OSI Model A P S T N D P

Upper layers7, 6, 5 don't deal with data delivery, provide standardization of how applications share data and communicate with one another.

7. **Application –** Doesn't provide services to the other layers, but it does communicate with user applications and selects the appropriate network application for those applications.
6. **Presentation** - Data representation, encryption, and compression. Supports different protocols for text, data, sound, graphics, and images. (ASCII, EBCDIC, MIDI, MPEG, GIF, JPEG, PICT, TIFF)
5. **Session** – Establishes, manages and terminates sessions between apps. A session is a dialog between Presentation layers of two or more systems. Protocols include NFS, SQL, ASP, and RPC.

Middle provides end-to-end data transportation services to the upper layers

4. **Transport**- Performs flow control by buffering, multiplexing, and parallelization. Provides end-to-end services by segmenting upper layers, establishing end-to-end connection, sending segments, and ensuring reliable data transport. Data Unit is Segments.

Lower

3. **Network** – Determines the best path from one network to another (path determination), packet switching, also known as the domain of routing. Routers work at this layer. Uses routing protocols (RIP, OSPF), and routed protocols (IP, IPX) to provide logical addresses. Data Unit is Packets
2. **Data Link -** Made up of the LLC and MAC sublayers. Bridges/switches work at this layer. Allows upper layers to work independently of the physical media. Performs physical hardware addressing, Optional flow control, and error notification. LLC (Logical Link Control) is where framing occurs by the IEEE standards. MAC sublayer deals with hardware functions and maintains the physical address (48 bits, burned onto card by manufacturer) of the network card going into each host or gateway. Data Unit is Frames.
1. **Physical** - Where signals are converted to bits for transport across a LAN. Mechanical and electrical functions of the OSI model. Communicate with peer layers regarding activating, maintaining, and deactivating a circuit. Data Unit is Bits.

Devices at the OSI Layers

Device	Layer	Data Unit
Router	Network	Packets
Bridge	Data Link	Frames
Switch	Data Link	Frames
Hubs	Physical	Bits

5 Steps of data encapsulation:

1. User information is converted to **data** (App – Session)
2. Data is converted to **segments** (Transport)
3. Segments are converted to **packets** (Network)
4. Packets are converted to **frames** (Data Link)
5. Frames are converted to **bits** (Physical)

Connection Oriented vs. Connectionless (Transport)

Connection Oriented requires a unique session or pipe to be established (TCP). Setup and maintenance procedures are performed to ensure delivery of messages. Establishes a Virtual Connection between the two devices.

Connectionless can be sent any time to any destination without any setup or acknowledgement (UDP). It is up to the application to determine if the data gets to the destination, instead of the protocols. The advantage is that it is faster and more efficient since it doesn't have acknowledgements.

Routing Protocols

Distance Vector Routing - Routing protocols that send their routing tables to their neighbors; uses the distance to a remote network to find the best path (RIP and IGRP)

Counting to Infinity - Distance vector routing error that can be remedied by Maximum Hop Count, Split Horizons, Route Poisoning, and Hold-Down timers.

Link State Routing - Sends the state of its own interfaces to every router in the network; determines the entire network topology, then uses SPF (Shortest Path First) algorithm to find best route. (OSPF,EIGRP(hybrid DV+LS))

Link State routing problems - Router resource usage, bandwidth consumption, and update synchronization.

Solutions - Lengthening the update frequency, exchanging route summaries, using time stamps, or using sequence numbers can remedy the problems.

Routing Problems:

Convergence – Time it takes all routers to receive an update and agree on optimal routes through the internetwork.

Routing Loops - When two or more routers have not yet converged and are broadcasting inaccurate routes.

Routing Problems' Solutions:

Hold-downs - Prevent regular update messages from reinstating a route that is down.

Route Poisoning - If a router's connected network goes down, it sets its hop count to the maximum amount to make the network unreachable.

Split Horizons - Specify that a router can't send information about a route out the interface they originated from.

Maximum Hop Count - DV (RIP) permits hot count of up to 15. So a packet that is caught in a routing loop will only travel 15 hops, on the 16th the network is deemed unreachable and the packet is discarded.

Configuring Routing Protocols

Configuring Static Routes

Syntax:

```
ip route [dest] [mask] [next_hop | exit_int]
```

Example:

```
R_3(config)#ip route 192.168.1.0 255.255.255.0 serial0
```

Configuring RIP (Routing Information Protocol):

Syntax:

```
Router(config)#router rip
Router(config-router)#network <network #>
```

Example:

```
Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#network 192.168.1.0
```

Configuring IGRP (Interior Gateway Routing Protocol)

Syntax:

```
Router(config)#router igrp <autonomous system #>
Router(config-router)#network <network #>
```

Example:

```
Router(config)#router igrp 200
Router(config-router)#network 10.128.22.0
Router(config-router)#network 192.168.1.0
```

