Unit 1

Chapter 1: Understanding Networks and their Building Blocks

I. Introduction to Networks

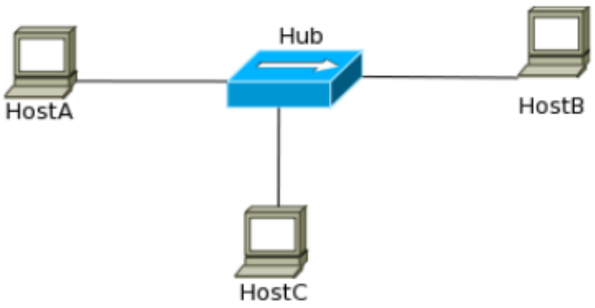
Network is a collection of interconnected devices (such as computer, printers, etc.)

Some advantages of networks
- Decrease cost
- Saves time
- Saves effort
- Increase productivity
- Resource optimization

How do network works?

Most basic form of network

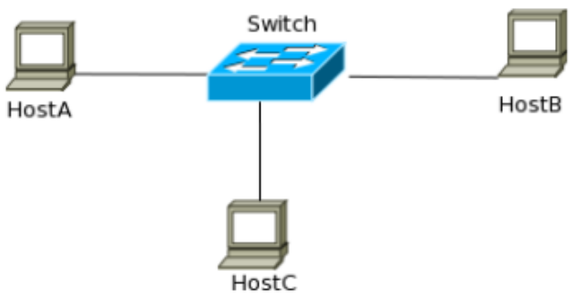
Network with a HUB



Message Delivery:
- Unicast
- Broadcast
- Multicast

Problems with using a HUB?
- Repeats information received from one host to all other hosts
- Creates a shared medium where only a single host can send a packets at a time. The shared network medium is called a single **Collision Domain.**

A switched network



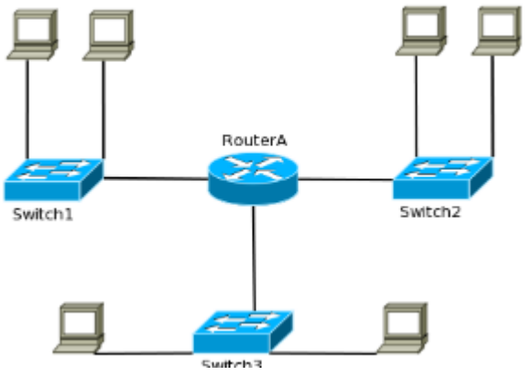
*__Switch__ – overcomes the problems associated with hubs. It break up collision domain for every port.
*Switches do not flood every frames out to all ports, creating one broadcast domain.

Exercise: Determine the number of collision domain in the given topology

Problem with using a Switch

Too many broadcast message will slow down the network, creating a **broadcast storm.**

Router in an internetwork



*__Router__ – breaks up a broadcast domain and do now allow broadcast to be transmitted across different networks.

Essential functions:

Packet Switching – switches packets between network

Communication between **Network** – allows communication between networks connected to it.

Path Selection – select the best path to reach a network

Packet Filtering – drops or forwards packets

II. Networking Types

Lan – covers a limited geographical area. Ethernet is the most commonly used technology in LANs.

WAN – covers a large geographical area. Used to connect LANs.

III. Internetworking Models

Internetworking Models – created to support and promote inter-operability between different vendors.

OSI – layered approach created to promote communication between devices of various vendors.

TCP/IP – similar with OSI, but is more commonly used.

