OSI Model

- It divides the network communication process into smaller and simpler components, facilitating component development, design, and troubleshooting.
- It allows multiple-vendor development through the standardization of network components.
- It encourages industry standardization by clearly defining what functions occur at each layer of the model.
- It allows various types of network hardware and software to communicate.
- It prevents changes in one layer from affecting other layers to expedite development.

OSI Model


7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical

PHYSICAL

- The Physical Layer defines how to move **Bits** from one device to another. It details how cables, connectors and network interface cards are supposed to work and how to send and receive bits.

DATA

- The Data Link layer formats the message into a *data frame*, and adds a header containing the hardware destination and source address to it. This header is responsible for finding the next destination device on a local network.

DATA

- This layer is subdivide into 2 sub-layers: logical link control (LLC) and media access control (MAC).
- **Logical Link Control** – used for flow control and error detection.
  Media Access Control – used for hardware addressing and for controlling the access method.
- The MAC sublayer carries the physical address of each device on the network. This address is more commonly called a device's MAC address. MAC address is a 48 bits address which is burned into the NIC card on the device by its manufacturer.

NETWORK

- This layer provides logical addresses which routers will use to determine the path to forward the packets to the destination. In most cases, the logic addresses here means the IP addresses.

TRANSPORT

- This layer maintains flow control of data and provides for error checking and recovery of data between the devices.
- The most common example of Transport layer is Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

SESSION

- The *Session layer is responsible for setting up, managing, and dismantling sessions between* Presentation layer entities and keeping user data separate.

PRESENTATION

- This layer ensures the presentation of data, that the communications passing through are in the appropriate form for the recipient. In general, it acts as a translator of the network. For example, you want to send an email and the Presentation will format your data into email format. Or you want to send photos to your friend, the Presentation layer will format your data into GIF, JPG or PNG… format.

APPLICATION

- This is the closest layer to the end user. It provides the interface between the applications we use and the underlying layers. But notice that the programs you are using (like a web browser – IE, Firefox or Opera…) do not belong to Application layer. Telnet, FTP, email client (SMTP), HyperText Transfer Protocol (HTTP) are examples of Application layer.

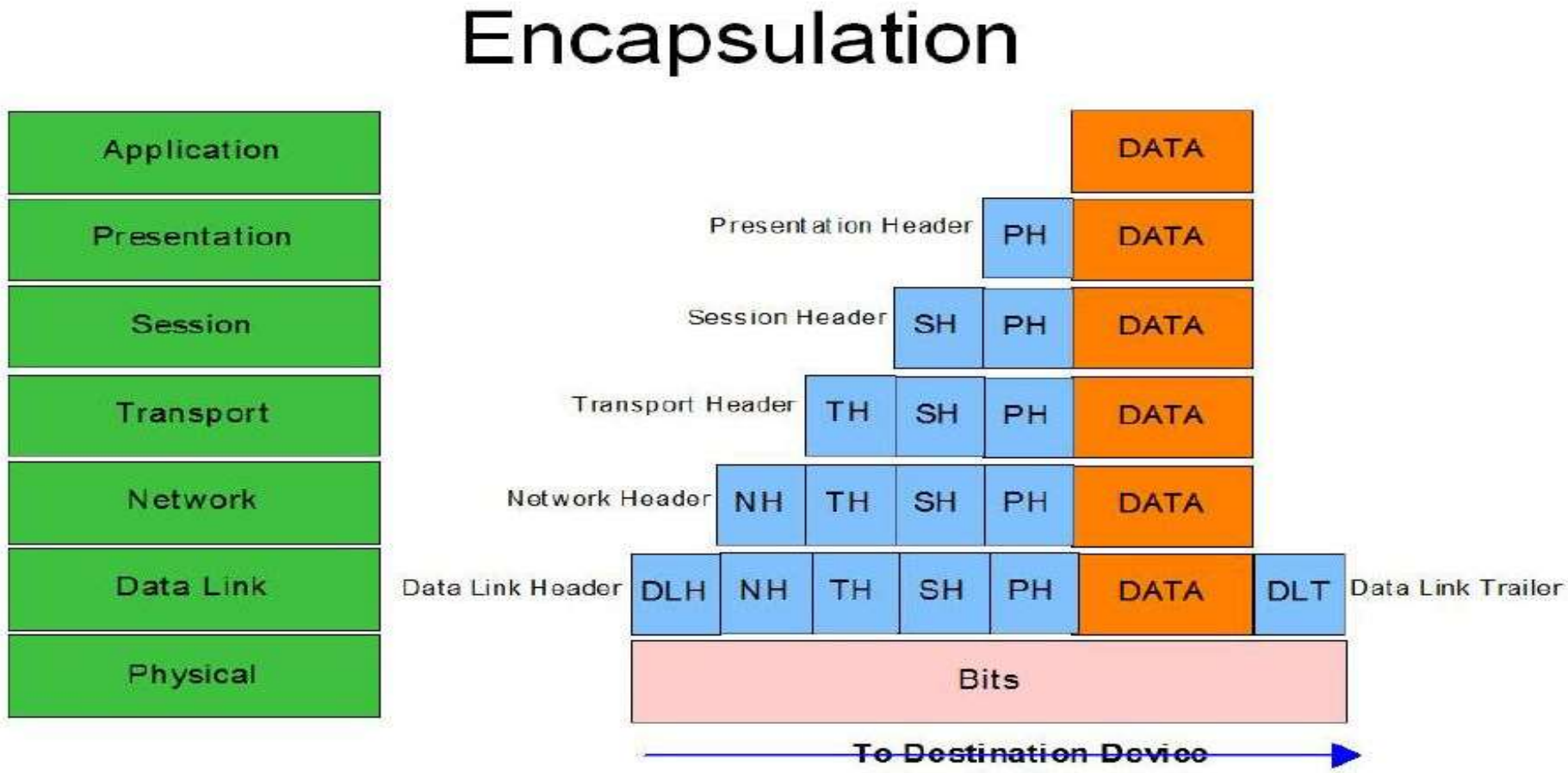
APPLICATION

- FTP (File Transfer Protocol)
- TFTP (Trivial File Transfer Protocol)
- HTTP / HTTPs (Hyper Text Transfer Protocol / Secure)
- DNS (Domain Name System)
- DHCP (Dynamic Host Confutation Protocol)
- SSH/Telnet (Secure Shell)
- ARP/RARP (Address Resolution Protocol/ Reverse)
- ICMP (Internet Control Message Protocol)
- POP (Post Office Protocol)
- SMTP (Simple Mail Transfer Protocol)

Comparison

Layer	Description	Popular Protocols	Protocol Data Unit	Devices operate in this layer
Application	+ User interface	HTTP, FTP, TFTP, Telnet, SNMP, DNS...	Data	
Presentation	+ Data representation, encryption & decryption	+ Video (WMV, AVI...) + Bitmap (JPG, BMP, PNG...) + Audio (WAV, MP3, WMA...)	Data	
Session	+ Set up, monitor & terminate the connection session	+ SQL, RPC, NETBIOS names...	Data	
Transport	+ Flow control (Buffering, Windowing, Congestion Avoidance) helps prevent the loss of segments on the network and the need for retransmission	+ TCP (Connection-Oriented, reliable) + UDP (Connectionless, unreliable)	Segment	
Network	+ Path determination + Source & Destination logical addresses	+ IP + IPX + AppleTalk	Packet/Datagram	Router
Data Link	+ Physical addresses Includes 2 layers: + Upper layer: Logical Link Control (LLC) + Lower layer: Media Access Control (MAC)	+ LAN + WAN (HDLC, PPP, Frame Relay...)	Frame	Switch, Bridge
Physical	Encodes and transmits data bits + Electric signals + Radio signals	+ FDDI, Ethernet	Bit (0, 1)	Hub, Repeater...

ENCAP


Encapsulation
Application
Presentation
Session
Transport
Network
Data Link
Physical
DATA
Presentation Header
PH
Session Header
SH
Transport Header
TH
Network Header
NH
Data Link Header
DLH
DLT
Data Link Trailer
Bits
To Destination Device

OSI vs TCP/IP

TCP/IP	OSI Model	Protocols
Application Layer	Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP, POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
	Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
	Session Layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
Transport Layer	Transport Layer	TCP, UDP
Internet Layer	Network Layer	ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP
Link Layer	Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
	Physical Layer	Bluetooth, Ethernet, DSL, ISDN, 802.11 Wi-Fi

TCP vs UDP

TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement

TCP 3 Way HS

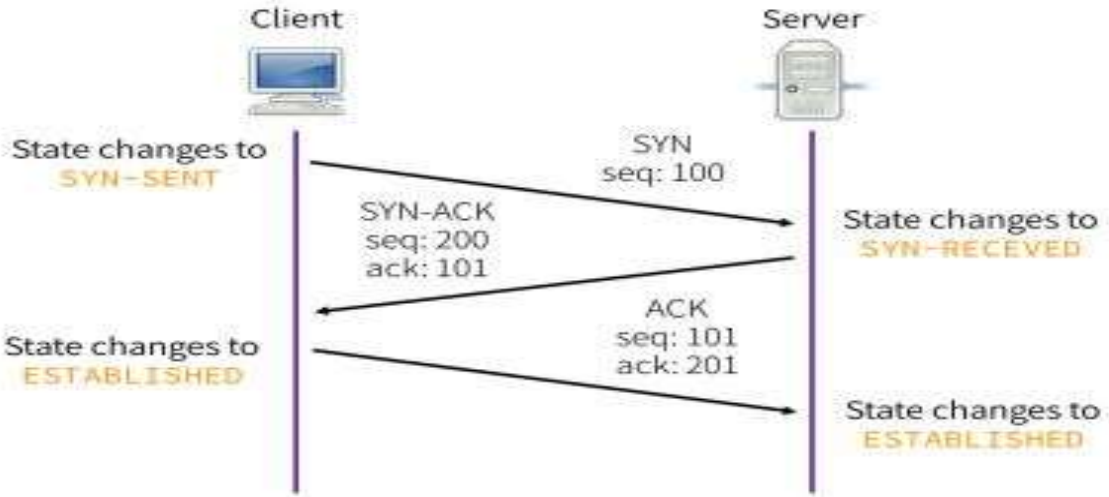
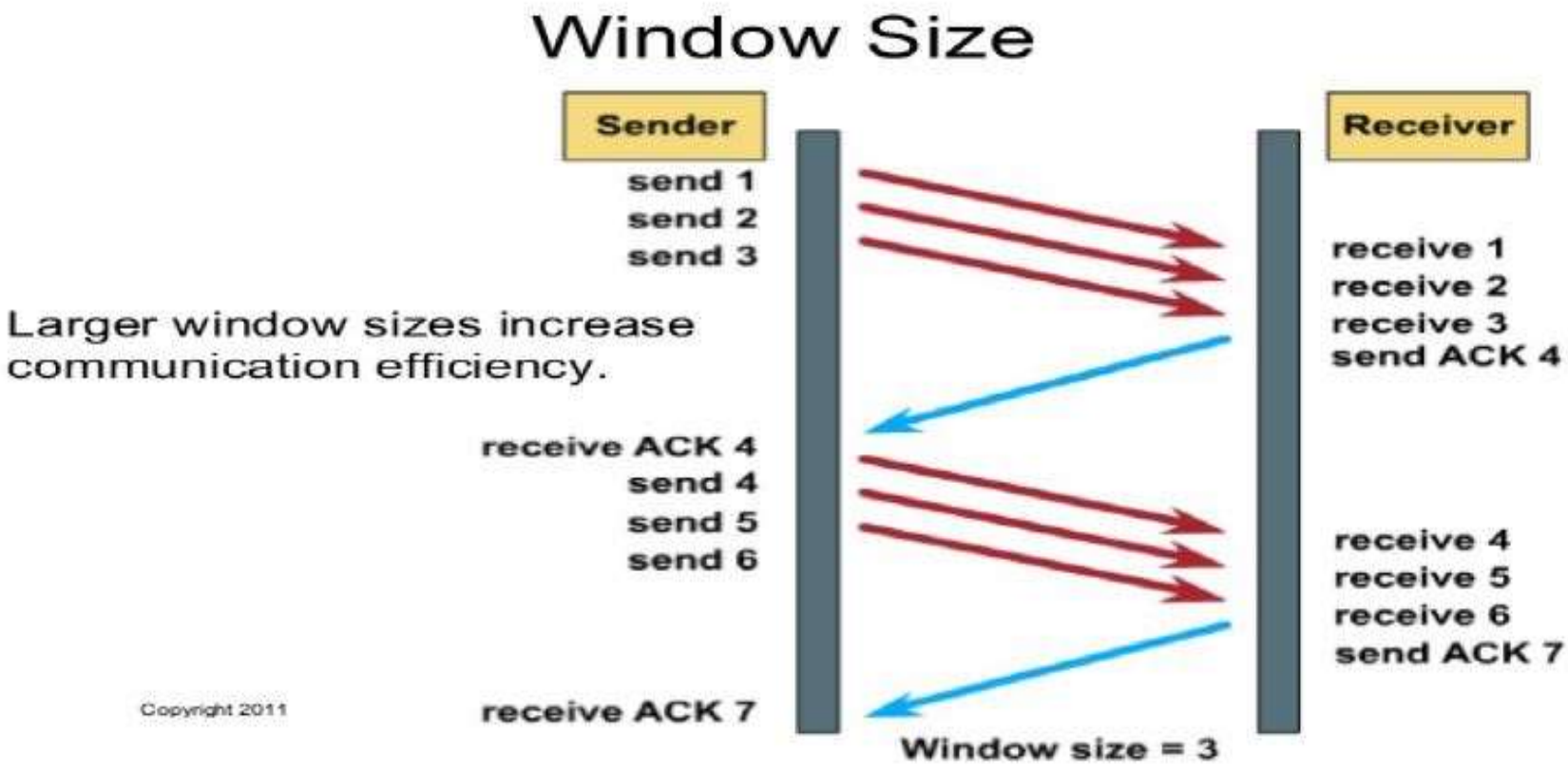


