NETWORK ESSENTIALS

NETWORK ESSENTIALS

Types of Network

1. LAN
2. WAN
3. INTERNET

Types of LAN

1. Client/Server
2. Peer to Peer

Network Components

1. Network Hardware
2. Network Software

Network Hardware

1. Network Interface Card (NIC)
2. Transmission Media
3. Two or more Computers
4. Network Devices

Network Software

1. Network Operating System (NOS)

Transmission Media

1. Twisted Pair Cable
2. Coaxial Cable
3. Fiber Optic Cable
4. Wireless LAN

TIA Standard (Telecommunication Information Association)

Twisted Pair Cable

1. Unshielded twisted pair (UTP)
2. Shielded twisted pair (STP)

UTP categories

a.	CAT 1	used for telephone (1 pair)
b.	CAT 2	4 MbPS for token ring (2 pairs)
c.	CAT 3	10 MbPS for Ethernet (4 pairs)
d.	CAT 4	16 MbPS for Fast Token Ring (4 pairs)
e.	CAT 5	100 MbPS for Fast Ethernet (4 pairs)
e.	CAT 5e	1 GbPS for Gigabit Ethernet
f.	CAT 6	1 Gbps for MultiGigabit

CABLE SPECIFICATIONS

Gigabit	1000 BASE T	1000MbPS	
Fast	10 BASE T	10 MbPS	Baseband Twisted Pair (100 mts)
Ethernet	100 BASE T	100 MbPS	Baseband Twisted Pair (100 mts)
	100 BASE TX	100 MbPS	Baseband (220 mts)

Connector RJ 45

STP Connector

RJ 45, RJ 11, RS- 232, RS -449
155 MbPS

Connections

1. STRAIGHT THROUGH (T568A – T568 A)
2. CROSS OVER (T568A – T568 B)

STRAIGHT THROUGH

	T 568 A	**T 568 A**
1.	Green White (T_X +)	Green White
2.	Green (TX-)	Green
3.	Orange White (RX +)	Orange White
4.	Blue	Blue
5.	Blue White	Blue White
6.	Orange (RX-)	Orange
7.	Brown White	Brown White
8.	Brown	Brown

[1-3, 2-6]

CROSS OVER

	T 568A	**T 568 B**
1.	Green White [TX +]	Orange White
2.	Green [TX -]	Orange
3.	Orange White [RX +]	Green White
4.	Blue	Blue
5.	Blue White	Blue White
6.	Orange [RX -]	Green
7.	Brown White	Brown White
8.	Brown	Brown

COAXIAL CABLE [RG /68]

1. THIN NET [0.25 “]
2. THICK NET [0.4 “]

CABLE SPECIFICATION

10 Base 2	Thin net	200 mts [6 mm]
10 Base 5	Thick net	500 mts [13 mm]

Connectors

BNC [BAYONET- NEILL-CONCELMAN]
It includes T-connector
Parallel connector
Terminator

VAM PIRE TAP	Standard Ethernet [thick net]
BNC	Thin Ethernet

FIBER OPTIC

SPECIFICATION

1000 Base LX	Long wavelength , Multimode [3 km] or Single Mode [100 km]
1000 Base SX	Short wavelength,
10 Base F	2000 mts

FIBER OPTIC

Multi Mode	used LED	used in LAN's
Single Mode	used LASER	used in telephone network

Connectors
* SC
* ST

NETWORK TECHNOLOGIES

1. ETHERNET
2. TOKEN RING
3. FDDI [Fiber Distributed Data Interface]

ETHERNET

- 10 MbPS
- Revisions
    - Fast Ethernet [IEEE 802.3U] 100 MbPS
    - Gigabit Ethernet [IEEE 802.5] 100 MbPS or 1 GbPS

CSMA/CD [Carrier Sense Multiple Access / Collision Detection]

- Ethernet` at Data Link layer is responsible for Ethernet addressing, commonly referred to as hardware addressing or MAC addressing
- Ethernet is also responsible for framing packets received from the network layer and preparing them for transmission on the local network through Ethernet CONTENTION Media Access Method

ETHERNET FRAME FORMAT IEEE 802.3

PRE	SFD	DA	SA	LENGTH/TYPE	DATA/PAD	FCS

PRE – Preamble – 7 bytes in alternating 1's, 0's – indicating the receiver stations that frame is coming

SFD – Start Frame Delimiter / synch – 1 byte

1,0,1,0,1,0,10,1	1,1,1,1,1,1,1,1
Alternations	all 1's
1, 0	

- PRE uses either SFD or synch

DA – Destination Address – 6 bytes
LSB is 0 – Individual Address
1 – Group Address

TOKEN RING [IEEE 802.5]

- No collisions
- Ideal for applications [factory automation]
- 4 or 16 MbPS

Logically a ring but physically a star configuration to MAU relays

- Token ring LANs continuously pass a token or a Token Ring frame
- MAU [Multistation Access Unit]

FDDI [Fiber Distributed Data Interface]

- 100 MbPS Token passing network
- Fiber optic cable with mass length of 2 km
- Dual-ring architecture for redundancy
- Used for corporate and carrier backbones

CDDI [Copper Distributed Data Interface]

- implements FDDI over STP and UTP cable

Dual Ring Architecture

- Primary ring for data transmissions
- Secondary ring for reliability and robustness

Components

- Single attachment station (SAS) for PC's
- Dual attachment stations (DAS) for servers
- Concentrator

FDDI concentrator

- also called as Dual- attached concentrator (DAC)
- Building block of an FDDI network
- Attaches directly to both rings and ensures that any SAS failure or power-down does not bring down the ring

NETWORK TOPOLOGIES

Defines network device organization.
Four common types

- BUS Topology
- TREE Topology
- STAR Topology
- RING Topology

Topologies are logical Architecture
Actual devices need not be physically organized in these configurations

BUS and TREE Topology
TREE Topology branch with multiple nodes.

STAR Topology

- used in Ethernet and Token Ring
- 5 to 100+ devices

OSI Reference Model

Application layer, Presentation layer, Session layer, Transport layer [segment]
Network layer [packets], Data link layer [frame], Physical layer [bits]

APPLICATION LAYER

- Provides network services to application processes like e-mail, File Transfer, and Terminal Emulation.