Checking Router Status Commands

Command	Effect
Basic Router Operations	
`enable | disable`	Enter privileged mode | exit to usr
`Ctrl+P`	Previous command
`Ctrl+N`	Next command
`Ctrl+A`	Move to beginning of the line
`Ctrl+E`	Move to the end of the line
`Ctrl+F`	Forward one character
`Ctrl+B`	Back one character
`Esc+B`	Moves back one word at a time
`Esc+A`	Moves forward one word at a time
`<shift>+<ctrl>+6 X`	Shift between telnet sessions
`<tab>`	Completes commands
Viewing Router Information	
`show version`	IOS Version Information
`show memory`	Memory statistics.
`show protocols`	Active network routing protocols.
`show running-config`	Current config in RAM.
`show startup-config`	Saved config in NVRAM.
`show interfaces`	Interface status + config.
`show flash`	IOS file and free space.
Cisco Discovery Protocol (CDP)	
`show cdp`	cdp info (broadcast holdtime).
`show cdp neighbor`	This shows all devices directly connected to the router, hold time, local and remote port, ID, platform and capability info.
`show cdp neighbor detail`	Adds IP / IPX addresses to above info.
`show cdp entry [*(all) | NAME]`	Shows info for all entries (*) or only one (NAME).
`show cdp traffic`	Shows traffic statistics.
`show cdp interface [type number]`	Display info about the interfaces on which CDP is enabled
`cdp run`	Enables CDP (global configuration)
`cdp enable`	Enables CDP for an interface (interface configuration mode)
`cdp timer` *seconds*	Specifies CDP updates frequency.
`cdp holdtime` *seconds*	Specifies the hold time to be sent in the CDP update packets.
TCP/IP	
`no ip routing`	Disables IP routing.
`show ip route`	View IP routing table.
`show ip interface`	IP interface info (IP access lists)
`debug ip rip`	Shows routing updates as they are received and sent.
`debug igrp events`	Shows a summary of the IGRP routing info that is running on the network.
`debug igrp transactions`	Show message requests from neighbor routers asking for updates and the broadcasts sent to them.
IPX/SPX	
`ipx routing`	Enables IPX and (enables RIP routing automatically).
`ipx maximum-paths <1-512>`	IPX load balancing. (default 1)
`show ipx route`	Views IPX routing tables.
`show ipx interface`	IPX interface info (IPX access lists)
`show ipx servers`	Lists the IPX servers discovered through SAP.
`show ipx traffic`	View info about the number and type of IPX packets transmitted and received.
`debug ipx routing activity`	Displays messages relating to IPX routing activity.
`debug ipx routing events`	Displays messages relating to IPX routing events.
`debug ipx sap`	Debug IPX sap packets
Backup Configurations	
`copy run start`	Copy current config to NVRAM
`copy start run`	Copy config from NVRAM to RAM
`copy run tftp`	Copy config to TFTP server
`copy tftp run`	Restore config from Server
`copy flash tftp`	Backup IOS to TFTP server
`copy tftp flash`	Restore IOS from TFTP server
`boot system flash [filename]`	Tells router which IOS file in flash to boot.
`boot system tftp [filename]`	Tells router which IOS file to request from tftp server
Set Passwords (Global Config Mode)	

`line con 0`
`line aux 0`
`line vty 0 4`
	-Selects Console
	-Selects Auxiliary
	-Selects Telnet

`login` `password` *cisco*	-Allows logins and -sets the password to *cisco*
`enable password` *cisco*	-Set password for privilege mode to *cisco*
`enable secret` *cisco2*	-Set encrypted password to *cisco2*

Configure Logical Addresses

TCP/IP -32 bits

Syntax:

```
Router#configure terminal
Router(config)#interface <type> <Number>
Router(config-if)#ip address <addr> <mask>
Router(config-if)#no shut
```

Example:

```
Router(config)#interface Ethernet 0
Router(config-if)#ip address 192.168.1.100
255.255.255.0
Router(config-if)#no shutdown
```

IPX (only configure network ID, MAC is used for host ID) –80 bits

Syntax:

```
Router#configure terminal
Router(config)#ipx routing
Router(config)#interface <type> <Number>
Router(config-if)#ipx network <#> encapsulation
<type>
Router(config-if)#no shutdown
```

Example:

```
Router(config)#ipx routing
Router(config)#interface Ethernet 0
Router(config-if)#ipx network 2aa encap arpa
Router(config-if)#no shutdown
```

Subinterfaces (For IP or IPX)

Syntax:

```
Router(config)#int <type> <#.subinterface #>
```

Examples:

IP

```
Router#configure terminal
Router(config)#interface serial 0.1
Router(config-subif)#ip address 192.168.1.1
255.255.255.0
```

IPX

```
Router(config)#int ethernet0.1
Router(config-subif)#ipx network 1 encap snap
Router(config-subif)#int ethernet0.2
Router(config-subif)#ipx network 2 encap sap
```

Configure DCE Serial Interface

Command or Prompt Level	Effect of Command
1. Prompt is `Router>`	
`enable`	Enters privileged mode.
2. Prompt changes to `Router#`	
`show controllers serial 1`	Tells you information about the physical interface itself, it also gives you the cable type and whether it is a DTE or DCE interface.
`configure terminal`	Enter Global Configuration mode.
3. Changes prompt to `Router(config)#`	
`interface serial 1`	Enter interface configuration mode.
4. Changes prompt to `Router(config-if)#`	
`clock rate 64000`	Changes clock rate to 64000 bits per second.
`bandwidth 56`	Bandwidth in Kilobits.
`no shutdown`	Brings up the interface.
`Ctrl+Z`	Exits Global Configuration mode.
5. Prompt changes to `Router#`	
`show interface s1`	Shows interface status and configuration.

FRAME RELAY

Viewing Configurations

`show frame-relay pvc [type number [dlci]]`	Lists all PVCs and DLCIs Type, number, & DLCI optional.
`show interface serial 0`	View DLCI and LMI info.
`show frame-relay map`	Display the current Frame Relay map entries.
`show frame-relay lmi`	View LMI statistics.

Enabling Frame Relay

`encapsulation frame-relay <type>`	Enables Frame Relay
`keepalive <seconds>`	Defines the keepalive interval, must be less than the switch default 10 sec

Frame Relay Encapsulation Types

`cisco`	Default
`ietf`	Used for connecting to non-Cisco equipment

Specifying LMI Type

`frame-relay lmi-type <type>`	Specifies LMI type

LMI Types

`cisco`	LMI defined by the Gang of Four (default).
`ansi`	ANSI standard T1.617 Annex D provides for 976 virtual circuit addresses and uses DLCI 0 as the management circuit.
`q933a`	ITU-T Q.933 Annex A, similar to ANSI T1.617 Annex D, uses DLCI 0 as a management circuit.

-**LMI** is a standard signaling mechanism between CPE (usually a router) and the Frame Relay connection. It provides the CPE with a local DLCI number and gives that DLCI number network-wide or local significance.

-IOS **11.2 and up**, supports LMI autosense, which enables the interface to automatically determine the LMI type.

PPP Point-to-Point Protocol

Point-to-Point protocol is a Data Link layer protocol that can be used over **asynchronous** serial (dial-up) and **synchronous** serial (ISDN) media and that uses the LCP (Link Control Protocol) to build and maintain data-link connections. The basic purpose of PPP is to transport layer-3 packets over a Data Link layer point-to-point link. PPP consists of two main components, **LCP** (Link Control Protocol - used to establish, configure, and test the connection) and **NCP** (Network Control Protocol - configures many different layer protocols).