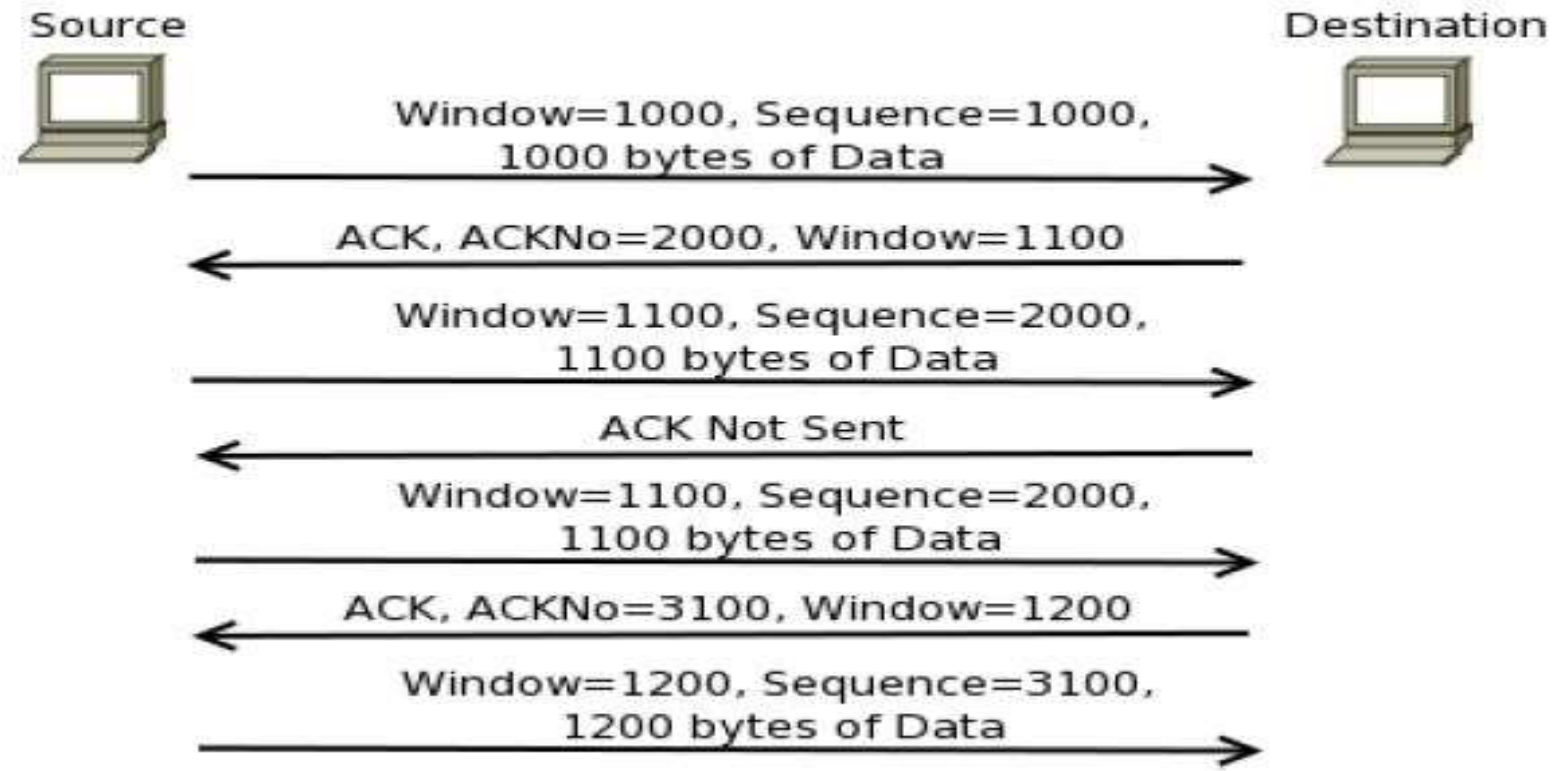
Figure 1. TCP three-way handshake diagram. TCP, Transmission Control Protocol; SYN, Synchronize; ACK, Acknowledgement.

1. The client sends a SYN (synchronize) packet to the server, which has a random sequence number.
2. The server sends back a SYN-ACK packet, containing a random sequence number and an ACK number acknowledging the client's sequence number.
3. The client sends an ACK number to the server, acknowledging the server's sequence number.
4. The sequence numbers on both ends are synchronized. Both ends can now send and receive data independently.

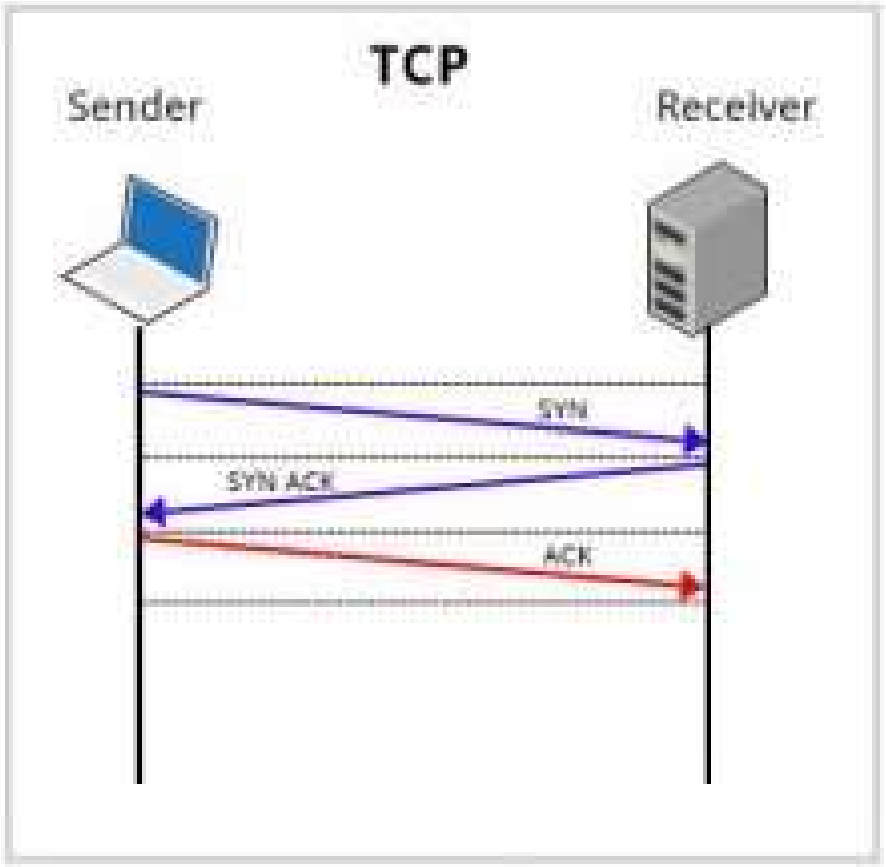
WIN SIZE

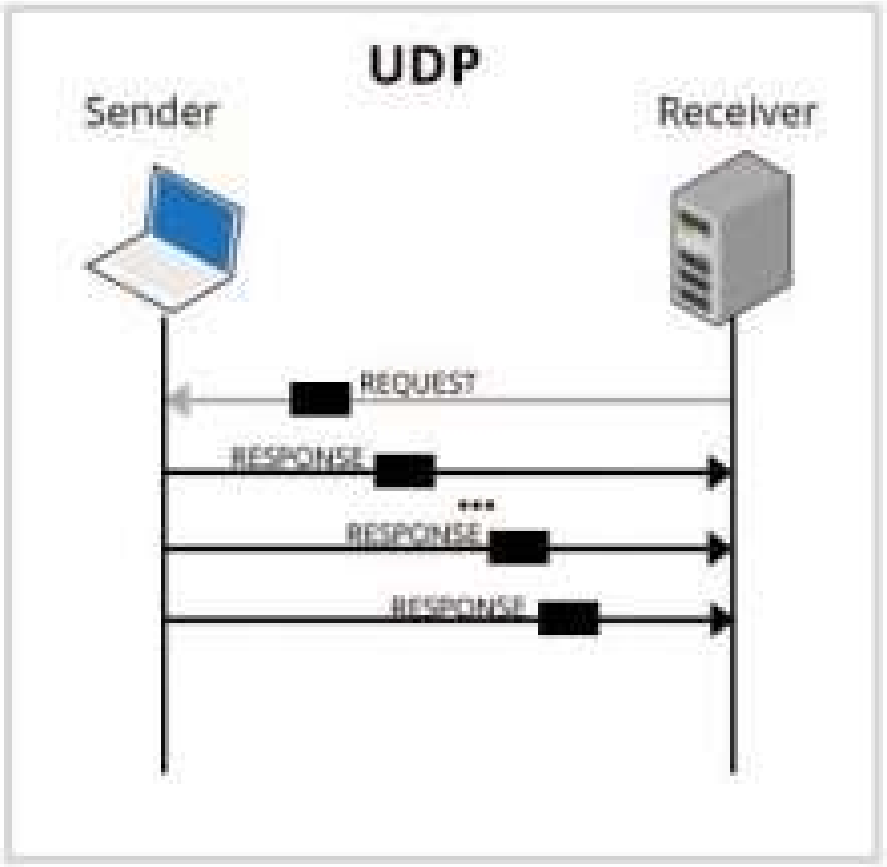

Window Size
Sender
Receiver
send 1
send 2
send 3
receive 1
receive 2
receive 3
send ACK 4
Larger window sizes increase communication efficiency.
receive ACK 4
send 4
send 5
send 6
receive 4
receive 5
receive 6
send ACK 7
Copyright 2011
receive ACK 7
Window size = 3

WIN SIZE


Source
Destination
Window=1000, Sequence=1000,
1000 bytes of Data
ACK, ACKNo=2000, Window=1100
Window=1100, Sequence=2000,
1100 bytes of Data
ACK Not Sent
Window=1100, Sequence=2000,
1100 bytes of Data
ACK, ACKNo=3100, Window=1200
Window=1200, Sequence=3100,
1200 bytes of Data

UDP Data Flow





Port No

S.L.	Application Layer Protocol	Transport Layer Protocol	Port Number
1	FTP	TCP	20, 21
2	TFTP	UDP	69
3	SSH	TCP	22
4	Telnet	TCP	23
5	SMTP	TCP	25
6	HTTP	TCP	80
7	HTTPS	TCP	443
8	DNS	TCP/UDP	53
9	DHCP Server	UDP	67
10	DHCP Client	UDP	68
11	LDAP	TCP	389
12	SMB	TCP	445
13	POP3	TCP	110

Cisco PoE Explained – What is Power over Ethernet?

All devices need electricity for them to operate. What if devices are installed farther from the power outlet like an access point that needs to be installed on an upper level to provide good quality Wi-Fi signal and coverage? One best solution is by using Power over Ethernet (PoE), typically on a networking device like a network switch.

Power over Ethernet (PoE) is a technology that transmits both electrical power and network data over an ethernet cable. With PoE, each Ethernet interface of LAN switches can supply power to devices like VoIP phones, IP cameras or security cameras, and wireless access points (AP).

How Does Power over Ethernet Work?

Some devices are not capable of being powered through Ethernet ports, which might destroy the device if being plugged into a PSE (PoE Switch). PSE must also ensure that the power level supplied to PD is enough and will not destroy it. To meet those requirements, PoE has an IEEE standardized mechanism called auto negotiation.

Auto negotiation initiates a handshake procedure that establishes how much power the PD or connected device requires. The handshake needs to be established while PD is off, as PD needs the power to boot and initialize. Using auto negotiation, PSE (PoE Switch) avoids powering up devices that are not capable of receiving power over ethernet ports. Thus, it avoids damaging the Ethernet port or the device itself.

PoE (Power over Ethernet) Standards

During autonegotiation, the PD is signalling the PSE of how much wattage of power it requires. The below standards are the power in watts that the PSE will supply to PD based on its requirement:

1. **PoE** –IEEE 802.3af standard that supplies up to 15 watts of DC power from PSE and 12.95 watts from PD due to losses on an ethernet cable. It uses two pairs of wires like CAT3 or CAT5 cables as a medium.

2. **PoE+** – IEEE 802.3at standard that supplies power up to 30 watts of DC power from PSE and 25.5 watts from PD due to losses on an ethernet cable. It is also using two pairs of wires like CAT5 or higher as a medium.

3. **UPoE (Universal PoE)** – IEEE 802.3bt standard that supplies power up to 60 watts of DC power from PSE and 51 watts from PD due to losses on an ethernet cable. It uses four pairs of wire as a medium.

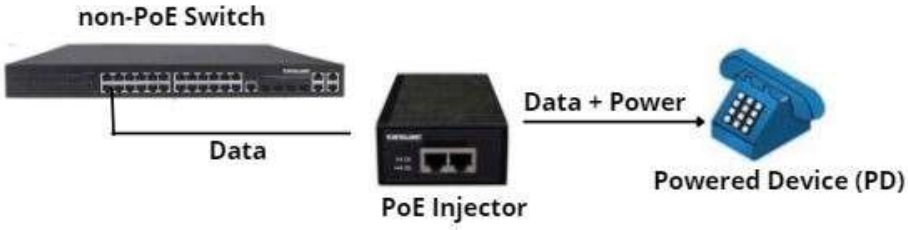
4. **UPoE+ (Universal PoE +)** – IEEE 802.3bt standard that supplies power up to 100 watts of DC power from PSE and 71.3 watts from PD due to losses on an ethernet cable. It is also using four pairs of ethernet cabling as a medium.

PoE Implementation

Implementing PoE on the LAN network connection requires an effort for planning and designing. Powered devices, power requirements, switch ports, switch power supplies, and PoE standards should be checked before implementing PoE on the LAN network. Below are the ways we can implement PoE on our network using network switches.

1. **Endspan** – is a PoE switch and sometimes called “endpoint”. The ethernet port of the switch can supply both power and data to devices that support PoE like PD.

2. **Midspan** – if there is an existing non-PoE switch on the network and needs to power up a device that requires PoE, then a PoE device needs to be put in between the non-PoE switch and a PD. The PoE device will connect to the non-PoE switch and will supply power to PD. A commonly known midspan is a PoE injector.

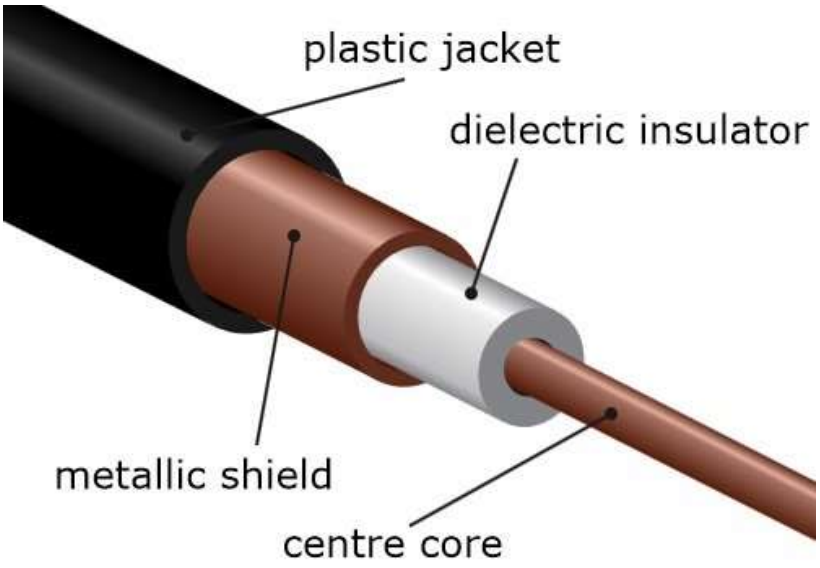


Types of Ethernet cabling

There are three cable types commonly used for Ethernet cabling: coaxial, twisted pair, and fiber-optic cabling. In today's LANs, the twisted pair cabling is the most popular type of cabling, but the fiber-optic cabling usage is increasing, especially in high performance networks. Coaxial cabling is generally used for cable Internet access. Let's expain all three cable types in more detail.

