Introduction to:
Networks,
Ethernet, TCP/IP,
IPv4 and IPv6 addressing,
Network configuration in Linux

Hari.K
NIELIT Calicut

What is a Network?

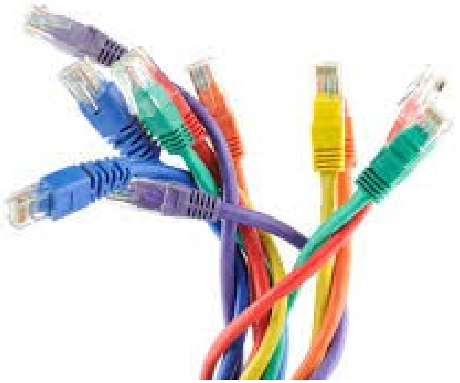
- A network is simply defined as something that connects things together for a specific purpose.
- The term network is used in a variety of contexts, including telephone, television, computer, or even people networks.

NIC

- A network interface card (NIC) is a circuit board or card that is installed in a computer so that it can be connected to a network.
- A network interface card provides the computer with a dedicated, full-time connection to a network.
-

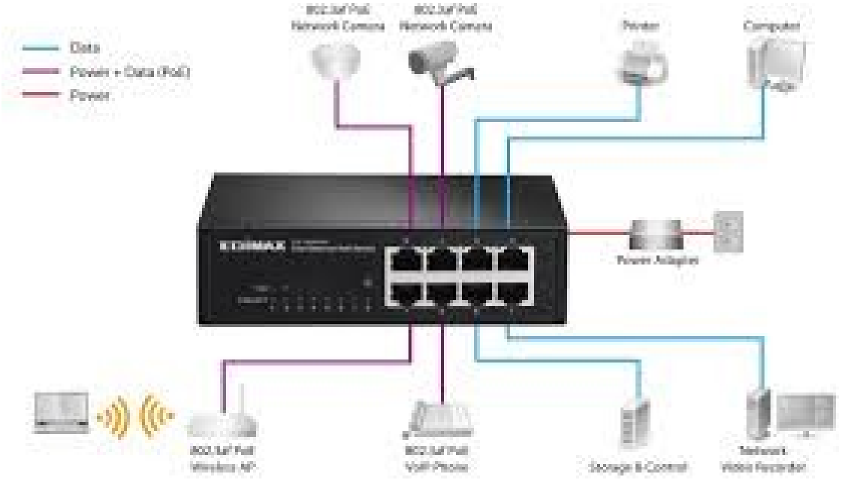
Cables

- Networking cables are networking hardware used to connect one network device to other network devices or to connect two or more computers



Switch

- A network switch (also called switching hub, bridging hub, officially MAC bridge) is a computer networking device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device.



Protocols

- **Protocols** are rules that govern how devices communicate and share information across a network.
- Examples of protocols include:
  - IP – Internet Protocol
  - HTTP - Hyper Text Transfer Protocol
  - SMTP – Simple Mail Transfer Protocol
- *Multiple protocols often work together to facilitate end-to-end network communication, forming protocol suites or stacks.*

Network reference models

- Network reference models were developed to allow products from different manufacturers to interoperate on a network.
- A network reference model serves as a blueprint, detailing standards for how protocol communication should occur.
  - Open Systems Interconnect (OSI) and Department of Defense (DoD) models

Basic Network Types

- Network types are often defined by function or size.
- The two most common categories of networks are:
  - LANs (Local Area Networks)
  - WANs (Wide Area Networks)

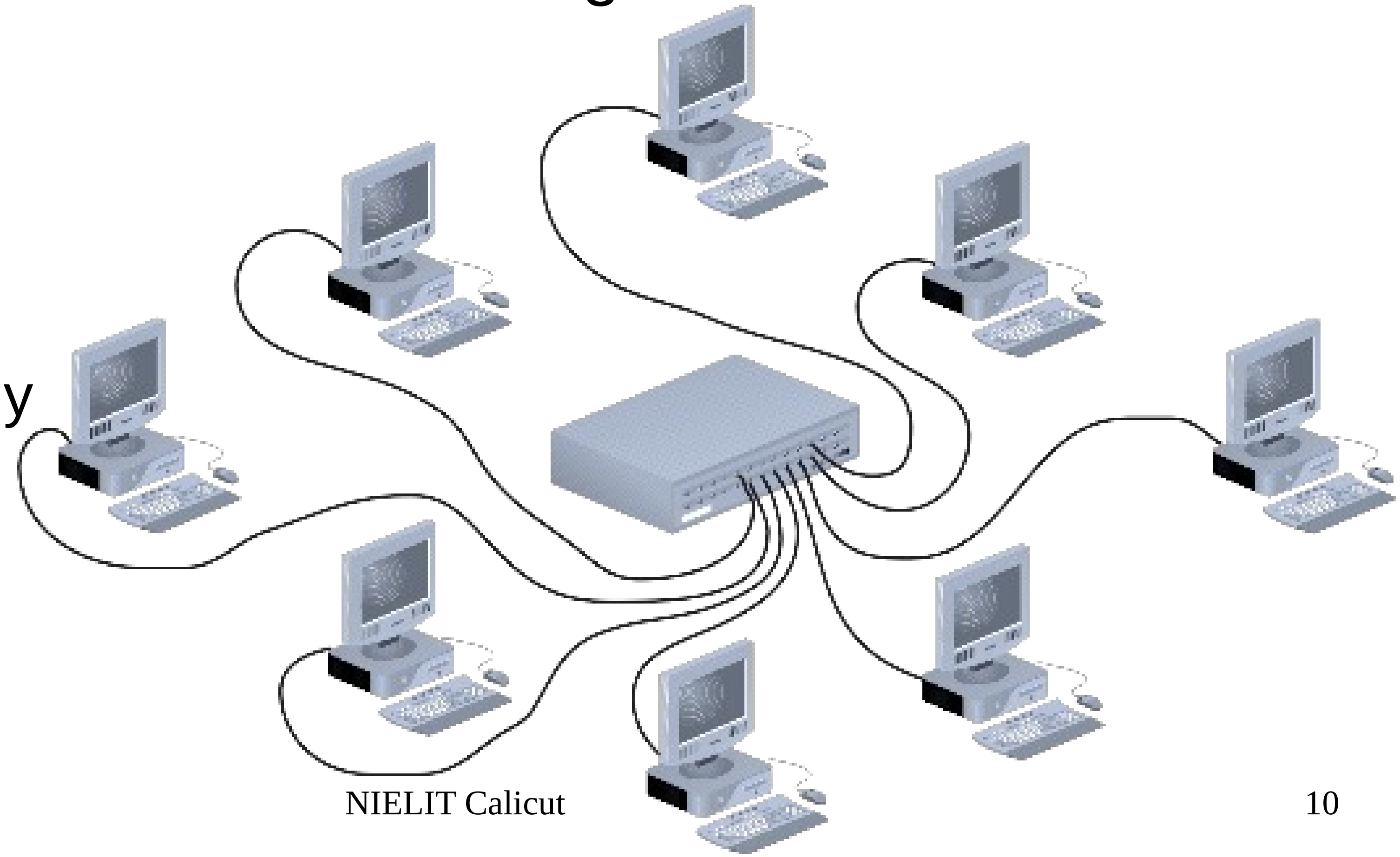
LAN

- A LAN is generally a high-speed network that covers a small geographic area, usually contained within a single building or campus.
- A LAN is usually under the administrative control of a single organization.
- Ethernet is the most common LAN technology.

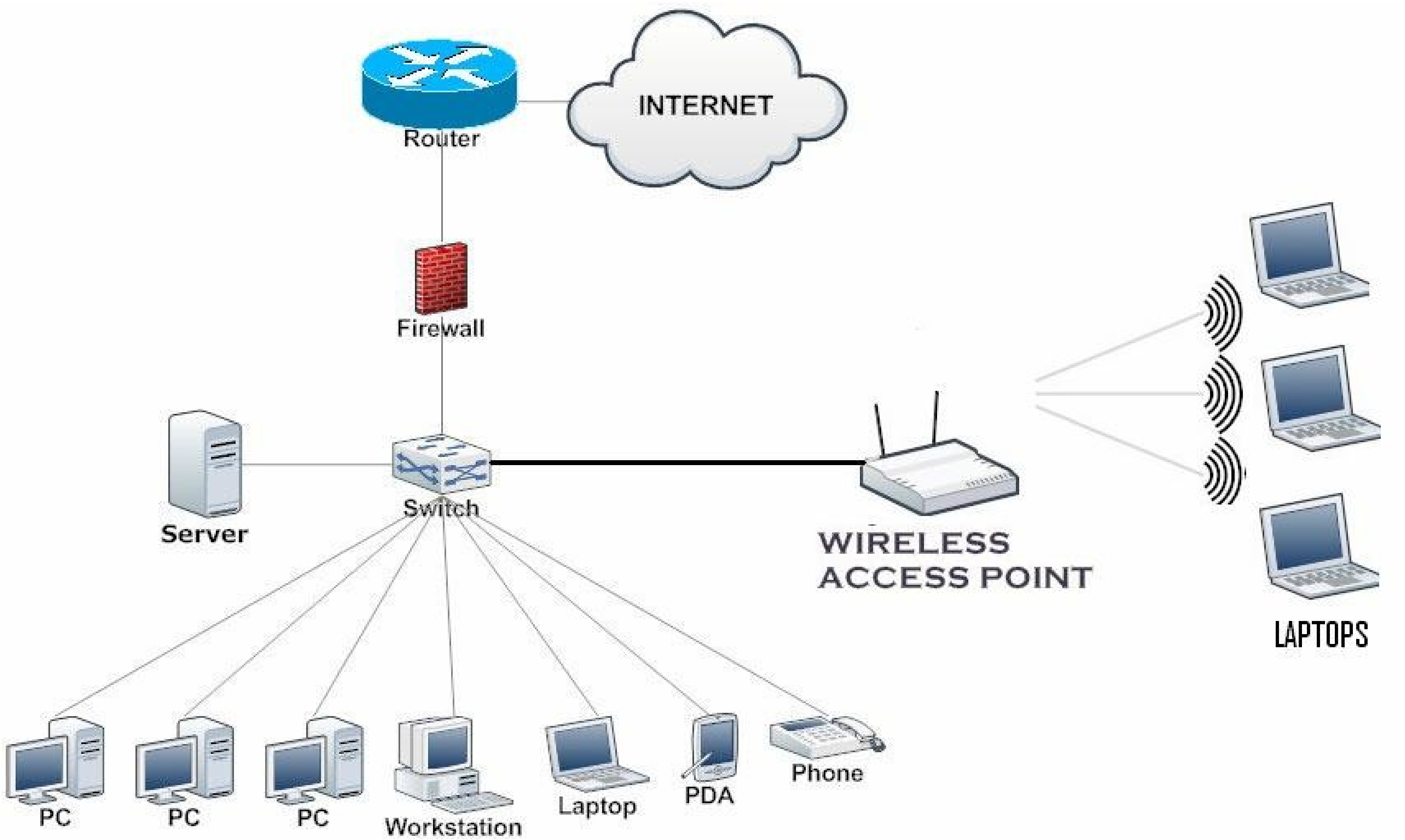
Topology

A network topology is the arrangement of anetwork, including its nodes and connecting lines.

Star Topology



Typical SOHO LAN

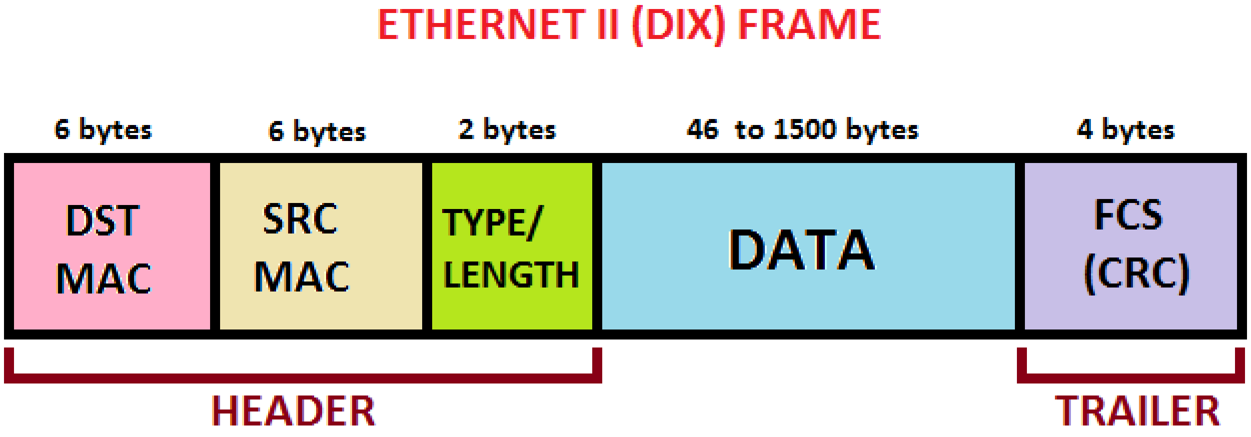


Ethernet

- **Ethernet** is a family of technologies that provides data-link and physical specifications for controlling access to a shared network medium.
- It has emerged as the dominant technology used in LAN networking.

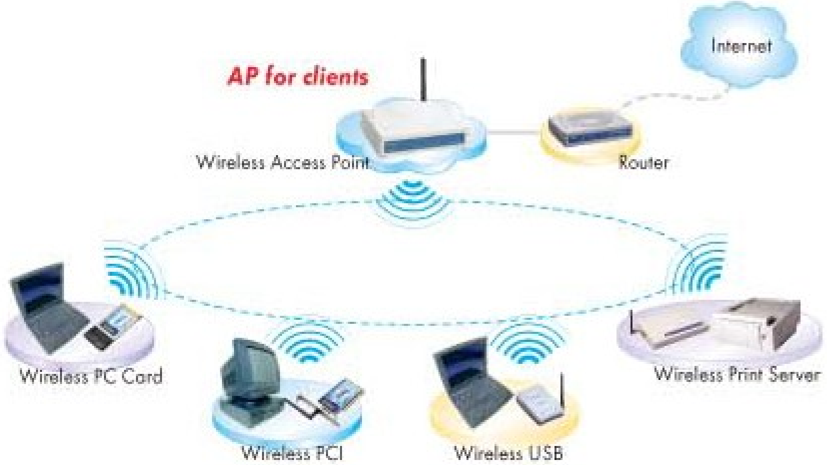
Ethernet Address & Frame format

- Part of every Network Interface Card (NIC)
- 48 Bit long (6 Bytes)
- Also called MAC address
- Unique



Wireless Access Point/Router

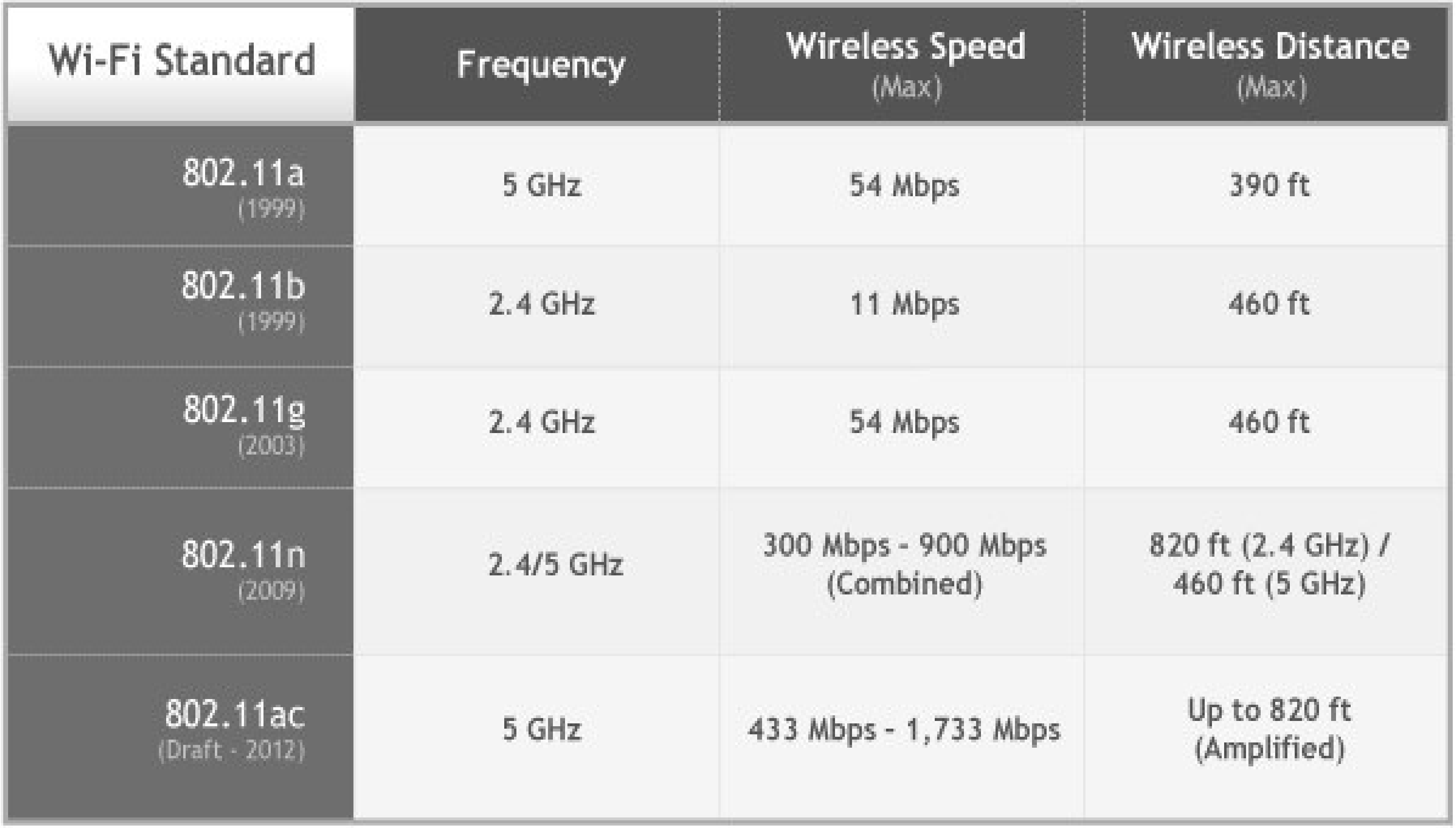
- A wireless access point (WAP) is a networking hardware device that allows a Wi-Fi compliant device to connect to a wired network.
- A wireless router is a device that performs the functions of a router and also includes the functions of a wireless access point



IEEE 802.11

- IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands.
- They are created and maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802).

