	16	8	4	2	1	
Logical Network 1	0	1	0	0	0	0	0	0	64
First Host	0	1	0	0	0	0	0	1	65
Last Host	0	1	1	1	1	1	1	0	126

For the hosts on subnet 1 you can use the range of addresses from .65 to .126; broadcast address 192.168.1.127

Four Logical Networks

Address	192 . 168 . 1 . 128
Subnet Mask	255 . 255 . 255 . 192

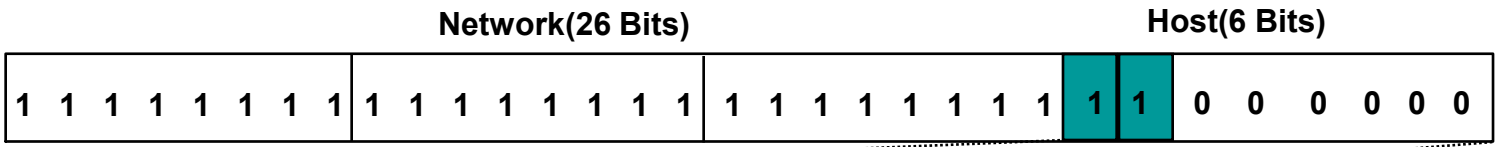


	128	64	32	16	8	4	2	1	=
Logical Network 2	1	0	0	0	0	0	0	0	128
First Host	1	0	0	0	0	0	0	1	129
Last Host	1	0	1	1	1	1	1	0	190

For the hosts on subnet 2 you can use the range of addresses from .129 to .190; broadcast address 192.168.1.191

Four Logical Networks

Address	192 . 168 . 1 . 192
Subnet Mask	255 . 255 . 255 . 192



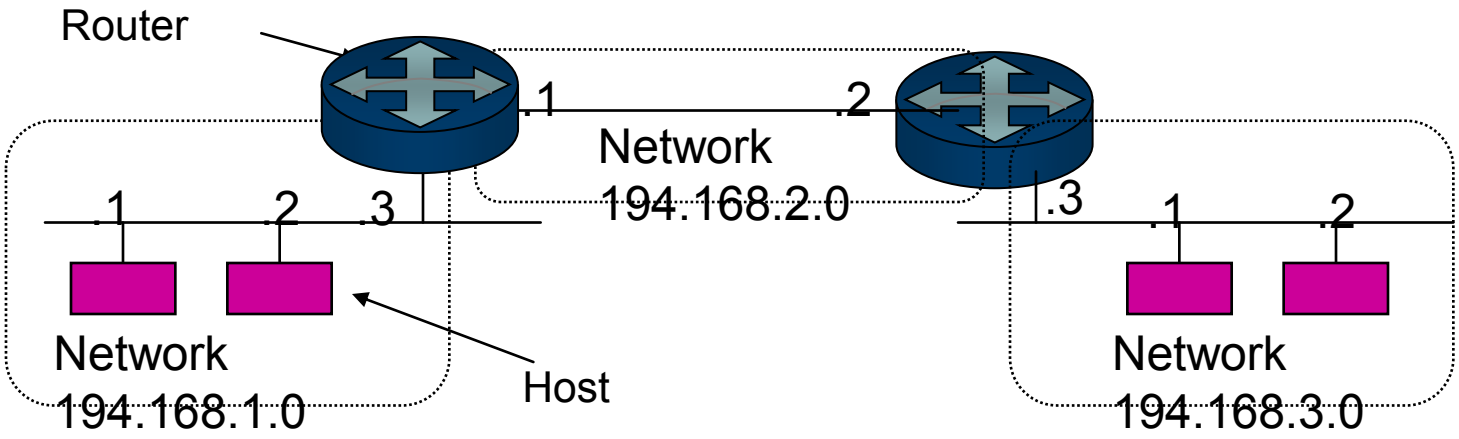
	128	64	32	16	8	4	2	1	
Logical Network 3	1	1	0	0	0	0	0	0	192
First Host	1	1	0	0	0	0	0	1	193
Last Host	1	1	1	1	1	1	1	0	254

For the hosts on subnet 3 you can use the range of addresses from .193 to .254; broadcast address 192.168.1.255

Subnet Masks - Binary Representation

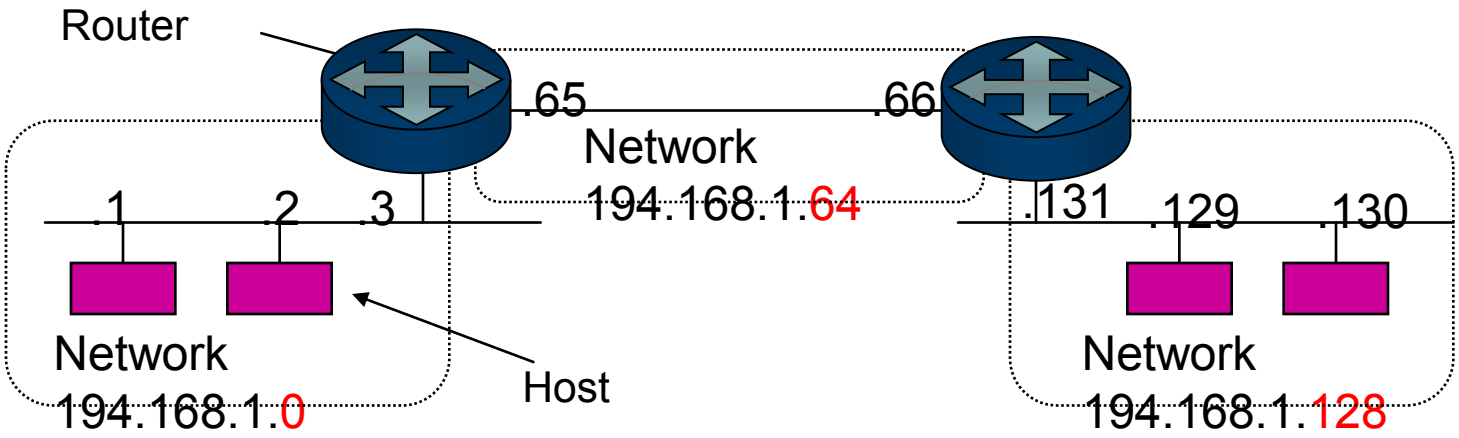
Decimal Hex	Binary	
.128	80	10000000
.192	C0	11000000
.224	D0	11100000
.240	F0	11110000
.248	F8	11111000
.252	FC	11111100
.254	FE	11111110
.255	FF	11111111

Subnetting Example



- Consider three networks with class C addresses and default subnet mask (255.255.255.0)
- How can we use only one class C network to obtain at least three subnets?