Coaxial cabling

A coaxial cable has an inner conductor that runs down the middle of the cable. The conductor is surrounded by a layer of insulation which is then surrounded by another conducting shield, which makes this type of cabling resistant to outside interference. This type of cabling comes in two types – thinnet and thicknet. Both types have maximum transmission speed of 10 Mbps. Coaxial cabling was previously used in computer networks, but today are largely replaced by twisted-pair cabling (Photo credit: Wikipedia)

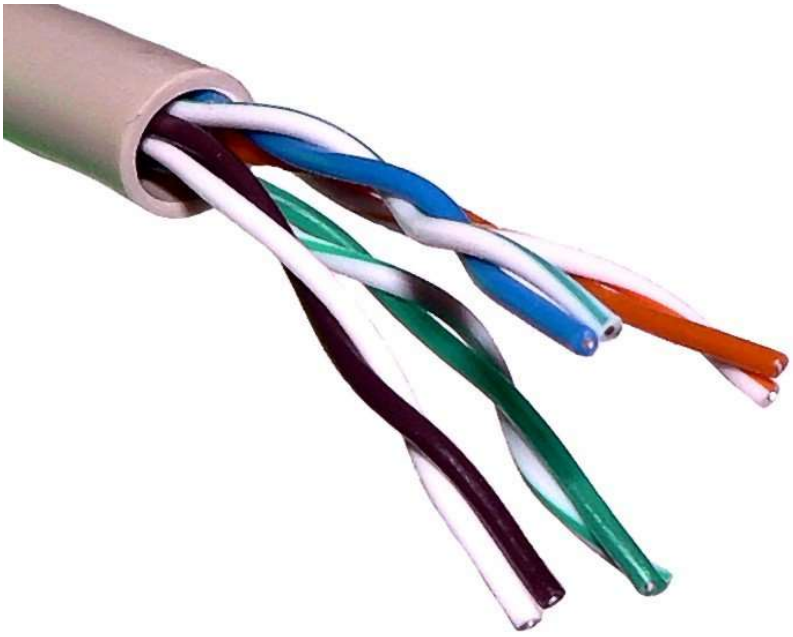


Twisted-pair cabling

A twisted-pair cable has four pair of wires. These wires are twisted around each other to reduce crosstalk and outside interference. This type of cabling is common in current LANs.

Twisted-pair cabling can be used for telephone and network cabling. It comes in two versions, **UTP (Unshielded Twisted-Pair)** and **STP (Shielded Twisted-Pair)**. The difference between these two is that an STP cable has an additional layer of insulation that protects data from outside interferences.

Here you can see how a twisted pair cable looks like (Photo credit: Wikipedia):



A twisted-pair cable uses 8P8C connector, sometimes wrongly referred to as RJ45 connector (Photo credit: Wikipedia).

Fiber-optic cabling

This type of cabling uses optical fibers to transmit data in the form of light signals. The cables have strands of glass surrounded by a cladding material (Photo credit: Wikipedia):

This type of cabling can support greater cable lengths than any other cabling type (up to a couple of miles). The cables are also immune to electromagnetic interference. As you can see, this cabling method has many advantages over other methods but its main drawback is that it is more expensive.

There are two types of fiber-optic cables:

- **Single-mode fiber (SMF)** – uses only a single ray of light to carry data. Used for larger distances.
- **Multi-mode fiber (MMF)** – uses multiple rays of light to carry data. Less expensive than SMF.

Four types of connectors are commonly used:

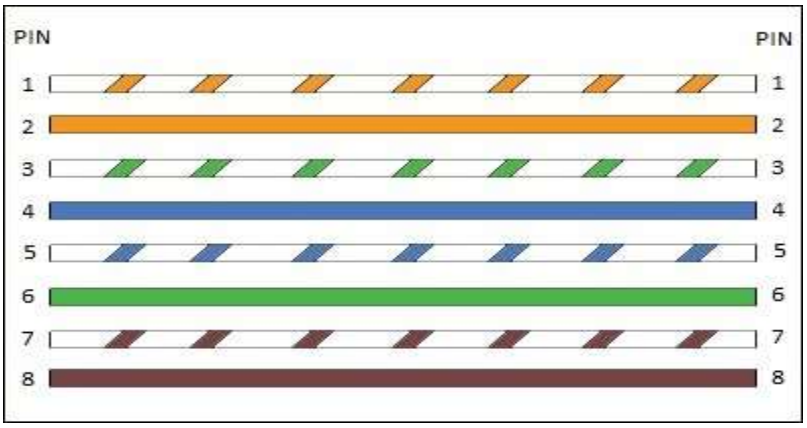
- ST (Straight-tip connector)
- SC (Subscriber connector)
- FC (Fiber Channel)
- LC (Lucent Connector)

Types of Ethernet cables – straight-through and crossover

Ethernet cables can come in two forms when it comes to wiring:

1. Straight-through cable

This cable type has identical wiring on both ends (pin 1 on one end of the cable is connected to pin 1 at the other end of the cable, pin 2 is connected to pin 2 etc.):



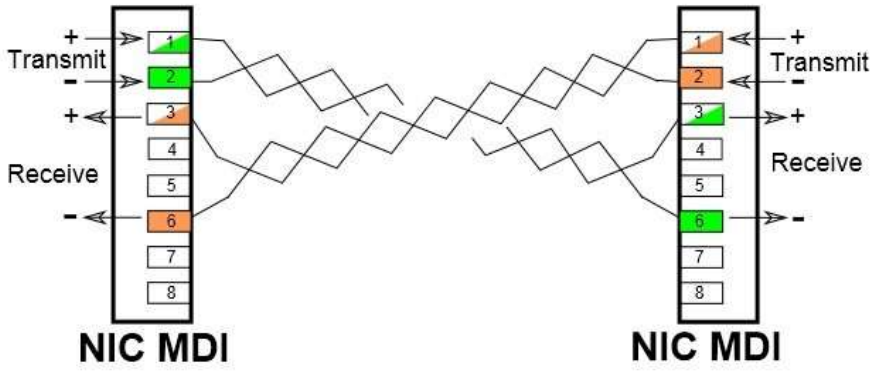
This type of cable is used to connect the following devices:

- computer to hub
- computer to switch
- router to hub
- router to switch

Computers and routers use wires 1 and 2 to transmit data and wires 3 and 6 to receive data. Hubs and switches use wires 1 and 2 to receive data and wires 3 and 6 to send data. That is why, if you want to connect two computers together, you will need a crossover cable.

2. Crossover cable

With the crossover cable, the wire pairs are swapped, which means that different pins are connected together – pin 1 on one end of the cable is connected to pin 3 on the other end, pin 2 on one end is connected to pin 6 on the other end (Photo credit: Wikipedia):



This type of cable is used when you need to connect two devices that use same wires to send and receive data. For example, consider connecting two computers together. If you use straight-through cable, with identical wiring in both ends, both computers will use wires 1 and 2 to send data. If computer A sends some packets to computer B, computer A will send that data using wires 1 and 2. That will cause a problem because computers expect packets to be received on wires 3 and 6, and your network will not work properly. This is why you need to use a crossover cable for such connections.

NETWORK

- Protocol suits
- Carries Information
- Using specific software and hardware

LAN

- Local Area Network links network devices in such a way that personal computer and workstations can share data, tools and programs. Data transmits at a very fast rate as the number of computers linked are limited. LAN's cover smaller geographical area and are privately owned. One can use it for an office building, home, hospital, schools, etc. LAN is easy to design and maintain.
- A Communication medium used for LAN has twisted pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.

MAN

- MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but resides in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). It's hard to design and maintain a Metropolitan Area Network.
- It is costly and may or may not be owned by a single organization. The data transfer rate of MAN is moderate.

WAN

- Wide Area Network is a computer network that extends over a large geographical area. A WAN could be a connection of LAN connecting to other LAN's via telephone lines and radio waves.
- Wide Area Network may or may not be privately owned. A Communication medium used for wide area network is PSTN or Satellite Link. Due to long distance transmission, the noise and error tend to be more in WAN. Propagation delay is one of the biggest problems faced here.

COMPAIRSON

BASIS OF COMPARISON	LAN	MAN	WAN
Expands to	Local Area Network	Metropolitan Area Network	Wide Area Network
Meaning	A network that connects a group of computers in a small geographical area.	It covers relatively large region such as cities, towns.	It spans large locality and connects countries together. Example Internet.
Ownership of Network	Private	Private or Public	Private or Public
Design and maintenance	Easy	Difficult	Difficult
Propagation Delay	Short	Moderate	Long
Speed	High	Moderate	Low
Fault Tolerance	More Tolerant	Less Tolerant	Less Tolerant
Congestion	Less	More	More
Used for	College, School, Hospital.	Small towns, City.	Country/Continent.

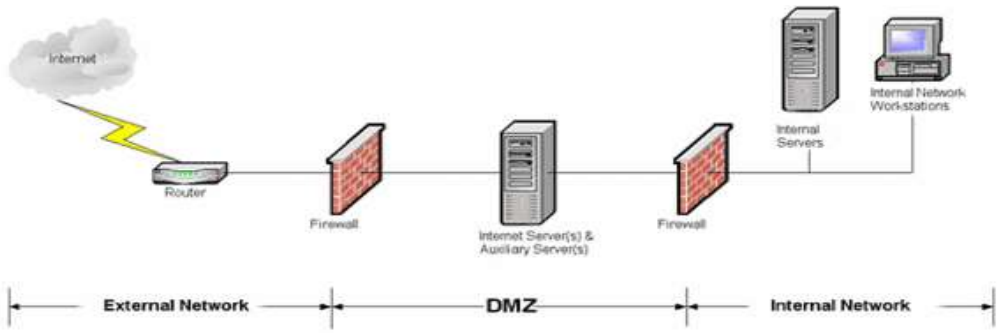
KEY Difference

Key Differences Between LAN, MAN and WAN

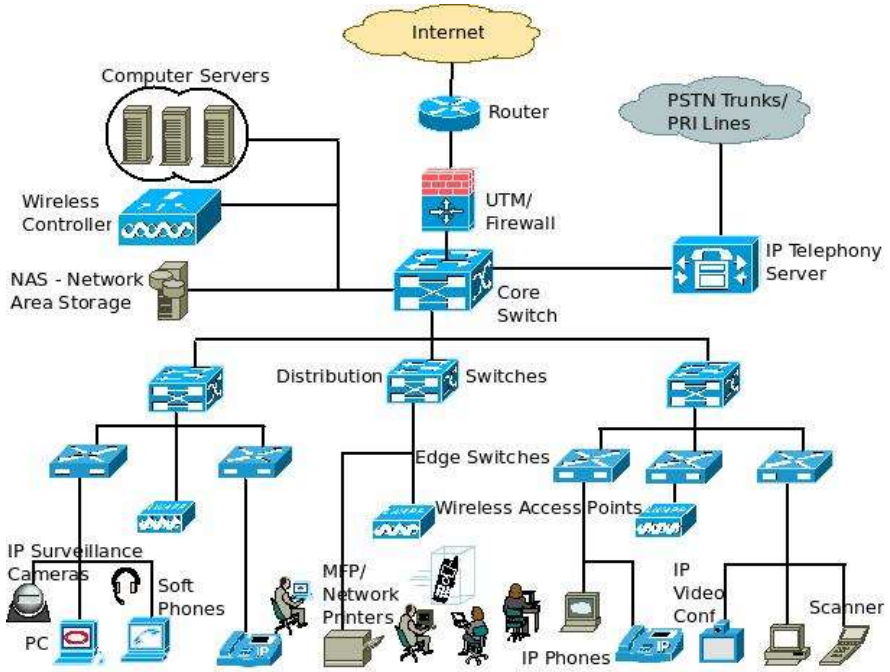
1. The geographical area covered by LAN is small, whereas, MAN covers relatively large and WAN covers the greatest of all.
2. LAN is confined to schools, hospitals or buildings, whereas, MAN connects small towns or Cities and on the other hand, WAN covers Country or a group of Countries.
3. Devices used for transmission of data are-
   LAN: WiFi, Ethernet Cables.
   MAN: Modem and Wire/Cable
   WAN: Optic wires, Microwaves, Satellites.
4. LAN's transmit data at a faster rate than MAN and WAN.
5. Maintenance of LAN is easier than that of MAN and WAN.
6. The bandwidth available for transmission is higher in LAN than MAN and WAN.
7. Data transmission errors and noise are least in LAN, moderate in MAN and high in WAN.

Network Topologies

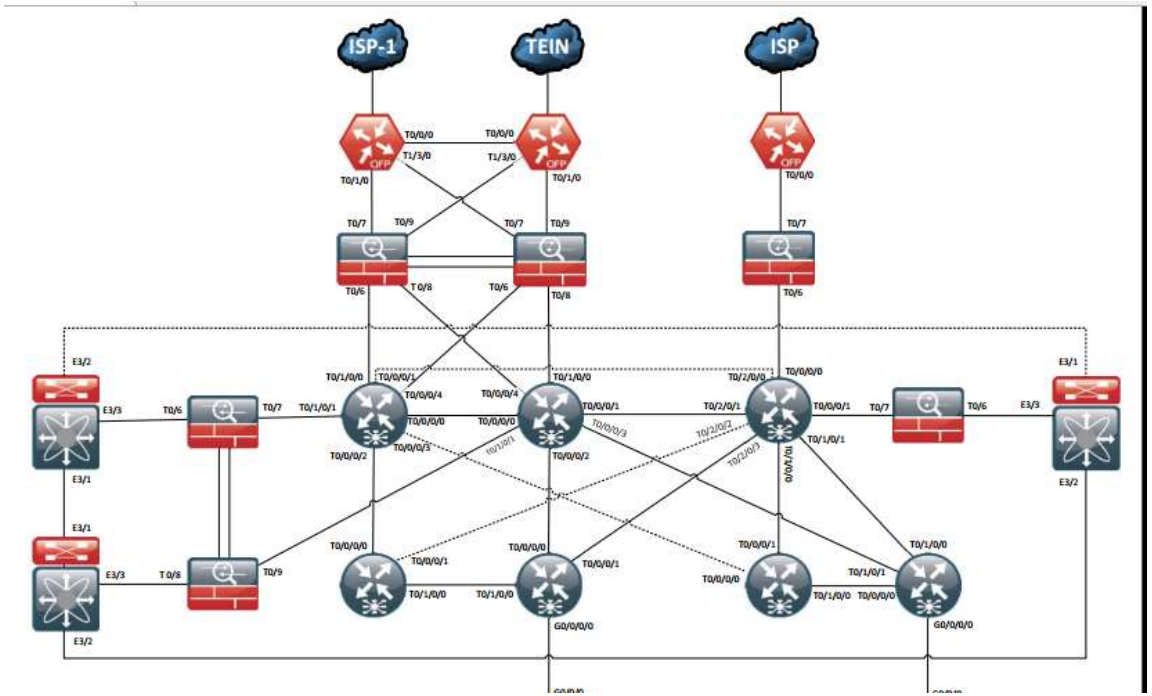
- Campus area Network
- Data Center
- Cloud, WAN
- SoHo
- Virtual environment