Wireless Standards



Wi-Fi Standard	Frequency	Wireless Speed (Max)	Wireless Distance (Max)
802.11a (1999)	5 GHz	54 Mbps	390 ft
802.11b (1999)	2.4 GHz	11 Mbps	460 ft
802.11g (2003)	2.4 GHz	54 Mbps	460 ft
802.11n (2009)	2.4/5 GHz	300 Mbps - 900 Mbps (Combined)	820 ft (2.4 GHz) / 460 ft (5 GHz)
802.11ac (Draft - 2012)	5 GHz	433 Mbps - 1,733 Mbps	Up to 820 ft (Amplified)

Packet Switching

- Packet switching is a method of grouping data which is transmitted over a digital network into packets.
- Packets are made of a header and a payload.
- Data in the header is used by networking hardware to direct the packet to its destination where the payload is extracted and used by application software.
- Packet switching is the primary basis for data communications in computer networks worldwide.

Internetwork

- An internetwork is a general term describing multiple networks connected together.
- The Internet is the largest and most well-known internetwork.

Internet Addressing

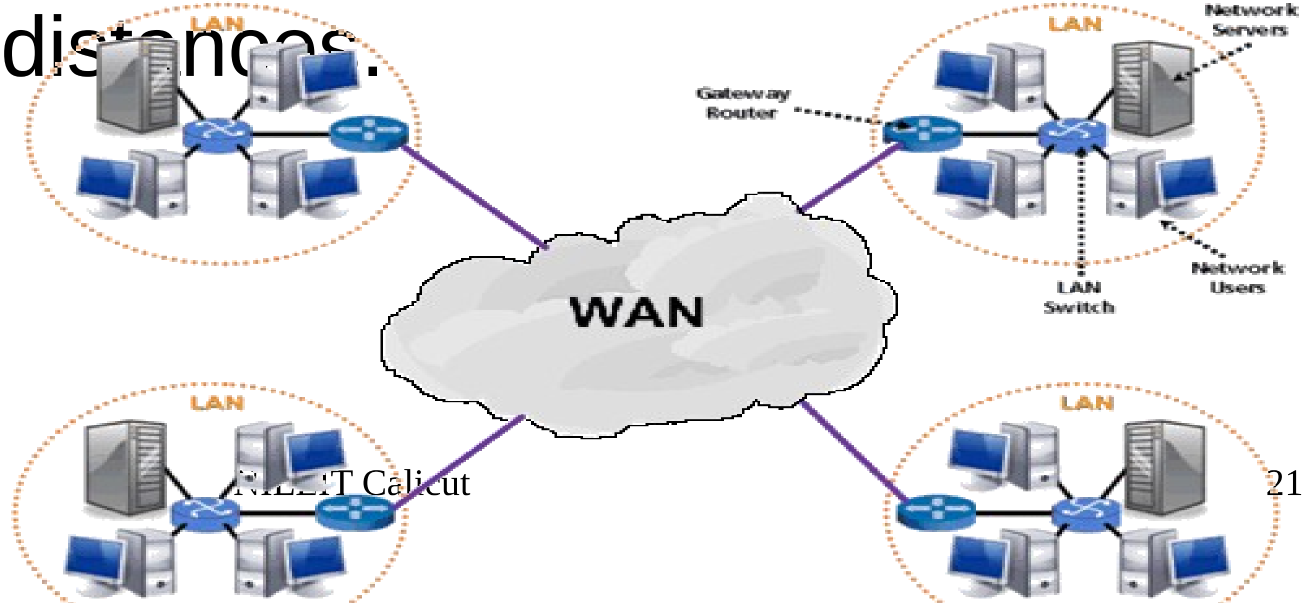
- An Internet Protocol address (IP address) is a numerical label assigned to each device (interface) connected to a computer network that uses the Internet Protocol for communication.
- An IP address serves two principal functions: host or network interface identification and location addressing.
- IPv4: uses 32-bit number.
  - 14.139.171.225
  - 192.168.30.22
- Ipv6: uses 128 bits for the IP address
  - 2405:8a00:a04a:1::9
  - fe80::527b:9dff:fe6c:cd4c

Router

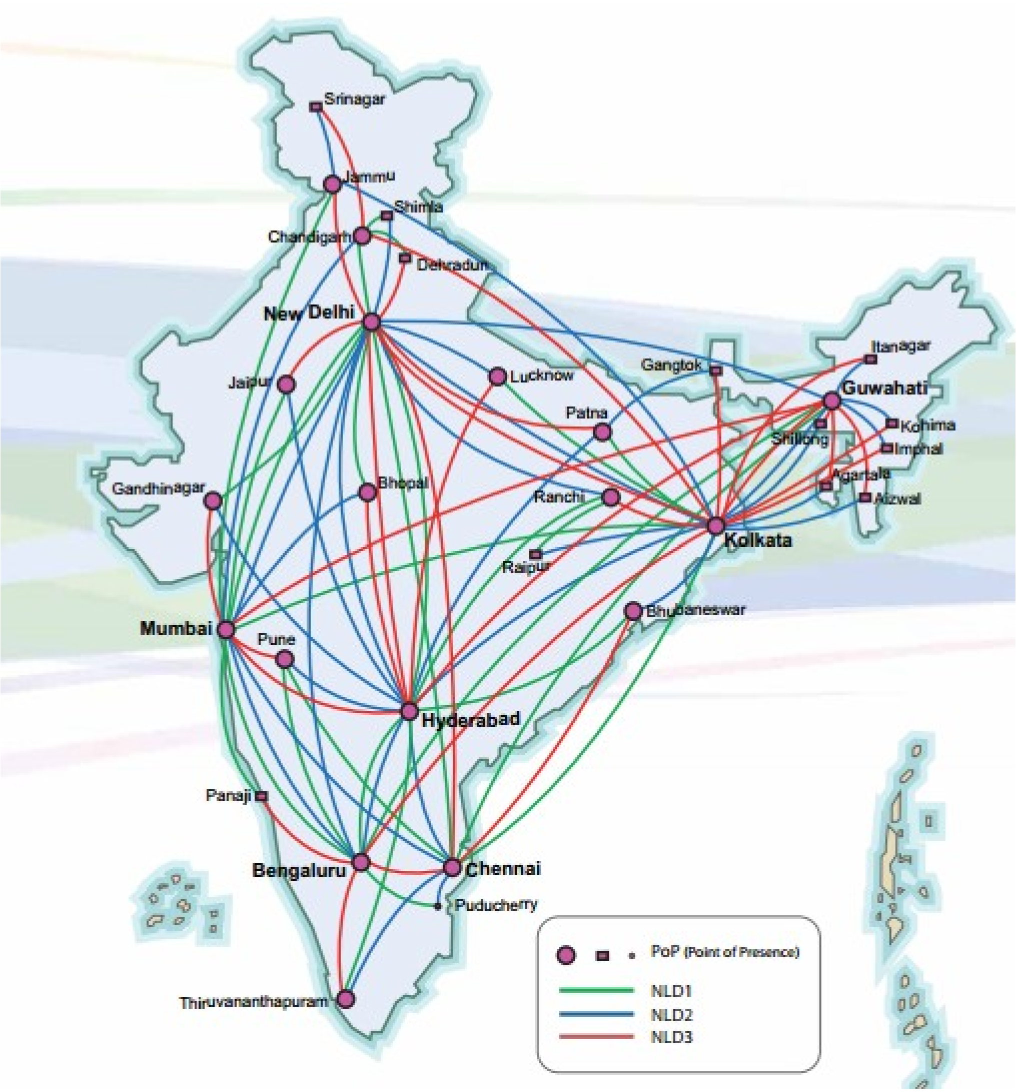
- A router is a networking device that forwards data packets between computer networks.
- Routers perform the "traffic directing" functions on the Internet.
- A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.

WAN

- A practical definition of a WAN is a network that traverses a public or commercial carrier, using one of several WAN technologies.
- A WAN is often under the administrative control of several organizations (or providers), and does not necessarily need to span large geographical distances.

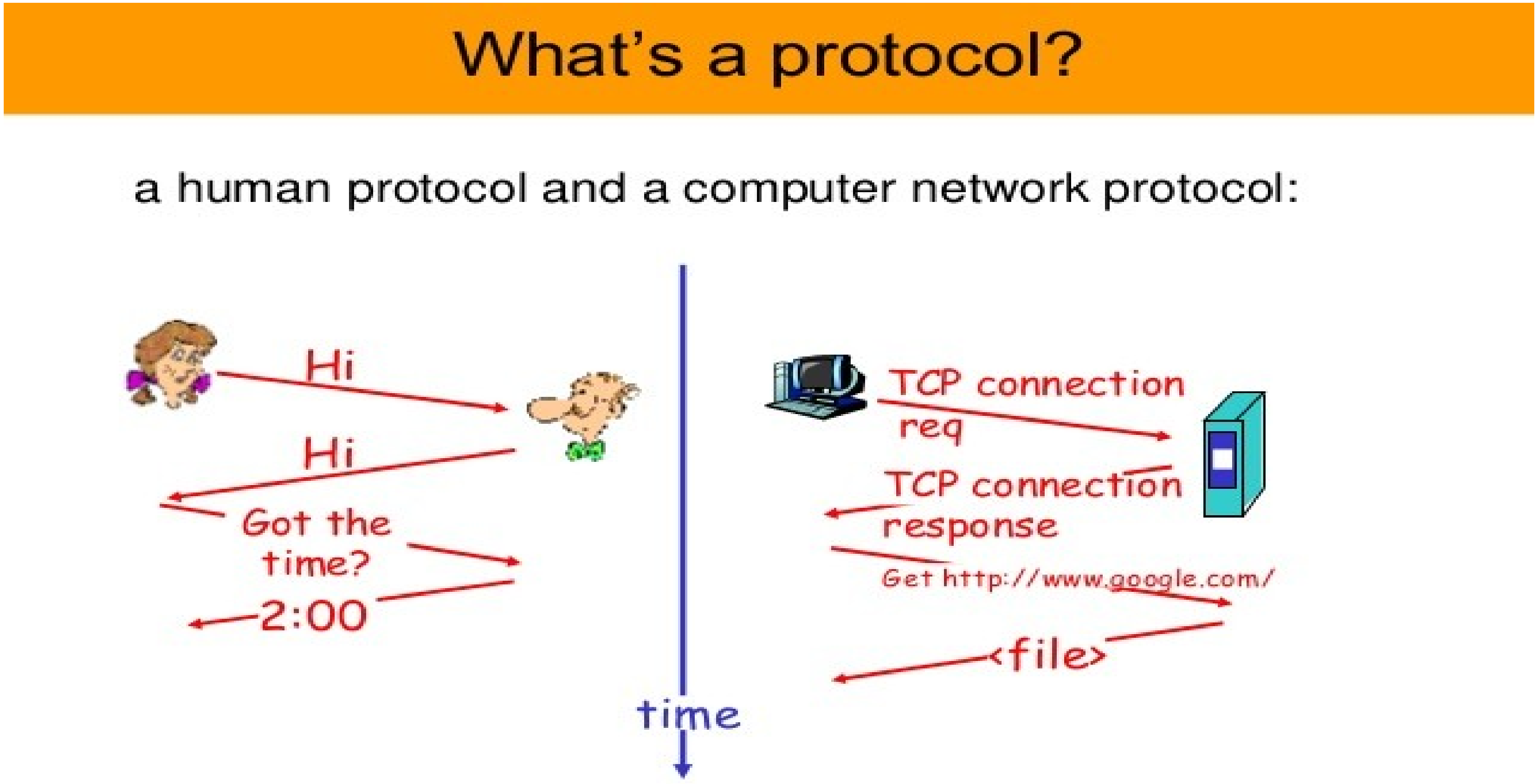


National Knowledge Network – An example of a WAN



Communication Protocol

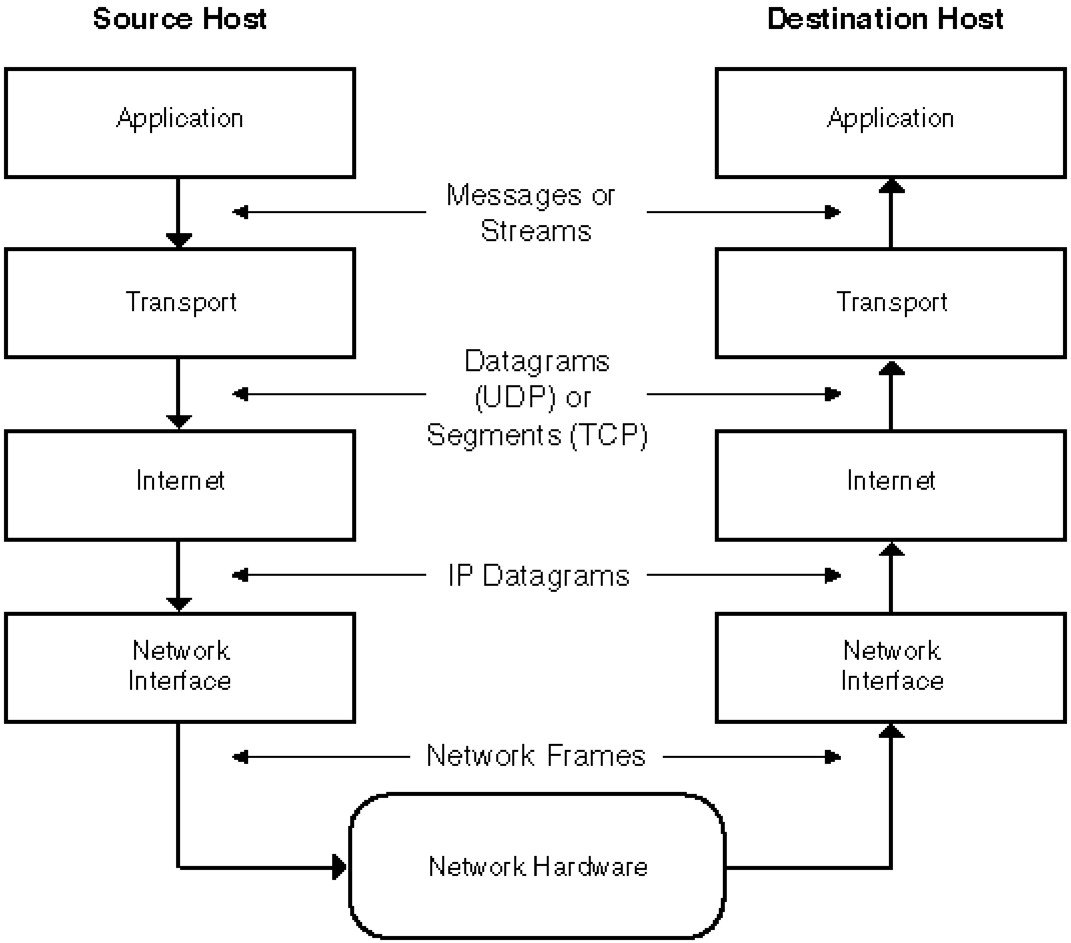
- In telecommunications, a communication protocol is a system of rules that allow two or more entities of a communications system to transmit information.

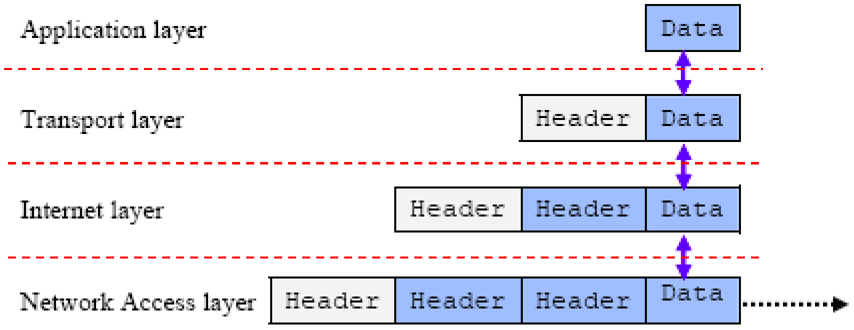


What's a protocol?

a human protocol and a computer network protocol:

TCP/IP Model


Source Host
Destination Host
Application
Application
Messages or Streams
Transport
Transport
Datagrams (UDP) or Segments (TCP)
Internet
Internet
IP Datagrams
Network Interface
Network Interface
Network Frames
Network Hardware


Application layer
Data
Transport layer
Header
Data
Internet layer
Header
Header
Data
Network Access layer
Header
Header
Header
Data

TCP/IP

- TCP/IP is the suite of communications protocols used to connect hosts on the Internet.
- TCP/IP uses several protocols, the two main ones being TCP and IP.
- TCP/IP is built into the UNIXoperating system and is used by the Internet, making it the de facto standard for transmitting data over networks.