NCP - A PPP protocol for negotiating OSI Layer 3 (the network layer) parameters.

HDLC -A method for encapsulating datagrams over serial links.

LCP -A protocol that establishes, configures, and tests data link connections used by the PPP Link Control Protocol offers PPP encapsulation different options, including the following:
Authentication - options includes PAP and CHAP
Compression -Data compression increases the throughput on a network link, by reducing the amount of data that must be transmitted.
Error Detection -Quality and Magic numbers are used by PPP to ensure a reliable, loop-free data link.
Multilink -Supported in IOS 11.1 and later, multilink is supported on PPP links between Cisco routers. This splits the load for PPP over two or more parallel circuits and is called a bundle.

PPP Session Establishment

Link-establishment phase -LCP packets are sent by each PPP device to configure and test the link. The LCP packets contain a field called the Configuration Option that allows each device to see the size of the data, compression, and authentication. If no Configuration Options are set, then the default config is used.
Authentication -If configured, either CHAP or PAP can be used to authenticate a link. Authentication only takes place before Network layer protocol information is read.
Network layer protocol phase -PPP uses the Network Control Protocol to allow multiple Network layer protocols to be encapsulated and sent over a PPP data link.

Configuring PPP

```
Router3(config)#int s0
Router3(config-if)#encapsulation ppp
Router3(config-if)#exit
Router3(config)#username Router2 password cisco
```

After you set the encapsulation to PPP, you have to exit to global configuration mode to set the username and password. The username is the hostname of the remote host connecting via PPP on the serial line; the password and encapsulation type must be the same for both routers.

Setting PPP Authentication

PAP-less secure of the two (sends passwords as plain text) *and* **CHAP** -uses a three-way handshake to force remote hosts to identify themselves after the link establishment phase is complete. The local router sends a challenge request to the remote device and the remote device sends a value calculated using a one-way hash function called MD5 (encryption).

```
Router3(config)# int s0
Router3(config-if)#ppp authentication chap pap
```

This tells the router to first use CHAP and then go to PAP if CHAP isn't available.

PPP Commands	
Command	**Description**
`show interface serial 0`	Shows encapsulation, open LCPs and more.
`debug ppp authentication`	View authentication process.
`ppp chap hostname` ***router2***	Specifies chap hostname.
`ppp chap password` *cisco*	Specifies chap password.

Setting Banners

Syntax:

```
Router(config)#banner ?
 LINE       c banner-text c, where 'c' is a
              delimiting character
 exec       Set EXEC process creation banner
 incoming   Set incoming terminal line banner
 login      Set login banner
 motd       Set Message of the Day banner
```

Example:

```
 Router(config)#banner motd #
 Enter TEXT message.  End with the character '#'.
    THIS IS THE MESSAGE OF THE DAY BANNER
 #
```

Disable Banner:

```
 Router#conf t
 Router(config)#no banner motd
```

Interface Descriptions

An interface description is limited to 80 characters and typically describes the function of the interface.

```
R2(config)#interface serial 1
R2(config-if)#description Link to East Office
```

ISDN Integrated Services Digital Network

ISDN is a circuit-switched service provided by Telco providers to allow voice, data, and video and audio transmissions over existing digital telephone lines. ISDN is often used as a low cost alternative to Frame Relay or T1 connections, while still offering a higher connection speed than an analog modem. ISDN service is offered at two levels: **Basic Rate Interface** (BRI) and **Primary Rate Interface** (PRI). BRI is typically used in small offices or for home connection, and PRI is used in larger environments because it provides higher bandwidth.

ISDN Bandwidth

BRI -**3** channels: **2** B-channels at 64 Kbps and **1** D-channel at 16 Kbps for a maximum data throughput of **128Kbps**.
PRI -**23** B-channels and **1** 64Kbps D-channel for bit rate of up to **1.544Mbps**.
European ISDN PRI -**30** 64Kbps B-channels and **1** 64Kbps D-channel for a total interface rate of **2.048 Mbps.**

In both ISDN BRI and PRI, a single D-channel is used for signaling information, and the B-channels are used to carry the data. Because the control communications are conducted on a channel that is separate from the data transfer, ISDN is said to be out of band signaling.

LAPD

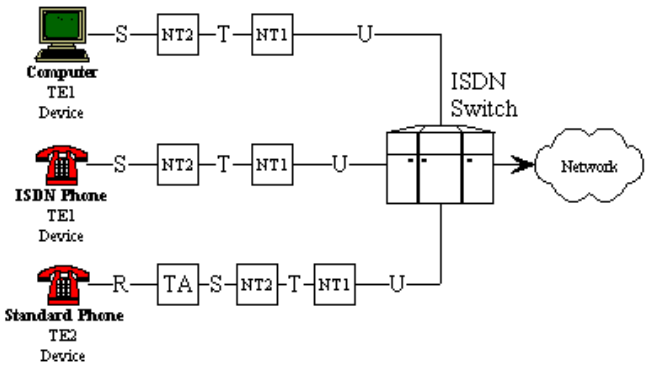
Layer 2 of the ISDN signaling protocol is Link Access Procedure, D channel, it is used by ISDN to pass the signaling messages between the router and the ISDN switch at the local CO. LAPD is similar to HDLC and LAPB. As the expansion of the LAPD acronym indicates, it is used across the D-channel to ensure that control and signaling information flows and is received properly.

ISDN Protocol Series

Protocol Series	Description	Examples
E	Telephone and network standards.	E.163 - Telephone numbering E.164- ISDN addressing
I	Methods, terminology, concepts, and interfaces.	I.100 - Terminology, structure, + concepts I.300 - Networking recommendations
Q	Signaling and switching standards	Q.921 - Data Link layer LAPD procedures Q.931 - Network layer functions

ISDN Functions and Devices

Terminal Adapter (TA) --- A converter device that allows non-ISDN devices to operate on an ISDN network.
Terminal Equipment 1(TE1) --- A device that supports ISDN standards and that can be connected directly to an ISDN network connection. For example, ISDN telephones, personal computers, or videophones could function as TE1s.
Terminal Equipment 2(TE2) --- A non-ISDN device, such as an analog phone or modem, which requires a TA in order to connect to an ISDN network.
Network Termination 1 (NT1) --- A small connection box that is attached to ISDN BRI lines. This device terminates the connection from the Central Office (CO).
Network Termination 2 (NT2) --- A device that provides switching services for the internal network. This type of interface is typically used with PRI lines, when they need to be divided for several functions. For example, some channels may be used for WAN data communications and others for the telephone system and/or video tele-conferencing.