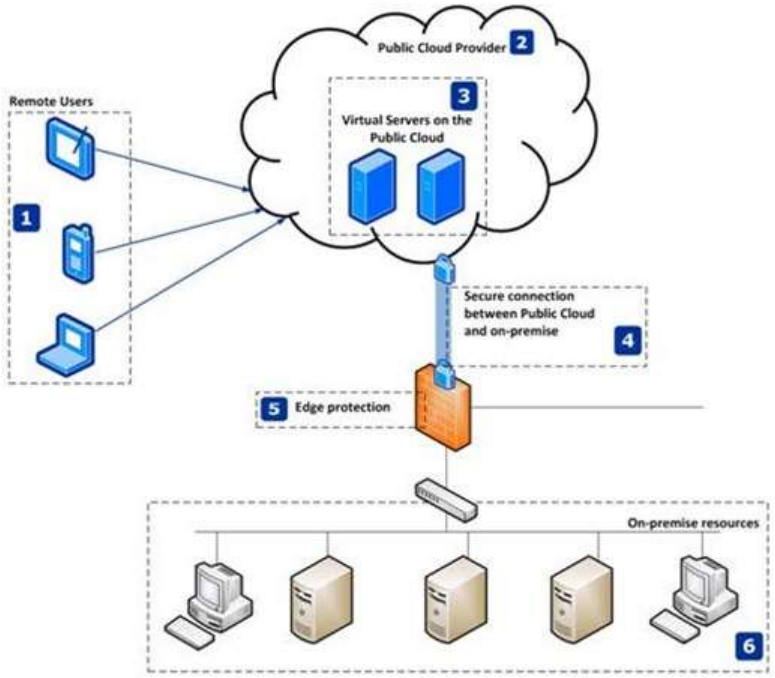
Campus area Network



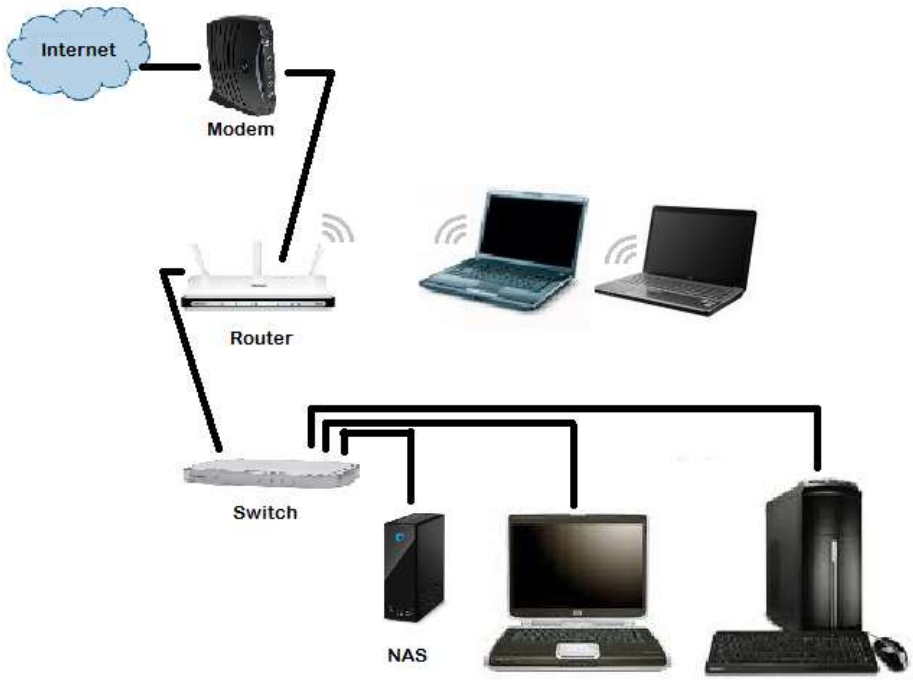
Data Center



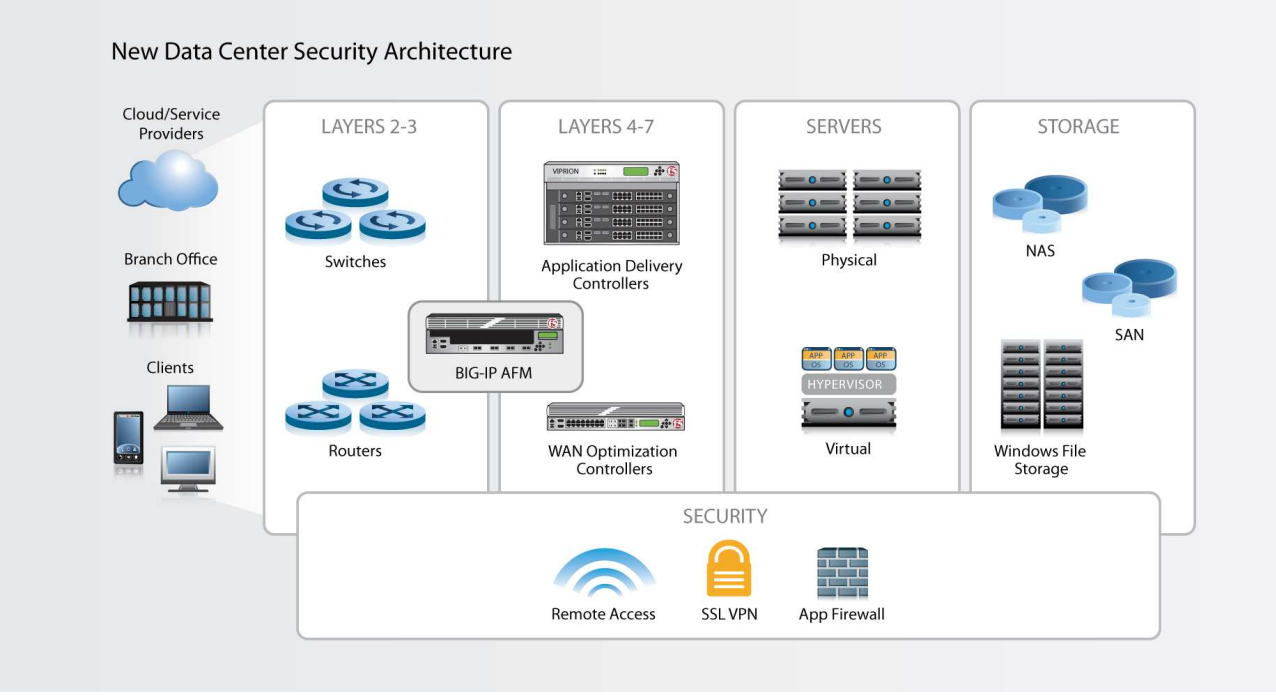
Cloud, WAN


Public Cloud Provider 2
3
Virtual Servers on the Public Cloud
Remote Users
1
Secure connection between Public Cloud and on-premise 4
5 Edge protection
On-premise resources
6

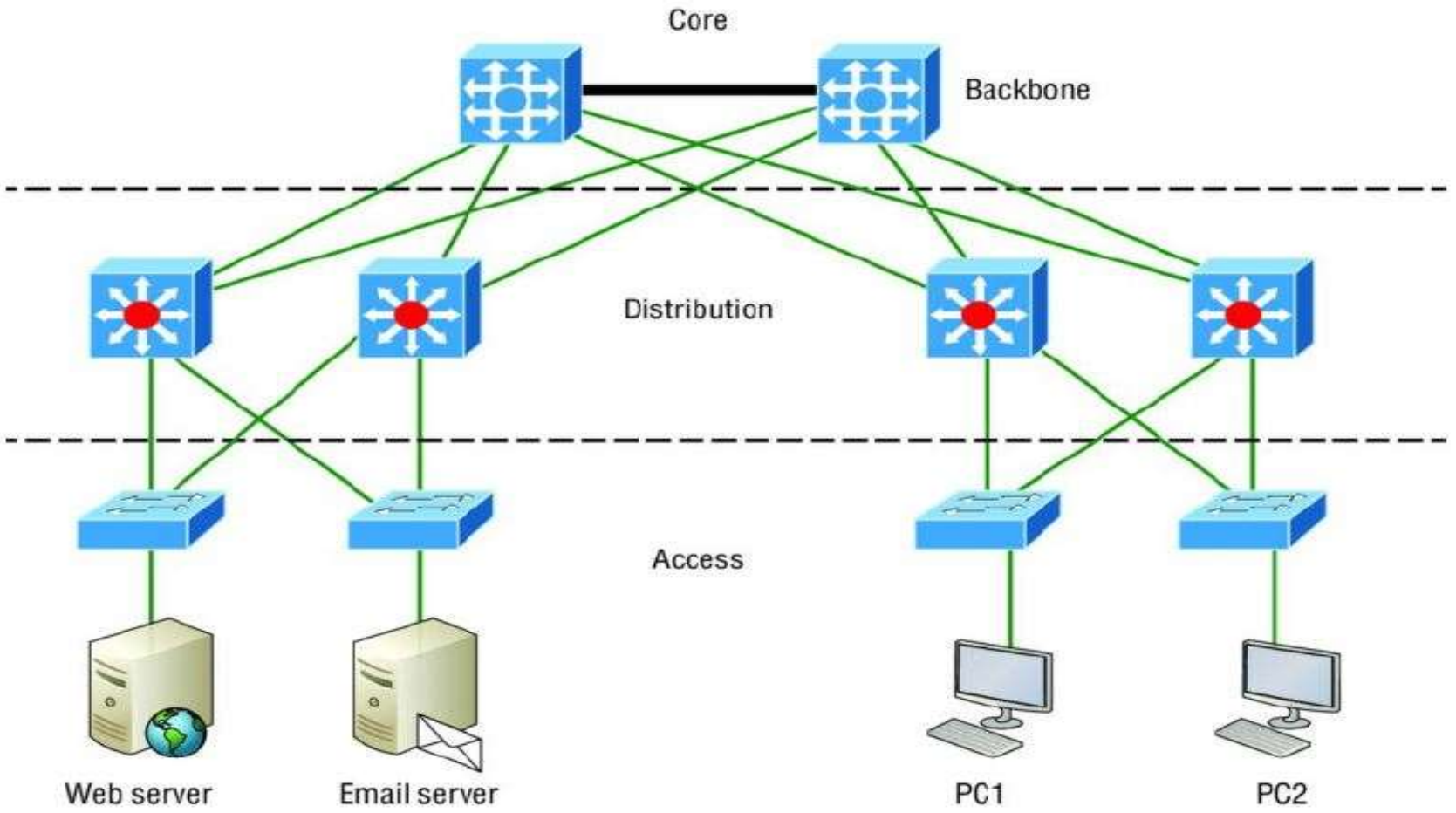
SOHO(Small Office Home Office)



Virtual environment



The Cisco Three-Layer Hierarchical Model



CORE

- Never do anything to slow down traffic. This includes making sure you don't use access lists, perform routing between virtual local area networks, or implement packet filtering.
- Don't support workgroup access here.
- Avoid expanding the core (e.g., adding routers when the internetwork grows). If performance becomes an issue in the core, give preference to upgrades over expansion.

Here's a list of things that we want to achieve as we design the core:

- Design the core for high reliability. Consider data-link technologies that facilitate both speed and redundancy, like Gigabit Ethernet with redundant links or even 10 Gigabit Ethernet.
- Design with speed in mind. The core should have very little latency.
- Select routing protocols with lower convergence times. Fast and redundant data-link connectivity is no help if your routing tables are shot!

DISTRIBUTION

- Routing
- Implementing tools (such as access lists), packet filtering, and queuing
- Implementing security and network policies, including address translation and firewalls
- Redistributing between routing protocols, including static routing
- Routing between VLANs and other workgroup support functions
- Defining broadcast and multicast domains

ACCESS

- Continued (from distribution layer) use of access control and policies
- Creation of separate collision domains (micro segmentation/switches)
- Workgroup connectivity into the distribution layer
- Device connectivity
- Resiliency and security services
- Advanced technology capabilities (voice/video, etc.)

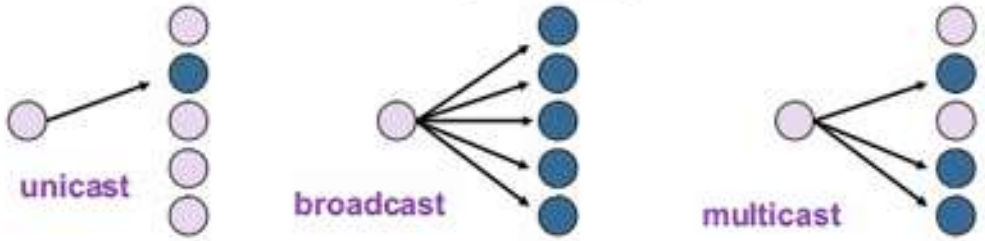
IP Service Type

- Unicast, Mulicast, Broadcast
- ARP
- Default Gateway

Unicast Multicast Broadcast

IP Service

- IP supports the following services:
  - one-to-one (unicast)
  - one-to-all (broadcast)
  - one-to-several (multicast)

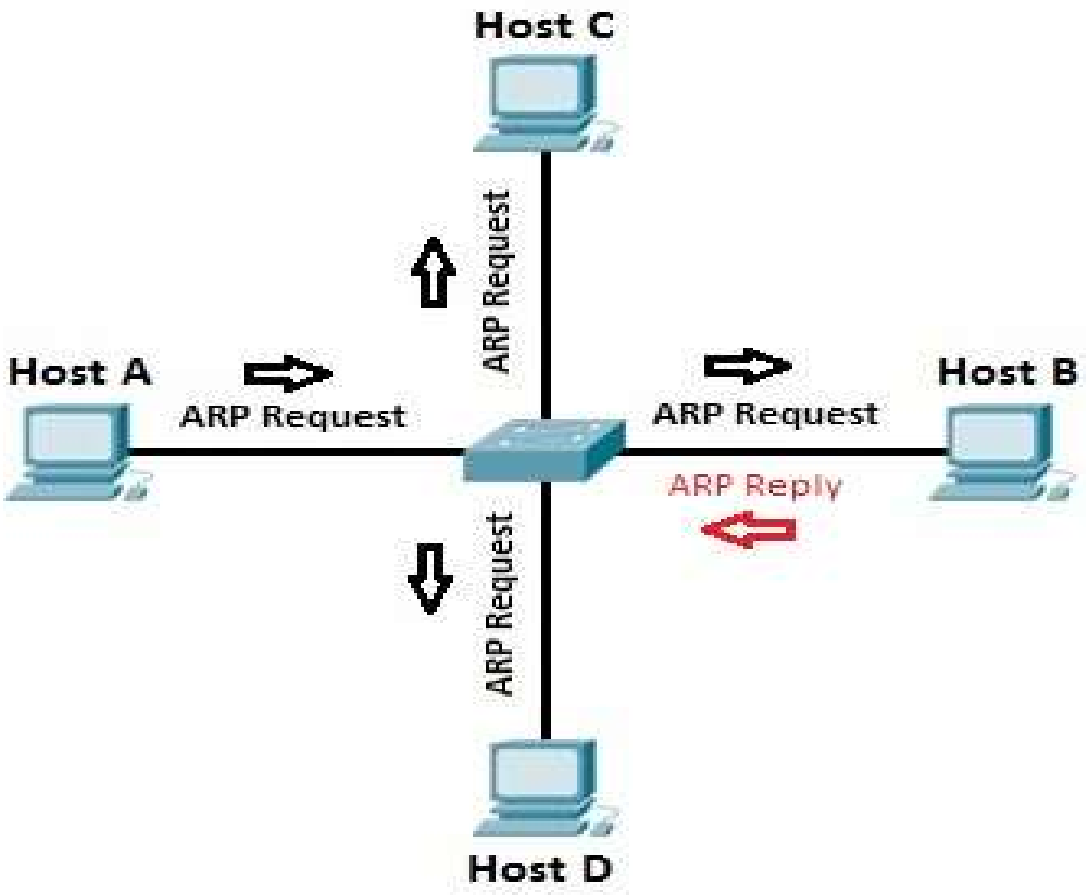


- IP multicast also supports a many-to-many service.
- IP multicast requires support of other protocols (IGMP, multicast routing)

ARP

- ARP (Address Resolution Protocol) is a network protocol used to find out the hardware (MAC) address of a device from an IP address.
- It is used when a device wants to communicate with some other device on a local network.

