

# Cisco Certified Network Associate CCNA 2.0

## Version 3.0.0


psssst...
CLICK HERE to
Download a FREE
Cisco® CCNA
Exam!
TechSkills
Hey,
I'm serious!
CLICK HERE to
Download a FREE
Cisco® CCNA
Exam now!
So what are you
waiting for?
TechSkills

# Cisco Certified Network Associate CCNA 2.0

**Version 3.0.0**



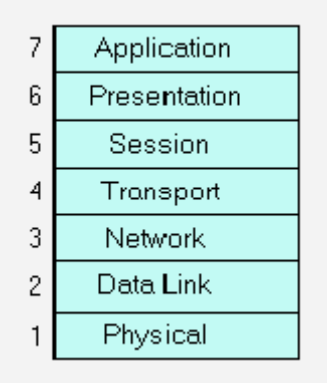
## Abstract:

This study guide will help you to prepare for Cisco exam 640-507, Cisco Certified Network Associate 2.0. Exam topics include Bridging, Switching, Network and WAN Protocols, Reference Model and Layered Communication, Routing, Network Management, LAN Design, Physical Connectivity, Cisco Basics, IOS and Network Basics.

## Find even more help here:

## Contents:

# OSI Reference / Network Protocols




**Application** – The application layer provides services directly to applications. The functions of the application layer can include identifying communication partners, determining resource availability, and synchronizing communication . Some examples of application layer implementations include TCP/IP and OSI applications such as Telnet, FTP, and SMTP, File Transfer, Access, and Management (FTAM), Virtual Terminal Protocol(VTP), and Common Management Information Protocol (CMIP).

**Presentation** –The presentation layer provides a variety of coding and conversion functions that are applied to application layer data. These functions ensure that information sent from the application layer of one system will be readable by the application layer of another system. Examples of presentation layer coding and conversion schemes include ASCII, EBCDIC, JPEG,GIF, TIFF, MPEG, QuickTime, various encryption methods, and other similar coding formats.

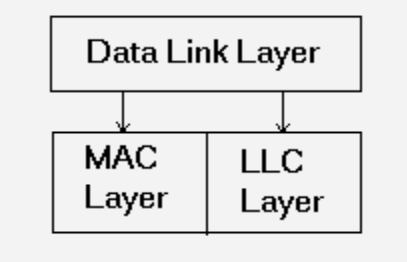
**Session** –The session layer establishes, manages, maintains, and terminates communication sessions between applications. Communication sessions consist of service requests and service responses that occur between applications located in different network devices. Some examples of session layer implementations include Remote Procedure Call (RPC), Zone Information Protocol (ZIP), and Session Control Protocol (SCP).

**Transport** – The transport layer segments and reassembles data into data streams. It is also responsible for both reliable and unreliable end-to-end data transmission. Transport layer functions typically include flow control, multiplexing, virtual circuit management, and error checking and recovery. Some examples of transport layer

implementations include Transmission Control Protocol (TCP), Name Binding Protocol (NBP), and OSI transport protocols (SPX).

**Network** –The network layer uses logical addressing to provide routing and related functions that allow multiple data links to be combined into an internet work. The network layer supports both connection-oriented and connectionless service from higher-layer protocols. Network layer protocols are typically routing protocols. However, other types of protocols, such as the Internet Protocol (IP), are implemented at the network layer as well. Routers reside here at the network layer. Some common routing protocols include Border Gateway Protocol (BGP), Open Shortest Path First(OSPF), and Routing Information Protocol (RIP). Packets and data grams are sent across this layer of the OSI model (IPX).

**Data Link** – The data link layer provides reliable transmission of data across a physical medium. The data link layer specifies different network and protocol characteristics, including physical addressing, network topology, error notification, sequencing of frames, and flow control. The Data link layer is composed of two sublayers known as the Media Access Control (MAC) Layer and the Logical Link Control (LLC) layer.This can be seen in the following diagram:




The LLC sublayer manages communications between devices over a single link of a network. LLC supports both connectionless and connection-oriented services used by higher-layer protocols. The MAC sublayer manages protocol access to the physical network medium. The IEEE MAC specification defines MAC addresses, which allow multiple devices to uniquely identify one another at the data link layer. Data link layer implementations can be categorized as either LAN or WAN specifications. The most common LAN data link layer implementations include Ethernet/IEEE 802.3, Fast Ethernet, FDDI, and Token Ring/IEEE 802.5. The most common WAN data link layer implementations include Frame Relay, Link Access Procedure, Balanced (LAPB), Synchronous Data Link Control (SDLC), Point-to-Point Protocol (PPP), and SMDS Interface Protocol (SIP).

**Physical** – The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between communicating network systems.
Physical layer specifications define such characteristics as voltage levels, timing of

voltage changes, physical data rates, maximum transmission distances, and the physical connectors to be used. Physical layer implementations can be categorized as either LAN or WAN specifications. Some common LAN physical layer implementations include Ethernet/IEEE 802.3, Fast Ethernet, FDDI, and Token Ring/IEEE 802.5. Some common WAN physical layer implementations include High-Speed Serial Interface (HSSI),SMDS Interface Protocol (SIP), and X.21bis.