ISDN Reference Points

R -- The **R-interface** is the wire or circuit that connects the TE2 to the TA.
S -- The **S-interface** is a four-wire cable from TE1 or TA to the NT1 or NT2, which is a two-wire termination point.
T -- The point between the NT1 and NT2, which is also the **T-interface**. This four-wire cable is used to divide the normal telephone company two-wire cable into four-wire, which then allows the connection of up to eight ISDN devices.
S/T -- When NT2 is not used on a connection that uses NT1, the connection from the router or TA to the NT1 connection is typically called S/T. This is essentially the combination of the S and T reference points.

U -- The **U-interface** is the actual two-wire cable, also called the local loop, which connects the CPE to the Telco provider.

Service Profile Identifiers (SPIDs)

Many Telco providers utilize ISDN switches, which require SPIDs for dial-in access. An ISDN device can access each ISDN channel via its SPID number. You can configure the router to utilize a single or multiple SPIDs when making a connection to the ISDN provider. The ISDN provider must assign the SPID numbers for each channel, which is usually an 8 to 14-digit number.

Settings SPIDS

The following commands show an ISDN BRI connection (two SPIDS for 2 B-channels):

```
R3(config)#isdn switch-type dms-100
R3(config)#interface bri 0
R3(config-if)#isdn spid1 0835866201 8358662
R3(config-if)#isdn spid2 0835866401 8358664
```

If you want your Cisco router to answer incoming calls over your ISDN line, you can configure an ISDN subaddress. When multiple devices are attached to an ISDN BRI, you can ensure that only a single device answers an incoming call by verifying the number or subaddress in the incoming call against the device's configured number or subaddress or both.

```
R3(config-if)#isdn answer 52069145241010 5551212
```

DDR Dial on Demand Routing

Dial-on-demand routing (DDR), is used to allow two or more Cisco routers to dial an ISDN dial-up connection on an as-needed basis. DDR is only used for low-volume, periodic network connections using either a PSTN or ISDN. This was designed to reduce WAN cost if you have to pay on a per-minute or per-packet basis. DDR configuration commands define host and ISDN connection information. An access list and DDR dialer group define what kind of traffic should initiate an ISDN call. You can configure multiple access lists to look for different types of interesting traffic. Interesting traffic is traffic that (when it arrives at the router) triggers the router to initiate the ISDN connection

Steps of How DDR Works

1.) Route to the destination network is determined.
2.) Interesting packet dictates a DDR call.
3.) Dialer information is looked up.
4.) Traffic is transmitted.
5.) Call is terminated when no more traffic is being transmitted over a link and the idle-timeout period ends.

Configuring a DDR Connection

```
R_3(config-if)#dial wait-for-carrier time 15
R_3(config-if)#dialer idle-timeout 300
R_3(config-if)#dialer load-threshold 125 either
R_3(config-if)#dialer map ip 192.168.52.1 name
CORP speed 56 5205551212
```

Specifying Interesting Traffic (allows IP, but not IGRP)

```
R_3(config)#dialer-list 1 protocol ip list 110
R_3(config)#access-list 110 deny igrp any any
R_3(config)#access-list 110 permit ip any any
R_3(config)#int bri0
R_3(config-if)#dialer-group 1
```

Sample ISDN Configuration

The routers are both using PPP encapsulation and CHAP authentication. The username has been set for the opposite router in each configuration and the password is the same on both. Each router has the ability to dial the other. The CORP router is located at the corporate network, which has other connections and uses IGRP to transfer routing tables on the corporate network. However, IGRP is not desired on the ISDN connection, so the CORP router has an access list specifically denying IGRP on the ISDN link. Both routers permit all IP traffic on the ISDN link and all IP traffic will be considered interesting or worth activating the ISDN link for. Multilink is enabled on both routers, and they will dial their additional lines when there is 50% (load-threshold uses a number between 1 and 255, with 255 being 100%) or more utilization on the first channel. The link will be terminated if there is no interesting traffic for 600 seconds (10 minutes). The IP routes are configured such that all traffic destined from the corporate network to 192.168.24.0 will be sent to the REMOTE router. Since the REMOTE router is a remote branch with no other connections, all traffic that is not specifically destined for 192.168.24.0 will be sent to the CORP router. Note that each router has its dialer mapped to the IP address of the other router.

Remote Network

```
Router Configuration:
Name: REMOTE
E0 IP address:192.168.24.1
Local Network:192.168.24.0
BRI 0 IP address:192.168.49.2
```

```
REMOTE(config)#hostname corp password 123pass332
REMOTE(config)#isdn switch-type dms-100
REMOTE(config)#interface bri 0
REMOTE(config-if)#encapsulation ppp
REMOTE(config-if)#ppp authentication chap
REMOTE(config-if)#spid1 5208881111 5270936
REMOTE(config-if)#spid2 5208881212 5270956
REMOTE(config-if)#ip address 192.168.49.2 255.255.255.0
REMOTE(config-if)#dialer idle-timeout 600
REMOTE(config-if)#dialer map ip 192.168.49.1 name corp
7045551212
REMOTE(config-if)#dialer load-threshold 125 either
REMOTE(config-if)#ppp multilink
REMOTE(config-if)#dialer-group 1
REMOTE(config-if)#exit
REMOTE(config)#dialer-list 1 protocol ip permit
REMOTE(config)#ip route 0.0.0.0 0.0.0.0 192.168.49.1
REMOTE(config)#ip route 192.168.49.0 255.255.255.0
192.168.49.1
```