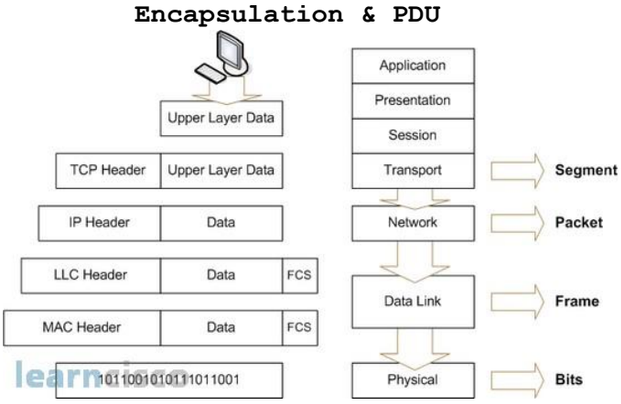
OSI Reference Model

Application – provides a user interface

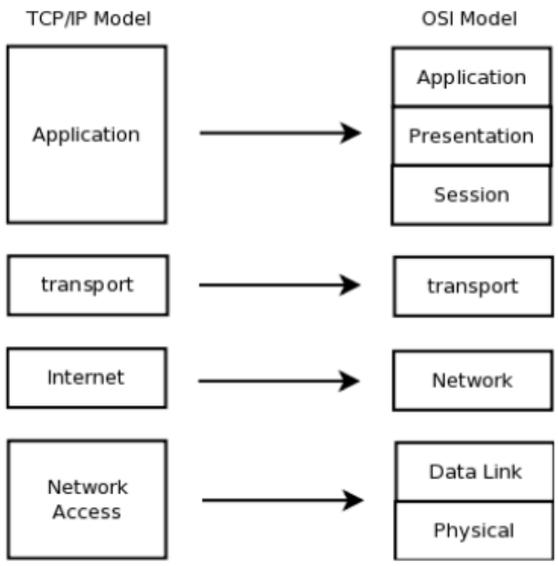
Presentation – presents data; handles encryption/decryption,

encoding/decoding, compression/decompression.
Session – maintains distinction between data of separate applications; provides dialog control between hosts.
Transport – provides end-to-end connection; provides reliable or unreliable delivery and flow control.
Network – provides logical addressing and path determination.
Data Link – Provides media access and physical addressing
Physical – converts digital data to signal over a physical medium; moves data between hosts.

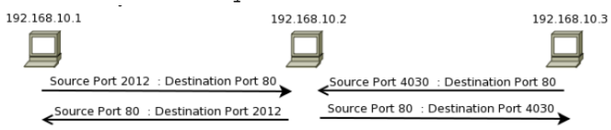
Encapsulation & PDU



IV. TCP/IP Reference Model



1. **Application Layer**
   Application Layer performs all functions of the OSI model's Application, Presentation and Session layers.
   Exercise: name some of the common application layer protocols used today.
2. **Transport Layer**
   Same as the OSI layer's Transport Layer. It is concerned with the end-to-end transportation of data and set-ups a logical connection between two hosts.
   Two Common Protocols under Transport Layer:
   TCP – connection oriented and reliable protocol
   UDP – connectionless and unreliable protocol
   Port Numbers – both protocols uses this concept by assigning port numbers to know which data belongs to which application.
   Socket – combination of IP address, protocol (TCP/UDP) and port numbers at both the receiving and sending hosts. Each socket is unique.



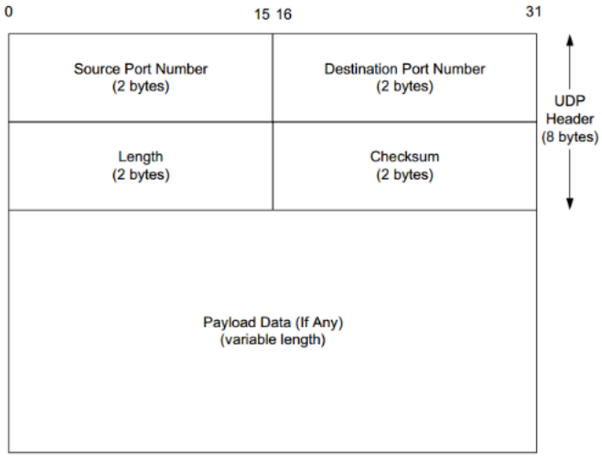
a. Transport Control Protocol
Functions of the TCP:
1. **Connection establishment** – using the 3-way handshake process.
2. **Data segmentation** – limits the data (MTU) to be sent across the network.
3. **Flow control** – determines the number of segments that can be sent at a time.
4. **Reliable delivery with Error recovery**
5. **Ordered delivery** – uses the sequence number to mark the order
6. **Connection termination** – using the 2-way handshake process
7.

Fields of the TCP Header

Source Port (16 bits)			Destination Port (16 bits)
Sequence Number (32 bits)			
Acknowledgement Number (32 bits)			
Header (4 bits)	Reserved (6 bits)	Code Bits (6 bits)	Window (16bits)
Checksum (16bits)			Urgent (16bits)
Options (0 to 32 bits)			

b. UDP
- UDP neither establishes a connection
- Unreliable protocol that delivers data
= Faster than TCP
- Does not create delay (since TCP holds data till it receives acknowledgement)

Fields of the UDP Header

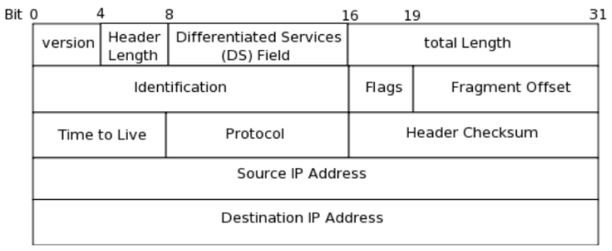


3. Internet Layer

Provides the ff.:
1. Logical addressing
2. Path determination
3. Path forwarding

Most common protocol:
1. IP (Internet Protocol)
2. ICMP (Internet Control Message Protocol)
3. Routing Protocols

Fields of IPv4 Header



ICMP – management protocol and messaging service for IP.