PRESENTATION LAYER

- Data representation
- Ensures data is readable by receiving system
- Format of data
- Data structure
- Negotiates data transfer syntax for application layer
- Compression, decompression, encryption and decryption

SESSION LAYER

- Inter-host communication
- Establishes, manages, and terminates sessions between applications

TRANSPORT LAYER

- End-to-end connection reliability
- Concerned with data transport issues between hosts
- Data transport reliability
- Establishes, maintains, and terminates virtual circuits
- Fault detection and recovery
- Information flow control

NETWORK LAYER

- Addresses the best path
- Provides connectivity and path selection between two end systems
- Domain of routing

DATA LINK LAYER

- Access to media
- Provides reliable transfer of data across media
- Physical addressing, network topology, error notification and flow control

PHYSICAL LAYER

- Binary transmission
- Through wires, connectors, voltages, data rates

TCP/ IP

A suite of protocols

TCP

- Rules that dictate how packets of information are sent across multiple networks
- Addressing
- Error checking

IP

- Determines where packets are routed based on their destination addresses
- Breaks packets into smaller packets and reassembles them.

DOD model	OSI model
Application / process	Application
	Presentation
	Session
Host-to-host	Transport
Internet	Network
Network Access	Data link
	Physical

TCP/IP PROTOCOL SUIT

PROTOCOLS

The Process / Application layer protocols

1. **Telnet – Terminal Emulation**

- allows a user on a remote client machine called the Telnet client, to access the resources of another machine, the Telnet Server [virtual terminal]
  [port no. 23]

2. **File Transfer Protocol**

- FTP is a program operating as protocol
- Used for file transfer between two systems
- Can access both directories and files and can accomplish certain types of directory operations.
- FTP uses Telnet to transparently log on to FTP server.
- Uses authentication secured with user names and passwords.

** **Directory Manipulation**

- Typing file contents
- Copying file between hosts
- It can't execute remote files as programs. [port no. 21]

3. TFTP – Trivial File Transfer Protocol

- Stock version of FTP
- Fast
- No directory-browsing abilities
- Sends or receive much smaller blocks of data than FTP
- No authentication, so its insecure   [port no. 69]

4. NFS – Network File System

- protocol specializing in file sharing
- allows two different types of file system to interoperate   port no

5. SMTP – Simple Mail Transfer Protocol

- Used to send mail or e-mail
- POP 3 used to receive mail [port no. 110]
- Port no. 25

6. LPD – Line Printer Daemon

- designed for printer sharing
- LPD along with LPR [Link Printer Program]
- Allows print jobs to be spooled and sent to network printers using TCP/IP
- Port no.

<u>X WINDOWS</u>

* Designed for client-server operations on a GUI
* Port no.

SNMP – Simple Network Management Protocol

- collects and manipulate valuable network information
- it receives BASELINE – a report delimiting the operation traits of a healthy network
- this protocol stands as watch dog [AGENTS]
- Agents send an alert called a TRAP to the management
- Port no. 161 / 162

DNS – Domain Name Service

- it resolves host name alternative to IP address
- port no. 53

DHCP – Dynamic Host Configuration Protocol

- it assigns IP address to hosts
- can provide following information
  * IP, subnet mask, domain name, default gateway, DNS, WINS

BOOTP – Boot strap protocol

- port no. 69

NETWORK PROTOCOLS

1. **IPX / SPX–**
   Inter Network Packet Exchange / Sequenced Packet Exchange
   Netware Core Protocol developed by Novell.

2. **NETBIOS / NETBEUI**
   Network Basic Input Output System / NETBIOS Enhanced User Interface
   Developed by IBM refined by Microsoft
   Used by Windows NT for LAN management
   For file and printer sharing

3. **TCP / IP**
   Set of protocols used in Internet

4. **APPLETALK**
   Used by MACINTOSH computers

5. **DLC / Data Link Control – developed by IBM**
   To connect Token- ring based workstations to IBM mainframe.
   Also used by printer manufacturers to connect remote printers to network print servers.

Host-To-Host Layer Protocols

1. TCP – Transmission Control Protocol

- Connection-oriented
- Sequenced
- Full- duplex
- Reliable and accurate
- Error checking
- Segment (20 to 24 bytes)
- Windowing Flow control

2. UDP – User Datagram Protocol

- Connection-less
- Fast
- No acknowledgement
- Un sequenced
- No windowing or flow control

Internet Layer Protocols

1. **IP** – Internet Protocol
2. **ICMP –** Internet Control Message Protocol

- It is a management protocol and messaging service provider for IP

3. **ARP-** Address Resolution Protocol

- finds the MAC address of the host from a known IP address

4. **RARP** – Reverse Address Resolution Protocol

- Requests for IP address with help of MAC address in diskless machines

IP HEADER

Source IP address	131.107.7.29
Destination IP address	131.107.3.44
Protocol	TCP or UDP
Checksum	4 DF 5
Time To Live [TTL]	60

TTL – value which determines how long the packet lives on the wire before it's discarded

IP on the router

- Decrements the TTL
- Calculates new checksum
- Obtains hardware address
- Forwards the packet

In IP layer, the packet is defragmented into three parts. Each part has the following information (header)

Eg**. FLAG**
Indicates other fragment follows
Flag is not added to the last packet because no other fragments follow it

FRAGMENT ID
Identify all fragments that belong together

FRAGMENT OFFSET

IP ADDRESS [32 bit – 4 octets] IPV 4

IPV 4 – 32 bits
IPV 6 – 128 bits

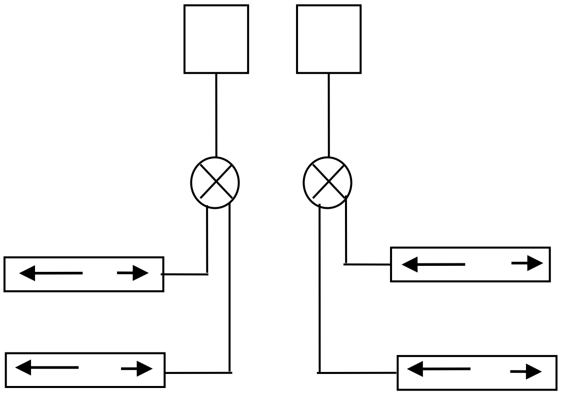
Subnet mask
Class A – 255.0.0.0
Class B - 255.255.0.0
Class C - 255.255.255.0