Corporate network

```
Router Configuration:
Name: CORP
BRI 1 IP address:192.168.49.1
```

```
CORP(config)#hostname remote password 123pass332
CORP(config)#isdn switch-type dms-100
CORP(config)#interface bri 1
CORP(config-if)#encapsulation ppp
CORP(config-if)#ppp authentication chap
CORP(config-if)#spid1 7047773333 5265933
CORP(config-if)#spid2 7047774444 5265944
CORP(config-if)#ip address 192.168.49.1 255.255.255.0
CORP(config-if)#dialer idle-timeout 600
CORP(config-if)#dialer map ip 192.168.49.2 name remote
5205551212
CORP(config-if)#dialer load-threshold 125 either
CORP(config-if)#ppp multilink
CORP(config-if)#dialer-group 1
CORP(config-if)#exit
CORP(config)#ip route 192.168.24.0 255.255.255.0
192.168.49.2
CORP(config)#dialer-list 1 protocol ip list 110
CORP(config)#access-list 110 deny igrp any any
CORP(config)#access-list 110 permit ip any any
```

ISDN Commands

Command	Description
`clear interface`	Disconnects all current connections
`show dialer`	Shows the current dialer status, including the time that the link has been active
`debug dialer`	Displays the configuration and operation of the dialer
`debug q921`	Used to see layer-2 information only
`debug q931`	Show the call setup and teardown
`show ip route`	Show all routes the router knows about
`show isdn active`	Displays the status of the ISDN connection while the call is in progress
`show isdn status`	Gives status information for ISDN connections
`show interface bri 0`	Shows you the configuration statistics and speed of your ISDN BRI interface

Supported ISDN Switch Types

Identifier	Description
`basic-nil`	AT&T basic rate switches
`basic-5ess`	AT&T 5ESS basic rate switches
`basic-dms100`	Nortel DMS-100 basic rate switches
`basic-4ess`	AT&T 4ESS primary rate switches
`primary-5ess`	AT&T 5ESS primary rate switches
`primary-dms100`	Nortel DMS-100 primary rate switches
`vn2`	French VN2 ISDN switches
`vn3`	French VN3 ISDN switches
`ntt`	Japanese NTT ISDN switches
`basic-1tr6`	German 1TR6 ISDN switches

Access Lists

Access List Type	Number
Standard IP Access Lists	1-99
Extended IP Access Lists	100-199
Standard IPX Access Lists	800-899
Extended IPX Access Lists	900-999
IPX SAP Filters	1000-1099

Standard IP Access List

Syntax:

```
access-list 1-99 [permit|deny] [source address]
[source wildcard mask]
```

Example:

```
Router(config)#access-list 1 deny 192.168.1.0
0.0.0.255
Router(config)#access-list 1 permit 0.0.0.0
255.255.255.255    (same as any)
```

Apply the Access List:

```
Router(config)#int e0
Router(config-if)#ip access-group 1 out
```

Standard IPX Access List

Syntax:

```
access-list 800-899 [permit|deny] [source net/
node address] [dest network/ dest address]
```

Example:

```
Router(config)#access-list 800 deny 500 200
Router(config)#access-list 800 permit -1 -1
```

Apply the Access List:

```
Router(config)#int e0
Router(config-if)#ipx access-group 800 in
```

Extended IP Access List

Syntax:

```
access-list 100-199[permit|deny][protocol][src
IP addr][src wildcard mask][dest IP addr][dest
IP addr][dest wildcardmask][operator][port][log]
```

Example:

```
Router(config)#access-list 100 deny tcp host
192.168.1.10 host 192.168.2.2 eq www
Router(config)#access-list 100 permit ip any any
Router(config)#int e0
Router(config-if)#ip access-group 100 in
```

This access list will block 192.168.1.10 from accessing TCP port www (http[80]) on host 192.168.2.2. The host is a short cut to use the 0.0.0.0 wildcard mask. Since extended IP access lists use destination addresses, the list should be applied as close to the source as possible to reduce unnecessary traffic on the network.

Extended IPX Access list

Syntax:

```
access-list 900-999 [permit|deny] [protocol]
[source network/node address] [socket] [dest
network/node addr] [socket]
```

Example:

```
R_1(config)#access-list 900 deny -1 500 0 200 0
R_1(config)#access-list 900 permit -1 -1 0 -1 0
R_1(config)#int e0
R_1(config-if)#ipx access-group 900 in
```

Extended IPX access lists allow you to filter based on source and destination network or node address, IPX protocol type (a -1 specifies all IPX protocols), and IPX socket #.

IPX SAP Filters

Syntax:

```
access-list 1000-1099 [permit|deny] [src network
/ node addr] [service-type]
```

Example:

```
Router(config)#access-list 1000 200 0
Router(config)#access-list 1000 permit -1 0
```

To apply a SAP filter to an int. for inbound filtering use the cmd:

```
Router(config)#int e0
Router(config-if)#ipx input-sap-filter [list#]
```

Or for outbound filtering use the cmd:

```
Router(config)#int e0
Router(config-if)#ipx output-sap-filter [list#]
```

This would block all advertisements from network 200 from being passed to other routers on the internetwork. Again you can use the command **`show access-list`** to see the access lists.

Controlling VTY Access

Example:

```
R_2(config)#access-list 15 permit 192.168.1.71
R_2(config)#line vty 0 4
R_2(config-line)#access-class 15 in
```

This will stop all hosts except 192.168.1.71 from telneting into the router. This is accomplished by only allowing one host and

then not permitting any other hosts since there is an implicit deny at the end of all access lists.

Access List Commands

Command	Description
`show access-lists`	Displays all access lists and their parameters configured on the router. This command doesn't show which interface the list is configured on.
`show access-list [list#]`	Shows only the parameters for the access list specified. This command does not show you the interface the list is configured on.
`show ip access-list`	Shows only the IP access lists configured on the router.
`show ipx access-list`	Shows only the IPX access lists configured on the router.
`show ip interface`	Shows which interfaces have IP access lists on them.
`show ipx interface`	Shows which interfaces have IPX access lists on them.
`show running-config`	Shows the access lists and which interfaces have access lists set.
`any`	Keyword used to represent all hosts or networks, replaces 0.0.0.0 255.255.255.255 in access list.
`host`	Keyword that specifies that an address should have a wildcard mask of 0.0.0.0.(i.e. will match only 1 host)
`clear access-list counter [list#]`	Clears extended access lists counter of the number of matches per line of the access list.
`-1`	Applies to any IPX network or any protocol when used in extended IPX access lists.
`0`	Used for all sockets in extended IPX access lists.
`ip access-group`	Applies an IP access list to an interface.
`ipx access-group`	Applies an IPX access list to an interface.
`ipx input-sap-filter`	Applies an inbound IPX SAP filter to an interface.
`ipx output-sap-filter`	Applies an outbound IPX SAP filter to an interface.