ICMP messages:
1. **Echo Reply –** uses "Ping" to send echo requests to check network connectivity.
2. **Destination Network Unreachable** – packet cannot be routed in which the destination address resides
3. **Time Exceeded** – TTL of a packet expires (reduces to zero)
4. **Request Time Out** – destination host might be down or unreachable (different network, shutdown, behind a firewall, etc.)

4. Network Access Layer

Corresponds with the Data Link & Physical Layers of OSI reference model

Protocol used: Ethernet

V. Cisco 3 Layer Model

Three-layer hierarchical Model – defined by Cisco that provides a hierarchical and modular method of building networks that makes it easy to implement, manage, scale and troubleshoot networks.

3 Layers:
1. Core Layer
2. Distribution Layer
3. Access Layer

1. Core Layer

Backbone of an internetwork and is the most critical layer.

Sole function is to transport large amount of data fast.

Two major requirement: Speed and Fault Tolerance

What should be done in this layer?
1. Routing protocols should have low converge time.
2. Network Access Layer technologies should be fast with low latency
3. Redundancy

2. Distribution Layer

Provide routing, filtering, and WAN access

Determine how packets can access the core.

Major requirement: Path Determination

What should be done in this layer?
1. Routing between subnets and route distribution between routing protocols.
2. Implement security policies, firewall, packet filtering, etc.
3. Breaking broadcast domain.

3. Access Layer

Edge of the network

Where end devices are connected

What should be done in this layer?
1. Access control and policies (addition to what exist in distribution layer).
2. Dynamic Configuration mechanisms
3. Breaking Collision Domains
4. Ethernet switching and stating routing

Chapter 2: IP Addressing and Subnets

I. Composition, Types and Classes

Term to remember:

- IP Address
  - Uniquely identifies a device
    - IPv4 – 32 bits
      - Divided into 4 optet, 8 bit each
    - IPv6 – 128 bits
- Network Address
  - Group name
- Subnet Mask
  - Identifies network/ host
  - Defines the range of IP Addresses

IP Address: Network & Host portion
5 Classes:

Reminder: 127 is for loopback IP address, (127.0.0.1) for pinging yourself

A: 0 – 126
B: 128 – 191
C: 192 – 223
D: 224 – 239
E: 240 – 255

II. Private and Public IP Addresses

IANA – responsible for managing and distributing IP addresses
*Private IP Addresses are for intranet
*Public IP Addresses are for internet
Ranges for Private IP addresses:

- Class A – 10.0.0.0 to 10.255.255.255 (1 network)
- Class B – 172.16.0.0 to 172.31.255.255 (16 networks)
- Class C – 192.168.0.0 to 192.168.255.255 (256 networks)

III. Subnetting (FLSM & VLSM)

Subnetting – Divide/segment large network into small ones
Subnetting Activity

- **FLSM**
  - Determine the number of network
  - 192.168.1.0/24 – Prefix Length or CIDR
  - IIIIIIII.IIIIIIII.IIIIIIII.
    00000000
    The first three octet is the network portion
    And the last octet is the host portion
  - IIIIIIII.IIIIIIII.IIIIIIII.
    II000000
    The highlighted ones are now the network portion
  - Problem 1:
    192.168.1.0/24 – 4 hosts
    2^n = 2^2 = 4
    IIIIIIII.IIIIIIII.IIIIIIII.
    II000000 /26 = + the n
    255.255.255.192
    1) 192.168.1.0/26
    2) 192.168.1.64/26
    3) 192.168.1.128/26
    4) 192.168.1.192/26
  - Problem 2:
    192.168.0.0/24 – 8 hosts
    2^n = 2^3 = 8 networks
    IIIIIIII.IIIIIIII.IIIIIIII.
    III00000 /27
    255.255.255.224
    1) 192.168.0.0/27
    2) 192.168.0.32/27 …
- **VLSM**
  - Determine the number of host
  - Problem:
    172.16.0.0/16 = 26 hosts
    2(^n)-2 = 2^5-2 = 30
    8.8.8.11100000/27
    255.255.255.224
    NA: 172.16.0.0/27
    1st: 172.16.0.1/27
    Last: 172.16.0.30/27
    BA: 172.16.0.31/27
    Next NA: 172.16.32/27