Subnetting Example



- We can use subnet mask 255.255.255.192 and obtain 4 networks with the following network IP addresses:
  - 192.168.1.0
  - 192.168.1.64
  - 192.168.1.128
  - 192.168.1.192

Exercises on IP Addressing

1. Choose one class B IP address from the following network IP addresses
   192.168.1.0 - 198.124.144.0 - 146.44.63.0 - 10.10.1.0
2. Which is the default subnet mask for class B IP addresses?
3. Now modify the subnet mask number to obtain subnets with at most 6 hosts for each subnet; find the right one among the following subnet numbers
   255.255.128.0 - 255.255.248.0 - 255.255.255.248

» Remember that in the range of IP addresses there must always be a network address and a broadcast address

Solutions

1. 146.44.63.0
2. 255.255.0.0
3. With mask 255.255.255.248 we obtain 8192 subnets and 6 hosts for each subnet

255 . 255 . 255 . 248

11111111.11111111.11111111.11111000

Three bits count from 0 to 7

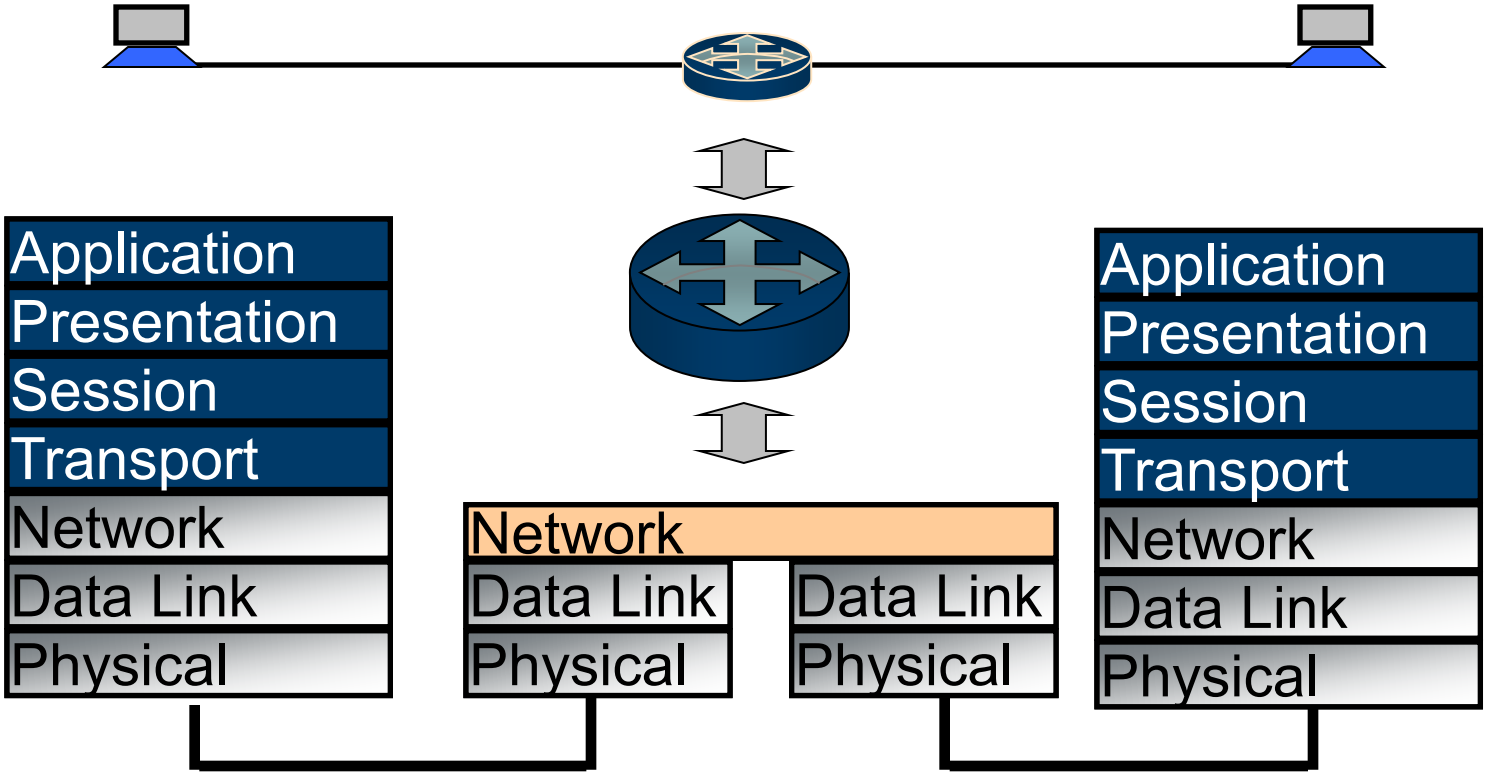
One IP address is needed for the network and one for the broadcast messages → 6 IP addresses are available for hosts

How Routers Work

How Routers Work

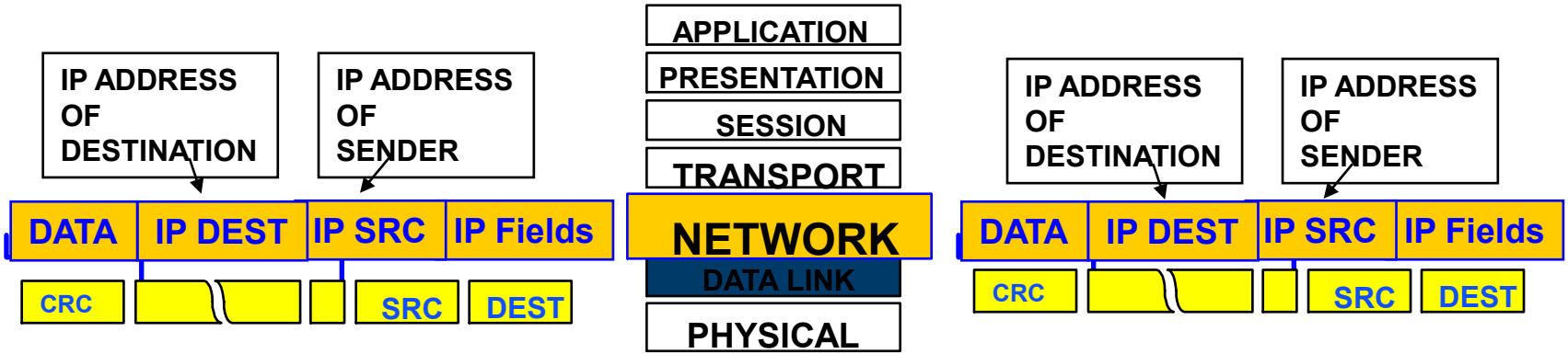
- A router works at the Network Layer
- Routers understand Network Layer Protocols and transfer data based on logical network addresses
- A router is able to take more intelligent routing decisions than bridges, based on higher layer protocols