ARP


Host C
ARP Request
Host A
ARP Request
ARP Request
Host B
ARP Reply
ARP Request
Host D

Default Gateway

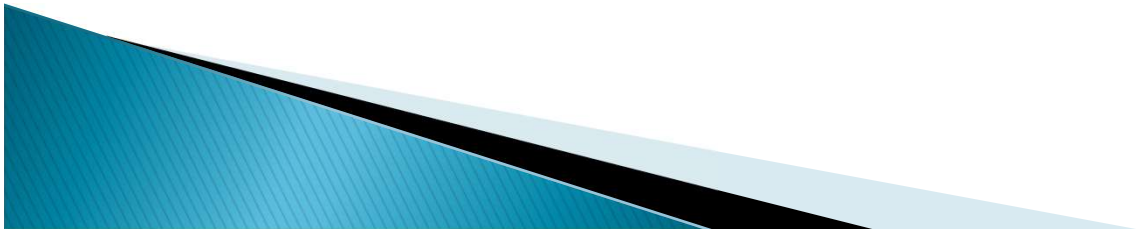
- A default gateway serves as an access point or IP router that a networked computer uses to send information to a computer in another network or the internet.
- Default simply means that this gateway is used by default, unless an application specifies another gateway.

Network Tool

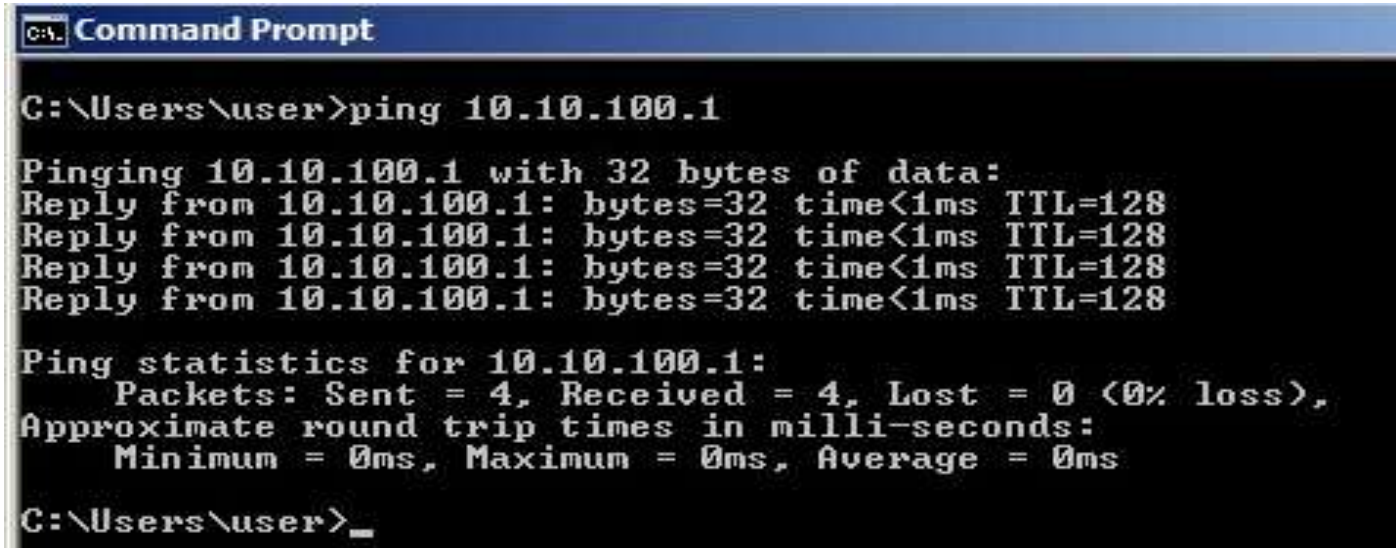
- Ping
- Traceroute

Ping

- ping is perhaps the most commonly used tool to troubleshoot a network.
- Ping (Packet Internet Groper) is included with most operating systems.
- It is invoked using a ping command and uses ICMP (Internet Control Message Protocol) to reports errors and provides information related to IP packet processing.



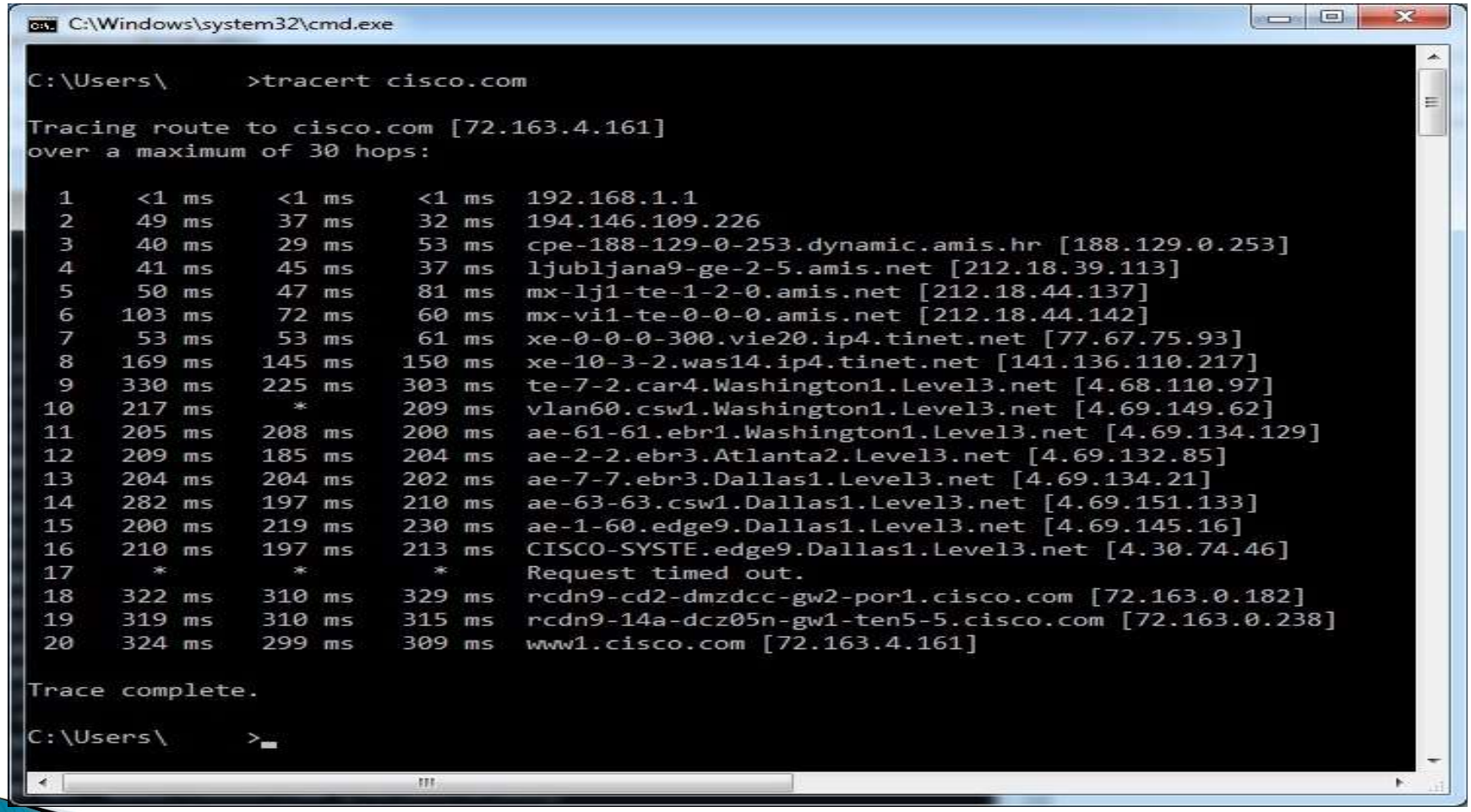
Ping


Command Prompt
C:\Users\user>ping 10.10.100.1
Pinging 10.10.100.1 with 32 bytes of data:
Reply from 10.10.100.1: bytes=32 time<1ms TTL=128
Reply from 10.10.100.1: bytes=32 time<1ms TTL=128
Reply from 10.10.100.1: bytes=32 time<1ms TTL=128
Reply from 10.10.100.1: bytes=32 time<1ms TTL=128
Ping statistics for 10.10.100.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\user>_

Traceroute

- **Traceroute** is a command-line interface based tool used to identify the path used by a packet to reach its target.
- This tool also uses ICMP messages, but unlike ping, it identifies every router in a path taken by the packets.
- Traceroute is useful when troubleshooting network problems because it can help identify where exactly the problem is. You can figure out which router in the path to an unreachable target should be examined more closely as the probable cause of the network's failure.

Traceroute


C:\Windows\system32\cmd.exe
C:\Users\ >tracert cisco.com
Tracing route to cisco.com [72.163.4.161]
over a maximum of 30 hops:
1 <1 ms <1 ms <1 ms 192.168.1.1
2 49 ms 37 ms 32 ms 194.146.109.226
3 40 ms 29 ms 53 ms cpe-188-129-0-253.dynamic.amis.hr [188.129.0.253]
4 41 ms 45 ms 37 ms ljubljana9-ge-2-5.amis.net [212.18.39.113]
5 50 ms 47 ms 81 ms mx-lj1-te-1-2-0.amis.net [212.18.44.137]
6 103 ms 72 ms 60 ms mx-vi1-te-0-0-0.amis.net [212.18.44.142]
7 53 ms 53 ms 61 ms xe-0-0-0-300.vie20.ip4.tinet.net [77.67.75.93]
8 169 ms 145 ms 150 ms xe-10-3-2.was14.ip4.tinet.net [141.136.110.217]
9 330 ms 225 ms 303 ms te-7-2.car4.Washington1.Level3.net [4.68.110.97]
10 217 ms * 209 ms vlan60.csw1.Washington1.Level3.net [4.69.149.62]
11 205 ms 208 ms 200 ms ae-61-61.ebr1.Washington1.Level3.net [4.69.134.129]
12 209 ms 185 ms 204 ms ae-2-2.ebr3.Atlanta2.Level3.net [4.69.132.85]
13 204 ms 204 ms 202 ms ae-7-7.ebr3.Dallas1.Level3.net [4.69.134.21]
14 282 ms 197 ms 210 ms ae-63-63.csw1.Dallas1.Level3.net [4.69.151.133]
15 200 ms 219 ms 230 ms ae-1-60.edge9.Dallas1.Level3.net [4.69.145.16]
16 210 ms 197 ms 213 ms CISCO-SYSTE.edge9.Dallas1.Level3.net [4.30.74.46]
17 * * * Request timed out.
18 322 ms 310 ms 329 ms rcdn9-cd2-dmzdcc-gw2-por1.cisco.com [72.163.0.182]
19 319 ms 310 ms 315 ms rcdn9-14a-dcz05n-gw1-ten5-5.cisco.com [72.163.0.238]
20 324 ms 299 ms 309 ms www1.cisco.com [72.163.4.161]
Trace complete.
C:\Users\ >

IPv4 Address

- IP address is the way to present a host in a network.
- IPv4 address is a 32bit.
- Example Address 192.168.0.0/24
  - 4 Octet Number in a format.
- Total 5 Classful Address in IPv4
  - Class A (0-127.255.255.255)
  - Class B-(128-191.255.255.255)
  - Class C-(192-223.255.255.255)
  - Class D-(224-239.255.255.255)
  - Class E-(240-255.255.255.255)

IPv4 Address

- Class A have 8bits network and 24bits host.
- Class B have 16bits network and 16bits host.
- Class C have 24bits Network and 8bits host.
- Class D used for Multicast Address.
- Class E used for Future use.
- 127.0.0.0/8 used for loopback address.
- 169.254.0.0/16 used for link local address.

SubnetMask

Class	Format	Default Subnet Mask
A	network.host.host.host	255.0.0.0
B	network.network.host.host	255.255.0.0
C	network.network.network.host	255.255.255.0

CIDR(Classless inter-domain routing)

- **CIDR (Classless inter-domain routing)** is a method of public IP address assignment. It was introduced in 1993 by Internet Engineering Task Force with the following goals:
  - to deal with the IPv4 address exhaustion problem
  - to slow down the growth of routing tables on Internet routers
- Before CIDR, public IP addresses were assigned based on the class boundaries:
  - **Class A** – the classful subnet mask is /8. The number of possible IP addresses is 16,777,216 (2 to the power of 24).
  - **Class B** – the classful subnet mask is /16. The number of addresses is 65,536
  - **Class C** – the classful subnet mask is /24. Only 256 addresses available.

CIDR(Classless inter-domain routing)

- Before CIDR, a company get classfull IP Address like as /8,/16,/24
- But they didn't need all those IP's
- To mitigate above issue classless IP is assigned.
- For example, if a company needs 12 public IP addresses, it would get something like this: **190.5.4.16/28**.

Dotted Decimal Value	CIDR notation
255.0.0.0	/8
255.128.0.0	/9
255.192.0.0	/10
255.224.0.0	/11
255.240.0.0	/12
255.248.0.0	/13
255.252.0.0	/14
255.254.0.0	/15
255.255.0.0	/16
255.255.128.0	/17
255.255.192.0	/18
255.255.224.0	/19
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

Subnetting

- Subnetting is a practice of dividing the network into two or more smaller networks.
- CIDR(Classless Inter domain Routing)
- Example: 192.168.39.72/26
  - Network ID
  - Subnet Mask
  - First Usable IP
  - Last Usable IP
  - Broadcast IP

IPv4 Address Type

- **Unicast**
  - Send to One.
- Broadcast
  - Send to Many.
- Multicast
  - Send to Group.