Cisco Hierarchical Model

There are three layers to the Cisco hierarchical model

1. The **core** (Backbone) layer provides optimal transport between sites.
2. The **distribution** layer provides policy-based connectivity.
3. The local-**access** layer provides workgroup/user access to the network.

Core Layer

Responsible for transporting large amounts of traffic reliably and quickly. Only purpose is to switch traffic as fast as possible (speed and latency are factors). Failure at the Core layer can affect every user.

Design specifications:

Don't Do at this layer

- Don't use access lists, packet filtering, or VLAN Routing.
- Don't support workgroup access here.
- Don't expand (more devices) **upgrade** instead (faster devices)

Do at this layer

- Design for high reliability (FDDI, Fast Ethernet with redundant links, or ATM).
- Design for speed and low latency.
- Use routing protocols with low convergence times.

Distribution Layer

Also called workgroup layer, is the communication point between access and core layers. Primary function, routing, filtering, WAN access, and determine how packets can access the Core layer if necessary. Determine fastest/best path and send request to Core layer. Core layer will then quickly transport the request to the correct service. Place to implement network policies.

Network Policies

- Access lists, packet filtering, queuing
- Security and network policies such as address translation and firewalling.
- Redistribution between routing protocols including static routing.
- Routing between VLANs and other workgroup support functions.
- Definition of broadcast and multicast domains.

Access Layer

- Controls user and workgroup access to internetwork resources.
- Also called desktop layer.
- The resources most user need will be available locally.
- Distribution layer handles traffic for remote services.
- Continued access control and policies.
- Creation of separate collision domains (segmentation)
- Workgroup connectivity in Distribution layer
- Technologies such as DDR and Ethernet switching are seen in the Access layer
- Static routing is here.

Configuring IPX Encapsulation

To enable IPX routing on interface Ethernet 0 using arpa (Ethernet_II) encapsulation use the command:

```
Router3(config)#ipx routing
Router3(config)#interface Ethernet 0
Router3(config-if)#ipx network 2 encap arpa
```

You can assign multiple networks with different encapsulation types by using the commands:

```
R3(config)#int e0.1
R3(config-subif)#ipx network 1 encapsulation sap
R3(config-subif)#int e0.2
R3(config-subif)#ipx net 2 encap novell-ether
```

Novell Frame Encapsulation

NetWare Frame Type	Cisco Keyword
Ethernet Frames	
Ethernet_802.3	`novell-ether (default)`
Ethernet_802.2	`Sap`
Ethernet_II	`arpa`
Ethernet_SNAP	`snap`
Token Ring Frames	
Token-Ring	`sap (default)`
Token-Ring_snap	`snap`

FDDI Frames	
Fddi_snap	`snap` (default)
Fddi_802.2	`sap`
Fddi_raw	`novell-fddi`

Routing Protocols' Administrative Distances

Route Source	Default Distance
Connected interface	0
Static Route	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
External EIGRP	170
Unknown	255

Changing the Configuration Register

To change the configuration register while running the system software, follow these steps:

Step 1 - At the privileged EXEC prompt `(Router#)`, enter the **`configure terminal`** command to enter global configuration mode.

```
Router#configure terminal
Router(config)#
```

Step 2 - Set the contents of the configuration register by entering the **`config-register`** ***`value`*** configuration command, where ***`value`*** is a hexadecimal number preceded by 0x as in the following example:

```
Router(config)# config-register 0x2142
```

Step 3 - Press **Ctrl-Z** to exit configuration mode.

Step 4 - Display the current configuration register value, which will be used at the next system reload, by entering the **`show version`** command.

The value is displayed on the last line of the screen display, as in the following example:

```
Configuration register is 0x2102 (will be 0x2142 at
next reload)
```

Step 5 - Restart the router. Changes to the configuration register take effect only when the system reloads.

Configuration Register Boot Field		
Boot Field	**Meaning**	**Used For:**
`00`	ROM monitor mode	To boot to ROM monitor mode, set the configuration register to **2100**. You must then manually boot the router with the b command. The router will show a **`rommon>`** prompt.
`01`	Boot image from ROM	To boot an IOS image stored in ROM, set the configuration register to **2101**. The router will show the **`router(boot)>`** prompt.
`02` to `0F`	Specifies a default boot filename	Any value from **2102** to **210F** tells the router to use the boot commands specified in NVRAM.

Name Resolution

Creating a Host Table

Syntax:

```
ip host name <tcp port #> <ip address>
```

The example turns off domain lookups and doesn't specify a port number because port 23 (telnet) is used by default.

Example:

```
Router_2#configure terminal
Router_2(config)#no ip domain-lookup
Router_2(config)#ip host router_3 192.168.1.6
```

Using DNS lookups

```
Router_2(config)#ip domain-lookup
Router_2(config)#ip name server 192.168.1.5
Router_2(config)#ip domain-name foo.bar
```

Layer 2 Switching

Layer 2 switching is hardware based, and tends to be faster than routers, because they don't look at the logical addressing (Network layer headers), they instead use the hardware address defined at the Data Link (MAC) layer to decide whether to forward or discard the frame. Switches use Application Specific Integrated Circuits (ASIC) to build and maintain filter tables.

Layer two switching is so efficient because it doesn't modify the data packet only the frame encapsulating the packet also causes it to be less error prone

Three functions of Layer 2 Switching

1.) **Address learning** - layer 2 switches retain, in their filter tables, the source hardware address and port interface it was received on.

2.) **Forward/Filter decisions** - when a frame is received, the switch looks at the destination hardware address and finds the interface it is on, in the filter table. If the address is unknown, the frame is broadcast on all interfaces except the one it was received on.

3.) **Loop Avoidance** - if multiple connections between switches exist for redundancy, network loops can occur. Spanning Tree Protocol is used to stop loops and allows redundancy.

Spanning Tree Protocol (STP)

IEEE 802.1d. Main task is to stop network loops from occurring on layer 2 devices. It monitors the network to find all the links and shuts down redundant ones to prevent loops.