Intermediate System



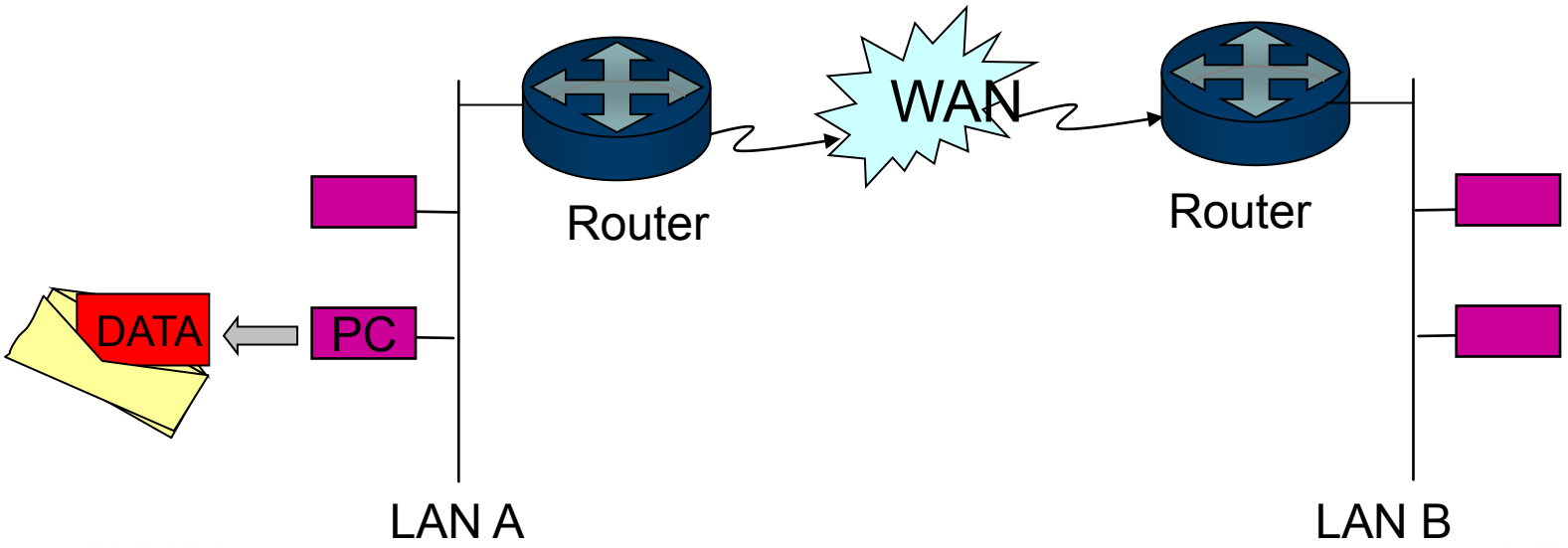
Routing by Network Address

- Routers are Intermediate Systems that read Network Layer Information to forward packets
- Routers use the destination address as access key to the routing table
- This technique used in IP, Decnet and OSI