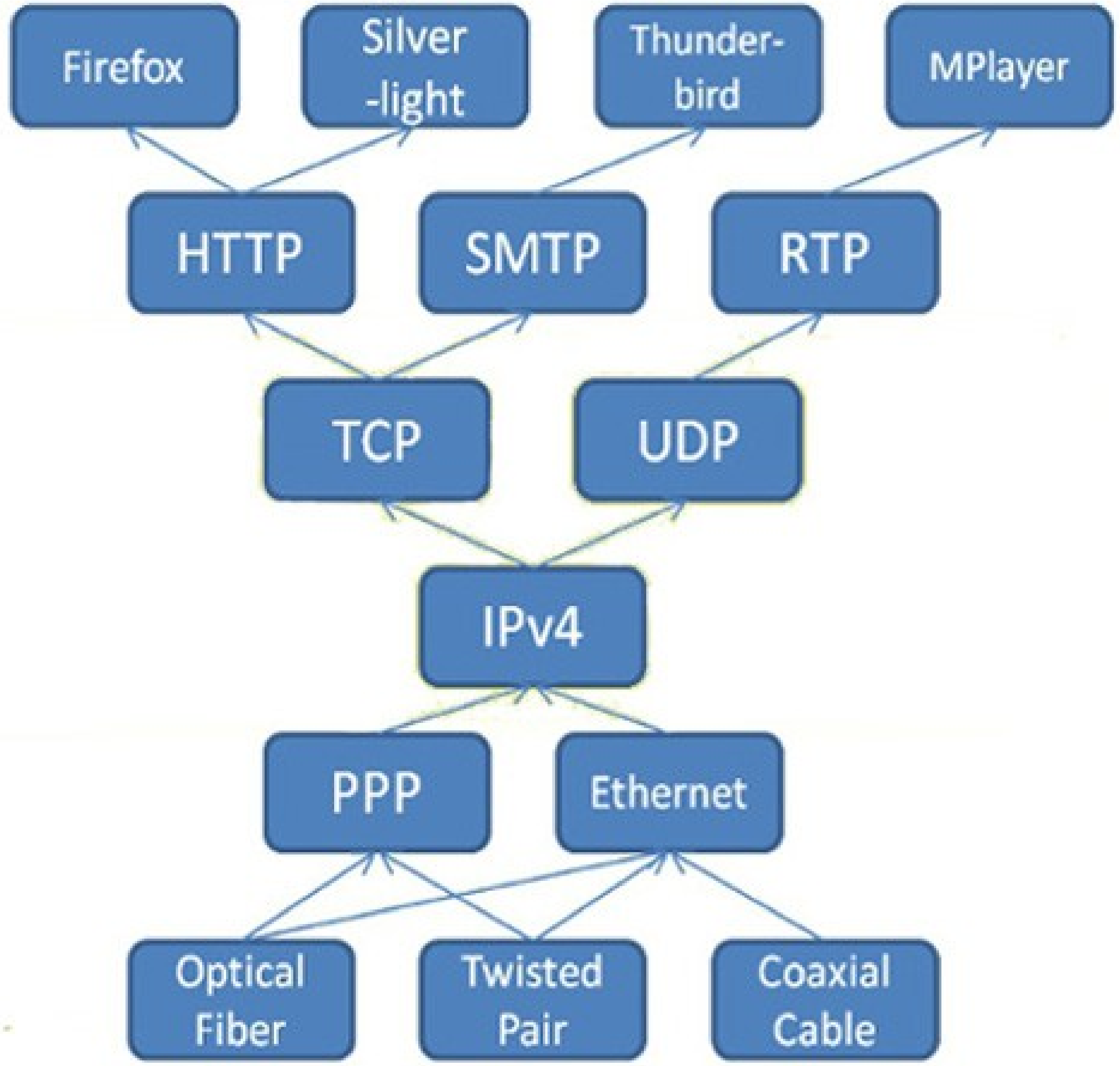
Address Resolution Protocol

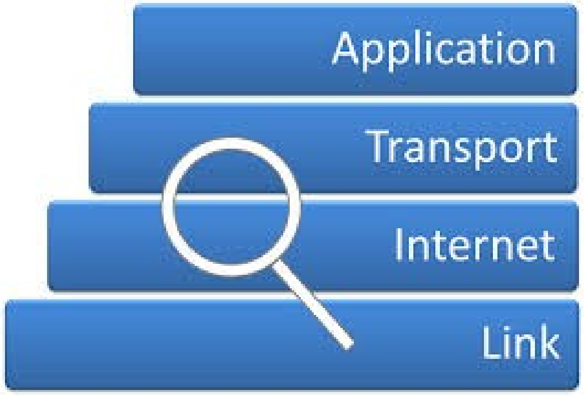
- The address resolution protocol (arp) is a protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol.

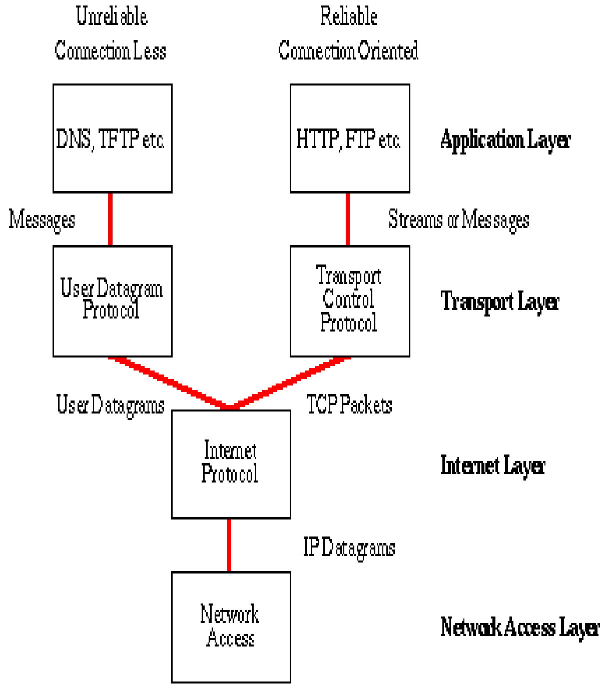
ICMP

- The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite.
- It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.

TCP/IP - Layers

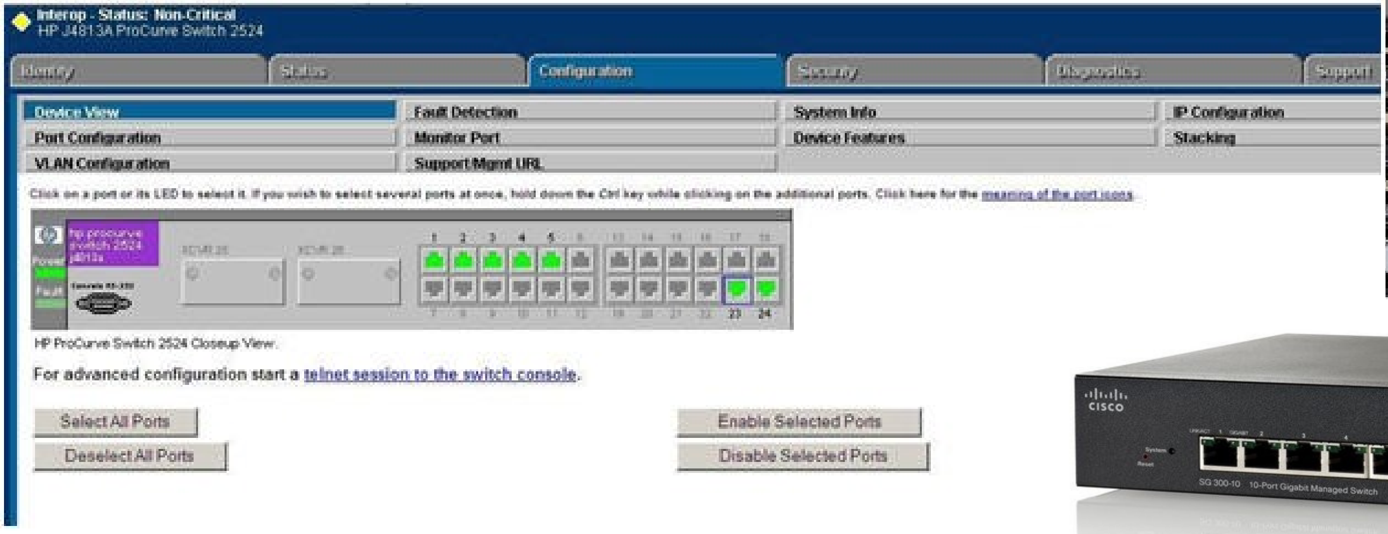






Managed Switches

- Managed switches give you more control over your LAN traffic and offer advanced features to control that traffic.



Interop - Status: Non-Critical
HP J4813A ProCurve Switch 2524

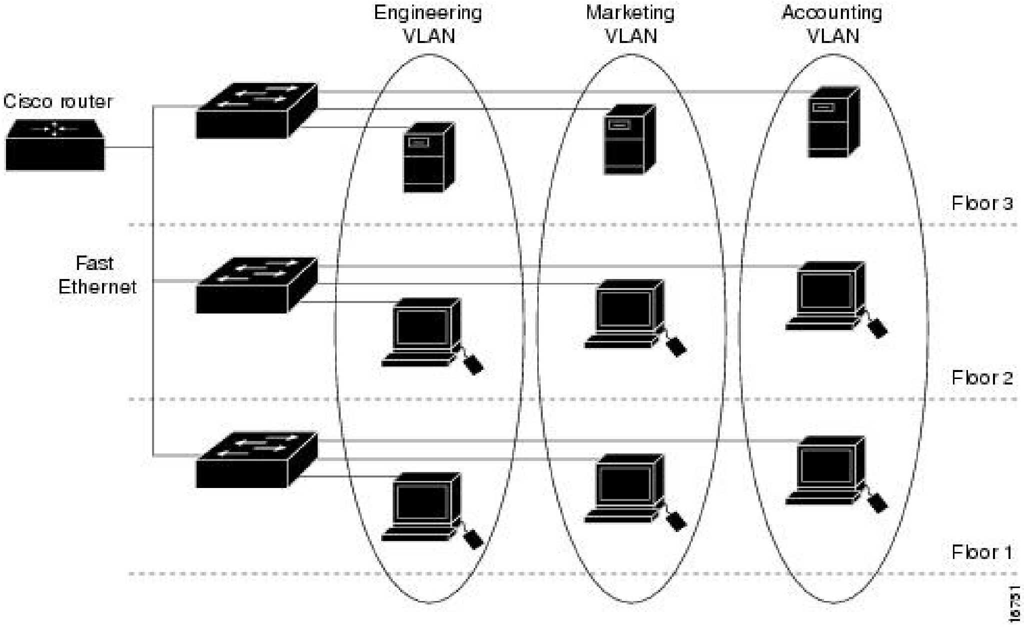
Click on a port or its LED to select it. If you wish to select several ports at once, hold down the Ctrl key while clicking on the additional ports. Click here for the meaning of the port icons.

HP ProCurve Switch 2524 Closeup View.

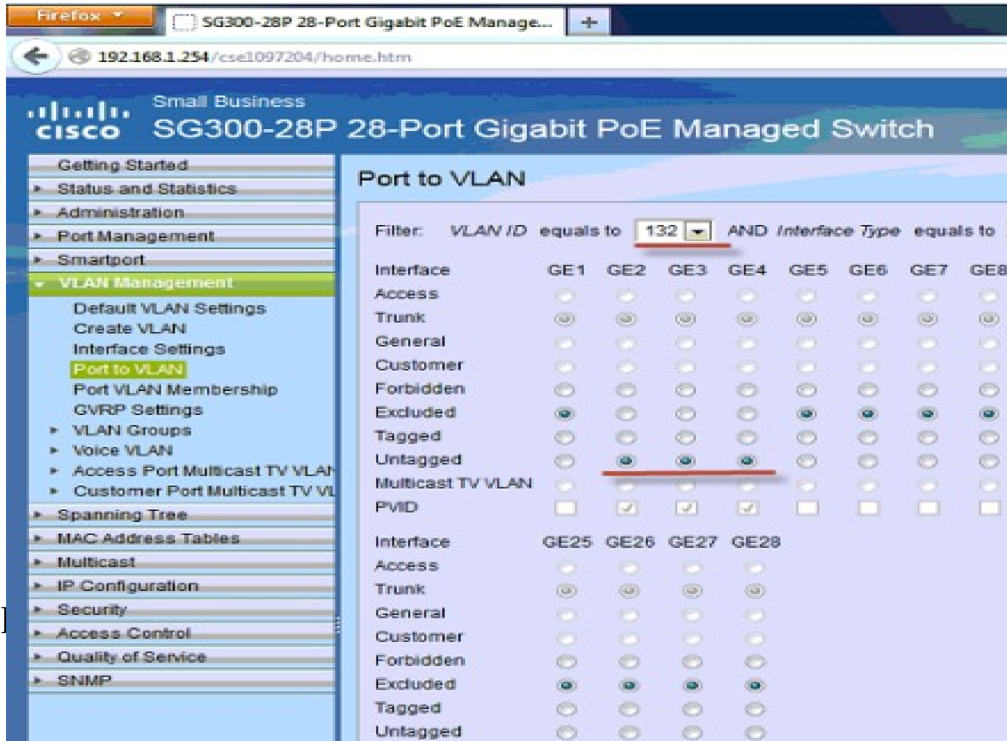
For advanced configuration start a telnet session to the switch console.

VLAN

- A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.



Cal



192.168.1.254/cse1097204/home.htm

Small Business

SG300-28P 28-Port Gigabit PoE Managed Switch

Port to VLAN

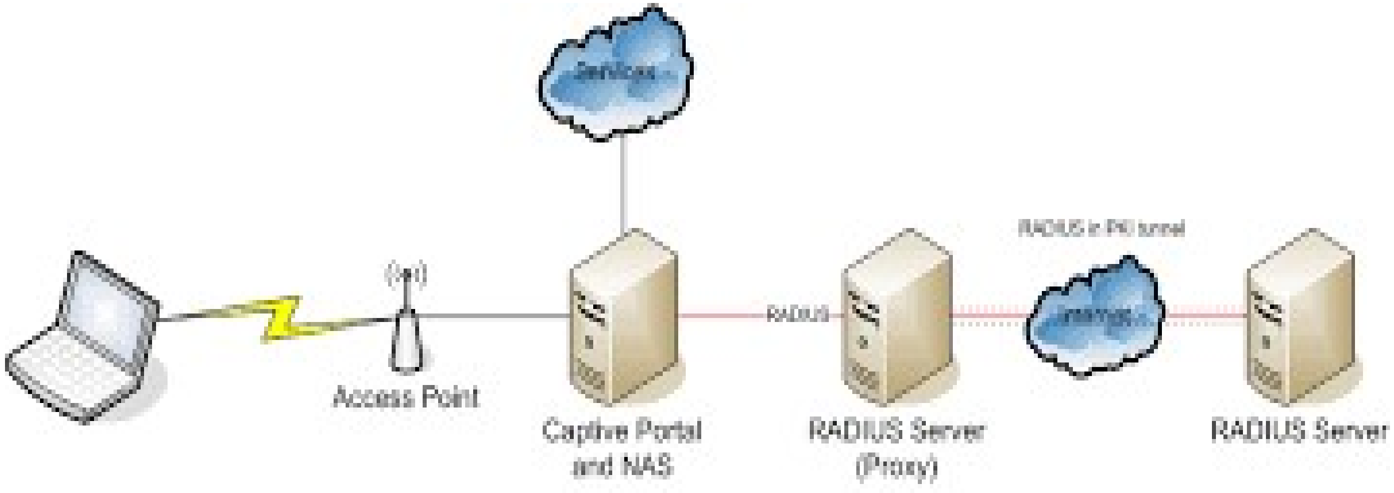
Filter: *VLAN ID* equals to 132 AND *Interface Type* equals to

Interface	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8
Access	○	○	○	○	○	○	○	○
Trunk	○	○	○	○	○	○	○	○
General	○	○	○	○	○	○	○	○
Customer	○	○	○	○	○	○	○	○
Forbidden	○	○	○	○	○	○	○	○
Excluded	●	○	○	○	●	●	●	●
Tagged	○	○	○	○	○	○	○	○
Untagged	○	●	●	●	○	○	○	○
Multicast TV VLAN	○	○	○	○	○	○	○	○
PVID	□	☑	☑	☑	□	□	□	□

Interface	GE25	GE26	GE27	GE28
Access	○	○	○	○
Trunk	○	○	○	○
General	○	○	○	○
Customer	○	○	○	○
Forbidden	○	○	○	○
Excluded	●	●	●	●
Tagged	○	○	○	○
Untagged	○	○	○	○