Chapter 3: Cisco Switches, Routers & IOS

I. Definition of Terms

IOS Shell
IOS Kernel
Bootstrap
RAM
NVRAM
ROM
Flash
IOS Modes

II. Shortcut Keys

Shortcut Keys	Purpose
Down Arrow	Scroll through command history
Up Arrow	Scroll backwards through commands
Tab	Completes the remainder of the partially entered command
Ctrl-A	Moves to the beginning of the line
Ctrl-E	Moves to the end of the line
Ctrl-Z or end	Exits the current mode and returns to User Exec mode
Ctrl-C	Aborts the current command
Ctrl + Shift 6	Interrupt an IOS process

III. Gathering & Verifying Information

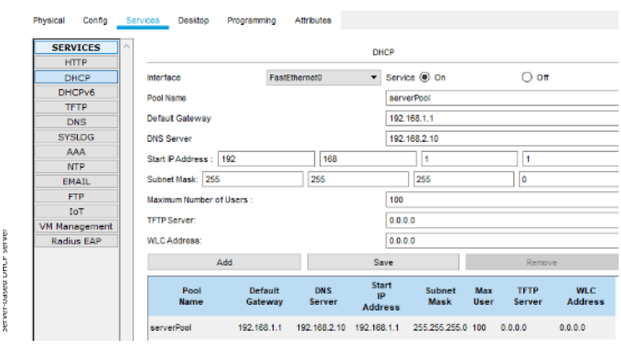
Using SHOW commands
- Running config
- Startup config
- Version
- Interface information
- Using pipes

IV. DNS &DHCP

Resolving Names of IOS
- ip name-server <local ip>
- ip host <word> <ip add>

Cisco IOS as the DHCP Server
- Ip dhcp pool <name>
- network <net add> <sub mask>
- default-router <gateway ip>
- dns-server <DNS IP address>
- ip dhcp excluded-address <start-IP> <end IP>

Server-based DHCP Server



Remote host is the DNS server IP add

V. Saving, Erasing & Backing Up Configs

Saving Commands
- **Enter the CLI of R0
- *copy run tftp
  - enter address remote host
  - enter source: R1-confg

Erase Commands

Backing up configs
- TFTP
- FTP
  - Configure the username and password
  - Conft# ip ftp username <username>
  - Conft# ip ftp password <password>
  - copy run tftp
    - enter address remote host

VI. Password Recovery

Reboot
Repeat Reboot
Boot up the device
Interrupt the boot up process using Ctrl-C
Change configure registry to 0x2142
Reboot
Copy start run
Change the enable password
Change configure registry to 0x2102
Save
- *disable
- *end
- *reboot
- *repeat reboot
- *common 1 > confreg 0x2142
- *common 2 > reset
- *Router# copy tftp running-config
  - Enter address remote host
  - enter source: R1-confg
- *copy startup-config running-config
- *ena sec cisco
- *enable secret class
- *end
- *conf t
- *config-register 0x2102
- *end
- *wr (save)

CDP Neighbor

- Cisco Discovery Protocol (CDP) is a proprietary protocol designed by Cisco to help in finding information about neighboring devices
- Devices connected to each other exchange CDP packets to learn about each other. This can be useful in troubleshooting and documenting the network
- Enable CDP globally: cdp run
- Enable CDP on an interface: cdp enable

*show cdp nei

IP helper-address

- Discover – udp broadcast
- Offer – udp unicast
- Request – udp broadcast
- Acknowledge – udp unicast

In router0 cli ***also in interface that is conn. to
Another router
- *ip helper-address <dns address>
- *no ip dhcp pool DHCP

In router1 *ip address dhcp

Chapter 4: IP Routing

A router must know the ff:

- Destination Address
- Neighbor routers from which it can learn about remote networks
- Possible routes to all remote networks
- The best route to each remote network
- Be able to maintain and verify routing information

I. Types of Routing

- Routing table is stored in Routing Information Base (RIB)
- Routing table consist of destination address, subnet mask & next hop towards the destination
- 3 ways a Router learn routes:
  - Static Routing
  - Default Routing
  - Dynamic Routing