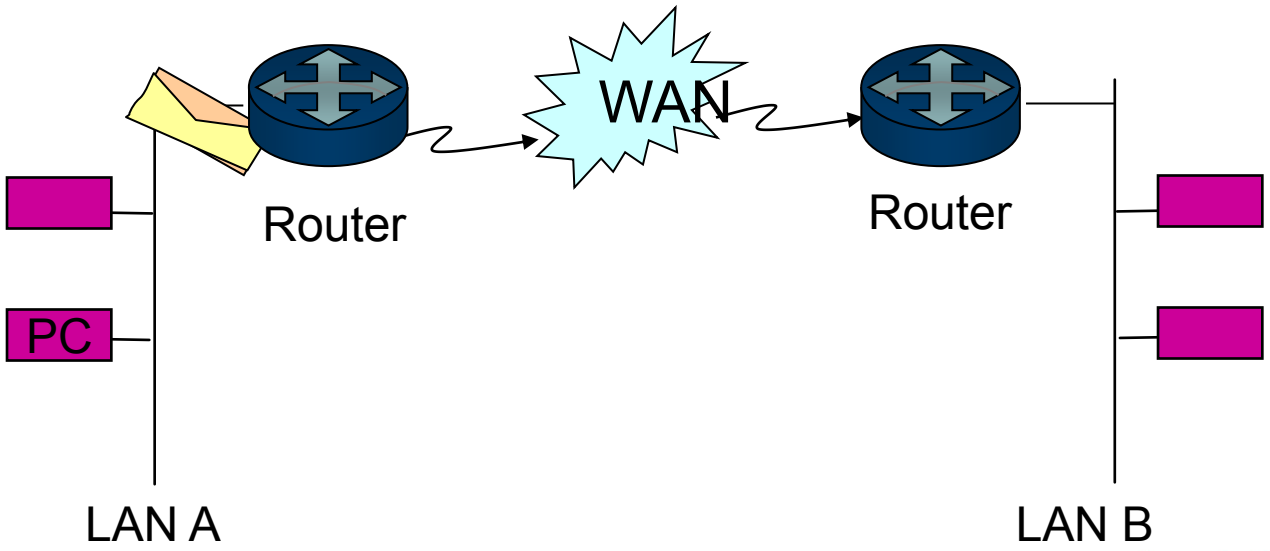
How Routers Work

» Data is encapsulated in a Layer 3 protocol by the PC



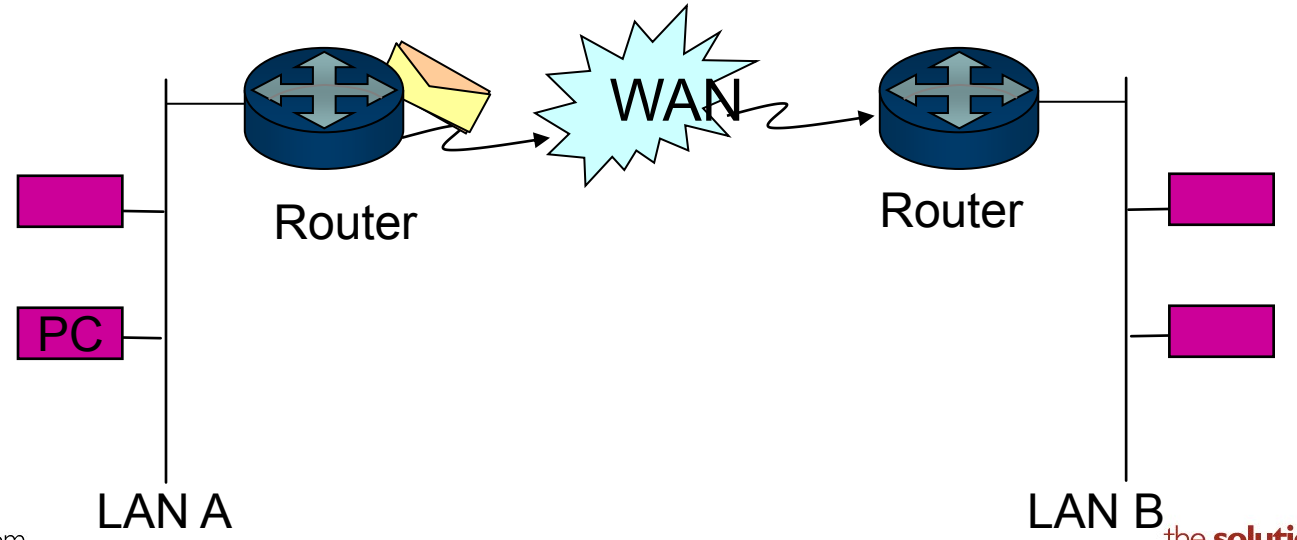
How Routers Work

» This is transmitted across the LAN to the router



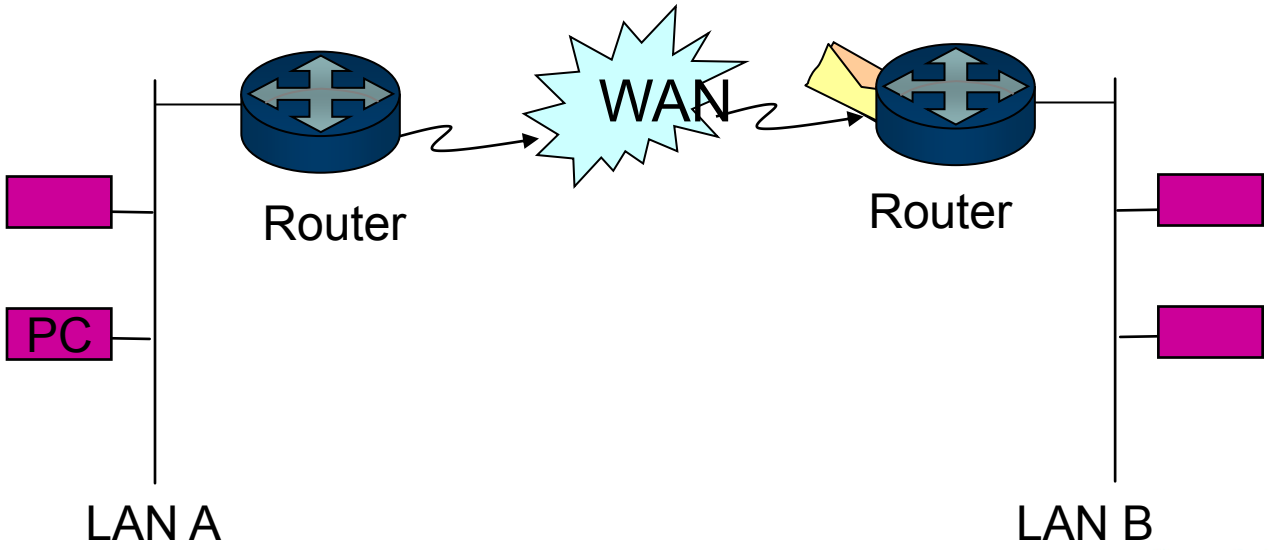
How Routers Work

» The router reads the Layer 3 address, reads the routing table and forwards this packet containing the data to a queue awaiting transmission across the WAN



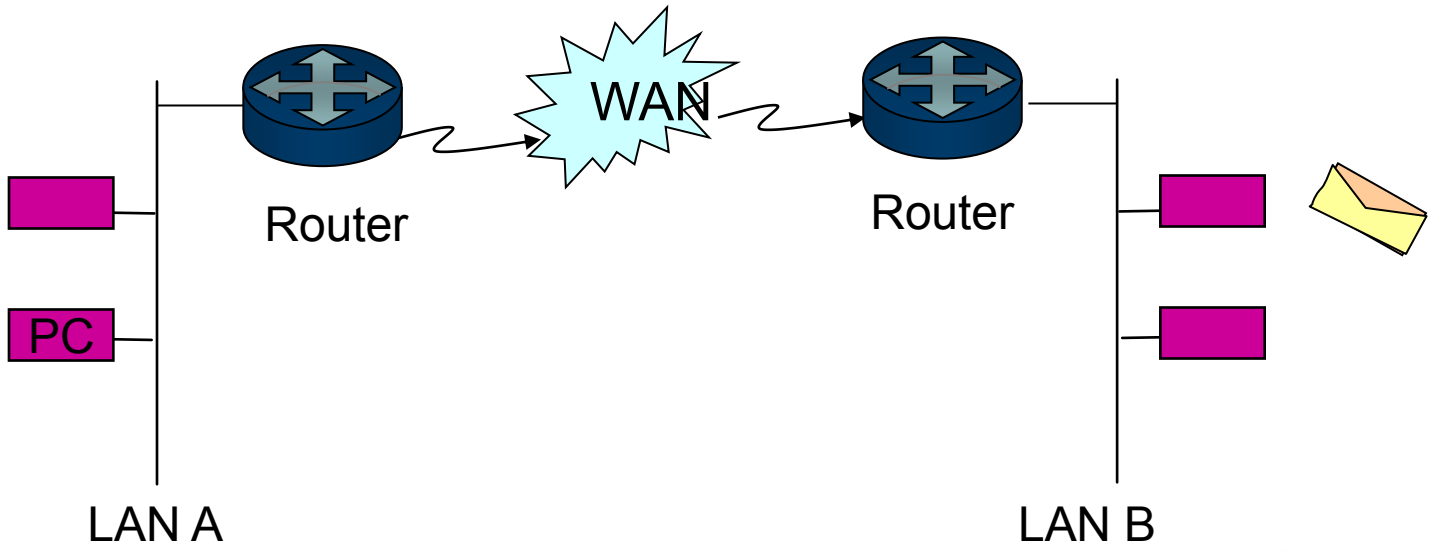
How Routers Work

» The Layer 3 packet containing the data is transported across the WAN to the router connected to the destination network