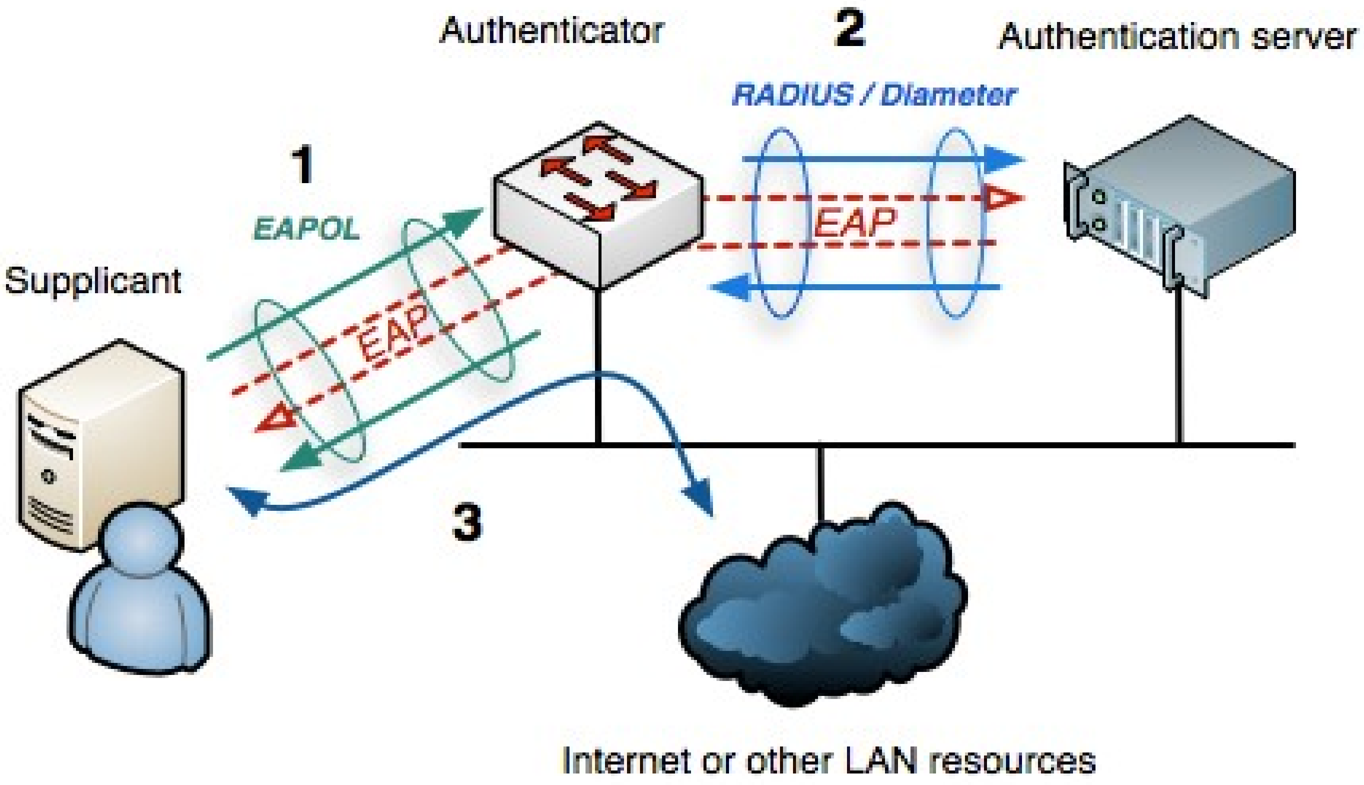
AAA Service

- An AAA server is a server program that handles user requests for access to computer resources and, for an enterprise, provides authentication, authorization, and accounting (AAA) services.



802.1x Authentication

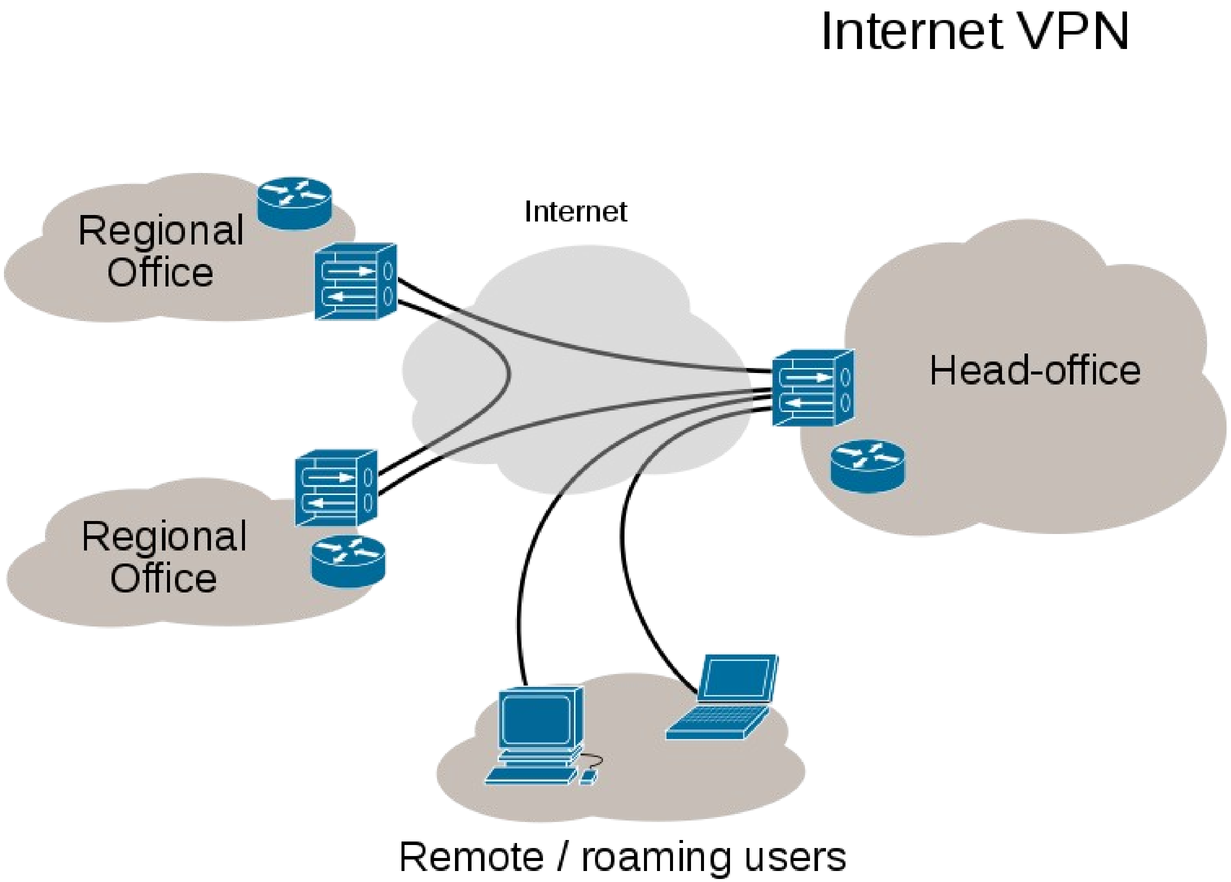
- It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.



DNS

- Domain Name Servers (DNS) are the Internet's equivalent of a phone book.
- They maintain a directory of domain names and translate them to Internet Protocol (IP) addresses.
- This is necessary because, although domain names are easy for people to remember, computers or machines, access websites based on IP addresses.

Virtual Private Networks (VPN)



A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

Network Troubleshooting commands

- Ipconfig/ifconfig
- Ping
- Arp
- Dig/nsloopup/host
- Tracert/mtr

Ethernet Technologies

Ethernet

- **Ethernet** is a family of technologies that provides data-link and physical specifications for controlling access to a shared network medium.
- It has emerged as the dominant technology used in LAN networking.

History

- Originally developed by Xerox in the 1970s, and operated at 2.94Mbps.
- The technology was standardized as Ethernet Version 1 by a consortium of three companies - DEC, Intel, and Xerox, collectively referred to as DIX - and further refined as **Ethernet II** in 1982.
- In the mid 1980s, the Institute of Electrical and Electronic Engineers (IEEE) published a formal standard for Ethernet, defined as the IEEE 802.3 standard.
- The original 802.3 Ethernet operated at 10Mbps

Advantages

Ethernet has several benefits over other LAN technologies:

- Simple to install and manage
- Inexpensive
- Flexible and scalable
- Easy to interoperate between vendors

Ethernet Cabling Types

- Ethernet can be deployed over three types of cabling:
  - Coaxial cabling – almost entirely deprecated in Ethernet networking
  - Twisted-pair cabling
  - Fiber optic cabling

Twisted Pair Cable

- The most common Ethernet cable
- Consists of two or four pairs of copper wires in a plastic sheath.
- Wires in a pair twist around each other to reduce crosstalk.
- Can be either shielded or unshielded

Twisted Pair Cable - categories

- Identified by the number of twists per inch of the copper pairs:
  - Category 3 or Cat3 - three twists per inch.
  - Cat5 - five twists per inch.
  - Cat5e - five twists per inch; pairs are also twisted around each other.
  - Cat6 – six twists per inch, with improved insulation.
- An RJ45 connector is used to connect a device to a twisted-pair cable.

Optical Fiber

- Ethernet supports two fiber specifications:
  - **Singlemode fiber** – consists of a very small glass core, allowing only a single ray or mode of light to travel across it. This greatly reduces the attenuation and dispersion of the light signal, supporting high bandwidth over very long distances, often measured in kilometers.
  - **Multimode fiber** – consists of a larger core, allowing multiple modes of light to traverse it. Multimode suffers from greater dispersion than singlemode, resulting in shorter supported distances.

Network Topologies

- A topology defines both the physical and logical structure of a network.
  - Bus
  - Star
  - Ring
  - Full or partial mesh
- Ethernet supports two topology types – bus and star.

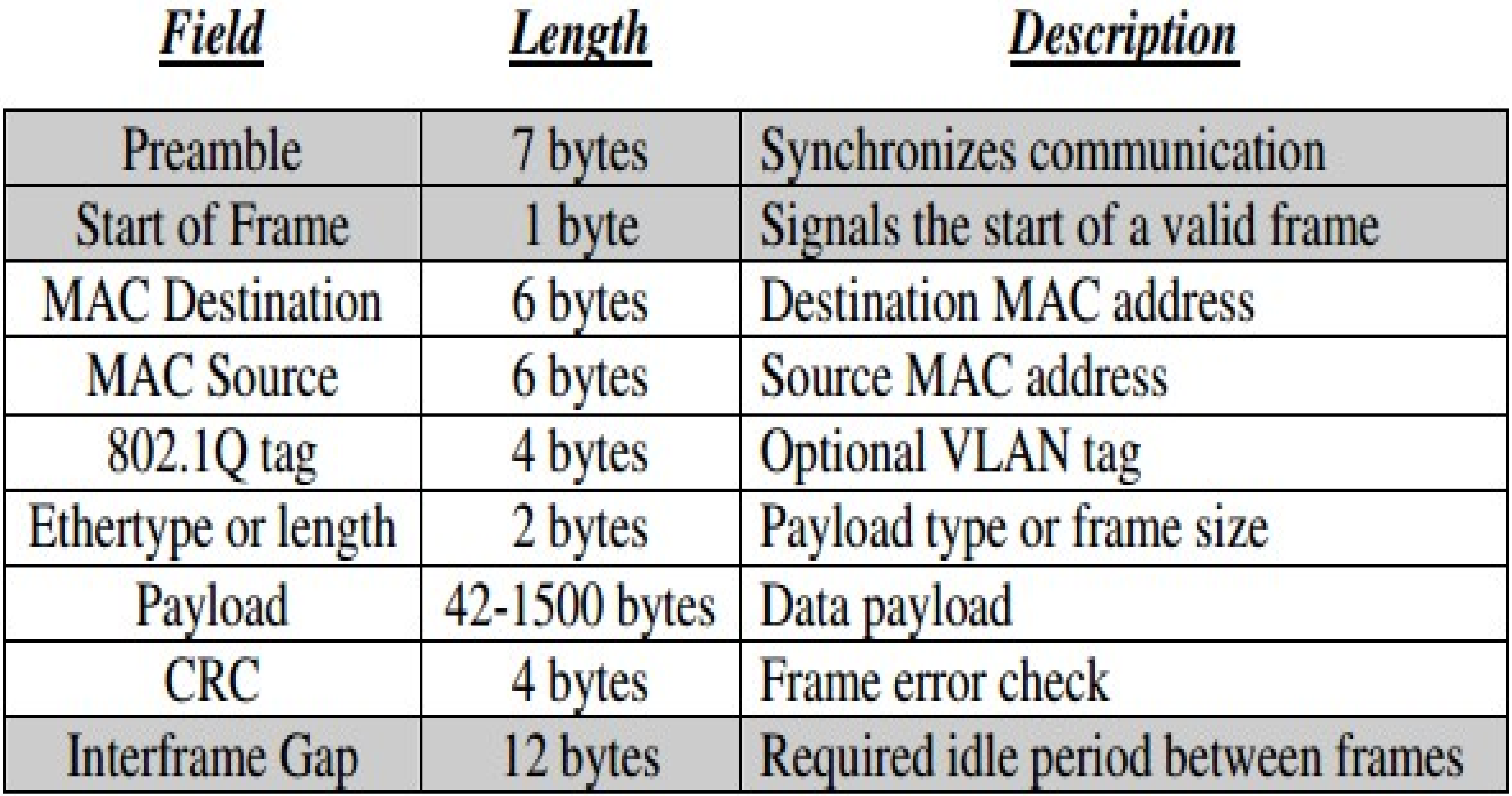
Ethernet Star Topology

- A **Switch** acts as the concentrating device.
- A switch builds a hardware address table, allowing it to make intelligent forwarding decisions based on frame (data-link) headers.
- A frame can then be forwarded out only the appropriate destination port, instead of all ports.

Ethernet Star Topology..

- Adding or removing hosts is very simple.
- Also, a break in a cable will affect only that one host, and not the entire network.
- There are two disadvantages to the star topology:
  - The switch represents a single point of failure.
  - Equipment and cabling costs are generally higher than in a bus topology.
- However, the star is still the dominant topology in modern Ethernet networks, due to its flexibility and scalability.
- Both twisted-pair and fiber cabling can be used in a star topology.

The Ethernet Frame



Field	***Length***	***Description***
Preamble	7 bytes	Synchronizes communication
Start of Frame	1 byte	Signals the start of a valid frame
MAC Destination	6 bytes	Destination MAC address
MAC Source	6 bytes	Source MAC address
802.1Q tag	4 bytes	Optional VLAN tag
Ethertype or length	2 bytes	Payload type or frame size
Payload	42-1500 bytes	Data payload
CRC	4 bytes	Frame error check
Interframe Gap	12 bytes	Required idle period between frames

Ethernet Header

- The preamble is 56 bits of alternating 1s and 0s that synchronizes communication on an Ethernet network.
- It is followed by an 8-bit start of frame delimiter (10101011) that indicates a valid frame is about to begin.
  - The preamble and the start of frame are not considered part of the actual frame, or calculated as part of the total frame size.
- Ethernet uses the 48-bit MAC address for hardware addressing.
- The first 24-bits of a MAC address determine the manufacturer of the network interface, and the last 24-bits uniquely identify the host.

Ethernet Header...

- The absolute minimum frame size for Ethernet is 64 bytes (or 512 bits) including headers.
- The maximum frame size for Ethernet is 1518 bytes – 18 bytes of header fields, and 1500 bytes of payload - or 1522 bytes with the 802.1Q tag.
- The 32-bit Cycle Redundancy Check (CRC) field is used for error detection.
- The 96-bit Interframe Gap is a required idle period between frame transmissions, allowing hosts time to prepare for the next frame.

Categories of Ethernet

- Are organized by their speed:
  - Ethernet (10Mbps)
  - Fast Ethernet (100Mbps)
  - Gigabit Ethernet
  - 10 Gigabit Ethernet
  - 40 Gigabit Ethernet

Physical Standards of Ethernet

- The physical standards for Ethernet are often labeled by their transmission rate, signaling type, and media type.
  - For example, 100baseT represents the following:
    - The first part (100) represents the transmission rate, in Mbps.
    - The second part (base) indicates that it is a baseband transmission.
    - The last part (T) represents the physical media type (twisted-pair).

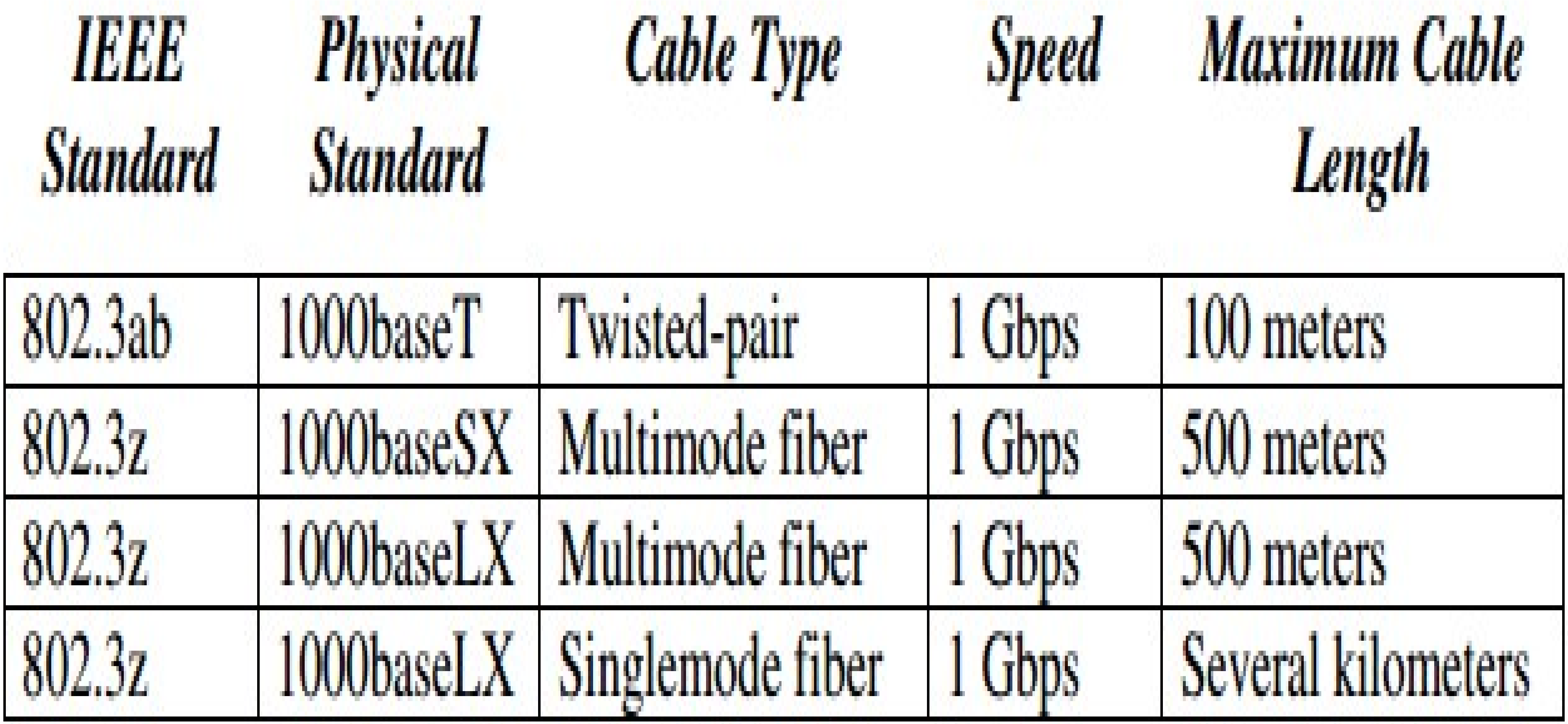
Baseband/Broadband

- Ethernet communication is **baseband**, which dedicates the entire capacity of the medium to one signal or channel.
- In **broadband**, multiple signals or channels can share the same link, through the use of modulation.