Subnetting

- Reduce network traffic
- Optimized network performance
- Simplified management
- Facilitates spanning of large geographical distances

0741CISCO LAYERS

1. Core Layer :
   Responsible for transporting large amounts of traffic both reliably and quickly. To switch traffic as fast as possible.
2. Distribution layer (workgroup layer) :
   Routing
   Implementation of tools such as access lists, packet filtering, address translation , firewall
   Redistribution between routing protocols, including static routing
   Routing between VLANs , and other workgroup support functions
   Definitions of broadcast and multicast functions
3. Access layer (desktop layer)
   Static routing, demand dynamic routing and Ethernet switching



CISCO HARDWARE BASICS

ROUTER

1. Microprocessor (MOTOROLA)
2. Motherboard / Chipsets
3. Memory
   Dynamic RAM (volatile) – current configuration file [Running – config]
   NVRAM [Non Volatile] – shared configuration file [Starter – config]
   FLASH - IOS resides
   ROM [BIOS]
   - POST
   - BSL – Boots from : FLASH / TFTP / MINI IOS
   - MINI IOS
4. Interfaces
   Console [con 0]
   Asynchronous serial port [RS 232]
   Connects to Com port of the system
   Auxilary port [Aux 0]
   For remote configuration
   Supports modem
5. LAN Interface

AUI [Attachment User Interface]
Ethernet E 0
Others - Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI

6. WAN Interface
   i. Serial 0
   ii. Serial 1
   iii. Others: ISDN, Frame Relay, ATM, DSL, VOIP
7. I / O Slots

EDITING TOOLS

Ctrl A – move cursor to beginning of the line
Ctrl E - move cursor to end of the line
Esc B - move cursor back one word
Esc F - move cursor forward by one word
Ctrl B - move cursor back by one character
Ctrl F – move cursor forward by one character
Ctrl D or Backspace – deletes a single character
Ctrl U – Erase a line
Ctrl R – redisplays a line
Ctrl W – erase a word
Ctrl Z – ends the configuration mode and returns to Exec mode
Tab – finishing typing a command
Ctrl P – shows last command typed
Ctrl N – shows previous command entered

IOS BASIC COMMANDS

Router >?	Help
Router > show?	Lists all the commands in Show
Router > s?	Lists all the commands starting with 'S'
Router > show terminal	shows terminal configuration and history buffer size
Router > show version	shows the version
Router > show flash	shows details of 'flash'
Router > enable	to enter privilege exec mode
Router # show history	show last ten commands
Router # terminal history size 20	to set history size to 20
Router # show running-configuration	to display contents of Dynamic RAM

SETTING PASSWORDS

1. To set console password

```
Router>enable
Router# config t
Router (config)# line console 0
Router (config-line) # login
Router (config-line) # password <pw>
Router (config-line) # Ctrl Z
Router# wr – to save the settings
```

2. **To set privilege password**

```
Router>enable
Router# config t
Router (config) # enable secret <pw>
Router (config) # Ctrl Z
Router# wr
```

3. **To set telnet password**

```
Router>enable
Router# config t
Router (config) # line vty 0 4
Router (config-line) # login
Router (config-line) # password <pw>
Router (config-line) # Ctrl Z
Router# wr
```

4. **To set auxiliary password**

```
Router>enable
Router# config t
Router (config) # line aux 0
Router (config-line) # login
Router (config-line) # password <pw>
Router (config-line) # Ctrl Z
Router# wr
```

5. Encrypting password

```
Router>enable
Router# config t
Router (config) # service password-encryption
Router (config) # Ctrl Z
Router# wr
```

6. To recover passwords

- The default configuration register value is 0 * 2102
- To ignore NVRAM content register value is 0 * 2142

Step 1. Press Ctrl + Break when router boots

Step 2 types 0 after creating break

```
>0
>o/r 0 * 2142
> I
..
..
Want to go to setup mode [Y/N]: N
```

NAT – NETWORK ADDRESS TRANSLATION

NAT allows a host that does not have a valid registered IP address communicate with other hosts through the internet

NAT uses a valid registered IP address to represent the non-registered IP address

PRIVATE ADDRESS

- Non-registered IP address used inside a network

RANGE **IP ADDRESS**

CLASS A – 10.X.X.X (10.0.0.0 to 10.255.255.255)
CLASS B - 172.16.X.X (172.16.0.0 to 172.31.255.255)
CLASS C - 192.168.X.X (192.168.0.0 to 192.168.255.255)

NAT - Static
Dynamic
Overloading

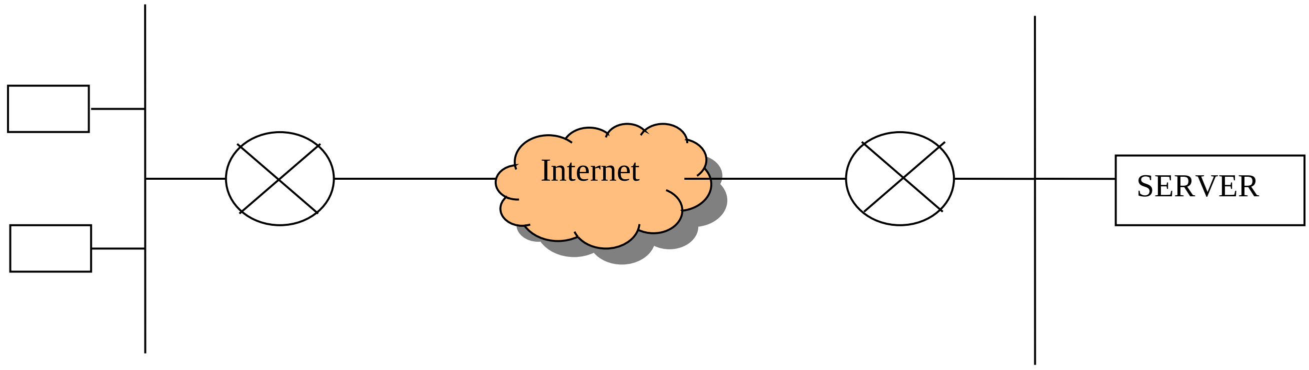
Static NAT

1 private address: 1 public address

Eg:	private	public
	10.1.1.1	200.1.1.1
	10.1.1.2	200.1.1.2
	10.1.1.3	

```
Router (config) # IP nat inside source static
                    192.168.10.1.  200.1.1.1
Router (config) # int e 0
Router (config# ip nat inside
Router (config) # int s 0
Router (config) # ip nat outside
Router# show ip nat translation
```