It first elects a ***root bridge*** (only 1 per network), root bridge ports are called designated ports, which operate in what are called forwarding-state ports. Forwarding-state ports can send and receive traffic. Other switches in your network are ***non-root bridges***.

The non-root bridges with the fastest link to the root bridge is called the ***root port***, sends and receives traffic.

Ports that have the lowest cost to the root bridge are called ***designated ports***. The other ports on the bridge are considered ***non-designated*** and will not send or receive traffic, (blocking mode).

Switches or bridges running STP, exchange information with what are called Bridge Protocol Data Units (**BPDU**) every 2 seconds. BPDUs send configuration information using multicast frames, BPDUs are also used to send the bridge ID of each device to other devices. The bridge ID is used to determine the root bridge in the network and to determine the root port. The

Bridge ID is 8 bytes long, includes priority and MAC address. Priority of IEEE STP version is 32,768.

STP Port States

Blocking - doesn't forward any frames, listens to BPDUs. Ports default to blocking when the switch powers on. Used to prevent network loops. If a blocked port is to become the designated port, it will first enter listening state.
Listening - listens to BPDUs to ensure no loops occur on the network before passing data frames.
Learning - learns MAC addresses and builds filter table, doesn't forward frames.
Forwarding - sends and receives all data on bridge ports.

LAN Switching Modes

Store and Forward - the entire frame is copied into its buffer and computes the Cyclic Redundancy Check (CRC). Since it copies the entire frame, latency varies with frame length. If the frame has a CRC error, is too short (<64 bytes), or is too long (>1518 bytes) it is discarded. If no error, the destination address (MAC) is looked up in the filter table and is sent to the appropriate interface. Is the default state for 5000 series switches
Cut Through - fastest switching mode as only the destination address is copied. It will then look up the address in its filter table and send the frame to the appropriate interface.
Fragment Free - modified form of Cut Through switching. The switch waits for the first 64 bytes to pass before forwarding the frame. If the packet has an error, it usually occurs in the first 64 bytes of the frame. Default mode for 1900 switches.

Virtual Local Area Networks

VLANs are formed to group related users together regardless of the physical connections of their hosts to the network. The users can be spread across a campus network or even across geographically isolated locations. Users can be organized into separate VLANs according to their department, location, function, application, or protocol used. The goal with VLANs is to group users into separate VLANs so their traffic will stay within the VLAN.

Benefits of VLANs

Broadcast Control - VLANs provide logical collision and broadcast domains that confine broadcast and multicast traffic to the bridging domain

Security - If a router is not used, no user outside the VLAN can communicate with users or access resources within a VLAN. Restrictions can also be placed on hardware addresses, protocols, and applications

Performance - You can isolate users that require high performance networks for bandwidth intensive projects, VLANs can isolate them from the rest of the network.

Network Management - Software on the switch allows you to reconfigure the logical layout of the LAN without having to change cable connections.

VLAN Memberships

Static VLANs - are the typical method of creating VLANs and are the most secure. The switch port you assign a VLAN association to always maintains that association until an administrator changes the port assignment.

Dynamic VLANs - determine a node's VLAN assignment automatically. Using intelligent management software, you can enable MAC addresses, protocols, of even applications to create dynamic VLANs

Frame Tagging

Switches use frame tagging to keep track of users and frames as they travel the switch fabric and VLANs. Switch fabric is a group of connected switches. Frame tagging assigns a unique user-defined ID to each frame. Also called VLAN ID or color.

Types of Links

Access Links - are only part of 1 VLAN are referred to as the native VLAN of the port. Any device attached to an access link is unaware of a VLAN membership. This device just assumes that it is part of broadcast domain, without any understanding of the physical network. Switches remove any VLAN information before it is sent to an access link device. Access link devices can't communicate with any devices outside their VLAN without a router or layer 3 device.

Trunk Links - can carry multiple VLANs and are used to connect switches to other switches, to routers, or servers. Trunk links are only supported on Fast or Gigabit Ethernet (100 or 1000Mbps). Cisco switches support two ways to identify which VLAN a frame belongs to: **ISL** and **802.1q**. Trunk links have a native or default VLAN that is used if the trunk link fails. Trunked links carry the traffic of multiple VLANs from 1 to 1005 at a time. Trunking allows you to make a single port a part of multiple VLANs, so you can be in more than one broadcast domain at a time. When connecting switches together, trunk links can carry some or all VLAN information across the link. If you don't trunk the links then the switch will only carry VLAN 1 information across the link. Cisco switches use the Dynamic Trunking Protocol (DTP) to manage trunks. DTP is a PPP that was created to send trunk information across 802.1q trunks.

Trunk types

Inter-Switch Link - ISL is a Cisco proprietary protocol for interconnecting multiple switches and maintaining VLAN information as traffic goes between switches. ISL is similar to 802.10 as they both multiplex bridge groups over a high-speed backbone (ISL runs only on Fast Ethernet). ISL is an external tagging process (original frame is encapsulated in a 26 byte ISL header with a 4 byte FCS at the end, 2 bytes are for the VLAN ID). Since the frame is encapsulated, only devices running ISL can read it. If you need a protocol for other than Cisco Switches use 802.1q. ISL frames can be up to **1522** bytes long.

IEEE 802.1q - Created by the IEEE as a standard method of frame tagging. It actually inserts a field into the frame to identify the VLAN. If you are trunking between a Cisco switch and a non-Cisco switch, you will need to use 802.1q for the trunk to work.

Local Area Network Emulation (LANE) - LANE is a service that provides interoperability between ATM-based workstations and devices connected to existing LAN technology. LANE uses MAC encapsulation because this approach supports the largest number of existing OSI layer 3 protocols. The end result is that all devices attached to an emulated LAN appear to be on one bridged segment. In ATM LANE environments, the ATM switch handles traffic that belongs to the same emulated LAN and routers handle inter LANE traffic.

IEEE 802.10 - Defines a method for securing bridging of data across a shared MAN backbone. The coloring (VLAN ID) of traffic across the FDDI backbone is achieved by inserting a 16-byte header between the source MAC and the Link Service Access Point (LSAP) of frames leaving a switch. This header contains the 4-byte VLAN ID or "color". The receiving switch removes the header and forwards the frame to interfaces that match the VLAN color.