Gigabit Ethernet

- Operates at 1000 Mbps, and supports both twisted-pair (802.3ab) and fiber cabling (802.3z).
- Gigabit over twisted-pair uses all four pairs, and requires Category 5e cable for reliable performance.
- Supports both half-duplex or full-duplex operation.

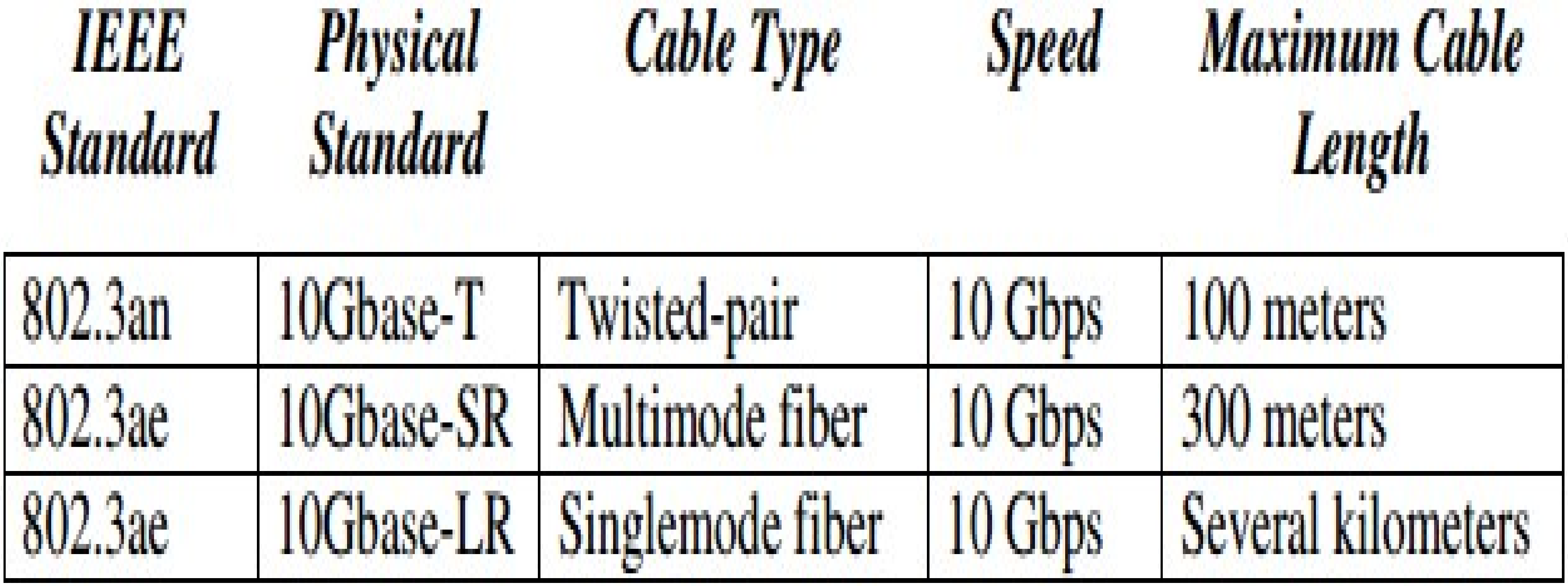
Gigabit Ethernet – Physical Standards



IEEE Standard	Physical Standard	Cable Type	Speed	Maximum Cable Length
802.3ab	1000baseT	Twisted-pair	1 Gbps	100 meters
802.3z	1000baseSX	Multimode fiber	1 Gbps	500 meters
802.3z	1000baseLX	Multimode fiber	1 Gbps	500 meters
802.3z	1000baseLX	Singlemode fiber	1 Gbps	Several kilometers

10 Gigabit Ethernet

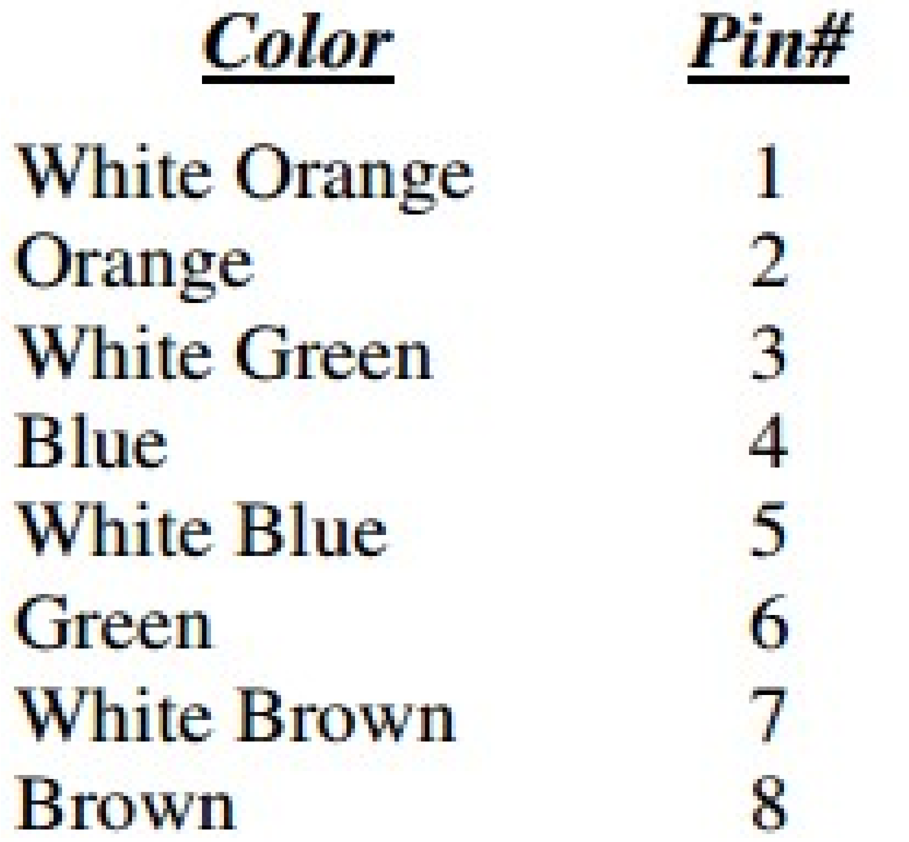
- Operates at 10000 Mbps, and supports both twisted-pair(802.3an) and fiber cabling (802.3ae).



IEEE Standard	Physical Standard	Cable Type	Speed	Maximum Cable Length
802.3an	10Gbase-T	Twisted-pair	10 Gbps	100 meters
802.3ae	10Gbase-SR	Multimode fiber	10 Gbps	300 meters
802.3ae	10Gbase-LR	Singlemode fiber	10 Gbps	Several kilometers

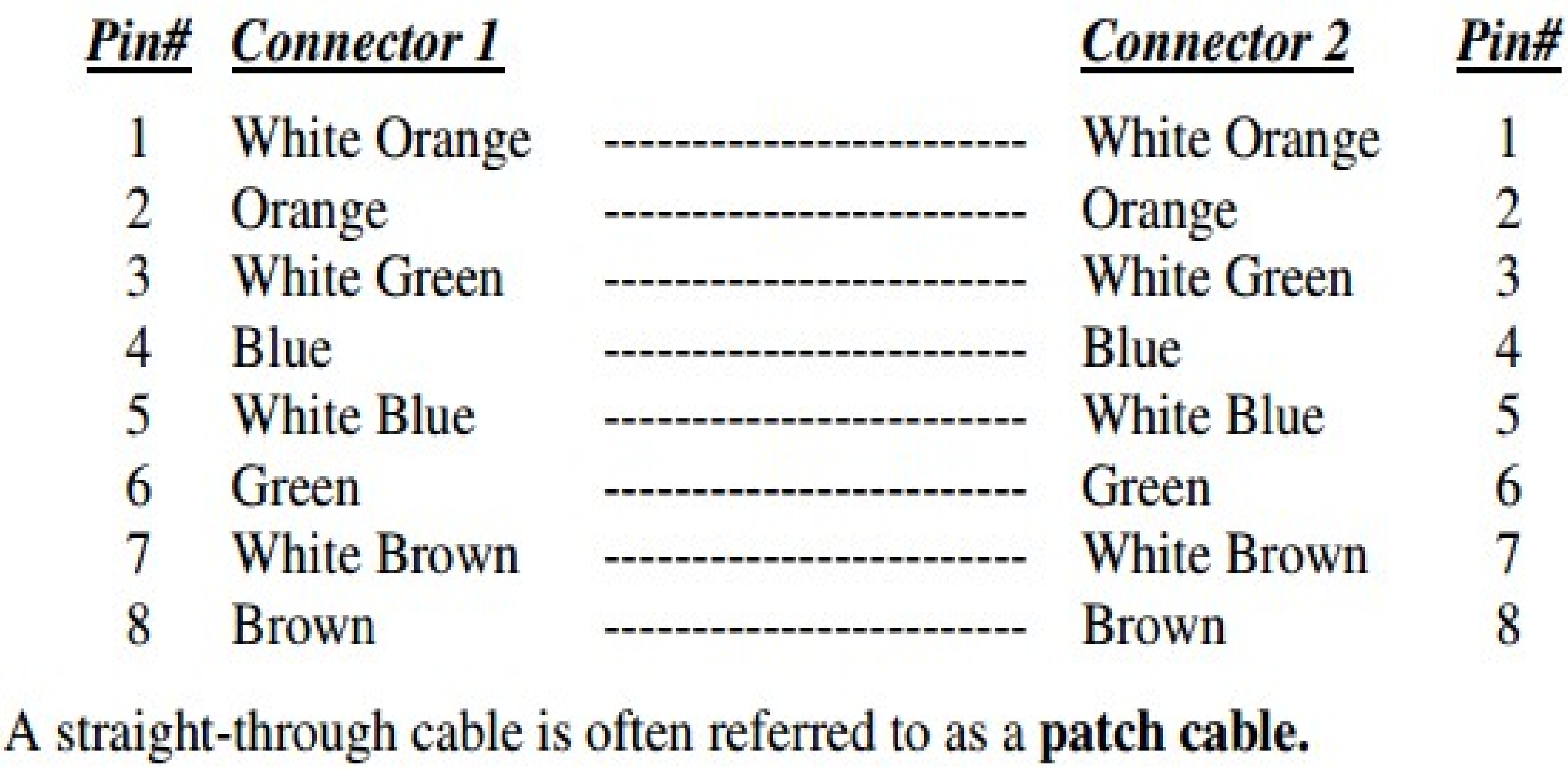
Twisted-Pair Cabling Overview

- TIA/EIA-568B Standard



Color	***Pin#***
White Orange	1
Orange	2
White Green	3
Blue	4
White Blue	5
Green	6
White Brown	7
Brown	8

Patch Cable



Pin#	Connector 1		Connector 2	Pin#
1	White Orange	------------------------	White Orange	1
2	Orange	------------------------	Orange	2
3	White Green	------------------------	White Green	3
4	Blue	------------------------	Blue	4
5	White Blue	------------------------	White Blue	5
6	Green	------------------------	Green	6
7	White Brown	------------------------	White Brown	7
8	Brown	------------------------	Brown	8

A straight-through cable is often referred to as a **patch cable.**

Power over Ethernet (PoE)

- Power over Ethernet (PoE) allows both data and power to be sent across the same twisted-pair cable, eliminating the need to provide separate power connections.
- PoE can be used to power many devices, including:
  - Voice over IP (VoIP) phones
  - Security cameras
  - Wireless access points
  - Thin clients
- Standards:
  - 802.3af - can provide roughly 13W of power to a device.
  - 802.3at - supporting 25W or more power to a device.

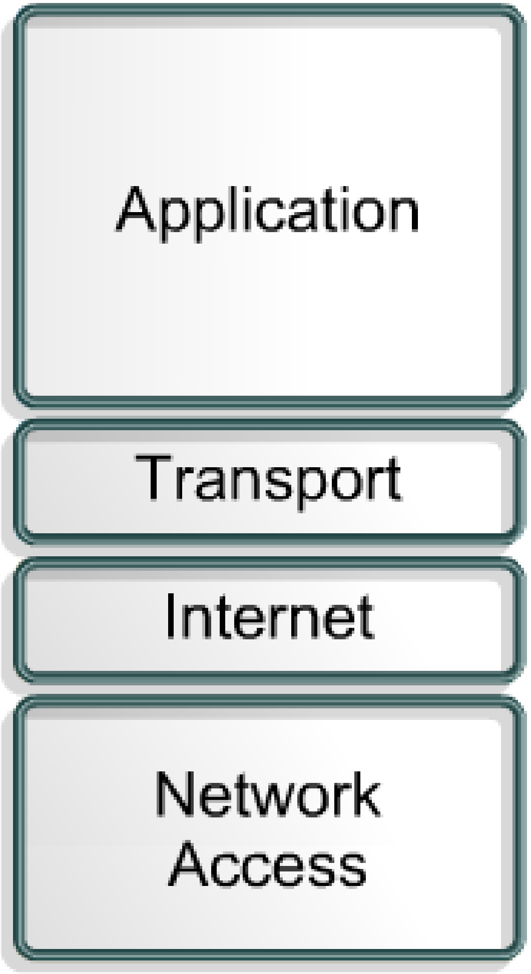
Questions?

Objectives

- Introduction to TCP/IP
- Internet addresses
- Obtaining an IP address

History and Future of TCP/IP

- The U.S. Department of Defense (DoD) created the TCP/IP reference model because it wanted a network that could survive any conditions.
- Some of the layers in the TCP/IP model have the same name as layers in the OSI model.



Application Layer

- Handles high-level protocols, issues of representation, encoding, and dialog control.
- The TCP/IP protocol suite combines all application related issues into one layer and ensures this data is properly packaged before passing it on to the next layer.