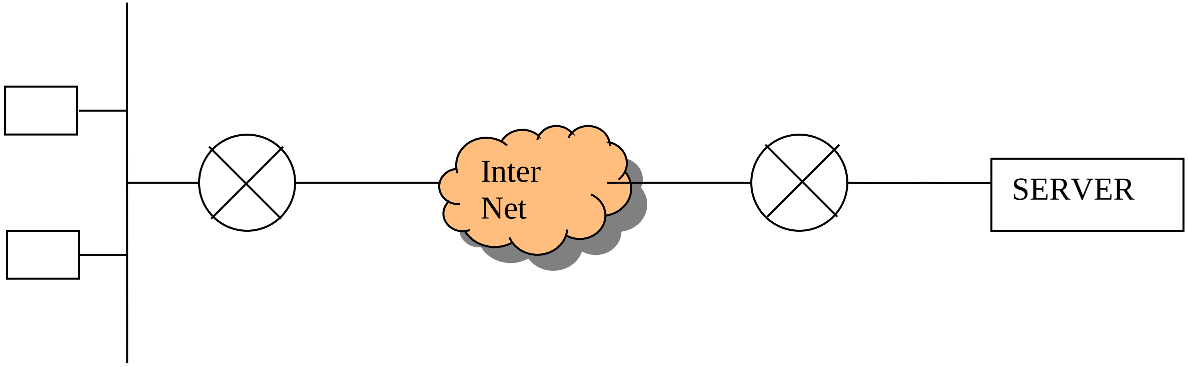
Static NAT



Dynamic NAT

- Sets up a pool of possible inside Global address and defines criteria for the set of inside local IP addresses whose traffic should be translated with NAT
- Address is dynamically assigned

Dynamic NAT



Dynamic NAT

```
Router(config)# access-list / permit 192.168.10.0  0.0.0.255
Router(config)# ip nat inside source list / pool hcl
Router(config)# ip nat pool hcl 200.0.0.1  200.0.0.5  netmask 255.255.255.0
Router(config)#int e 0
Router(config)# ip nat inside
Router(config)#int s 0
Router(config)#ip nat outside
Router(config)#debug ip nat     [*ping from source]
Router(config)#show ip nat translation
```

PAT

```
Router(config)#ip nat inside source list / pool hcl overload
Router(config)#ip nat pool hcl 200.1.0.1  200.0.0.2  netmask 255.255.255.0
Router(config)#int e 0
Router(config)#ip nat inside
Router(config)#int s 0
Router(config)#ip nat outside
Router(config)#debug ip nat   [ *telnet from source]
Router(config)#show ip nat translation
```

Overloading NAT with PAT

PAT – Port Address Translation

to support lots of inside local IP addresses with only a few inside Global, publicly registered IP address, NAT overload uses PAT. Instead of just translating the IP address, it also translates the port number.

IP ROUTING

1. Static
2. Default
3. Dynamic

Static Routing

Administrator manually adds routes in each router's routing table.

Command
Ip route < destination network > < mask > < next hop add or exit interface > < administrative distance > < permanent
Eg. Ip route 192.168.10.0   255.255.255.0   192.168.20.1

To show routing table

```
# show ip route
```

Default Routing

Used in sub network where there is only one way

```
Ip route 0.0.0.0   0.0.0.0   192.168.20.1
```

Administrative distances

Rate the trust worthiness of routing information received on a router from a neighbour router.

Default administrative distance

Connected interface	0
Static route	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
External EIGRP	170
Unknown	255 (this route will never be used)

DYNAMIC ROUTING

Protocols are used to find networks and update routing tables on routers
Routing protocols
Used to determine the path. Eg. RIP, IGRP, OSPF, etc.
Routed protocols
That carries the packets, e.g. IP, IPX, and AppleTalk.

Routing protocols

* Interior Gateway Protocols- used to exchange information inside the same autonomous system.
* Exterior Gateway Protocols - to communicate between autonomous systems. Eg. BGP

IGP → **Distance vector → RIP, IGRP**
→ **Link State → OSPF, NLSP**
→ **Hybrid → IS-IS, EIGRP**

RIP → Routing information protocol
IGRP → Interior Gateway Protocol (Cisco proprietary)
OSPF → Open Shortest Path First
NLSP → Network Link Service Protocol
IS-IS → Intermediate System- Intermediate System
EIGRP → Enhanced IGRP (Cisco proprietary)

RIP	**IGRP**
1. Max. hop is 15	Max. is 255, default is 100
2. Metric is hop	Composite metric (Bandwidth and Delay) default Also Reliability, load and MTU (Maximum Transmission unit)
3. No asynchronous	uses autonomous system no.
4. Full route table update every 30 sec	90 sec
5. Administrative Distance 120	100
6. Route by 'R'	Route specified by 'I'

RIP V1	**OSPF**
1. Maintains one table.	Maintains 3 tables A. routing table B. topology table C. neighboring table
2. Maintains one path to destination	maintains multiple path
3. advertise / update every 30 sec	every 30 mins
4. Advertise are broadcast packets.	Multicast packets
5. Entire routing table advertised.	Only changed entries
6. High traffic, bandwidth consumption And full in performance.	less traffic, no bandwidth consumption
7. The metric is hop.	Bandwidth, time delay, cost, traffic.
8. Max. Hop is 15, 16 th unreachable.	Unlimited.
9. Doesn't support classless routing.	Support classless routing.
10. The route specified by 'R'.	Route specified by 'O'.
11. Administrative distance is 120.	AD is 110.
12. Delay in convergence.	No delay in convergence.
13. Bellmanford Algorithm.	Dijkshetra Algorithm.