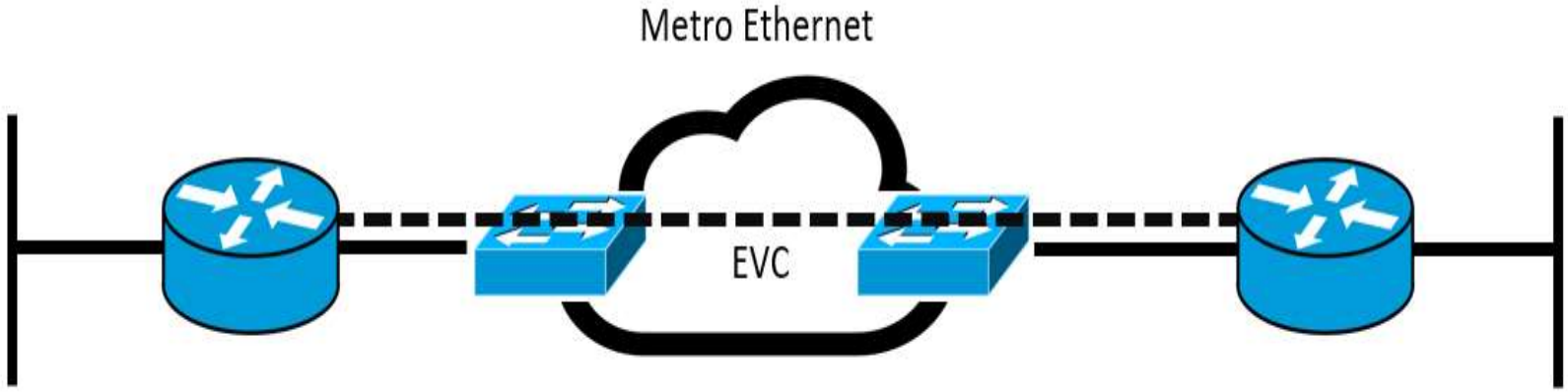
Private and Public IPv4 Address

- Public IP address
  - Routable in Internet
- Private IP Address
  - Not Routable in Internet
- Private IP Address Range
  - 10.0.0.0-10.255.255.255
  - 172.16.0.0-172.31.255.255
  - 192.168.0.0-192.168.255.255
- Except Private IP Address all are Public IP.

Network Topology

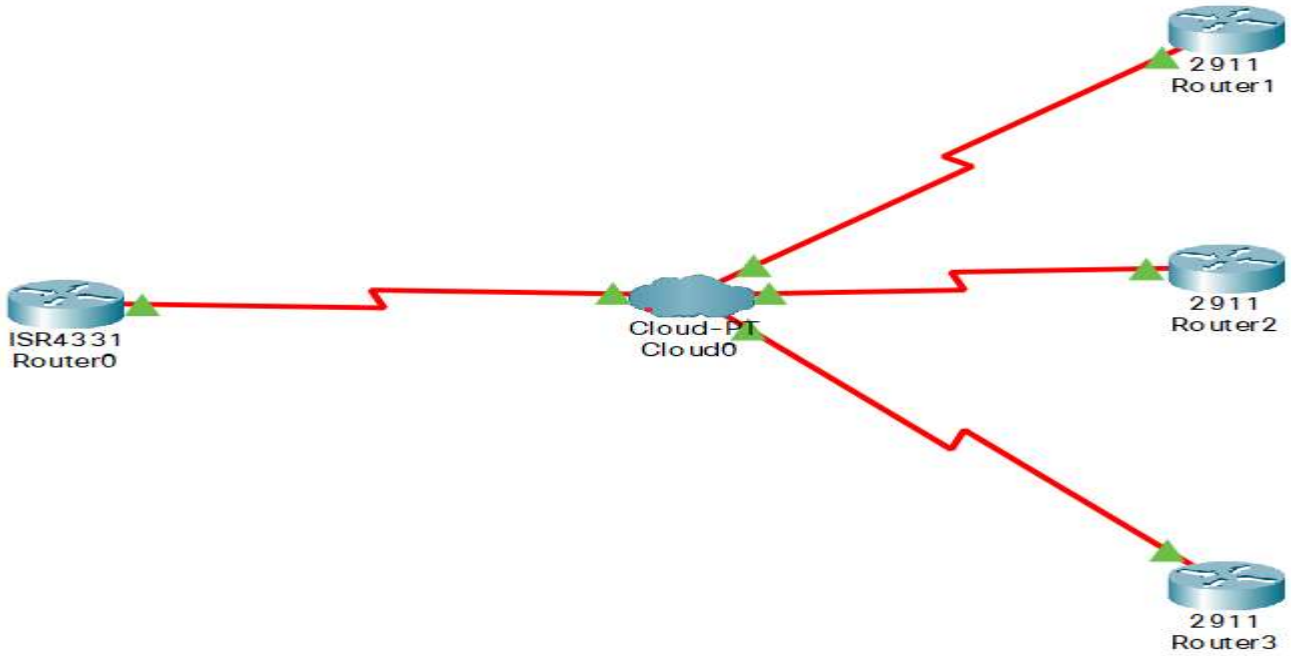
- Point to Point
- Point to Multipoint
  - STAR
  - MESH
  - HYBRIDE

Point to Point



The customer basically requires basic point-to-point network connectivity between two sites separated geographically that will allow them to send and receive Ethernet frames to each other as if they are connected directly.

Point to MultiPoint

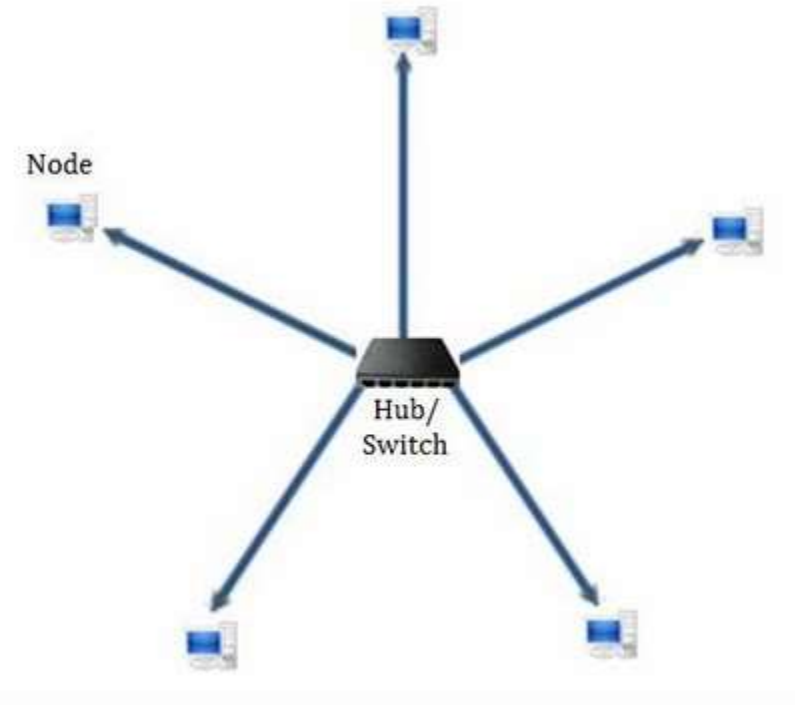


This WAN topology requires a central site device that directly sends Layer 2 frames to reach remote sites, but the remote sites can only send frames to the central site

STAR

- Have connections to networked devices that “radiate” out form a common point
- Each networked device in star topology can access the media independently
- Have become the dominant topology
- Stars have made buses and rings obsolete

Diagram



Advantage of STAR

1) Compared to Bus topology it gives far much better performance
2) Easy to connect new nodes or devices
3) Centralized management. It helps in monitoring the network
4) Failure of one node or link doesn't affect the rest of network

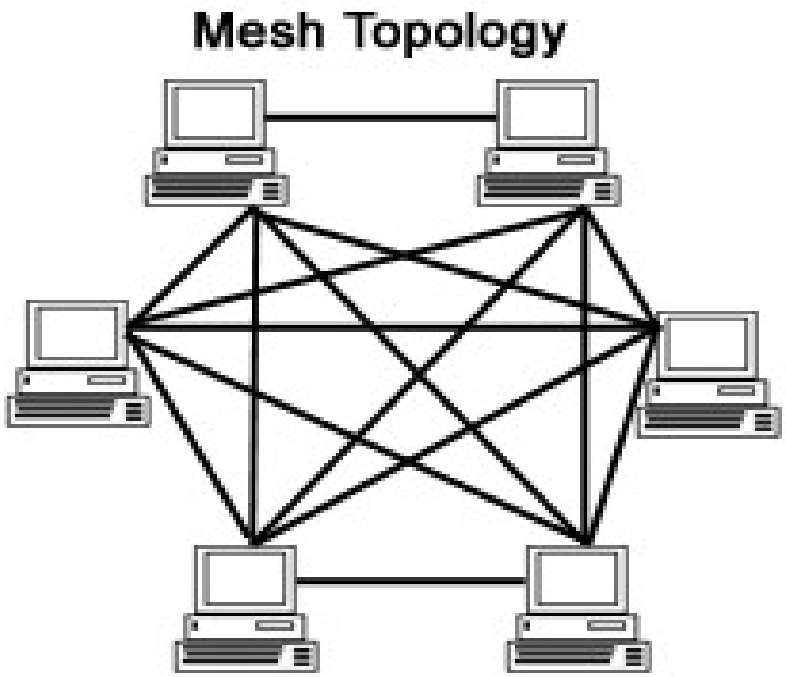
Disadvantage of STAR

1) If central device fails whole network goes down
2) The use of hub, a router or a switch as central device increases the overall cost of the network
3) Performance and as well number of nodes which can be added in such topology is depended on capacity of central device

MESH

- This topology features the ultimate reliability and fault tolerance
- Every networked node is directly connected to every other networked node
- Redundant routes to each location are plentiful, hence static routing impractical.
- Use dynamic routing protocols
- One application would be to provide interconnectivity for a limited number of routers that require high network availability

MESH Topology



ADVANTAGE & DISADVANTAGE

- Advantages:
  - Minimizes the number of hops between any two network-connected machines
  - Can be built with virtually any transmission technology
- Disadvantages:
  - These WANs can be fairly expensive to build
  - A finite (although substantial) limit on the scalability of the network

Hybrid Topology

- Hybrid topologies are mixture of both topologies.
- The reason of making hybrid topology is to eliminate the shortcoming of the network.

WAN Connection Types

- There are many WAN connections that we use to provide our connectivity to the internet. Below are the common options for WAN connectivity from the internet provider.
- **Leased Line**

This WAN connection type is a dedicated point-to-point link and fixed-bandwidth data connection. By using leased lined, your network will have a completely secured and reliable connection, high bandwidth, and superior quality of service. On the other side, leased lines can be expensive and not scalable as it is a permanent physical connection.

- **Digital Subscriber Line**

DSL is a medium used to transfer digital signals over the standard telephone lines. It uses a different frequency than the telephone is using so that you can use the internet while making a call. DSL is an older concept that provides a typical speed of around 6mbps. The good thing in DSL is the bandwidth is not shared and provides a constant speed.

WAN Connection Types

- **Cable Internet**

One way to provide broadband internet connection is by using cable internet from a local cable TV provider. It has quite a similarity with DSL as it also uses an existing cable modem from cable TV to send data. On this connection, the speed varies with the number of users on the service at a specific time.

- **Fiber Internet Access**

It is the newest broadband connection that provides the highest internet speed service to the customers. It is also commonly used in telecommunication backhaul connections because of the higher speed it can handle as compared to other cables. DWDM, SONET, and SDH are the ISP backhaul transport equipment that uses fiber optic cable. Fiber optic is also used in telecom packet switching networks or circuit switching networks.

WAN Connection Types

- **Multi-Protocol Label Switching (MPLS)**

MPLS is a type of VPN that uses labels on forwarding packets instead of IP addresses or layer 3 headers. It offers optimum security and routing for customer's sites. On MPLS, the service provider is participating in the customer's routing.

- **Wireless WAN**

Most of us are using mobile phones that use mobile data to connect to the internet. The commonly known connection types for wireless WAN are 3G, 4G, LTE, and 5G. It is the services offered by local ISP to provide wireless internet access to mobile devices via cellular sites. It uses specific frequencies to provide wider coverage and stronger signal to customers.

Understanding Variable Length Subnet Masks (VLSM)

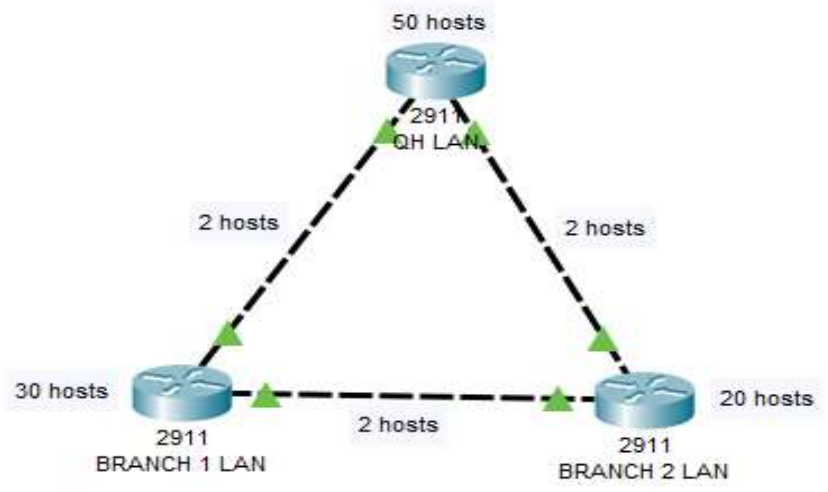
We have a limited number of private IPv4 addresses that can be used in every organization. As the Internet and most organizations are aggressively growing, we need a way to eliminate wasting IPv4 addresses. One of the ways that we can maximize the use of private IPv4 addresses in the organization is through subnetting.

The reason why we need subnetting is to efficiently distribute an IPv4 address with the least wastage and to create more networks with the smaller broadcast domains. To efficiently use subnetting, we can use Variable-Length Subnet Mask (VLSM).

With Variable-Length Subnet Mask (VLSM), we can allot the closest required number of IP addresses into a subnetwork in our LAN. We don't need to use a /23 subnet mask in all of our subnets, for example.

Steps to Implement Variable-Length Subnet Mask (VLSM)

We will use the below network topology as we go through the steps of the Variable-Length Subnet Masking (VLSM).



Step 1. Identify the host requirement. How many hosts or IP addresses are needed by the subnets in our LAN? We can arrange them from the highest host requirement to the lowest, as we will perform VLSM subnetting starting from the subnet with the highest host requirement. Don't forget to include the point-to-point (WAN) links as well.

- HQ LAN – 50 hosts
- BRANCH 1 – 30 hosts
- BRANCH 2 – 20 hosts
- WAN 1 (HQ to BRANCH 1) – 2 hosts
- WAN 2 (HQ to BRANCH 2) – 2 hosts
- WAN 3 (BRANCH 1 to BRANCH 2) – 2 hosts

The total host requirement for our network is 106 hosts, and we will perform VLSM subnetting on the HQ LAN subnetwork first.

Step 2. Determine the class of IP subnet. We need to determine the class of IP subnet that we will use based on the required number of hosts.

Class A has 16,777,216, Class B has 65,536, and Class C has 256 IP addresses. As per our network requirement, we need only 106 hosts, therefore we will use a Class C IP address space. In our example, we will use 192.168.10.0. It could also be that the organization bought an IP address space from the IP address authorities.

Step 3. Identify the host bits for every subnet. In our network topology example, HQ LAN has 50 hosts requirement, therefore we would have 6 host bits.