Application Layer Examples

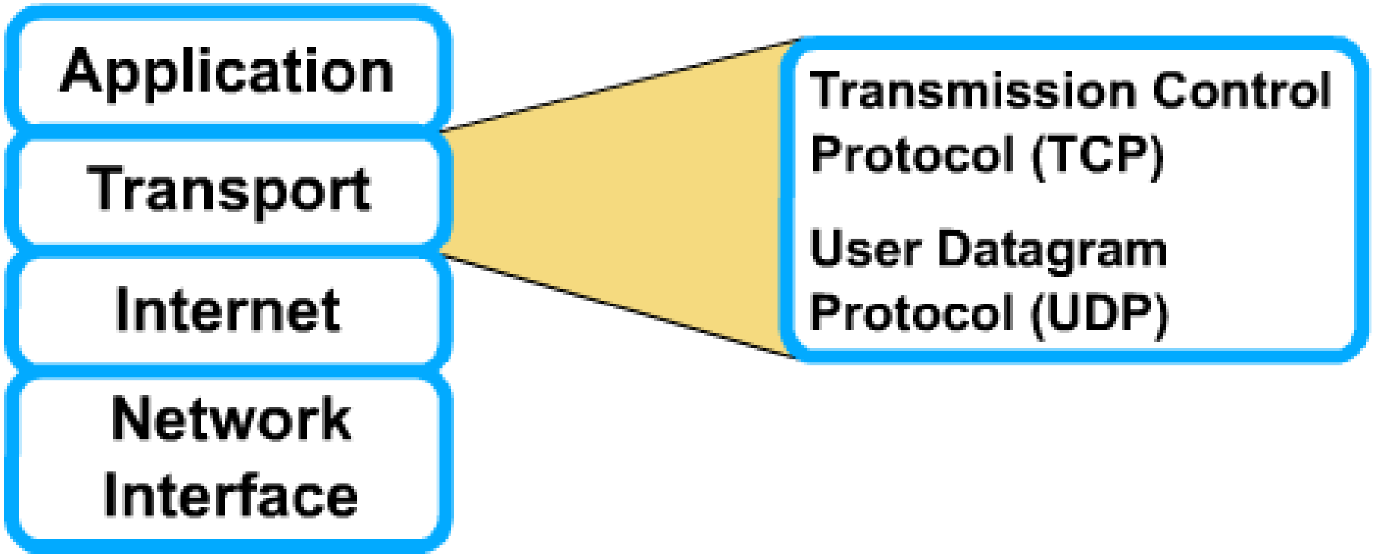
- Telnet – Provides the capability to remotely access another computer
- File Transfer Protocol – Download or upload files
- Hypertext Transfer Protocol – Works with the World Wide Web

Transport Layer

Five basic services:

- Segmenting upper-layer application data
- Establishing end-to-end operations
- Sending segments from one end host to another end host
- Ensuring data reliability
- Providing flow control

Layer 4 Protocols

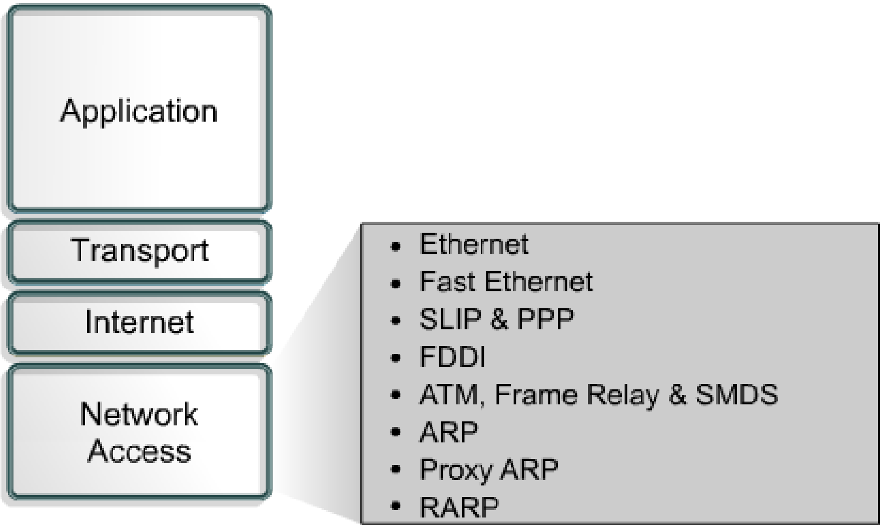

Application
Transport
Internet
Network Interface
Transmission Control Protocol (TCP)
User Datagram Protocol (UDP)

Internet Layer

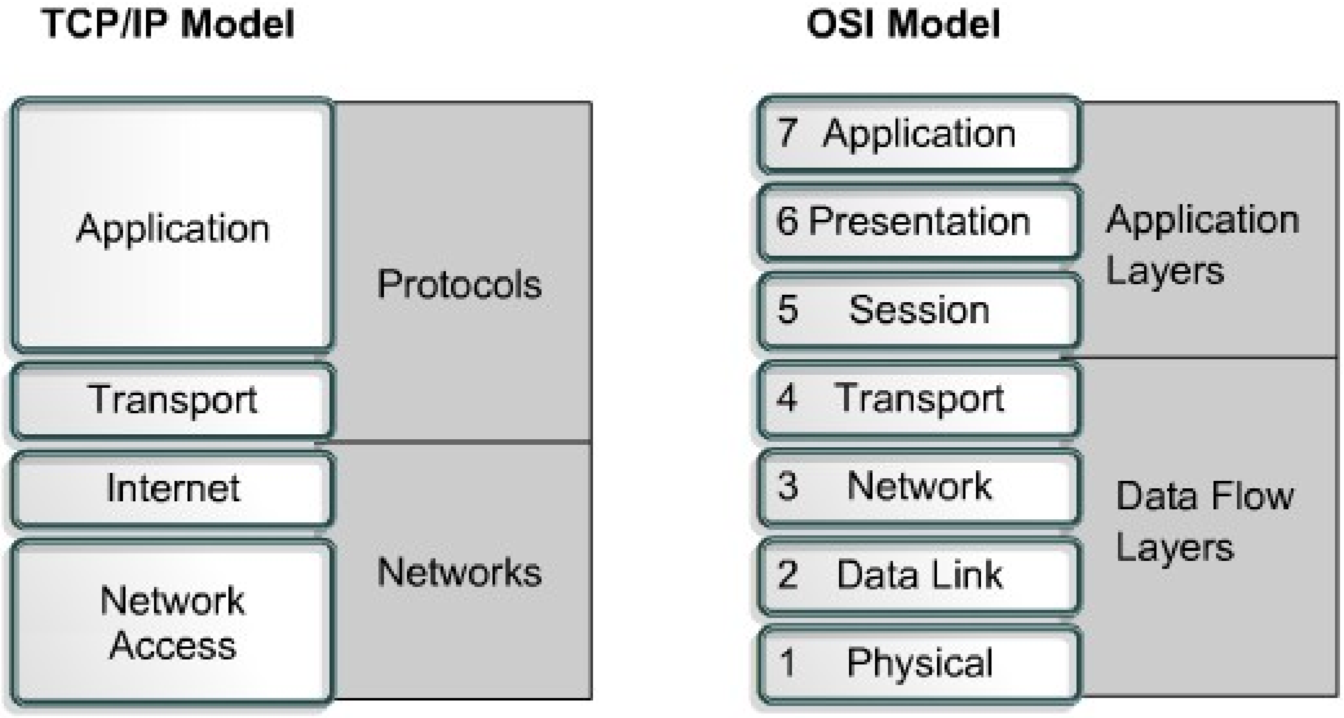
- The purpose of the Internet layer is to send packets from a network node and have them arrive at the destination node independent of the path taken.
- Internet layer protocols:
  - Internet Protocol (IP)
  - Internet Control Message Protocol (ICMP)
  - Address Resolution Protocol (ARP)
  - Reverse Address Resolution Protocol (RARP)

Network Access Layer

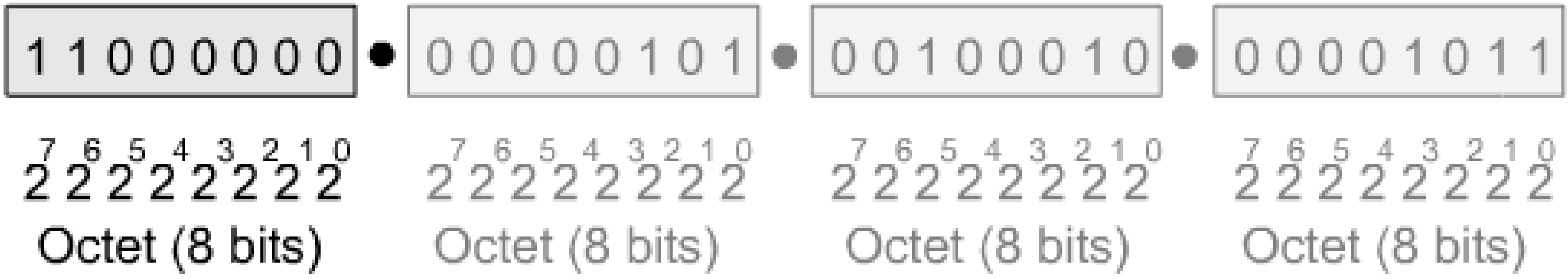
- The network access layer is concerned with all of the issues that an IP packet requires to actually make a physical link to the network media.
- It includes the LAN and WAN technology details, and all the details contained in the OSI physical and data link layers.

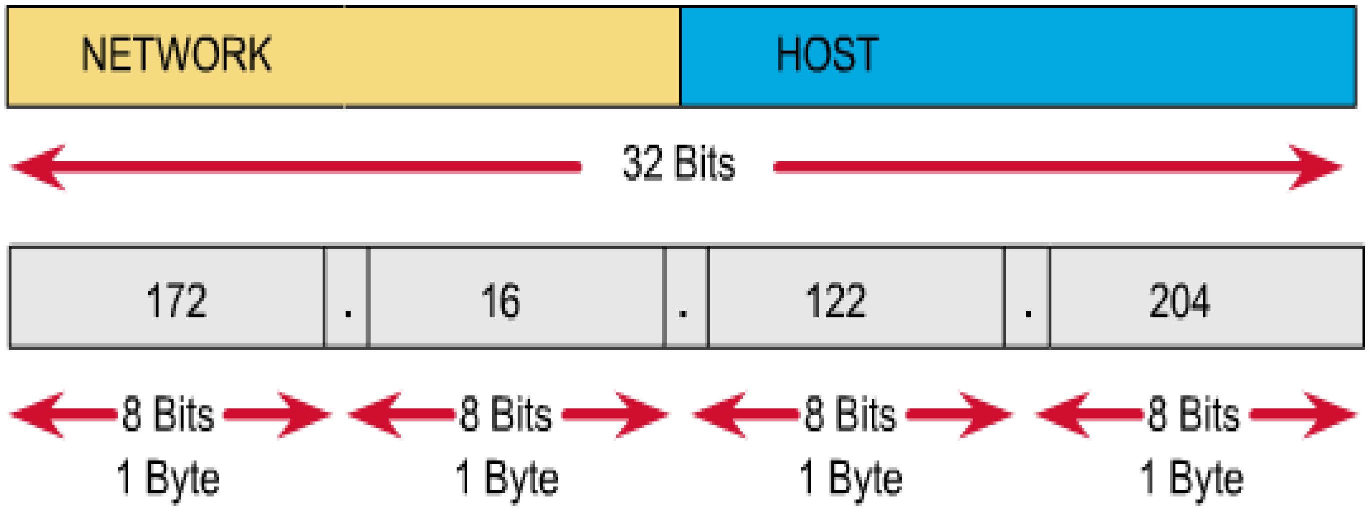


Comparing the OSI Model and TCP/IP Model

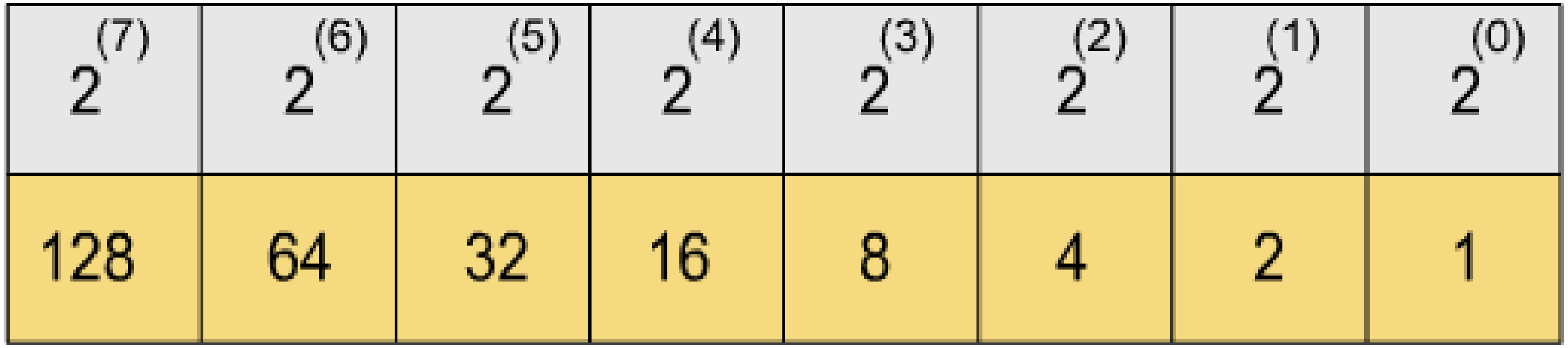


IPv4 Address as a 32-Bit Binary Number

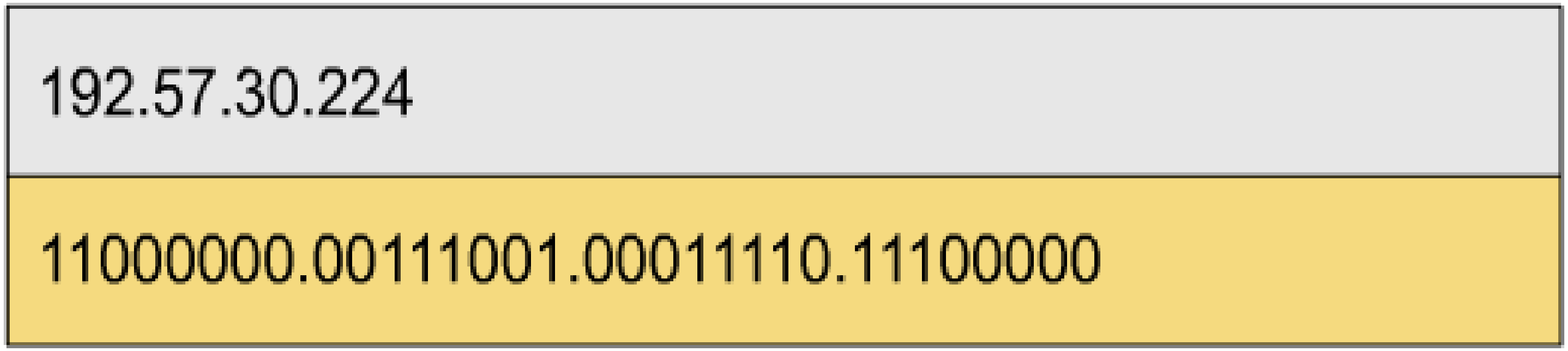




Binary and Decimal Conversion

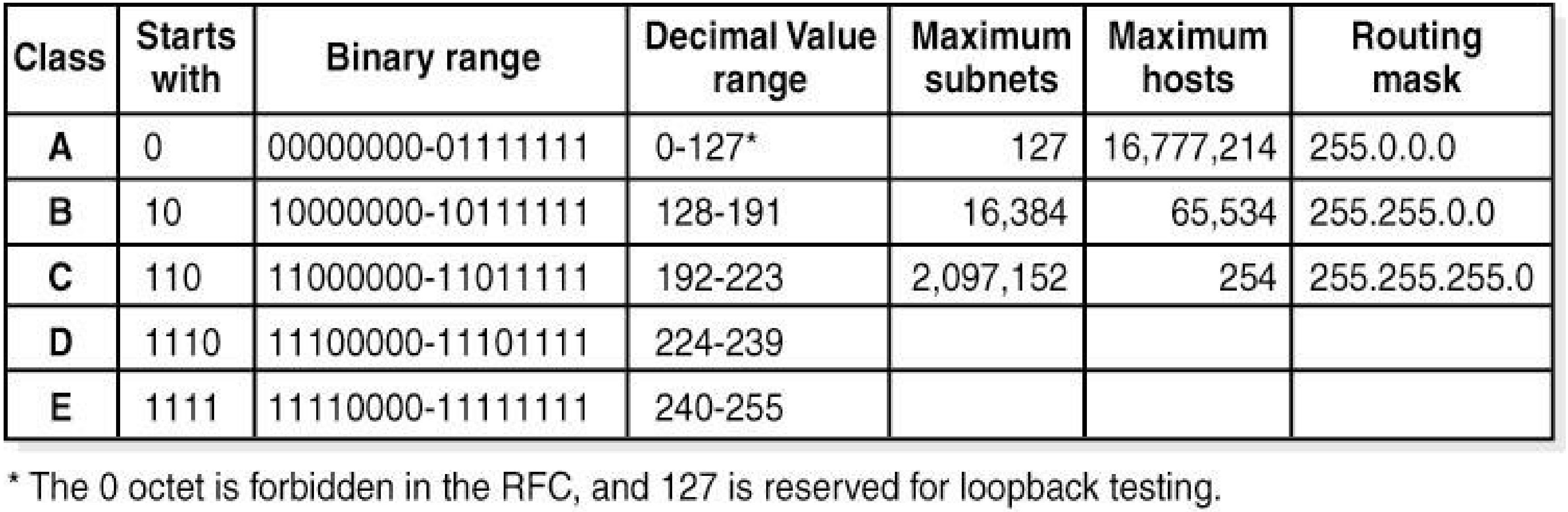


$2^{(7)}$	$2^{(6)}$	$2^{(5)}$	$2^{(4)}$	$2^{(3)}$	$2^{(2)}$	$2^{(1)}$	$2^{(0)}$
128	64	32	16	8	4	2	1



192.57.30.224
11000000.00111001.00011110.11100000

IP Addresses as Decimal Numbers

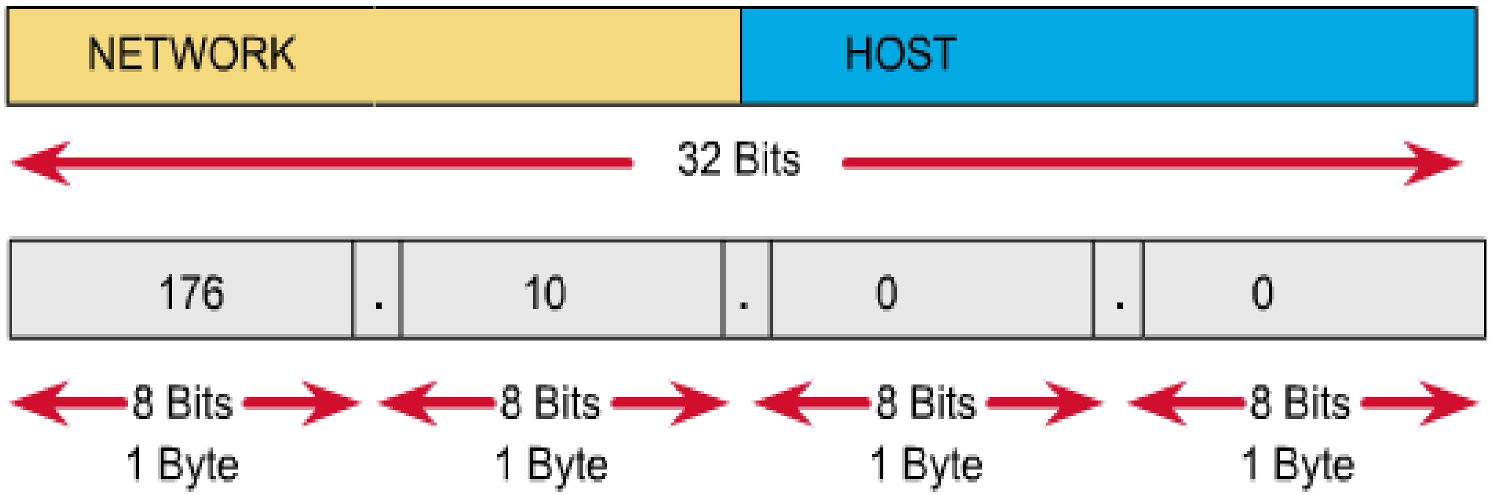


Class	Starts with	Binary range	Decimal Value range	Maximum subnets	Maximum hosts	Routing mask
A	0	00000000-01111111	0-127*	127	16,777,214	255.0.0.0
B	10	10000000-10111111	128-191	16,384	65,534	255.255.0.0
C	110	11000000-11011111	192-223	2,097,152	254	255.255.255.0
D	1110	11100000-11101111	224-239			
E	1111	11110000-11111111	240-255			

* The 0 octet is forbidden in the RFC, and 127 is reserved for loopback testing.