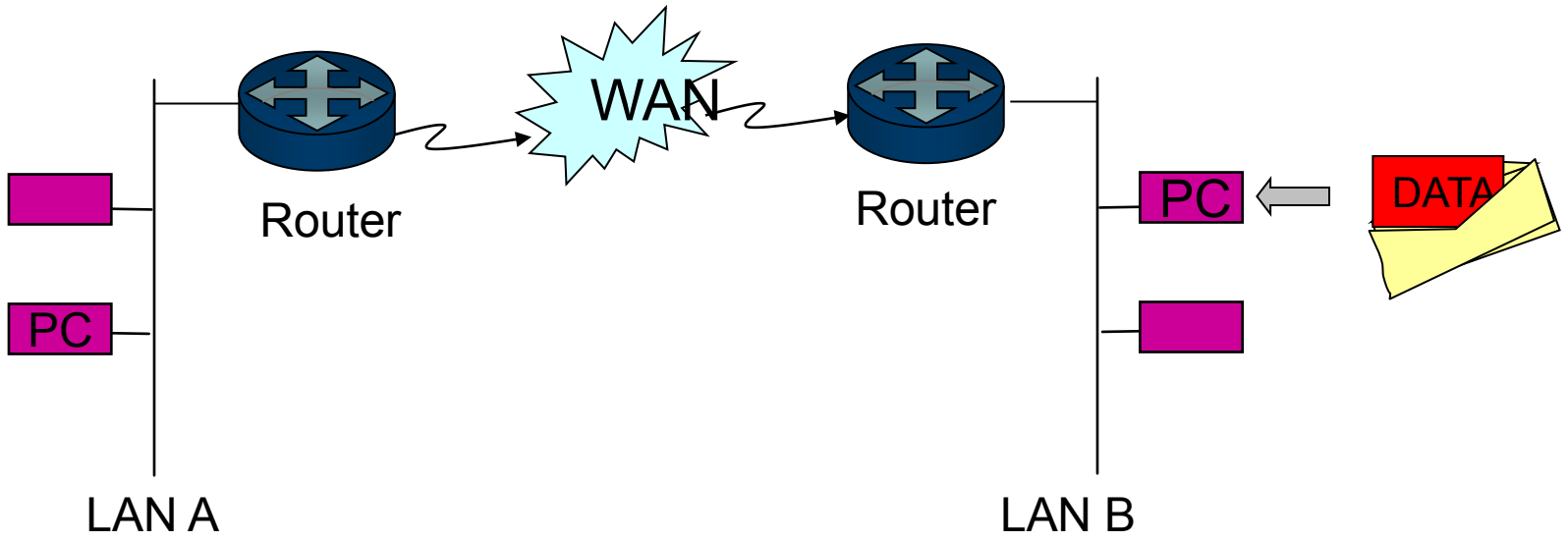
How Routers Work

» The router on the destination network reads the Layer 3 address and forwards the packet via a queue across the LAN to the destination host



How Routers Work

» The destination host reads data from the Layer 3 packet and the data contained can be used by upper layer protocols



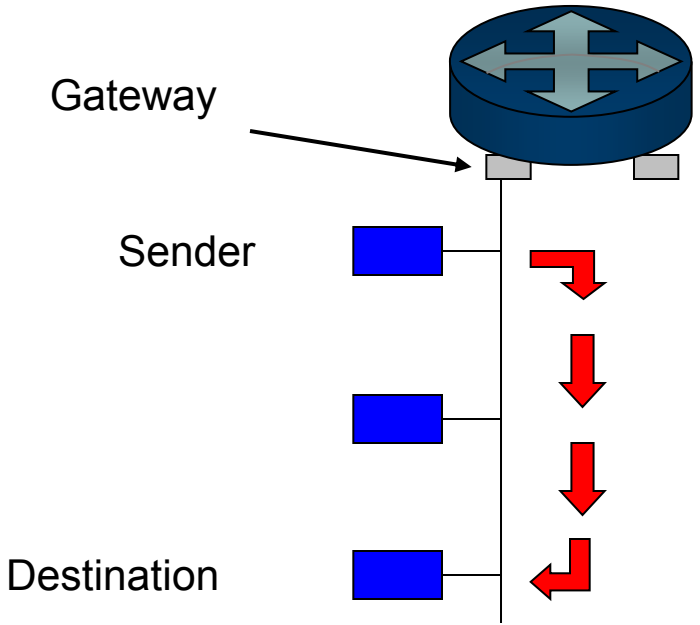
Routing operations

» It is possible to identify three different processes

- Datagram delivery
- Direct routing
- Indirect routing

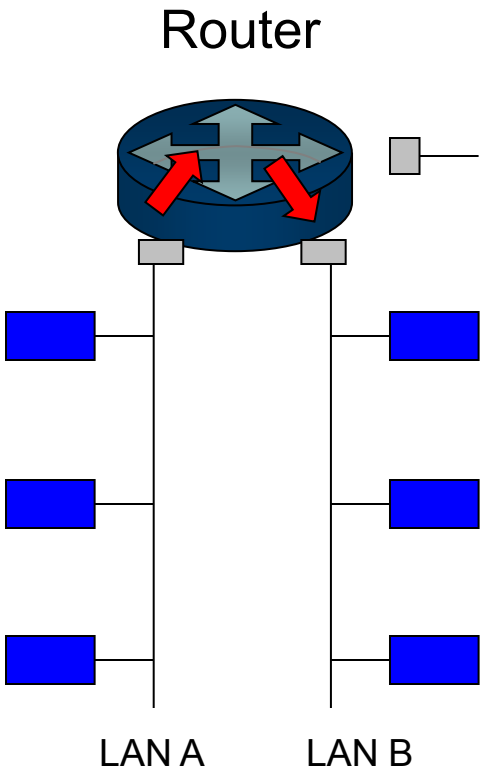
Datagram Delivery

- Transmission of an IP datagram between two machines on a single network does not involve gateways (routers)
- The sender encapsulates the datagram in a physical network frame, binds the destination IP address to a physical hardware address and sends the resulting frame directly to the destination
- Each PC can reach all the other ones without routing



Direct Routing

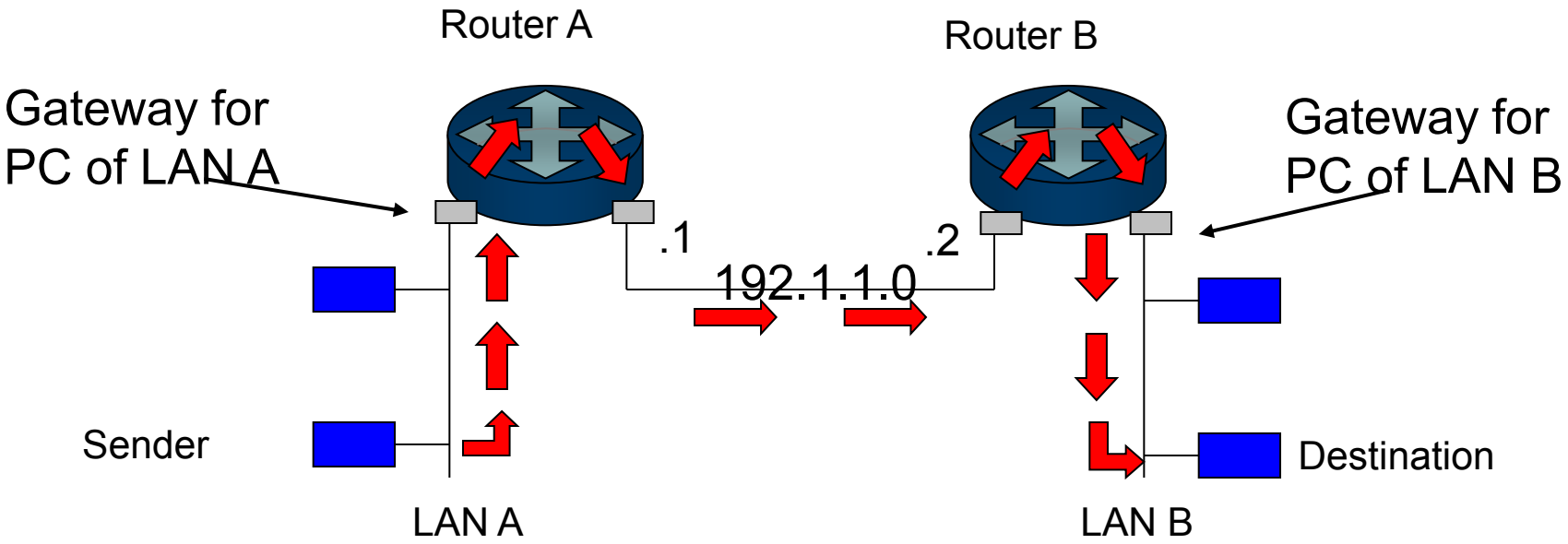
- All PCs on LAN A are able to communicate with all PCs on LAN B without routing instructions on the router
  - configure LAN interfaces Eth0 (LAN A) and Eth1 (LAN B) on the router
  - configure every PC with the right IP address and gateway number (IP address of the Eth interface)