EIGRP

1. Multiple path to destination.
2. Classless routing.
3. Cisco proprietary protocol.
4. Supports IP, IPX, Appletalk.
5. DUAL Algorithm (Diffusion Update Algorithm)
6. Reliable Transport protocol (RTP) for advertise.
7. Multiple autonomous systems in same router.
8. AD is 90.
9. Route is 'D'.
10. Metric – Bandwidth, time delay, cost, traffic.

<u>Extra commands to verify the configuration</u>

```
# show protocols →displays all the routed protocols and the interfaces upon which is enabled
# show ip protocols → shows only ip protocols
# debug ip rip
# debug ip igrp events → source destination updates and no. of routers
# debug ip igrp transactions → show transactions
# undebug all  → to turn off debugging
```

Or

```
# un all
```

<u>Configuration of RIP</u>

```
Router ( config ) # router rip
Router ( config-router ) # network 192.168.10.0 ( e 0 )
Router ( config-router) # network 192.168.20.0 ( s 0 )
Router ( config-router ) # exit
Router # show ip route
```

OSPF used LSO (Link State Update) – to indicate the other router to update with the new link status, when the old fails.

RIP propagations

```
Router ( config-router) # passive-interfaces s 0
```

Allows receiving rip updates but does not send out any updates

Configuring IGRP

```
# router igrp 10
# network 192.168.10.0
# network 192.168.20.0
```

<u>EIGRP</u>

- classless , distance vector protocol
- communicates with other routers via, RTP (Reliable Transport Protocol)
- selects the best path via Diffusing update algorithm (DUAL)
- Supports IP, IPX, Appletalk
- Supports multiple autonomous system on a single router
- Supports VLSM and summarization
- Metric – bandwidth, delay ,load and reliability

<u>Configuration EIGRP</u>

```
Router # config t
Router ( config ) # router eigrp 20
Router ( config-router) # network 192.168.10.0
Router ( config-router ) # network 10.0.0.0
```

To prohibit the interface from sending or receiving hello packets

```
Router ( config ) # router eigrp 20
Router ( config-router ) # passive-interface s 0
```

Verifying EIGRP

```
# show ip route eigrp
# show ip eigrp neighbors
# show ip eigrp topology
```

Trace route command

```
Router # trace route 192.168.10.2
```

Open Shortest Path First [OSPF]

OSPF calculates the best/shortest path to every network in the same area based upon the information collected in Topology database and algorithm called SPF (shortest path first)

Configuration

```
Router( config) # router Ospf 20
                # Network 10.0.0.0    0.255.255.255    area 0
```

Very configuration

```
                # show ospf interface
                # show ip ospf neighbour
                # show ip protocols
                # show ip ospf database
```

ACCESS CONTROL LISTS

- Standard [1-99] [1300- 1999]
- Extended [100-199] [2000-2699]
- Named access list

Standard – all decisions are made based on source IP address

Router (config) # access-list < number > [deny/ permit] [host any]

```
Router ( config ) # access-list 10 deny host 172.16.30.2   ( to deny a single host)
Router ( config ) # access-list 10 deny 172.16.30.0    0.0.0.255
Router ( config ) # access-list 10 permit any
Router ( config) # int e 0
Router ( config-if) # ip access-group 10 in

Router ( config-if) # int s 0
Router ( config-if) # ip access-group 10 out

        # Show ip interface
        # Show access-list [access-list no/ access-list name]
        # Show ip access-lists [access-list no/ access-list name]
        # show running-config
```

Extended Access list

Checks source address and as well as destination address. It can block depending upon port no.

```
# ip access-list 101 permit tcp 12.0.0.0   0.0.0.0   10.0.0.1   0.0.0.0   eq  21
# ip access-list 101 permit tcp 12.0.0.3   0.0.0.0  eq 23
# ip access-list 101 deny tcp host 12.0.0.5
# ip access-list 101 permit ip any any
```

Standard access list

```
# ip access-list standard siva
Std- nacl # deny 12.0.0.0
            # permit any
            # exit

# int e 0
# ip access-group siva out
```

WAN TECHNOLOGIES

Types of WAN connections

1. Leased line connections
2. Circuit switched connections
3. Packet switched connections

Leased-line connections

- can be called a point-to-point (dedicated connection)
- Provides a single, pre-established WAN communication path.
- Synchronous
- Speed T3 (45 Mbps)
- Synchronous communications involve digital signals that are transmitted with precise clocking
- Very expensive.

Circuit-switching

- provides a dedicated physical circuit, which stays in place between the sender and the receiver for the duration of the communication session.
- Telephone company network uses the system to provide basic telephone services or (ISDN – Integrated Services Digital Network)
- Basic telephone services are asynchronous serial communication.

Packet-switching

- Packet-switching method involves network devices sharing a single point-to-point link.
- Point-to-point link is used to transport packets from source to destination over a telecommunication carrier network.
- Statistically programmed switching devices provide physical connections
- Packet headers are used to identify the destination
- Less expensive
- Synchronous serial lines
- Speed 56 Kbps (T3)

Physical items needed for WAN link

1. Customer Premises Equipment (CPE)
2. A Demarcation (DEMARC)
3. A Local loop (last mile) – copper wire
4. a central office (CO) switch
5. a full network

Types of serial cable supported by CISCO devices

Serial cables can support leased-lines and packet-switched connections.

1. EIA / TIA – 232
2. EIA / TIA – 449
3. EIA / TIA – 530
4. X.25
5. V.35

DTE – Data Terminal Equipment is your CPE.

DCE – Data Communication Equipment – to convert the user data from DTE into a form that's acceptable to the WAN service provider.

The synchronous serial ports can be configured a either DTE or DCE, depending on the attached cable.

EIA / TIA – 530 serial ports can be configured as DTE only.

- External clocking from the channel service unit/ data service unit (CSU/DSU) or other DIC device is needed when the port is configured as DTE.
- When traffic is crossing the WAN link, each WAN connection uses a protocol to encapsulate it.
- WAN encapsulation protocols operate at layer 2 of the OSI model.
- The choice of encapsulation protocol depends on the WAN technology and the communication equipment.

WAN protocols

1. HDLC –High-level Data Link Control
2. PPP – Point-to-point protocol
3. SLIP – Serial Line Interface protocol
4. X.25
5. Frame Relay
6. ATM – Asynchronous Transfer Mode

HDLC – frame format

HDLC

- The default encapsulation type on point-to-point ,dedicated link is HDLC.
- It's typically used for communication between two Cisco devices and is a bit-oriented synchronous protocol.