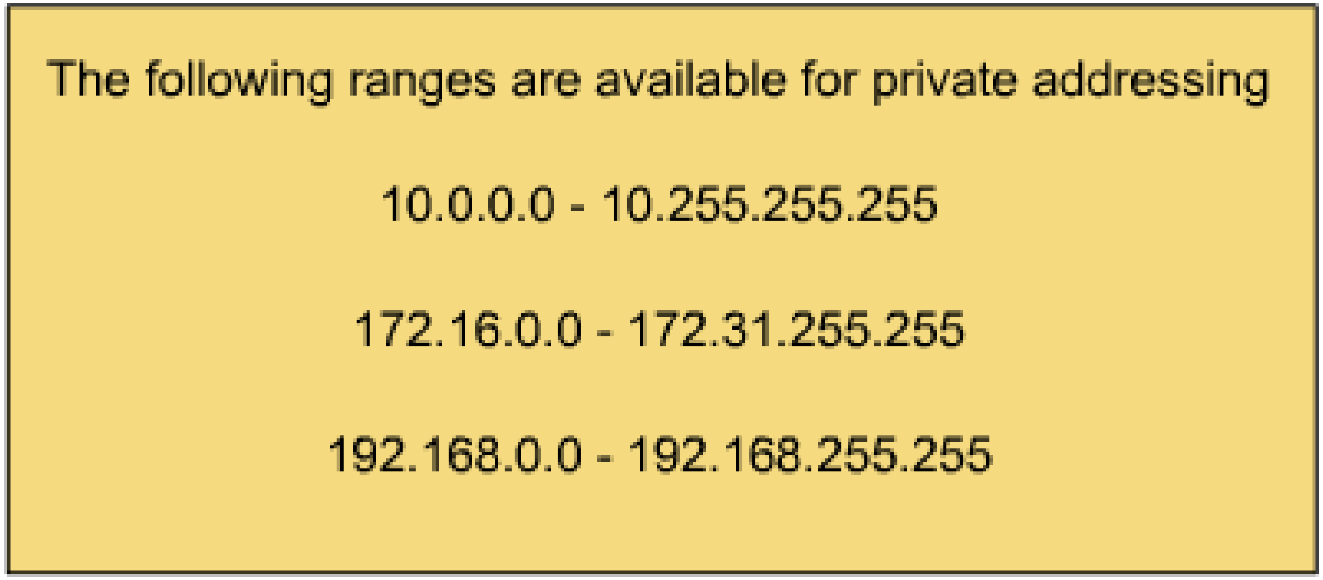
Network IDs and Broadcast Addresses

An IP address such as 176.10.0.0 that has all binary 0s in the host bit positions is reserved for the network address.



An IP address such as 176.10.255.255 that has all binary 1s in the host bit positions is reserved for the broadcast address.

Private Addresses



The following ranges are available for private addressing

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

Subnet Mask

- Determines which part of an IP address is the network field and which part is the host field
- Follow these steps to determine the subnet mask:
  - 1. Express the subnetwork IP address in binary form.
  - 2. Replace the network and subnet portion of the address with all 1s.
  - 3. Replace the host portion of the address with all 0s.
  - 4. Convert the binary expression back to dotted-decimal notation.

Obtaining an IP Address

- Static addressing
  - Each individual device must be configured with an IP address.
- Dynamic addressing
  - Reverse Address Resolution Protocol (RARP)
  - Bootstrap Protocol (BOOTP)
  - Dynamic Host Configuration Protocol (DHCP)
  - DHCP initialization sequence
  - Function of the Address Resolution Protocol
  - ARP operation within a subnet

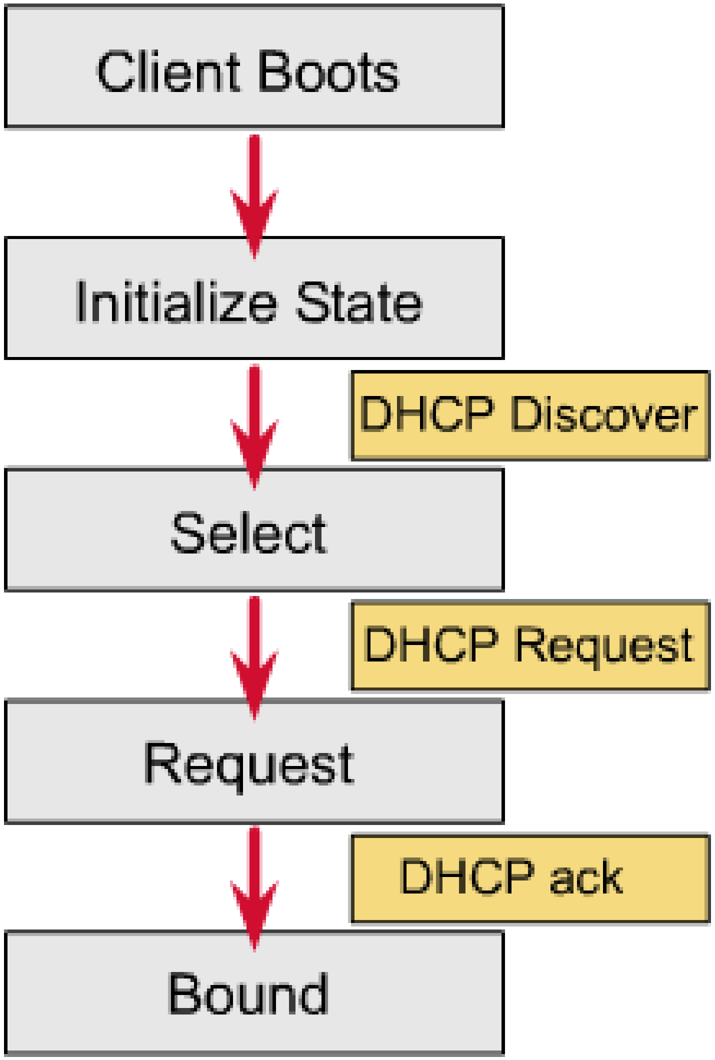
Static Assignment of IP Addresses

- Each individual device must be configured with an IP address.

Dynamic Host Configuration Protocol

- Allows a host to obtain an IP address using a defined range of IP addresses on a DHCP server.
- As hosts come online, contact the DHCP server, and request an address.

DHCP Initialization Sequence



Client Boots

Initialize State

DHCP Discover

Select

DHCP Request

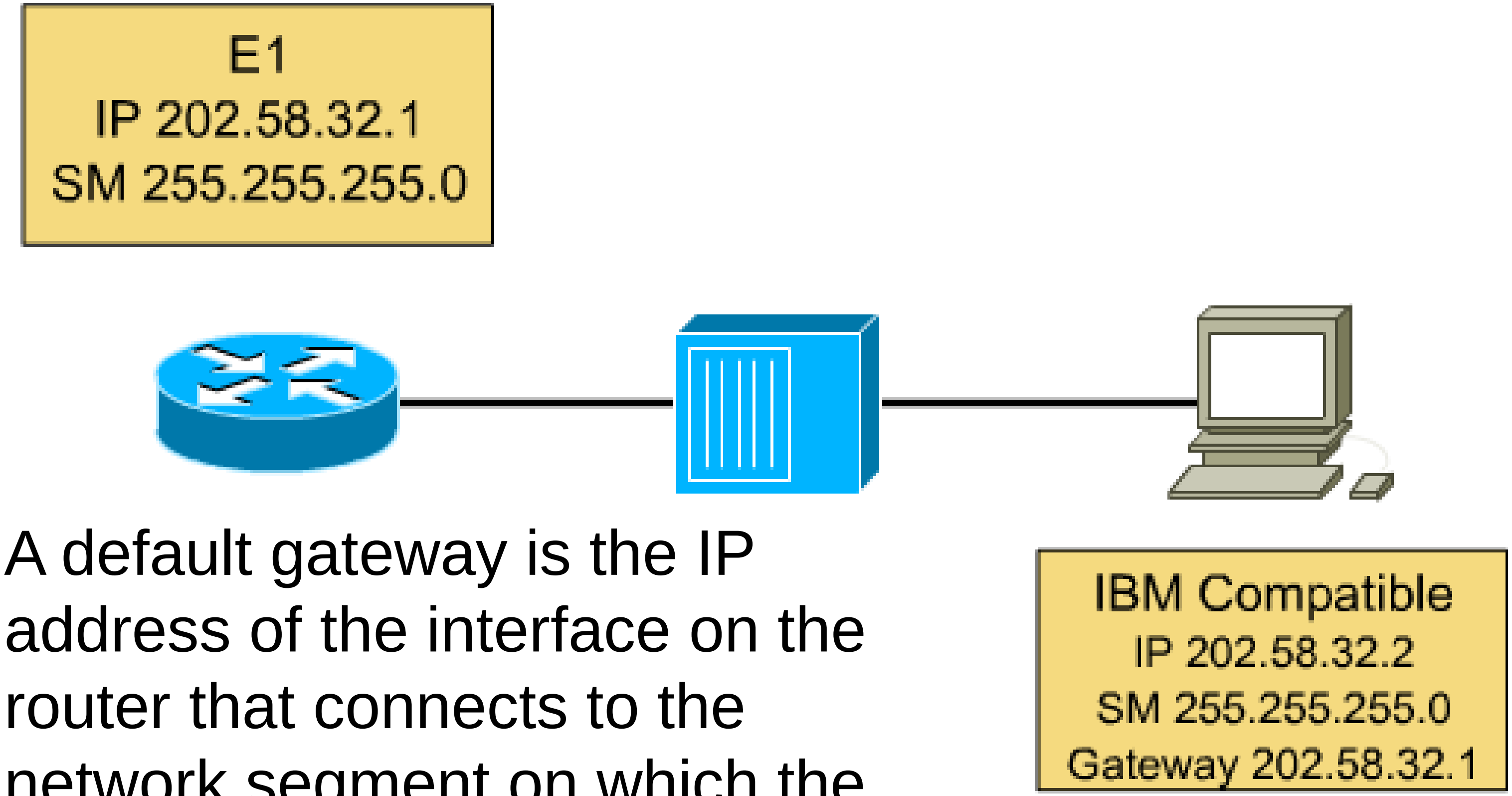
Request

DHCP ack

Bound

Client collects DHCP offer responses from the server.

Default Gateway



E1
IP 202.58.32.1
SM 255.255.255.0

IBM Compatible
IP 202.58.32.2
SM 255.255.255.0
Gateway 202.58.32.1

A default gateway is the IP address of the interface on the router that connects to the network segment on which the source host is located.

IPv6 Address

- An IPv6 address consists of 8 sets of 16-bit hexadecimal values separated by colons (:), totaling 128 bits in length. For example:

2001:0db8:1234:5678:9abc:def0:1234:5678

- Leading zeros can be omitted, and consecutive zeros in contiguous blocks can be represented by a double colon (::).
- Double colons can appear only once in the address. For example:

2001:0db8:0000:130F:0000:0000:087C:140B

- can be abbreviated as

2001:db8:0:130F::87C:140B

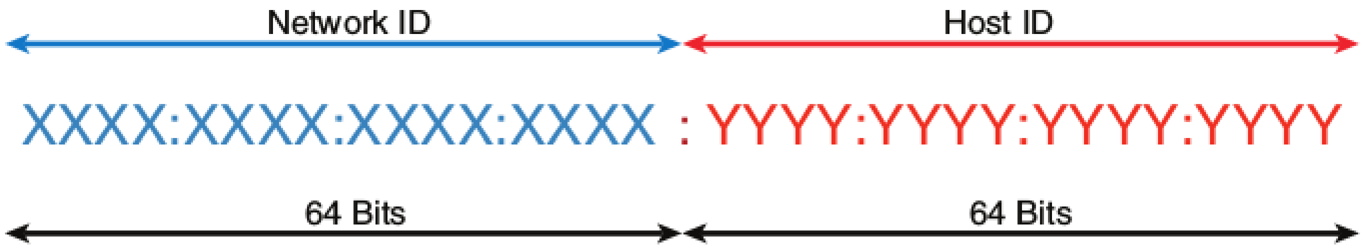
CIDR Representation

- As with the IPv4 Classless Inter-Domain Routing (CIDR) network prefix representation (such as 10.1.1.0/8), an IPv6 address network prefix is represented the same way:

2001:db8:12::/64

IPv6 Unicast Addresses – Network and Host IDs

- IPv6 unicast addresses generally use 64 bits for the network ID and 64 bits for the host ID.



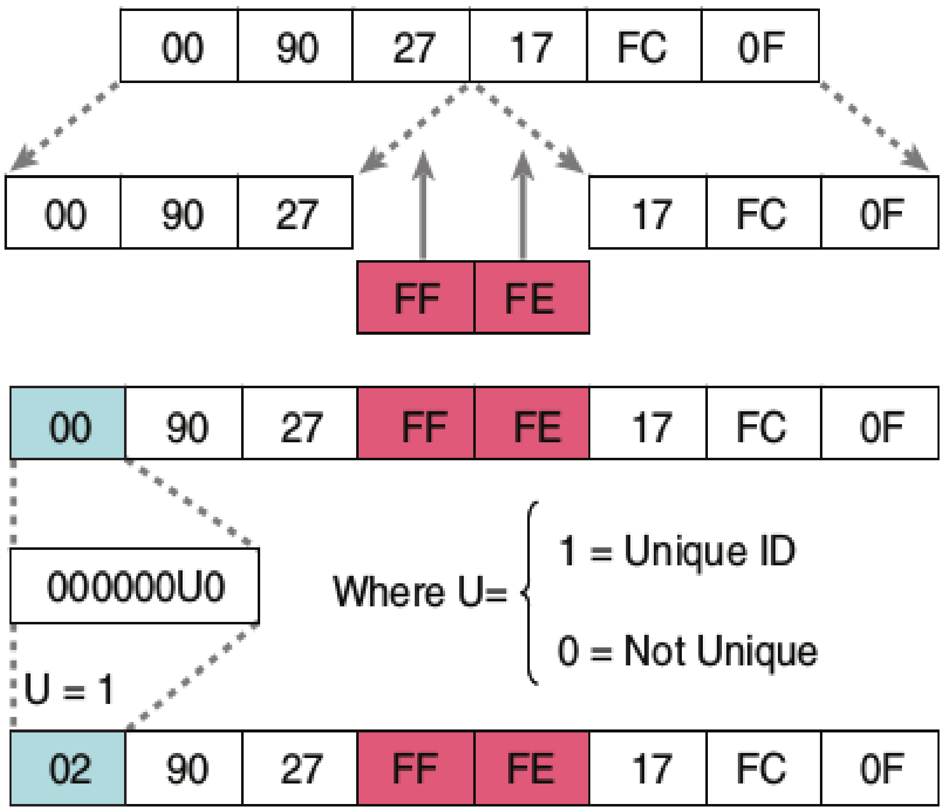
IP Assignment

- The network ID is administratively assigned, and the host ID can be configured manually or auto-configured by any of the following methods:
  - Using a randomly generated number
  - Using DHCPv6
  - Using the Extended Unique Identifier (EUI-64) format.

Extended Unique Identifier (EUI-64) format

- This format expands the device interface 48-bit MAC address to 64 bits by inserting FFFE into the middle 16 bits.
- Cisco commonly uses the EUI-64 host ID format for Cisco IP Phones, gateways, routers, and so forth.

Conversion of EUI-64 MAC Address to IPv6 Host Address Format



Types of IPv6 Addresses

- As with IPv4, IPv6 addresses are assigned to interfaces; however, unlike IPv4, an IPv6 interface is expected to have multiple addresses.
- The IPv6 addresses assigned to an interface can be any of the following types:
  - Unicast address
  - Multicast address
  - Anycast address

Unicast address

- Identifies a single node or interface.
- Traffic destined for a unicast address is forwarded to a single interface.