Indirect Routing

- Transmission of an IP datagram between two machines on different networks is achieved via gateways (routers)
- With indirect routing, the sender must identify a router to which the datagram can be sent (gateway address)
- Routers in a TCP/IP internet form a cooperative, interconnected structure: datagrams pass from router to router until they reach a router that can deliver the datagram directly

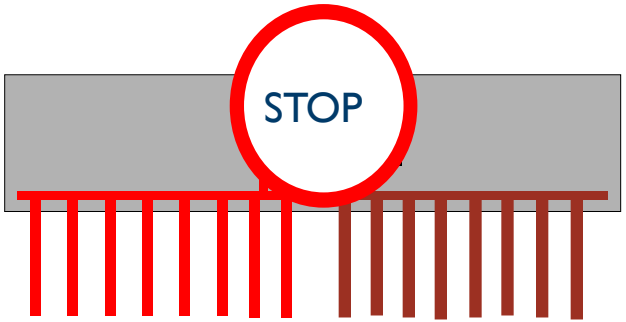
Indirect Routing



- To allow packets to be forwarded from the sender to the destination, it is necessary to add a routing instruction to the routers, so that they know the path that traffic must follow

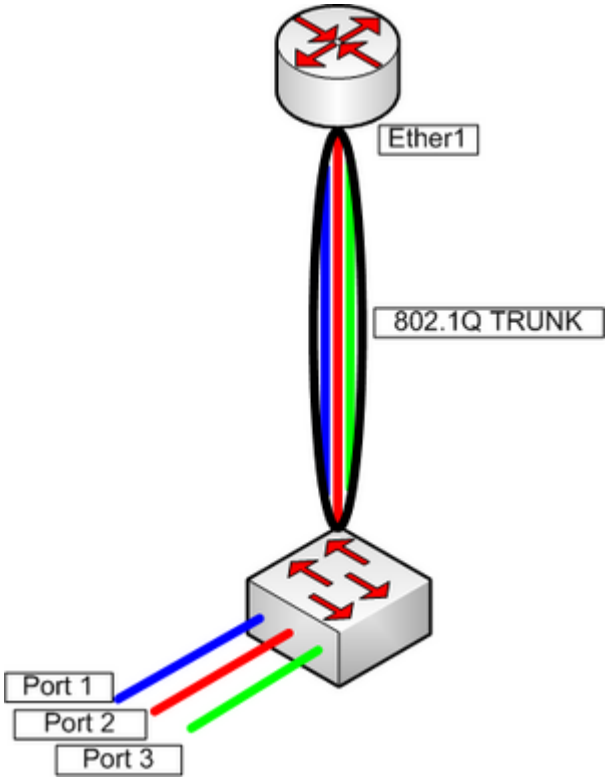
What's a L3 Switch?

- VLANs - security features
- Layer 2 switch no traffic can pass from one VLAN to another
- In the majority of real world applications, some traffic needs to pass from one VLAN to another, typically these include:
  - printers
  - file servers
  - backup servers
  - IT administrators



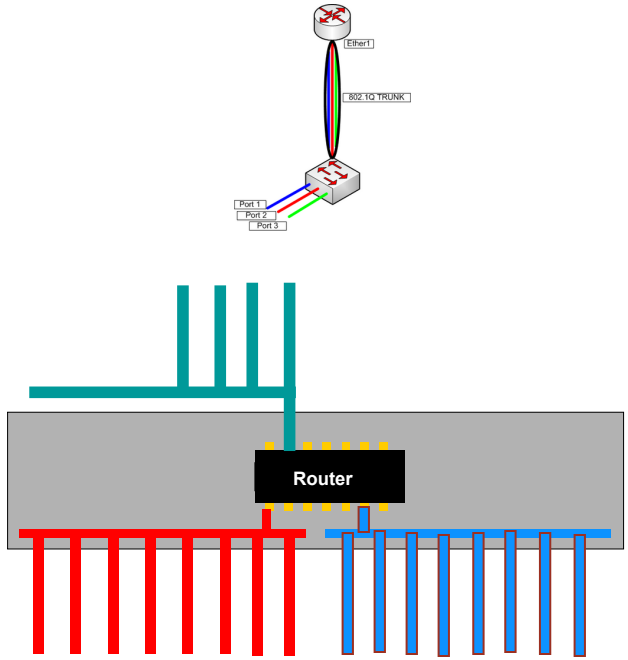
Communicating between VLANs

- External router could route between VLANs…
  - Require a physical interface per VLAN or 802.1q
  - Router are not optimize for routing high traffic between vlans



Layer 3 Switches

- Layer 3 switches forward traffic between VLANs without the problems associated with external routers
  - Scalable without need for dedicated port per interface
  - Uses hardware routing ASIC chips forwarding at Gigabit wire speeds.



NAT

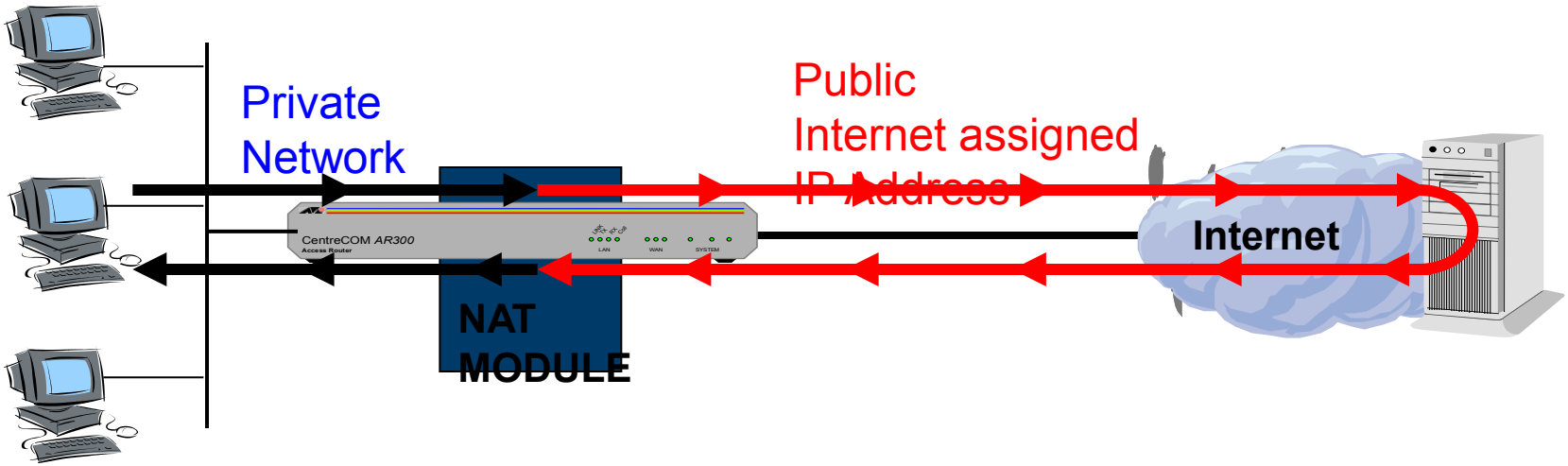
Network Address Translation

NAT

- With NAT, multiple users can connect to Internet using a single IP address
- All IP addresses of the users are translated into one IP global address
- In this way, we can reduce connection costs