2^6 host bits will give us 64 hosts, minus 2 for the network address and broadcast address, which is equal to 62 usable host addresses. It suffices our 50 hosts requirement for HQ LAN.

Step 4. Calculate the subnet mask. Identify the network bits and determine the subnet mask of the subnet. We can get the subnet mask by subtracting the host bits from 32 (the total IPv4 address bits). For HQ LAN, it's 32 – 6 host bits, which is equal to a /26. The subnet mask for HQ LAN is /26 and its long format is 255.255.255.192

Step 5. Get the increment. To determine in which block of number should we go up, we can use the formula of **2^host bits**. For HQ LAN, it is 2^6 host bits, which will give us an increment of 64.

Step 6. Determine the network address, broadcast address, and IP address range. Starting from the base IP address, we will go up or increment in the value computed in Step 5.

For our network, we have a base IP address of 192.168.10.0. For HQ LAN, we will increment in a block of 64 as calculated in Step 5. Moreover, since it is in the Class C IP address space, as identified in Step 2, we will increment in the 4th octet.

That will be:

192.168.10.0 +64 (Current subnet)

192.168.10.64 (Base IP address for the next subnet)

We determined that the network address for HQ LAN subnet is 192.168.10.0. The broadcast address will be 1 less than the next IP subnet. That's 192.168.10.64 – 1, which is 192.168.10.63.

Finally, to get the HQ LAN usable IP address range, it is the IP address range in between the network address and the broadcast address, 192.168.10.1 to 192.168.10.62.

Completing the Variable-Length Subnet Mask Subnetting Process

Now, we are done with subnetting the HQ LAN. To fully implement VLSM, we need to do subnetting as well on the remaining LAN and WAN networks, which are BRANCH 1 LAN, BRANCH 2 LAN, WAN 1, WAN 2, and WAN 3.

The next subnet to be subnetted in VLSM will be the BRANCH 1 LAN as it has the next highest number of hosts. We will start with 192.168.10.64 as our network address as it is where we ended with our first IP subnet, HQ LAN.

Follow the steps we did on HQ LAN to perform VLSM subnetting on the remaining LAN and WAN subnets in our network diagram.

Below are the host bits, subnet mask, increment, network address, broadcast address, and usable IP address ranges of each subnet of the network topology we used in our example:

HQ LAN:

Number of Hosts – 50

Host Bits – 6 bits

Subnet Mask – /26 or 255.255.255.192

Increment – 64

Network Address – 192.168.10.0

Broadcast Address – 192.168.10.63

Usable IP Addresses – 192.168.10.1 to 192.168.10.62

BRANCH 1 LAN:

Number of Hosts – 30

Host Bits – 5 bits

Subnet Mask – /27 or 255.255.255.224

Increment – 32

Network Address – 192.168.10.64

Broadcast Address – 192.168.10.95

Usable IP Addresses – 192.168.10.65 to 192.168.10.94

BRANCH 2 LAN:

Number of Hosts – 20

Host Bits – 5 bits

Subnet Mask – /27 or 255.255.255.224

Increment – 32

Network Address – 192.168.10.96

Broadcast Address – 192.168.10.127

Usable IP Addresses – 192.168.10.97 to 192.168.10.126

WAN 1:

Number of Hosts – 2

Host Bits – 2 bits

Subnet Mask – /30 or 255.255.255.252

Increment – 4

Network Address – 192.168.10.128

Broadcast Address – 192.168.10.131

Usable IP Addresses – 192.168.10.129 to 192.168.10.130

WAN 2:

Number of Hosts – 2

Host Bits – 2 bits

Subnet Mask – /30 or 255.255.255.252

Increment – 4

Network Address – 192.168.10.132

Broadcast Address – 192.168.10.135

Usable IP Addresses – 192.168.10.133 to 192.168.10.134

WAN 3:

Number of Hosts – 2

Host Bits – 2 bits

Subnet Mask – /30 or 255.255.255.252

Increment – 4

Network Address – 192.168.10.136

Broadcast Address – 192.168.10.139

Usable IP Addresses – 192.168.10.137 to 192.168.10.138

Formula for Find Total Number of Host:

2^n The n represents the number of host bit in the subnet.

Example- 192.168.1.0/24

Here /24 means we have 24-bit network bit and 8-bit host bit. So as per formula total host is 2^8=256.

Formula for Find Number of usable Host:

2^n - 2. The n represents the number of host bit in the subnet.

So as per above example total usable host is 2^8-2=254

Calculate the Subnet Mask

For calculate subnet mask we have to work with network bit. As per above example 192.168.1.0/24 network bit is 24-bit and 8-bit is host bit. So we can write this in binary format as per below where we count network bit as 1 and host bit as 0.

11111111.11111111.11111111.00000000

Now if we convert it to decimal then it looks like 255.255.255.0.

Formula is 2726252423222120=128+64+32+16+8+4+2+1=255

Where only binary value is 1 we will add the values as per above formula. Also check below table.

	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0

IPv6 Address

- IPv6 address is a 128bit.
- Example Address **2001:0DB8:0000:0010:0000:0000:0000:0000**
  - 8 slots in hextet Separated by colon.
- Since it's hexadecimal each character contain 4bit=1nibble.
- Each hextet contain 16bits.
- The IPv6 address space is 128-bits (2^{128}) in size, containing 340,282,366,920,938,463,463,374,607,431,768,211,456 IPv6 addresses.

IPv6 addressing Abbreviations

- RULES for IPv6 addressing Abbreviations
- 1. Omit leading zero's
  - Condition A: Omit leading zero's as it is for those quartet with at least one nonzero hexadecimal
  - Condition B: Pure-zero quartet must have a single zero
- 2. Use double colon ONLY ONCE to replace long string of ZERO's

Example

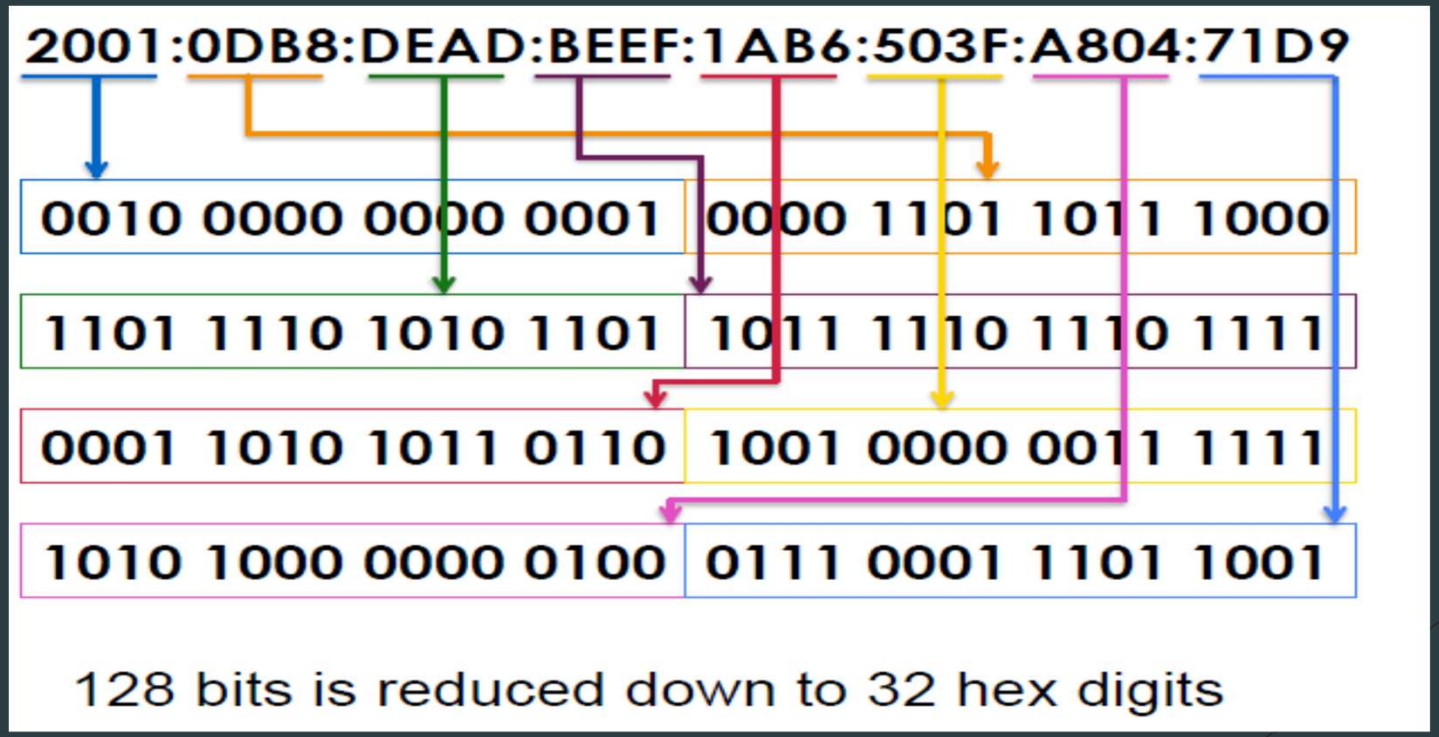
- 2001:0001:1010:0000:0000:0000:CAFE:FEED
- Rule #1 2001:1:1010:0:0:0:CAFE:FEED
  - we omit the leading zero's, we applied condition A and condition B
- Rule #2 2001:1:1010::CAFE:FEED

- 2001:0011:0000:0000:0CDC:0000:0000:FFFF

IPv6 Subnetting

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

IPv6 Subnetting



IPv6 Address Type

- Unicast
- Multicast
- Anycast

IPv6 Address Type

- **Global unicast** – similar to IPv4 public IP addresses. These addresses are assigned by the IANA and used on public networks.
  - Global Unicast prefix is 2000::/3
- **Unique local** – similar to IPv4 private addresses. They are used in private networks and aren't routable on the Internet.
  - Unique Local prefix is FD00::/8.
- **link local** – these addresses are used for sending packets over the local subnet. Routers do not forward packets with this addresses to other subnets. IPv6 requires a link-local address to be assigned to every network interface on which the IPv6 protocol is enabled.
  - Link Local prefix is FE80::/10.

IPV6 Address Type

- Multicast Address
  - Multicast addresses in IPv6 are similar to multicast addresses in IPv4. They are used to communicate with dynamic groupings of hosts, for example all routers on the link.
  - Multicast addresses prefix is **FF00::/8**
  - ff02::5 for OSPFv3 All SPF routers
  - ff02::6 for OSPFv3 All DR routers
  - ff02::8 for IS-IS for IPv6 routers
  - ff02::9 for RIP routers
  - ff02::a for EIGRP routers

IPV6 Address Type

- Modified EUI-64 address
  - An IPv6 unicast or anycast address is typically a 64-bit **interface identifier** used to identify a host's network interface. A 64-bit interface ID is created by inserting the hex value of **FFFE** in the middle of the MAC address of the network card.
  - Invert the 7th bit (from 0 invert to 1) or (from 1 invert it to)
- Example:
  - Mac Address : 00000C432A35

IPv6 Address Type

- Convert to binary and flip the seventh bit to one:
  - binary: 0000 0010 0000 0000 0000 1100 0100 0011 0010 1010 0011 0101
- Convert back to hex:
  - hex: 02000C432A35
- Insert FFFE in the middle:
  - interface ID: 02000CFFFE432A35

IPv6 Subnetting Exercise

- 2001:0db8:0000:0000:0000:0000:0000:0000
- 2001:0db8:0000:0000:d170:0000:1000:0ba8
- 2001:0db8:0000:0000:00a0:0000:0000:10bc
- 2001:0db8:0fc5:007b:ab70:0210:0000:00bb

ANY QUESTION??

Step 1: When System Configuration Dialog came type “no” and press enter

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no

Step 2: type “enable” and press enter

Router>enable

Step 3: type “show ip interface brief” for check the interfaces.

Router#show ip interface brief

Step 4: type “configure terminal” and press enter

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

Step 5: Now type “ipv6 unicast-routing” and press enter for **enable ipv6 in router.**

Router(config)#ipv6 unicast-routing
Router(config)#

Step 6: Now type “interface gigabitEthernet 0/0”and press enter for go to specific interface for assign ipv6.

Router(config)#interface gigabitEthernet 0/0
Router(config-if)#

Step 7: Now type “ipv6 enable” and press **enter for enable ipv6 on interface.**

Router(config-if)#ipv6 enable
Router(config-if)#

Step 7: Now type “ipv6 address 2001:abad:beef::1/64” and press enter for assign IPv6.

```
Router(config-if)#ipv6 address 2001:abad:beef::1/64
Router(config-if)#
```

Step 8: Now type “no shutdown” and press enter for up the interface.

```
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Router(config-if)#
```

Step 9: Type “exit” and press enter for go back to config mode.

```
Router(config-if)#exit
Router(config)#
```

Step 10: Type “exit” and press enter for go back to enable mode.

```
Router(config)#exit
Router#
```

Step 11: type “copy running-config startup-config” or “wr” and press enter for save the configuration in router

```
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#


Router#wr
Building configuration...
[OK]
Router#
```

You are done for assign IPv6 on interface. Do same step on Router 1 and check connectivity by ping.

Following ping is from Route 0. My Router 1 IPv6 address is 2001:ABAD:BEEF::2

```
Router#ping 2001:ABAD:BEEF::2
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:ABAD:BEEF::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Step 1: When System Configuration Dialog came type “no” and press enter

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no

Step 2: type “enable” and press enter

Router>enable

Step 3: type “show ip interface brief” for check the interfaces.

Router#show ip interface brief

Step 4: type “configure terminal” and press enter

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

Step 5: Now type “interface gigabitEthernet 0/0”and press enter for go to specific interface for assign ipv6.

Router(config)#interface gigabitEthernet 0/0
Router(config-if)#

Step 6: Now type “no shutdown” and press enter for up the interface.

Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Router(config-if)#

Step 7: Now type “ip address 192.168.1.1 255.255.255.252” and press enter for assign IPv4.

Router(config-if)# ip address 192.168.1.1 255.255.255.252
Router(config-if)#

Step 8: Type “exit” and press enter for go back to config mode.

```
Router(config-if)#exit
Router(config)#
```

Step 9: Type “exit” and press enter for go back to enable mode.

```
Router(config)#exit
Router#
```

Step 10: type “copy running-config startup-config” or “wr” and press enter for save the configuration in router

```
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

```
Router#wr
Building configuration...
[OK]
Router#
```

You are done for assign IPv4 on interface. Do same step on Router 1 and check connectivity by ping.