SLIP

- SLIP predates PPP.
- It uses a variation of TCP/IP and is a standard protocol for point-to-point serial connections

PPP

- PPP provides router-to-router and host-to-network connections over synchronous and asynchronous circuits.
- Can work with IP and IPX.
- Security mechanisms such as PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication protocol) are built into PPP.

Configuring PPP

```
Router ( config ) # int s 0
Router ( config-if ) # encapsulation PPP
Router ( config-if ) # exit
```

Configuration PPP authentication

Step 1. Setting username, password for remote router connecting to your router

```
Router ( config )# hostname Router A
Router A ( config )# username Router B password Cisco
Router A ( config )#  # exit
```

Step 2. Configuring PAP or CHAP

```
Router A ( config ) # int s 0
Router A ( config-if ) # PPP authentication chap pap
Router A ( config-if ) # exit
```

Verifying PPP encapsulation

```
Router A # show int s 0
```

PAP contains four main components

1. A physical layer International Standard for serial communication. i.e. EIA/TIA 232 C, V.24, V.35, and ISDN.
2. A method for encapsulating datagram over serial links. i.e. HDLC.
3. A method of establishing, configuring, maintaining and terminating the point-to-point connection. LCP – Line Control Protocol
4. NCP – Network Control Protocol – to allow communications of multiple network layer protocols.

PPP Session Establishment

1. Link-Establishment Phase – uses LCP.
2. Authentication Phase
   a. CHAP (Challenge Handshake Authentication protocol)
   b. PAP (Password Authentication Protocol)
3. Network Layer protocol phase – NCP

X.25

* It is a ITU-T standard (International Telecommunication Union – Telecommunication Standardization sector .
* It is an International body that develops world wide standards for telecommunication technologies.
* It defines how connections between DTE and the DCE are maintained.
* These connections are used for remote terminal access and computer communication in public network.
* X.25 is a precursor of frame relay, and it specifies Link Access Procedure Balanced (LAPB), which is a data-link layer protocol.

Frame Relay

- It is an Industry Standard Protocol.
- It can handle multiple virtual circuits, and is streamlined to cut out some of the lengthy processes that X.25 employs.

ATM

- It is an International Standard for cell relay.
- Cell relay is a network technology based on the use of small, fixed-size packets or cells.
- It allows data, voice, and video to be conveyed in fixed-length cells of 53 bytes.
- Fixed-length cells reduce transportation delays by allowing processing to occur in hardware.
- ATM used high speed transmission media such as

1. E3 (45 Mbps)
2. T3 (56 Kbps)
3. SONET (Synchronous Optical Network)

Configuring 1900 Series Switch

1. User(s) how active on management console
2. User interface menu

```
[m] menus
[k] Command line
[i] ip configuration

Enter selection: k

Switch > enable
Switch # config t
Switch ( config ) #  enable password level 1 Cisco
```

(setting password for user mode)

```
Switch ( config ) # enable password level 15 Cisco
```

(setting password for enable mode)

```
Switch ( config ) # enable secret Cisco
```

(setting secret password for enable mode)

```
Switch ( config ) # hostname 1900switch
```

(setting hostname)

```
                # ip address 192.168.10.1 255.255.255.0
                # ip default-gateway 192.168.10.2
```

To show VLAN information

```
Switch # show vlan brief
```

To show information about VLAN 2

```
Switch # show vlan id 2
```

To view the Spanning Tree information for a VLAN

```
Switch # show spanning-tree vlan 2
```

Assigning IP address to a switch

Reason - * for using Telnet
To connect to router for inter-vlan

* IP address should be given to default vlan i.e. vlan 1

```
Switch > enable
Switch # config t
Switch ( config ) # int vlan 1
Switch ( config –if ) # ip address 172.16.10.3 255.255.255.0
Switch ( config –if ) # no shutdown
Switch ( config –if ) # exit
Switch ( config ) # ip default-gateway 172.16.10.1
Switch (config ) # exit
```

ISDN – Integrated Services Digital Network

ISDN Switch types

	Type	**Keyword**
1.	AT/T basic rate switch	basic-5 ess
2.	Nortel DMS – 100 basic rate switch	basic-dms 100
3.	National ISDN-1 switch	basic-ni
4.	AT & T 4 ess (ISDN Pri only)	Primary- 4 ess
5.	AT & T 5 ess (ISDN Pri only)	Primary-5 ess
6.	Nortel DMS -100 (ISDN pri)	Primary- dms 100

Dial-on Demand Routing (DDR)

```
Router A (config ) # ip route 172.16.60.2 255.255.255.255 bri 0
```

DDR with Access-lists

```
Router ( config ) # dialer-list 1 protocol ip list 110
                  # access-list 110 permit tcp any any eq smtp
                  # access-list 110 permit tcp any any eq telnet
                  # int bri 0
                  # dialer-group 1
```

Configuring the Dialer information

```
Router ( config ) # int bri 0
                  # ip address 172.16.60.1 255.255.255.0
                  # no shut
                  # encapsulation PPP
                  # dialer-group 1
                  # dialer string 8350661
```

Or

```
                  # dialer map ip 172.16.60.2 name Router B 8350661
```

Basic Rate ISDN (BRI)

- 2 B + D = 16 Kbps
- 2 B = 64 Kbps
- Q 921 & Q 931 for D channel signaling
- SS 7 to set up the path

Configuring ISDN

```
Router A > enable
Router A ( config ) # isdn switch-type basic-dms 100
Router A ( config ) # int bri 0
Router A ( config-if) # encapsulation ppp
                       # isdn spid 1
                       # isdn spid 2
```

SPID –Service provider identification

Verifying ISDN connections

```
# show dialer
# show isdn status
# show ip route
```

Frame-Relay configuration

```
Router ( config ) # int s 0
Router ( config-if) # encapsulation frame-relay ( cisco or ietf)
                     # ip address 192.168.10.1 255.255.255.0
                    # frame-relay lmi-type ansi
                     # frame-relay interface-dlci 101
                     # exit
```

Monitoring frame relay

```
        # show frame lmi
        # show frame pvc
        # show int s 0
```