NAT

» Addresses are translated automatically between the private and the public network



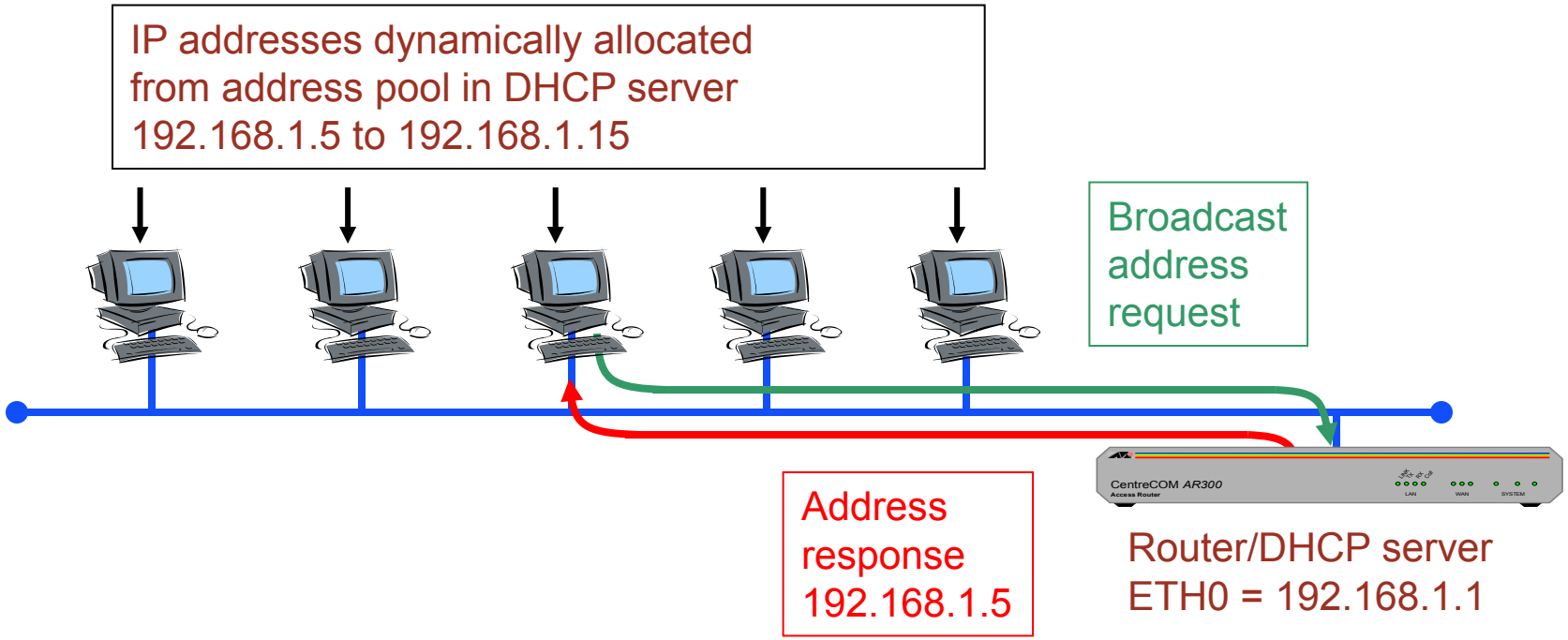
DHCP

Dynamic Host Configuration Protocol

DHCP

- The Dynamic Host Configuration Protocol provides a method for assigning configuration information to hosts on a TCP/IP network
- The IP configuration is stored on the router (DHCP server), and sent to hosts when they are switched on (DHCP clients)
- With the DHCP function, network management becomes easier, because you need to configure only the router and not every PC

DHCP Server

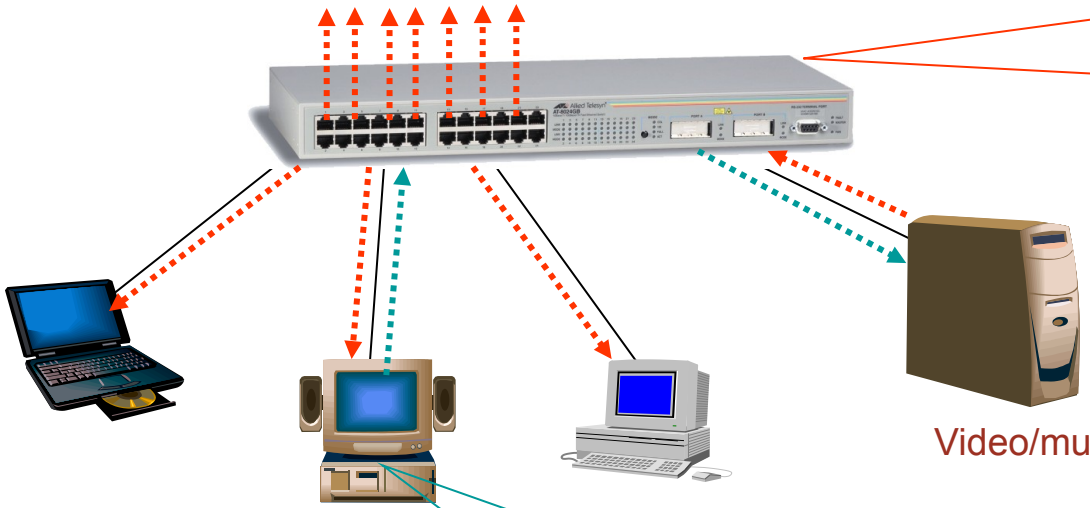

IP addresses dynamically allocated
from address pool in DHCP server
192.168.1.5 to 192.168.1.15
Broadcast
address
request
Address
response
192.168.1.5
CentreCOM AR300
Access Router
LAN
WAN
SYSTEM
Router/DHCP server
ETH0 = 192.168.1.1

Multicast

Multicast

- It is the process of transmitting an IP datagram to a group of hosts
- A host group may contain zero or more hosts
- Packets sent to a group address are only received by members of that group
- A multicast datagram is received by each member of the group as if the datagram had been sent individually to each host as a unicast datagram
- A host group is identified by a single IP address
- Multicast addresses are in the range
  - 224.0.0.0 through 239.255.255.255