Inter VLAN Communications

To communicate between VLANs you need to have a router with an interface for each VLAN or a router that supports ISL routing. The lowest Cisco router that supports ISL routing is the 2600 series. If you're using a router with one interface and ISL the interface should be at least 100Mbps (Fast Ethernet).

VLAN Trunking Protocol

Developed by Cisco, it is the industry's first protocol implementation specifically designed for large VLAN deployments.

VTP enhances VLAN deployment by providing the following:

- Integration of ISL, 802.10, and ATM LAN-based VLANs.
- Auto-intelligence within the switches for configuring VLANs.
- Configuration consistency across the network.
- An auto-mapping scheme for going across mixed-media backbones.
- Accurate tracking and monitoring of VLANs.
- Dynamic reporting of added VLANs across the network.
- Plug-and-Play setup and configuration when adding new VLANs.

To allow VTP to manage your VLANs across the network, you must first create a **VTP server**. All servers that need to share VLAN information must use the **same domain name**, and a **switch can only be in one domain at a time**. If all your switches are in the same VLAN then you don't need to use VTP. VTP information is sent via a trunk port. Switches advertise VTP management domain information, as well as configuration revision number and all known VLANs with any specific parameters.

Modes of VTP

Server - default mode for all catalyst switches. You need at least one to propagate VLAN data throughout the domain. The switch must be in server mode to create, add, or delete VLANs in a VTP domain. Advertisements are sent every 5 minutes or whenever there is a change.

Client - receives information from VTP servers and sends and receives updates, but can't make any changes. To add a port on a switch to a VLAN, first make it a client to update the database, then change it to a server to make the changes and have them advertised.

Transparent - doesn't participate in the VTP domain, but will still forward VTP advertisements through the configured trunk links. Can add and create VLANs as it doesn't share its database with any other switch, but the VLANs will only be considered locally significant.

VTP Pruning

It is disabled by default. Pruning is configuring VTP to reduce the amount of broadcasts, multicasts, and other unicast packets to help conserve bandwidth. When you enable VTP pruning on a server, you enable it for the entire domain. VLAN 1 can never prune because it is an administrative VLAN.

Cisco Discovery Protocol (CDP)

CDP is a media- and protocol-independent protocol that runs on all Cisco-manufactured equipment including routers, bridges, access and communication servers, and switches. Using CDP, you can view information about all the Cisco devices directly attached to the device. In addition, CDP detects native VLAN and port duplex mismatches.

CDP runs on all media that support Subnetwork Access Protocol (SNAP). CDP runs over the data link layer only. Cisco devices never forward CDP packets. When new CDP information is received, Cisco devices discard old information.

CDP Default Configuration	
Feature	**Default Value**
CDP global enable state	Enabled
CDP port enable state	Enabled on all ports
CDP message interval	60 seconds
CDP holdtime	180 seconds

CDP Commands are listed on page 2.

CDP Neighbor Information includes

- Neighbor's device ID
- Local port type and number
- Holdtime value (in seconds)
- Neighbor's hardware platform
- Neighbor's network device capability
- Neighbor's remote port type and number

CDP Neighbor Detail Information includes

Additional detail is shown about neighbors, including network address, enabled protocols, and software version.

High-Level Data Link Control

HDLC is the default encapsulation used by Cisco routers over synchronous serial links. HDLC is a bit-oriented ISO standard Data Link layer protocol. It specifies a method to encapsulate data over synchronous serial links using frame characters and checksums. HDLC is a point-to-point protocol used on leased lines between Cisco devices. If you need to establish a link between a Cisco device and a non-Cisco device, you must use PPP encapsulation instead of HDLC. No authentication can be used with HDLC. The reason each vendor has a proprietary encapsulation of HDLC is that they each have a different way for the HDLC protocol to communicate with the Network layer protocols, and the ISO standard doesn't allow for multiple protocols on a single link.

Ethernet Frames

Used at the Data Link layer to encapsulate packets handed down from the Network layer for transmission on a medium.
There are four types

1.) **Ethernet_II** frames have a ***type*** field in their frame

2.) **IEEE 802.3** frames have a ***length*** field in their frame,

3.) **IEEE 802.2** 802.3 frame can't contain information about the upper layer protocols (Network Layer), so it is combined with the 802.2 (LLC) frame to provide this function.

4.) **802.2 SNAP** (**S**ub**n**etwork **A**rchitecture **P**rotocol)

- SNAP was created because not all protocols worked well with the 802.3 frame, which has no ether-type field.
- 802.2 frame is an 802.3 frame with the LLC info in the data field of the header (has DSAP and SSAP).
- SNAP frame's DSAP and SSAP are always set to AA with the command field set to 3.
- SNAP is mostly seen with proprietary protocols such as AppleTalk and the Cisco CDP.

Setting Passwords

Setting the **enable** and **enable secret** password:

```
Router(config)#enable ccna
Router(config)#enable secret ccna2
```

Setting the **auxiliary port** password:

```
Router(config)#line aux 0
Router(config-line)#login
Router(config-line)#password ccna
```

Setting the **console** password:

```
Router(config)#line con 0
Router(config-line)#login
Router(config-line)#password ccna
```

Setting the **Virtual Terminal** (Telnet) password:

```
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password ccna
```

Subnet Masking

Process

1.) How many subnets?
$2^{(\text{masked bits})}$ - 2 = Subnets
2.) How many valid hosts per subnet?
$2^{(\text{unmasked bits})}$ - 2 = Hosts
3.) What are the valid subnets?
256-(subnet base)=Base number
4.) What are the valid hosts in the subnets?
All numbers between subnets minus the all 1s (**.255**) and all 0s (**.0**) host addresses.
5.) What is broadcast address of the subnet?
All the host bits turned on.

Example

255.255.255.192 = 11111111.1111111.1111111.11000000

1.) (2^2)-2 = **2** Subnets
2.) (2^6)-2 = **62** Hosts per subnet
3.) 256 - 192 = **64** (.01000000) {For the first subnet}
4.) **65** to **126** (.01000001 to .01111110) Valid hosts in the subnets
5**.) 127** (.01111111) Broadcast