LMI – Local Management Interface

- signaling standard used between the router and first frame relay switch
- Standards are * CISCO
    - ANSI
    - Q.933A

DLCI – Data Link Connection Identifier (!6-1007)

- Given by the service provider to identify the PVC (Permanent Virtual Circuit)
- IETF – Internet Engineering Task Force

Resolving hostnames

1. Building host table
2. using DNS

1. Building host table

- IP host < hostname > < tcp port no > < ip address >

Eg. Router (config) # ip host iiht 192.168.10.1

To see the host table

Router # show hosts

2. Using DNS

```
Router (config )# ip domain-lookup
                  # ip name-server 192.168.10.1
                  # ip domain-name iiht.com
                  # exit
```

SWITCHING

- Ethernet switches operate at layer 2 of the OSI model and function in a similar way to bridges.
- Ethernet switches and bridge forward and filter traffic based on MAC address.
- Switches and bridges identify host locations through a process known as Address learning.
- Switches and bridges provide Loop avoidance function in a network.
- When a switch is first initialized, it's MAC data base is empty. So it forwards the received message to all its port. This is known as Flooding.
- IEEE 802.1 Specifications defines a time limit of 300 seconds for MAC database entries to remain in the database.
- When the frame reaches the switch, the destination MAC address is compared to the entries in the MAC database. The switch then transmits the frame only to the port which matches the MAC address. This is known as FRAME FILTERING.
- Bridged and Switched networks are often designed with Redundant devices and links in order to prevent a single point of failure in a network.
- Redundant systems can cause bridge loops . ie problems caused due to bridge loops.

a. Broadcast storms
b. Multiple frame copies
c. Instability in the MAC database.

- Some layer-3 protocols use Time to line (TTL) mechanism which eliminates looping packets.
- TTL – Field in IP header to indicate how long a packet can travel before it is returned or discarded.
- Layer-2 protocols like Ethernet are unable to prevent packets from endlessly looping.
- To prevent broadcast storms, multiple frame copies and MAC database instability, a loop avoidance mechanism is used. i.e. SPANNING – TREE PROTOCOL (STP)
- STP is a link – management protocol that allows redundant systems to exist in the network but prevents undesired bridge loops.
- STP is a part of IEEE 802.LD standard , so it can function with complaint bridge and switches from other vendors.
- STP works by forcing certain redundant data paths into a standby or blocked state.
- When the topology of the network changes, STP reconfigures bridge ports to prevent the creation of new loops or loss of connectivity.
- Each port on a bridge or switch is included in STP support.
- All switches in a LAN participating in STP gather information on other switches in the network through an exchange of data messages. This is known as BRIDGE PROTOCOL DATA UNITS (BPDU)

ROOT BRIDGE ELECTION

Default priority of the bridges is 32,678
Root bridge will be a bridge with less Bridge ID. If the bridge ID is same for all the bridge, then the MAC address is considered. A bridge with less MAC address will be the rest bridge.

Root path cost
Path cost = 1000 / speed in Mbps

Port Speed	**STP Cost**
1 Gbps	1000/1000 = 1
100 Mbps	1000/10 = 10
10 Mbps	1000/10 = 100
56 Kbps	1000/56 = 17857

Root path will be path with less cost.

BPDU- BRIDGE PROTOCOL DATA UNITS

Information	**Length**
Protocol 10	2 bytes
Version	1
Type	1
Flags	1
Root B ID	8
Root path cost	4
Sending B ID	8
Port ID	2
Message age	2
Max. age	2
Hello time	2
Forward delay	2

Bridge ID
Bridge priority + MAC address
16 bytes + 48 bytes

Root Path Cost
Cost of the path from the Root Bridge, identified by the bandwidth.

Root Port
Port connected to the root bridge.

Designated port
Port coming out of a root bridge towards the destination.

Difference between Bridge and Switch

	Bridge	Switch
1.	Software based	Hardware based, it operate with ASIC.
2.	Uses software based STP process	Application-specific Integrated Circuits and a high-capacity switching bus.
3.	Slower	faster
4.	One spanning tree instance per port	many spanning tree instance per port
5.	Less number of ports (max. 16)	more number of ports (>100)
6.	Used to separate LAN traffic into segments	used to connect directly to end-users and other switches.
7.	Cannot offer dedicated bandwidth to each segment	can offer dedicated Bandwidth to end users.

Two ways of transmitting frame through a switch

1. **Store- and – Forward**
   a. Forwarding does not take place until the entire frame has been received by switch.
   b. Switch reads the destination and source address and performs CRC to ensure the frame is not damaged.
   c. If damaged, the frame is discarded.
   d. Latency time is high since it has to check the frame and also varies with regard to size of the frame.

Latency time is the delay between receiving a frame and forwarding

2. **Cut-through**
   a. Forwards the frame just by seeing the destination address only.
   b. Latency time is constant and less.

VLAN

1. Static - Administrator creates VLAN.
2. Dynamic – uses VMP3 (VLAN management policy server) to create VLANs.

Creating VLANs

```
1900 (config) # vlan 2 name sales
               # Vlan 3 name mark
               # Exit
 # Show vlan
```

Assigning switch ports

```
1900 ( config ) # int e 0/2
               # vlan-membership static 2
               # int e 0/3
               # vlan-membership static 3
```

Configuring trunk port

```
1900 ( config ) # int f 0/2l
              # trunk on
```

- 1900 switch only runs on DISK (Dynamic ISC) encapsulation.

VTP – VLAN Trunk Protocol

1. Messaging protocol that is used to distribute VLAN Configuration information.
2. Supports mixed-media backbones.
3. Takes control of addition, detection, and name changes on the network.

A VTP management domain can be either one switch or multiple interconnected switching sharing the same VTP server.
VLANs are not propagated over the network until 2 VTP domain name is specified or discovered.

VTP operates in three modes.

1. Server (default)
2. Client
3. Transparent

Server mode

- A switch acting at this mode can create, delete and modify VLAN's for the entire VTP domain.
- Advertise its VLAN configuration
- Synchronize its VLAN configuration with information received from other devices in the domain.
- Forward VTP advertisements received from other switches in the domain.
- It saves VLAN configuration into NVRAM and recreates VLAN whenever the switch is booting.