Without Multicast



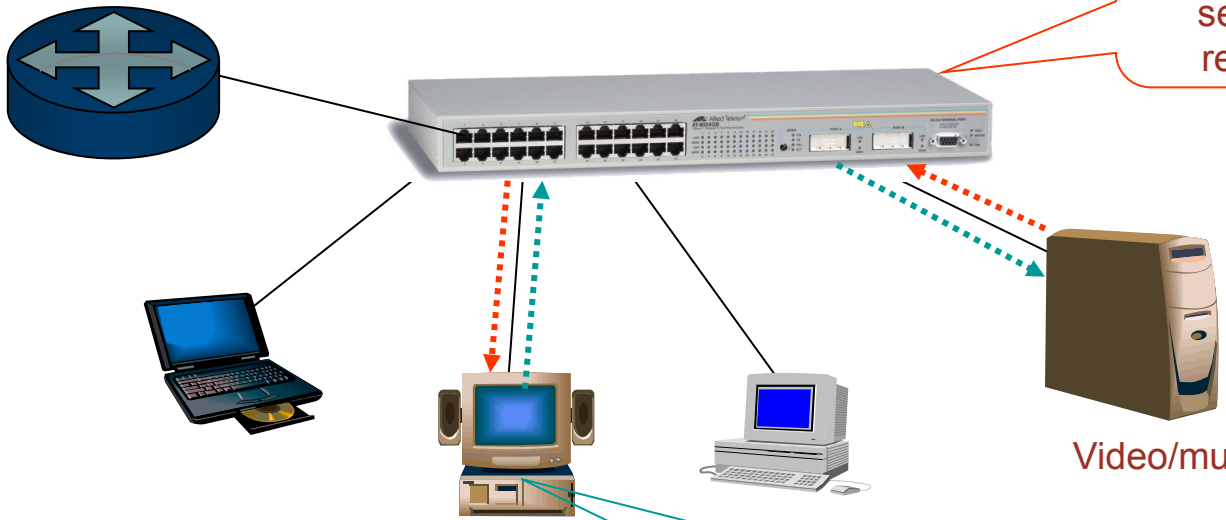
Switch processes multicast packet as broadcast and sends traffic out of all ports

Video/music Server

Request to join a music or video streaming channel

With Multicast

Router or L3 Switch with multicast support



Switch recognizes multicast packet and sends data only to requesting station

Video/music Server

Request to join a music or video streaming channel

IPv6

IPv6

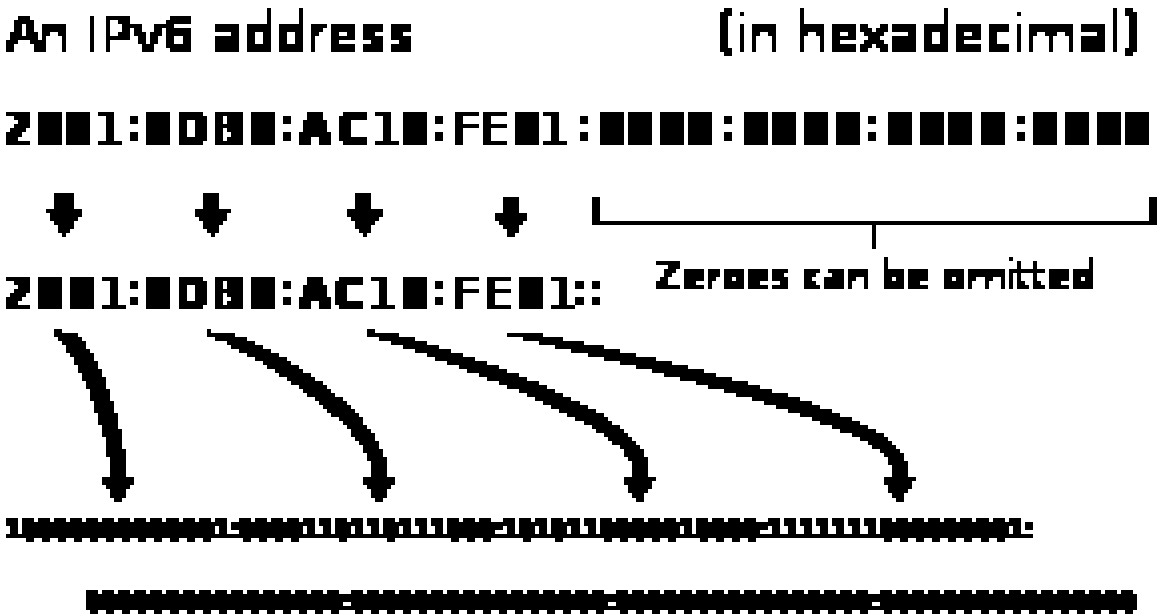
- Ratified by IETF in 1999 (RFC 2460).
- Solves limitation of IPv4 addressing.
- Solves other IPv4 short falls
- Several improvements :
  - 128 bits address format (16 bytes)
  - Auto-configuration
  - Mobility management
  - Fixed format headers
  - Security . . .

IPv6 address formats

» IPv6 addresses are 128 bits long.
  – IPv4 addresses are only 32 bits long

» IPv6 addresses are written as eight hexadecimal groups.
  – Each separated by a colon (:), consists of a 16-bit hexadecimal value.

Addressing


An IPv6 address
(in hexadecimal)
2001:0DB8:AC10:FE01:0000:0000:0000:0000
2001:0DB8:AC10:FE01::
Zeroes can be omitted

Addressing cont.

Prefix and interface ID

» IP addresses combine, in a single address, a
  – network identifier (called the prefix)
  – device identifier (the interface ID).

» The point at which to split the address into these two portions is given by the prefix length.

» The prefix length is written as /xx at the end of the address; e.g.

2001:0340:0000:0000:0000:F673:0029:0564/64

Prefix and Interface ID cont.

2001:0340:0000:0000:0000:F673:0029:0564/64

Prefix – 64 bits

Interface ID – 64 bits

2001:0340:0000:0000:0000:F673:0029:0564/48

Prefix – 48

Interface ID – 80 bits

Address optimization

To make IPv6 addresses easier to write, some zeros can be removed. The leading zeros in a 4-digit block can be removed.

Also, contiguous sets of 4 zeros, and their separating colons can be completely removed.

2001:0340:0000:0000:0000:F673:0029:0564

Address optimization cont.

To avoid ambiguity, it is only possible to have one place in the address where a continuous set of 0s is replaced by ::

So 2001:0340:0000:0000:F673:0000:0000:0564

can be written as

2001:340::F673:0000:0000:564

or

2001:340:0000:0000:F673::564

but NOT

2001:340::F673::564

IPv6 Routing Protocols

IP Routing Protocols

» A router must know to which interface it should send packets in order for them to reach their destination via the “best” route

» There are different choices for routing IP
  – Static Routes
  – RIPng (Routing Information Protocol)
  – OSPFv3 (Open Shortest Path First)

End

Thank you

Americas Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11