Multicast address

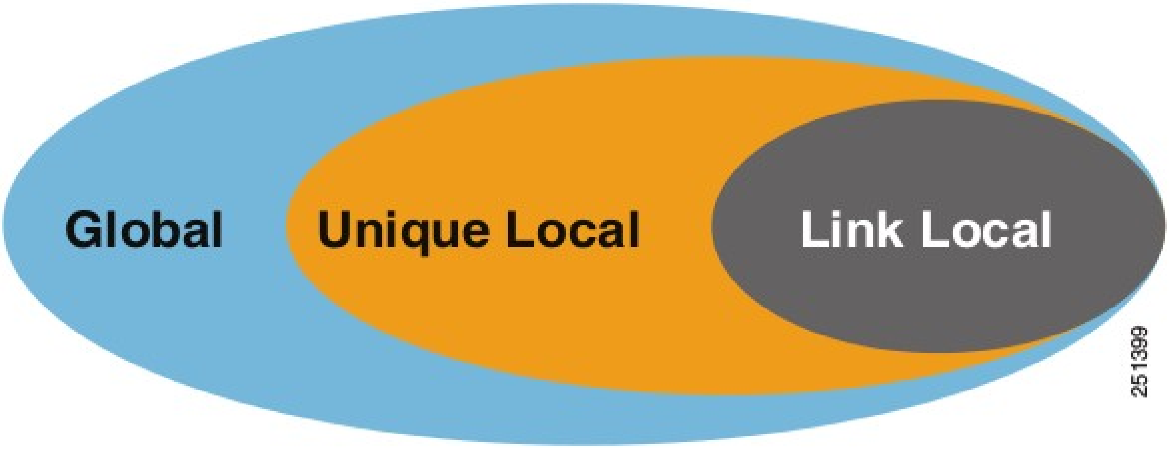
- Identifies a group of nodes or interfaces.
- Traffic destined for a multicast address is forwarded to all the nodes in the group

Anycast address

- Identifies a group of nodes or interfaces.
- Traffic destined to an anycast address is forwarded to the nearest node in the group.
- An anycast address is essentially a unicast address assigned to multiple devices with a host ID = 0000:0000:0000:0000. (Anycast addresses are not widely used today.)

Address Scopes

- An address scope defines the region where an address can be defined as a unique identifier of an interface.

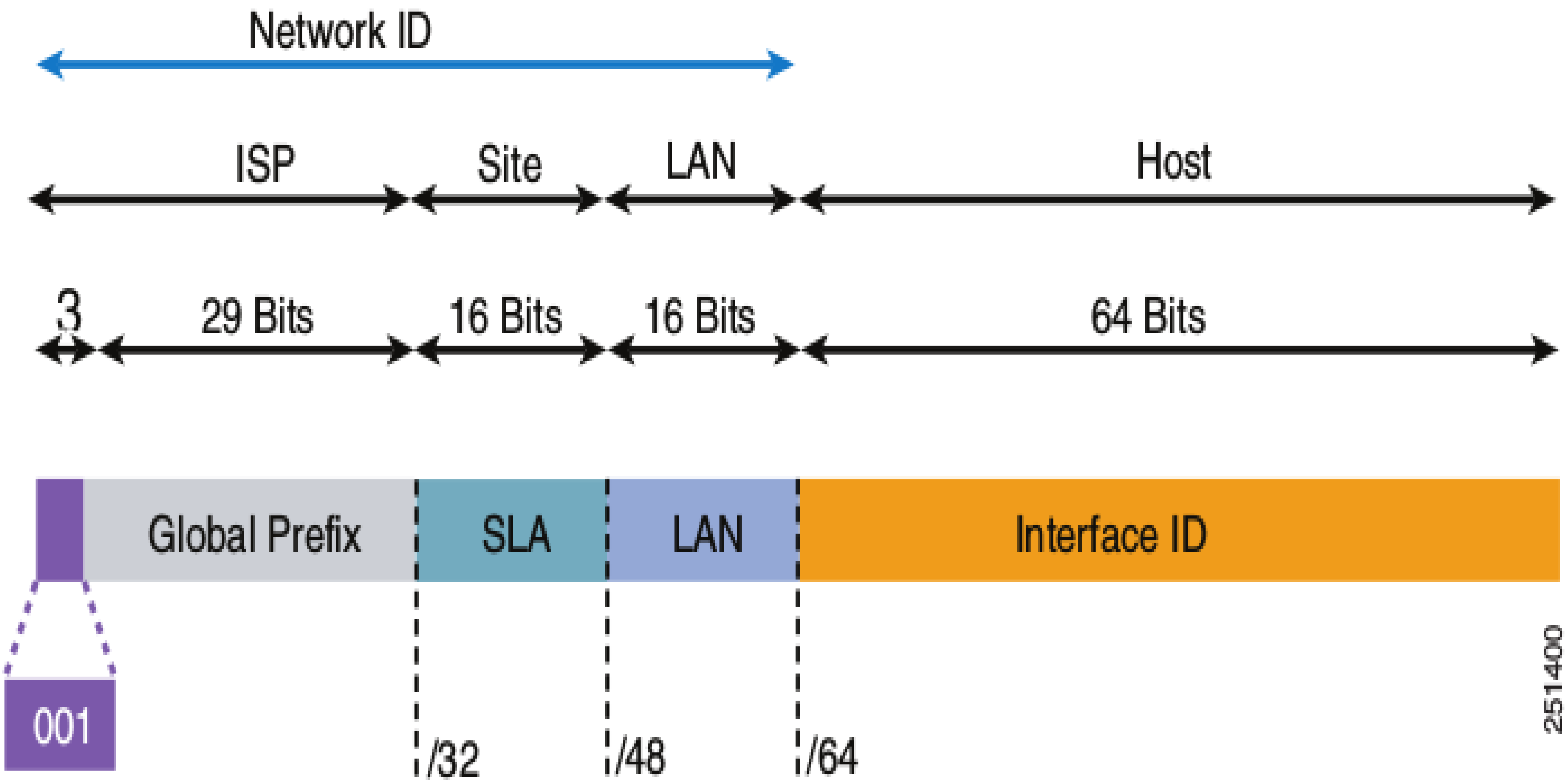


- These scopes or regions
  - **Link - link-local,**
  - **site network - unique local unicast**
  - **global network - global addresses**

Global Unicast Addresses

- Global unicast addresses are:
  - Routable and reachable across the Internet
  - IPv6 addresses for widespread generic use
  - Structured as a hierarchy to allow address aggregation
  - Identified by their three high-level bits set to 001 (2000::/3)

Global Unicast Address Format



Global Unicast Address Format...

- The global routing prefix is assigned to a service provider by the Internet Assigned Numbers Authority (IANA).
- The site level aggregator (SLA), or subnet ID, is assigned to a customer by their service provider.
- The LAN ID represents individual networks within the customer site and is administered by the customer.

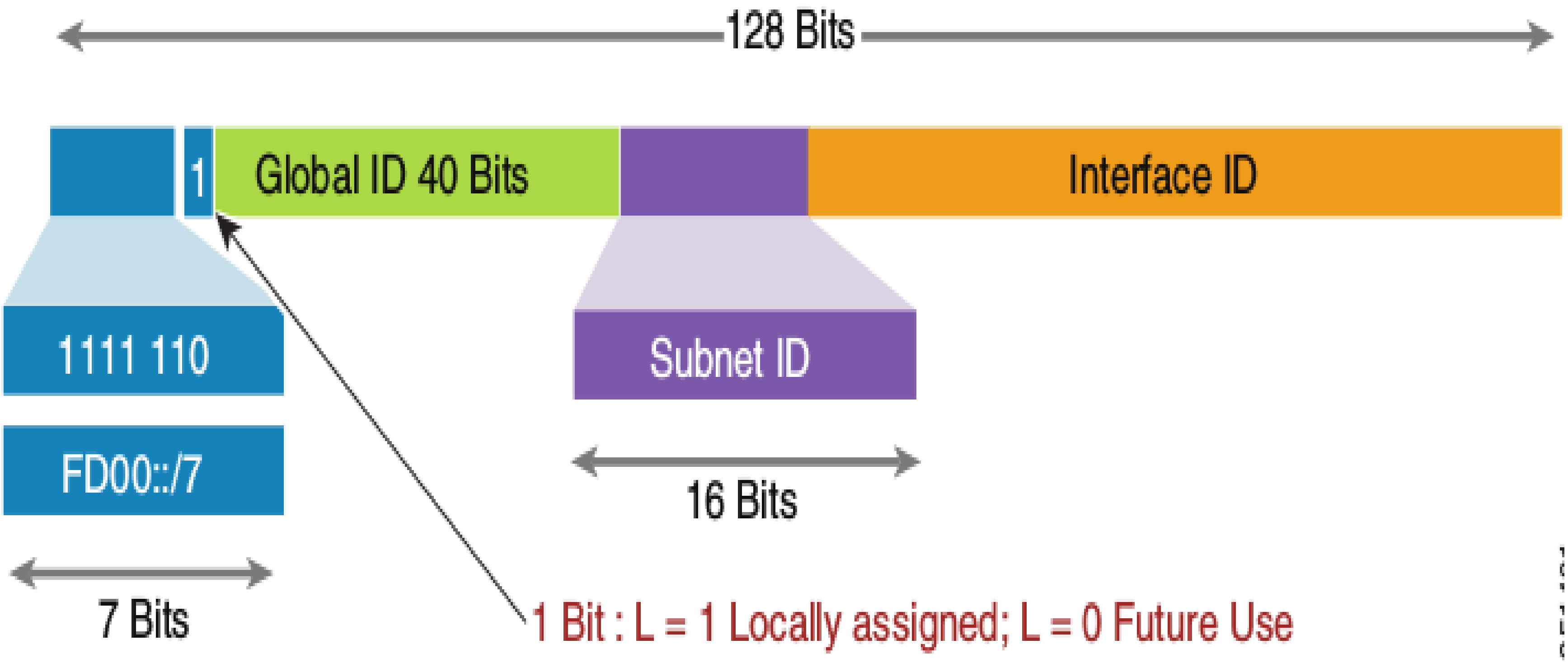
Global Unicast Address Format..

- The Host or Interface ID has the same meaning for all unicast addresses.
- It is 64 bits long and is typically created by using the EUI-64 format.
- Example of a global unicast address:
  - 2001:0DB8:BBBB:CCCC:0987:65FF:FE01:2345

Unique Local Unicast Addresses

- Unique local unicast addresses are:
  - Analogous to private IPv4 addresses (for example, 10.1.1.254)
  - Used for local communications, inter-site VPNs, and so forth
  - Not routable on the Internet (routing would require IPv6 NAT)

Unique Local Unicast Addresses..



Unique Local Unicast Addresses..

- Global IDs do not have to be aggregated and are defined by the administrator of the local domain.
- Subnet IDs are also defined by the administrator of the local domain.
- Subnet IDs are typically defined using a hierarchical addressing plan to allow for route summarization.

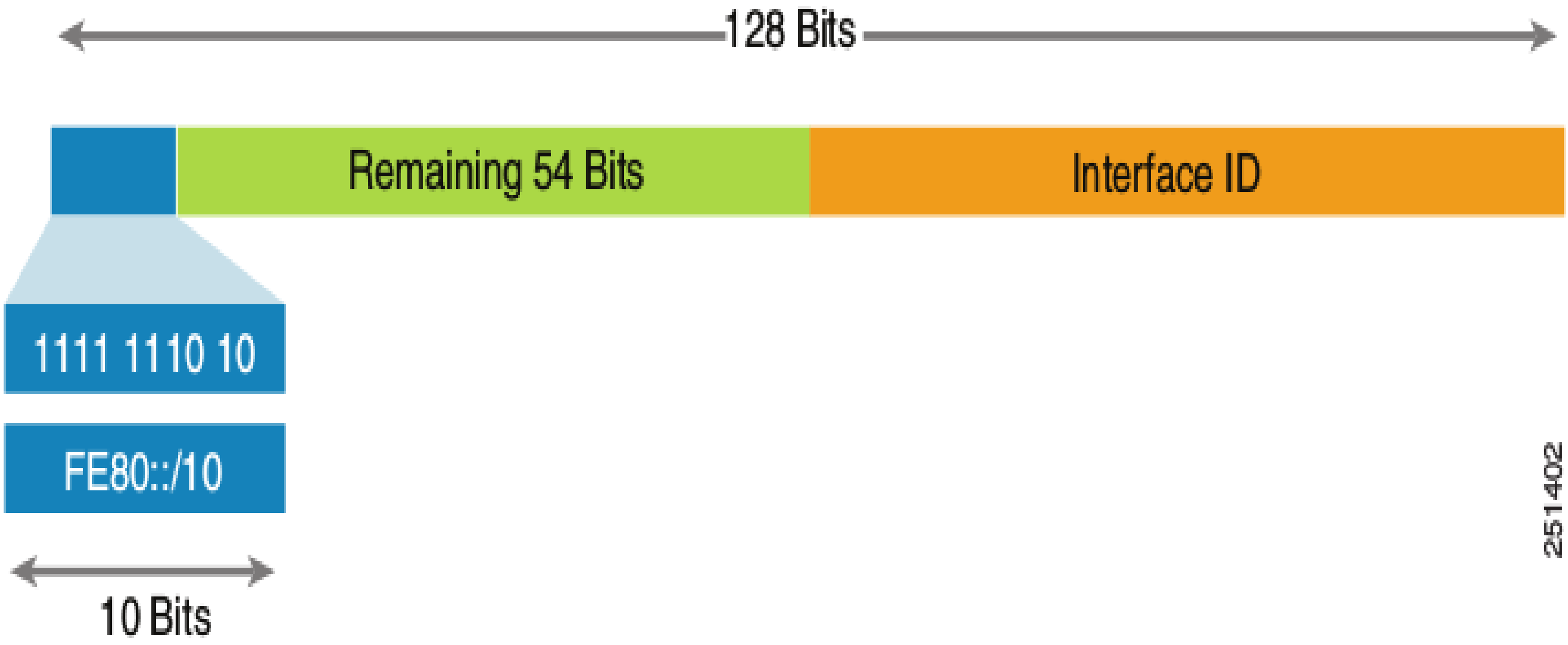
Unique Local Unicast Addresses..

- The Host or Interface ID has the same meaning for all unicast addresses.
- It is 64 bits long and is typically created by using the EUI-64 format.
- Example of a unique local unicast address:
  - FD00:aaaa:bbbb:CCCC:0987:65FF:FE01:2345

Link Local Unicast Addresses

- Link local unicast addresses are:
  - Mandatory addresses that are used exclusively for communication between two IPv6 devices on the same link
  - Automatically assigned by device as soon as IPv6 is enabled
  - Not routable addresses (Their scope is link-specific only.)
  - Identified by the first 10 bits (FE80)

Link Local Unicast Addresses..



The remaining 54 bits of the network ID could be zero or any manually configured value.
The interface ID has the same meaning for all unicast addresses. It is 64 bits long and is typically created by using the EUI-64 format.

IPv6 Multicast Addresses

- IPv6 multicast addresses have an 8-bit prefix, FF00::/8 (1111 1111).
- The second octet defines the lifetime and scope of the multicast address

Address Assignment for IPv6 Devices

- Manual Configuration
  - An IPv6 address can be configured statically by a human operator.
  - This can be an appropriate method of assigning addresses for router interfaces and static network elements and resources.
  - However, manual assignment is open to errors and operational overhead due to the 128-bit length and hexadecimal attributes of the addresses

IPv6 Stateless Address Auto-Configuration

- Stateless address auto-configuration (SLAAC) provides a convenient method to assign IP addresses to IPv6 nodes. This method does not require any human intervention from an IPv6 user.
- If you want to use IPv6 SLAAC on an IPv6 node, then it is important to connect that IPv6 node to a network with at least one IPv6 router.
- This router is configured by the network administrator and sends out Router Advertisement (RA) announcements onto the link.
- These announcements can allow the on-link connected IPv6 nodes to configure themselves with an IPv6 address and routing parameters, as specified in RFC2462, without further human intervention.
- With SLAAC, the node uses the IPv6 network prefix advertised in the link-local router's RAs and creates the IPv6 host ID by using the device's MAC address and the EUI-64 format for host IDs.

IP Configuration in Linux

- Centos 8
  - /etc/sysconfig/network-scripts/ifcfg-(interface-name)
    - Contents can be:
      - TYPE="Ethernet"
      - BOOTPROTO="none"
      - NAME="enp0s3"
      - IPADDR="192.168.2.10"
      - NETMASK="255.255.255.0"
      - GATEWAY="192.168.2.1"
      - DEVICE="enp0s3"
      - ONBOOT="yes"
  - systemctl restart NetworkManager
    - ifconfig
  - nmtui

Using Nmcli Tool

- nmcli con mod enp0s3 ipv4.addresses 192.168.2.31/24
- nmcli con mod enp0s3 ipv4.gateway 192.168.2.1
- nmcli con mod enp0s3 ipv4.method manual
- nmcli con mod enp0s3 ipv4.dns "8.8.8.8"
- nmcli con up enp0s3
- cat /etc/sysconfig/network-scripts/ifcfg-enp0s3

ip command

- `ip address`
- `ip address show enp3s0`
- `ip -s link`
- `ip -s link show enp3s0`
- `ip a add 192.168.2.50/24 dev enp3s0`
- `ip a del 192.168.2.50/24 dev enp3s0`
- `ip link set enp3s0 up`
- `ip link set enp3s0 down`
- `ip neighbour`

IPv6 in Linux

- /etc/sysconfig/network-scripts/ifcfg-enps03
  - IPV6INIT=yes – This initializes the interface for IPv6 addressing.
  - IPV6_AUTOCONF=yes – This enables the IPv6 auto-configuration for the interface.
  - IPV6_DEFROUTE=yes – This indicates that the default IPv6 route has been assigned to the interface.
  - IPV6_FAILURE_FATAL=no – indicates that the system won’t fail even when IPv6 fails.

IPv6 with ip command

- ip -6 addr
- ip -6 address add 2F00:0C98:2060:A000:0001:0000:1d1e:ca75/64 dev eth0
- ip -6 route add default via 2F00:0C98:2060:A000:0000:0000:0000:0001 dev eth0
- ping6 -c1 2F00:0C98:2060:A000:0000:0000:0000:0001
- ping6 -c1 www.google.com

Questions?