Client mode

- create VTP advertisements
- synchronize its VLAN configuration
- forward VTP messages.
- VTP transparent switch can create and modify VLANs. But it is confined to the local switch only. It is not transmitted to other switches in the domain.
- Does not participate in domain.

** VTP advertisements are automatically sent every five minutes or whenever a change occurs in a VLAN configuration. Advertisement includes 1. configuration-revision number.

*** **VTP PRUNING**- technique that uses VLAN advertisements to determine when a trunk connection is flooding messages unnecessarily.

Configuring VTP

```
1900 ( config ) # vtp server
                # vtp domain iiht
                # vtp password cisco
```

To see domain status, use

```
# show vtp ( statistics )
```

To configure VLAN

Step 1. Configure VTP (optional)
Step 2. Enable trunking
Step 3. Create VLAN’s
Step 4. Assign switch ports to one or more VLAN’s
Step 5. Configure a router for inter-VLAN communications (optional)

Step 1. Configure VTP

```
Switch > enable
Switch # vlan database
Switch ( vlan ) # vtp domain iiht
Switch ( vlan ) # vtp server
Switch ( vlan ) # exit
Switch ( vlan)
```

To show the VTP details

```
Switch # show vtp status
```

Step 2. To enable Trunking

```
Switch # config t
Switch ( config ) # int fa 0/24
Switch ( config ) # switch port mode trunk
```

Step 3. Configuring VLAN

```
Switch > enable
Switch # vlan database
Switch (vlan) # vlan 2 names Siva
Switch (vlan) # vlan 3 name kumar
  ……….
………..
Switch ( vlan ) # exit
```

Step 4.   Configuring ports

```
Switch > enable
Switch # config t
Switch ( config ) # int fast Ethernet 0/2
Switch ( config-if ) # switch port mode access
Switch ( config-if ) # switch port access vlan 2
Switch ( config-if ) # int fast Ethernet 0/3
Switch ( config-if ) # switch port mode access
Switch ( config-if ) # switch port access vlan 3
……………..
…………………
                         # Exit
```

Step 5. Configuring router for Inter-VLAN

```
Router > enable
Router # config t
Router ( config ) # int fa 0/0
Router ( config-if ) # no ip address
Router ( config-if ) # no shutdown
Router ( config-if ) # int fa 0/0.1
Router ( config-subif ) # ip address 172.16.0.1 255.255.0.0
Router ( config-subif ) # encapsulation dot1q 1
Router ( config-subif ) # int fa 0/0.2
Router ( config-subif ) # encapsulation dot1q 2
Router ( config-subif ) # ip address ……………
………………
Router ( config-subif ) # exit
```

<u>CDP – Cisco Discovery Protocol</u>

- to collect information about both locally attached and remote devices
- can gather hardware and protocol information about neighbour devices

CDP timers and hold time information

```
Router # sh cdp
Sending packets every 60 sec
Sending hold time value of 180 sec
```

To configure cdp timer and hold time

```
Router ( config) # cdp timer 90
Router ( config ) # cdp hold time 24
Router ( config ) exit
```

To turn off cdp completely

```
Router ( config ) # no cdp run
```

To turn off cdp for an interface

```
          # no cdp enable
```

To turn on cdp for an interface

```
                    # cdp enable
```

Gathering cdp information

1. # sh cdp neighbour
2. # sh cdp neighbor detail
3. # sh cdp traffic

STP

- Definition – allows link redundancy and prevents layer two loops
- Port states
- BPDO
- Root election
- Root path cost
- Root and designated ports
- Convergence
-

Port States

Turn on the switch → Blocking → Enabled
→ STP Disabled

1. Listening – the port listens for any message regarding the blocking state. This listening time is known as Forward Delay Timer (default is 15 sec)
2. Learning (default 15 sec) – if no message is received regarding the blocking state till 15 secs the ports moves to the learning state. In learning state, the switch identifies where it is located in the topology and maintains a database for forwarding. ie. Is known as Forwarding database
3. Forwarding state – forwards the data

NAT – Network Address Translation

- allows a host that does not have a valid registered IP address communicate with other hosts through the internet
- NAT used a valid registered IP address to represent the non-registered IP address.

Private Address

- non-registered IP address used inside a network

Range

Class C – 10.X.X.X (10.0.0.0 to 10.255.255.255)
Class B - 172.16.X.X (172.16.0.0 to 172.31.255.255)
Class C - 192.168.X.X (192.168.0.0 to 192.168.255.255)

NAT

- Static
- Dynamic
- Overloading

Static NAT

1 private address: 1 public address

E.g. Private	public
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

Static NAT

```
Router ( config) # ip nat inside source static 192.168.10.1    200.1.1.1
Router ( config ) # int e 0
Router ( config )   # ip nat inside
Router ( config ) # int s 0
Router ( config ) # ip nat outside
Router # show ip nat translation
```

Overloading NAT with PAT

PAT – Port Address Translation

- to support lots of inside local IP addresses with only a few inside global, publically registered IP address. NAT overload uses PAT. Instead of just translating the IP address, it also translates the port number.

PAT

```
    Router ( config )  # ip nat inside source list 1 pool hcl overload
                       # ip nat pool hcl 200.0.0.1  200.0.0.2 netmask 255.255.255.0
                        # int e 0
                        # ip nat inside
                        # int s 0
                        # ip nat outside
                        # debug ip nat ( * telnet from source )

                        # show ip nat translations
```

Dynamic NAT

- Sets up a pool of possible inside global address and defines criteria for the set of inside local IP addresses whose traffic should be translated with NAT.
- Address is dynamically assigned.

```
Router ( config ) # access-list 1 permit192.168.10.0   0.0.0.255
Router ( config ) # ip nat inside source list 1 pool hcl
Router ( config ) # ip nat pool hcl 200.0.0.1   200.0.0.5 netmask 255.255.255.0
Router ( config ) # int e 0
Router ( config ) # ip nat inside
Router ( config ) # int s 0
Router ( config ) # ip nat outside
                 # debug ip nat ( * ping from source )
```

Password recovery

Enable - go to privilege mode

```
Router # copy startup-config running –config
Router # config t
Router ( config ) # enable secret        < pw > → change pw
Router ( config ) # exit
Router ( config ) # config-register 0*2102      → to reset original configuration
Router # copy running-config startup-config
```