Following ping is from Route 0. My Router 1 IPv4 address is 192.168.1.2

```
Router#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Router

A router is a device that routes packets from one network to another. A router is most commonly an OSI Layer 3 device. Routers divide broadcast domains and have traffic filtering capabilities.

Cisco Router Command Mode

Mode	Prompt	Command to enter	Command to exit
User EXEC	Router >	Default mode after booting. Login with password, if configured.	Use **exit** command
Privileged EXEC	Router #	Use **enable** command from user exec mode	Use **exit** command
Global Configuration	Router(config) #	Use **configure terminal** command from privileged exec mode	Use **exit** command
Interface Configuration	Router(config-if)#	Use **interface type *number*** command from global configuration mode	Use **exit** command to return in global configuration mode
Sub-Interface Configuration	Router(config-subif)	Use **interface type *sub interface number*** command from global configuration mode or interface configure mode	Use **exit** to return previous mode. Use **end** command to return in privileged exec mode.
Setup	Parameter[Parameter value]:	Router will automatically insert in this mode if running configuration is not present	Press **CTRL+C** to abort. Type **yes** to save configuration, or **no** to exit without saving when asked in the end of setup.
ROMMON	ROMMON >	Enter **reload** command from privileged exec mode. Press **CTRL + C** key combination during the first 60 seconds of booting process	Use **exit** command.

IOS basic commands

In this article we will go through some basic IOS commands.

Hostname command

The *hostname* command is used to configure the device hostname. Because this command changes a device configuration, it must be entered in the global configuration mode. After typing the command, the prompt will change and display the new hostname.

Here is an example that shows you how to change a hostname of a device.
First, enter the global configuration mode by typing the *enable* command in the user EXEC mode and the *configuration terminal* command in the privileged EXEC mode. Once inside the global configuration mode, type the command *hostname R1*. Notice how the prompt was changed to reflect the configured value.

```
Router>
Router>enable
Router#config
Router#configure te
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

No shutdown command

By default, all interfaces on a Cisco router are turned off. To enable an interface, the *no shutdown* command is used. You first need to enter the submode of the interface that you want to configure. You can do that by using the global configuration mode command *interface INTERFACE_TYPE/ INTERFACE_NUMBER*. You can get a list of available interfaces by typing the '?' character after the interface command.

You may notice that the promt has changed to reflect the mode you are currently in. For the interface mode the *HOSTNAME#(config-if)* prompt is shown.

Once inside the interface mode, you can enable an interface by typing the *no shutdown* command.

```
R1(config)#interface fa0/1
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

R1(config-if)#
```

IP address command

```
Router(config-if)#ip address 10.0.0.2 255.0.0.0
Router(config-if)#no ip address
```

Setting up passwords

Each Cisco IOS device has the built-in authentication features. There are three basic ways to configure authentication on a device:

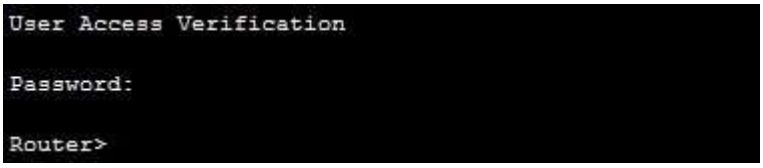
- **Configure a password for the console access** – by default, the console access doesn't require a password. You can configure a password for the console access by using the following set of commands:

```
HOSTNAME(config) line console 0

HOSTNAME(config-line) password cslkuril

HOSTNAME(config-line) login
```

This will force a user to type the password when trying to access the device through the console port.



- **Configure a password for the telnet access** – by default, the telnet access is disabled. You need to enable it. This is done using the following sequence of commands:

```
HOSTNAME(config) line vty 0 4

HOSTNAME(config-line) password cslkuril

HOSTNAME(config-line) login
```

- **Configure a password for the privileged EXEC mode** – from the privileged EXEC mode you can enter the global configuration mode and change the configuration of a device. Therefore, it is important to prevent an unauthorized user from entering the global configuration mode. You can do that by setting up a password to enter the privileged EXEC mode. This can be done in two ways:

```
HOSTNAME(config) enable password cisco

HOSTNAME(config) enable secret cisco
```

Both of the commands above accomplish the same thing, but with one major difference. The *enable secret PASSWORD* commands encrypts the password, while the *enable*

password PASSWORD command doesn't, which means that an unauthorized user could just read a password from the device configuration:

```
Building configuration...

Current configuration : 553 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
!
enable password cisco
```

Notice how the password (*cisco*) is visible in the device's configuration.

Service password-encryption command

By default, passwords configured using the enable password command and passwords for the console or telnet access are stored in clear text in the configuration file. This presents a security risk because an attacker could easily find out passwords. The global configuration *service password-encryption* command encrypts all passwords configured.

It is important to note that this type of password encryption is not consider especially secure, since the algorithm used can be easily cracked. Cisco recommends using this command only with additional security measures.

Configuring banners

You can display a banner on a Cisco device. A banner is usually shown before the login prompt. It is usually some text that appears on the screen when a user connects to the device (e.g. some legal information).

The most commonly used banner is the **Message Of The Day (MOTD)** banner. This banner, if configured, is shown before the login prompt to every user that is trying to establish a session with the device. The following global configuration command is used to configure a MOTD banner:

```
hostname(config)# banner motd DELIMITING_CHARACTER TEXT Unauthorized access forbidden!
```

A delimiting character is a character of your choice. Its purpose is to signify the start and end of a text that will appear in the banner. For example, the command *banner motd # Unauthorized access forbidden! #* will show the following text: **Unauthorized access forbidden!**

Show version command

The show version command is used to display information about a Cisco device. The command can be entered in both the user EXEC and privileged EXEC mode. By using this command, you can find out many useful information about your Cisco device, such as:

- Software Version – IOS software version
- System up-time – time since last reboot
- Software image name – IOS filename stored in flash
- Hardware Interfaces – interfaces available on device
- Configuration Register value – bootup specifications, console speed setting, etc.
- Amount of RAM memory – amount of RAM memory
- Amount of NVRAM memory
- Amount of Flash memory

Show history command

An IOS device stores, by default, 10 last commands you have entered in your current EXEC session. You can use the *show history* command from the user EXEC or privileged EXEC mode to display them.

Show running-configuration & show startup-configuration commands

After you have changed the configuration of your device you can verify its configuration. To display the current configuration, type *show running-configuration* from the privileged EXEC mode. This show the configuration that is stored in a device's RAM.

```
Router#show running-config
Building configuration...

Current configuration : 474 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
```

After you have stored your running configuration into the startup configuration, you can view the saved configuration using the *show startup-config* command from the privileged EXEC mode.

This command shows the configuration that is currently stored in the device's NVRAM. This configuration will be loaded next time the device is restarted.

```
Router#show startup-config
Using 474 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
```

Introduction Of DHCP Server

- DHCP (Dynamic Host Configuration Protocol)
- DHCP is a network protocol that is used to assign various network parameters to a device. This greatly simplifies administration of a network, since there is no need to assign static network parameters for each device.

- DHCP is a client-server protocol. A client is a device that is configured to use DHCP to request network parameters from a DHCP server. DHCP server maintains a pool of available IP addresses and assigns one of them to the host. A DHCP server can also provide some other parameters, such as:

  subnet mask

  default gateway

  domain name

  DNS server

How DHCP Work

- DHCP client goes through the four step process:

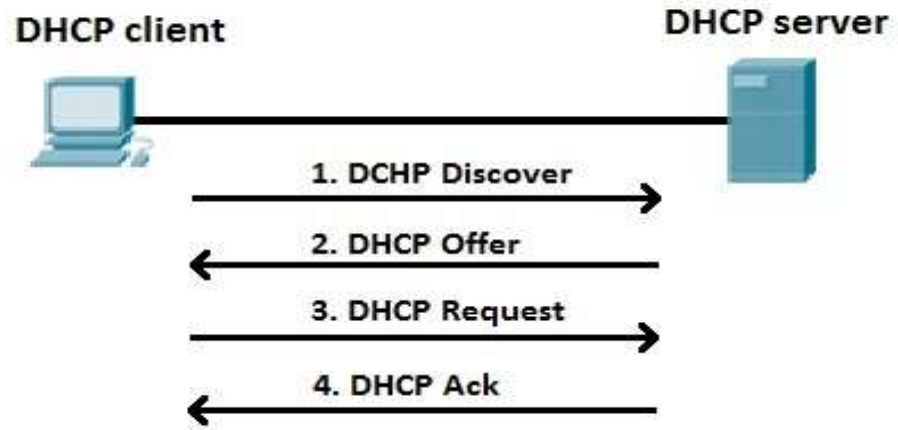
1. A DHCP client sends a broadcast packet (**DHCP Discover**) to discover DHCP servers on the LAN segment.

2. The DHCP servers receive the DHCP Discover packet and respond with **DHCP Offer** packets, offering IP addressing information.

3. If the client receives the DHCP Offer packets from multiple DHCP servers, the first DHCP Offer packet is accepted. The client responds by broadcasting a **DHCP Request** packet, requesting the network parameters from the server that responded first.

4. The DHCP server approves the lease with a **DHCP Acknowledgement** packet. The packet includes the lease duration and other configuration information.

How DHCP Work



Configure DHCP Server On Cisco Router

- A Cisco router can be configured as a DHCP server. Here are the steps:
  1. Exclude IP addresses from being assigned by DHCP by using the *ip dhcp excluded-address FIRST_IP LAST_IP*
  2. Create a new DHCP pool with the *ip dhcp pool NAME* command.
  3. Define a subnet that will be used to assign IP addresses to hosts with the *network SUBNET SUBNET_MASK*command.
  4. Define the default gateway with the *default-router IP* command.
  5. Define the DNS server with the *dns-server IP* address command.
  6. (Optional) Define the DNS domain name by using the *ip domain-name NAME* command.
  7. (Optional) Define the lease duration by using the *lease DAYS HOURS MINUTES* command. If you don't specify this argument, the default lease time of 24 hours will be used.

DHCP Example

- Floor1(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.50
- Floor1(config)#ip dhcp pool Floor1DHCP
- Floor1(dhcp-config)#network 192.168.0.0 255.255.255.0
- Floor1(dhcp-config)#default-router 192.168.0.1
- Floor1(dhcp-config)#dns-server 192.168.0.1

DHCP Example

- In the example above we can see that we've configured the DHCP server with the following parameters:
  1. the IP addresses from the **192.168.0.1 - 192.168.0.50** range will not be assigned to hosts
  2. the DHCP pool was created and named **Floor1DHCP**
  3. the IP addresses assigned to the hosts will be from the **192.168.0.0/24** range
  4. the default gateway's IP address is **192.168.0.1**
  5. the DNS server's IP address is **192.168.0.1**

Checking DHCP

- Floor1#show ip dhcp binding

  IP address Client-ID/ Lease expiration Type

  Hardware address

  192.168.0.51 0060.5C2B.3DCC -- Automatic

Any Question?

What is IP routing?

IP routing is the process of sending packets from a host on one network to another host on a different remote network. This process is usually done by routers. Routers examine the destination IP address of a packet , determine the next-hop address, and forward the packet. Routers use routing tables to determine the next hop address to which the packet should be forwarded

Connected routes

- Subnets directly connected to a router's interface are added to the router's routing table. Interface has to have an IP address configured and both interface status codes must be in the up and up state. A router will be able to route all packets destined for all hosts in subnets directly connected to its active interfaces.

Static

- Routers forward packets using either route information from route table entries that you manually configure or the route information that is calculated using dynamic routing algorithms.

Static

- Static routes, which define explicit paths between two routers, cannot be automatically updated; you must manually reconfigure static routes when network changes occur. Static routes use less bandwidth than dynamic routes. No CPU cycles are used to calculate and analyze routing updates.

Static

- You should use static routes in environments where network traffic is predictable and where the network design is simple. You should not use static routes in large, constantly changing networks because static routes cannot react to network changes. Most networks use dynamic routes to communicate between routers but might have one or two static routes configured for special cases.

Default Route

- Default routes are useful when dealing with a network with a single exit point. It is also useful when a bulk of destination networks have to be routed to a single next-hop device. When adding a default route, you should ensure that the next-hop device can route the packet further, or else the next hop device will drop the packet.

Default Route

- Another point to remember is that when a more specific route to a destination exists in the routing table, the router will use that route and not the default route. The only time the router will use the default route is when a specific route does not exist.

Default Route

- ip route 0.0.0.0 0.0.0.0 *next-hop*

Netwotk Route

Network Route

একটি Network থেকে আর একটি Network এ Data Packet পাঠানোর যে পথ সেটিই হলো Network Route । Network Route করার জন্য Router এর Routing Table এর সহায়তা নেওয়া হয়। Network Route সাধারণত তিন ধরণের হয় :

1. Static Route
2. Default Route
3. Dynamic Route

1. Static Route :
Static Route এর ক্ষেত্রে Router এর Routing Table এ Destination Network সমূহের Information অর্থাৎ Destination Network এর IP, Subnet Mask এবং সেই Network এ পৌঁছানোর Path ইত্যাদি Manually বলে দিতে হয়।

2. Default Route:
Destination Network এর নিকট পৌঁছানো জন্য যতগুলো Network অতিক্রম করতে হয় উহাদের Details Information জানা না থাকলে Router Default হিসাবে যে বেছে নিবে সেটিই হলো Default Route। প্রতিটি Router এ একটি Default Route নির্ধারণ করে দেওয়া থাকে যাতে Routing Table এ কোনো Destination এর Path খুঁজে না পেলে Data কে Default Route এর মাধ্যমে Destination এর নিকট পাঠাতে পারে।

3. Dynamic Route :
যদি কোনো Protocol এর সহায়তা নিয়ে Router এর Routing Table কে Update করা হয় তবে সেই পদ্ধতিকে Dynamic Routing বলে। প্রধানত: দুইটি কাজ করে :- 1. Dynamically Routing Table Update করা ও 2. Best Path Selection করা।

Netwotk Route

Static Route ও **Dynamic Route** এর তুলনামূলক পার্থক্য :

S.L.	Static Route	Dynamic Route
01	এক্ষেত্রে Routing Table Manually Update করে দিতে হয়।	এক্ষেত্রে Routing Table Update করার জন্য Protocol Use করা হয়। যেমন : RIP, EIGRP, OSPF ইত্যাদি।
02	এক্ষেত্রে Manually Path Select করে দিতে হয়।	এক্ষেত্রে Dynamic Routing Protocol তার নিজস্ব Logic অনুযায়ী Path Select করে। যেমন : RIP Router Count করে। OSPF Bandwidth Count করে।
03	এক্ষেত্রে কোনো Link Down হয়ে গেলে Manually অন্য Path Select করে দিতে হয়।	Dynamic Routing Protocol একটি নিদ্রিষ্ট সময় পর্যন্ত অপেক্ষা করে Dynamically অন্য Link Up করে দেয়। যেমন : RIP 240 second অপেক্ষা করে । EIGRP 15 second অপেক্ষা করে।
04	এক্ষেত্রে Data Send এবং Receive করার জন্য 100% Bandwidth ব্যবহার করা হয়।	Dynamic Routing Protocol এ Neighbor Router এর জন্য বিভিন্ন ধরণের Message Generate করতে হয়। যেমন : Hello Message, Update Message ইত্যাদি। এই Message গুলো Send ও Receive করার জন্য Bandwidth এর একটি নিদ্রিষ্ট Percent Reserve করে রাখা হয়।
05	ছোট Topology এর ক্ষেত্রে Static Route ভালো কাজ করে।	তুলনামূলক বড় Topology এর ক্ষেত্রে Dynamic Route ভালো কাজ করে।