II. Static Routing

- Route is manually added by an administrator
- Best in small networks
- **Advantages:**
  - No overhead
  - Adds a certain degree of security
- **Disadvantages:**
  - Prior knowledge of the network
  - Every change should be done manually
  - Unmanageable in large networks
- *Ip route <destination> <netmask> <next hop | exit interface>*

III. Default Routing

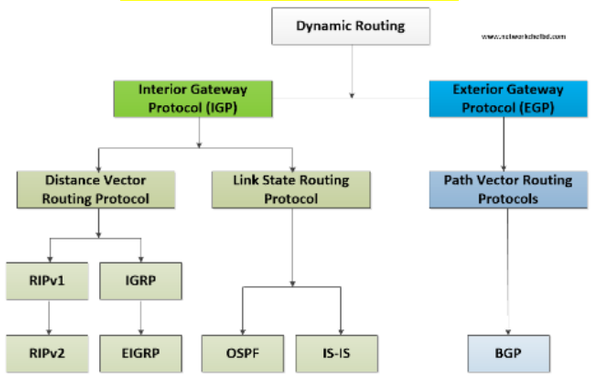
- All routers are configured to send all packets towards a single router
- Very useful method for small networks with a single entry and exit point
- Used in addition to any unknown destination to a single next hop address
- Useful when a bulk of destination networks have to routed
- Note: when a more specific route to a destination exists in the routing table, the router will use that rout and not the default route.
- *Ip route 0.0.0.0 0.0.0.0 <next_hop>*

IV. Dynamic Routing

- Algorithms are used to automatically propagate routing information
- Best in large networks
- Greater CPU and bandwidth usage
- Every routing protocol defines its own rules for communication between holders and selecting the best route.

V. Routing Protocols

- Classified as IGP & EGP
- **IGP** – exchange routing information within internetworks that fall under a single administrative domain (also called as AS)
- **EGP** – exchange routing information between different administrative domain.



VI. Administrative Distance & Routing Metrics

- **Administrative Distance:**
  - Trustworthiness of routing information received by a router
  - Used when multiple routing protocol is present on a single router.
  - Value from 0 to 255. Lowest value will be selected.
  - Any route with an AD value of 255 will never be used.

AD Values

Routing Protocol	Administrative Distance
RIP	120
OSPF	110
EIGRP	90
Static Routes	1
Directly Connected	0

- **Routing Metrics:**
  - A metric (or cost) of a route is calculated differently by each protocol.
  - Used when single routing protocol with multiple paths is running on a router.

VII. Choosing Routes:

1. When a routing protocol has more than one path to a destination, it will use the metrics to present a route to the router.

2. When a router is presented with multiple routes to a destination, it will use AD to decide which one to use and will install that route in the routing table.
3. Finally when a routers needs to route a packet, it will look at the routing table and use the route longest match prefix (subnet mask).

VIII. Classes of Routing Protocols

- **Distance Vector**
  - Uses distance to measure the cost of a route.
  - Periodically send their entire routing table.
  - Slower to converge, consume a lot more bandwidth & CPU.
- **Link State**
  - Form a neighbor relation with other routers before sharing routing information.
  - Exchange connectivity related information (links states)
  - Link state updates are sent out only when there is a change
  - Converge faster than distance vector.
- **Hybrid**
  - Use aspects of both distance vector and link state protocols.
  - Ex. EIGRP

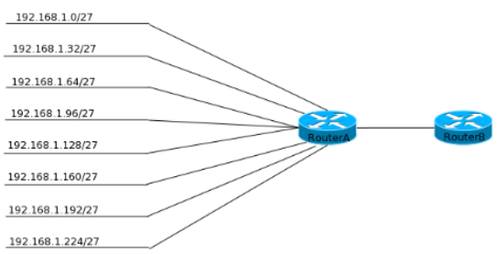
IX. Routing Loops

1. **Maximum Hop Count** – set to 15
2. **Split Horizon** – prohibiting a router from advertising a route back onto the interface from which it was learned
3. **Route Poisoning** – lost route is advertised with hop count of more than the maximum hop count
4. **Hold Downs** – prevents a router from learning new info about a failed route until time expires

X. Routing Redistribution

- Route redistribution is the process of distributing routes learned from one source to another
- Useful when networks are expanding, merging or in a phase of transition

XI. Route Summarization



- 192.168.1.0/25
- 192.168.1.128/25
- 192.168.2.0/24
- 192.168.3.0/24
- 192.168.4.0/26
- 192.168.4.64/26
- 192.168.4.128/26
- 192.168.4.192/26