## Steps of Data Encapsulation

1. User information is converted to *data*
2. *Data* converted to *segments*
3. *Segments* converted to *packets* or *data grams*
4. *Packets* and *data grams* are converted to *frames*
5. *Frames* are converted to *bits*

| | | | | |
|---|---|---|---|---|
| | | | Application | |
| | | | Presentation | |
| | Upper Layer Data | | Session | PDU |
| TCP Header | Upper Layer Data | | Transport | Segment |
| IP Header | Data | | Network | Packet |
| LLC Header | Data | FCS | Data Link | Frame |
| Mac Header | Data | FCS | Physical | Bits |
| | 010110101101010101 | | | |

**Data link addresses**

Physical address. Flat addressing scheme where the physical address is burned into a network card (MAC address)

**Network address**

Logical address. IP or IPX –hierarchical scheme. The address is assigned to a machine manually or dynamically.

- Physical through Transport layers are the Data Flow Layers
- Session through Application layers are the "Application" (Upper) Layers
- Hubs work on the Physical layer (Layer 1 device)
- Switches and Bridges work on the Data Link Layer (Layer 2device)
- Routers work on the Network layer (Layer 3 device)

# Network Structure Defined by Hierarchy

**Core Layer** = Multi-layer switch

- Purpose is to switch traffic as fast as possible
- Characteristics:
    - Fast transport to enterprise services (e-mail, internet access, video conferencing)
    - No packet manipulation

**Distribution Layer** = Routers
Primary function: perform potentially "expensive" packet manipulations such as routing, filtering, and WAN access. Characteristics include:

- Access Layer Aggregation Point
- Routing traffic
- Broadcast/Multicast Domains
- Media Translation
- Security
- Possible point for remote access

**Access Layer** = Switches and Routers
End station entry point to the network

**IPX**

**To turn on:**

- <>
- ipx routing

**Then, on interface:**

- ipx network {#} encapsulation {sap, arpa, snap, hdlc,novell-ether} {sec}
- ipx network 3100 encapsulation sap sec

**To monitor:**

- <>
- sh ipx traffic
- sh ipx int e0

**Frame Types:**

- 802.3 – novell-ether – default
- 802.2 – sap
- Ethernet_II – arpa
- Ethernet_snap – snap

## LAN Switching

**Switching** – examines MAC address. Same as multi portbridge

**Three Switch Functions**

- Address learning
- Forward/filter decision
- Loop avoidance

**Address Learning**: maintains MAC address table used to track the location of devices connected to the switch.

**Forward/filter decision:** when a frame arrives with a known destination address, it is forwarded only on the specific port connected to that station.

**Broadcast and Multicast frames:** may be of interest to all stations. The switch normally floods to all ports other than the origination port. A switch never learns a broadcast or multicast address because broadcast and multicast addresses never appear as the source address of a frame.

- All nodes on an Ethernet network can transmit at the same time, so the more nodes you have the greater the possibility of collisions happening. This can slow the network down.

**Redundant Topology –** eliminates single points of failure. Causes broadcast storms, multiple frame copies, and MAC address table instability problems.

**Multiple Frame Copies –** when a new switch is added, the other switches may not have learned its correct MAC address. The host may send a unicast frame to the new switch. The frame is sent through several path sat the same time. The new switch will receive several copies of the frame. This causes MAC Database Instability.

**MAC Database Instability** – results when multiple copies of a frame arrive on different ports of a switch.

**Multiple Loop Problems –** complex topology can cause multiple loops to occur. Layer 2 has no mechanism to stop the loop. This is the main reason for Spanning – Tree Protocol.

**Spanning-Tree Protocol** (STP) IEEE 802.1d. –developed to prevent routing loops. STA (Spanning-Tree Algorithm) is implemented by STP to calculate a loop-free network topology. In most switches, BPDU (Configuration Bridge Protocol Data Unit), are sent and received by all switches, and processed to determine the spanning-tree topology. (STP is on by default).

- A port is in either a forwarding or blocking state. Forwarding ports provide the lowest cost path to the root bridge. All ports start in the blocking state to prevent bridge loops. The port stays in a blocked state if the spanning tree determines that there is another path to the root bridge that has a better cost. **Blocking ports can still receive BPDUs**.

**Spanning-Tree operation –** Selects one root bridge. All the ports are designated ports (forwarding). For non-root bridge, there will be one root port. This offers the lowest cost path from non-root bridge to the root bridge. On each segment, there is one designated part. This port also has the lowest cost to the root bridge.

## Time to Convergence

The time for all the switches and bridges ports transition to either the forwarding or blocking state. When network topology changes, switches and bridges must re-compute the Spanning-Tree Protocol, which disrupts traffic.

### Bridging Compared to LAN Switching

**Bridging**: primarily software based. One spanning-tree instance per bridge. Usually up to 16 ports per bridge.
**LAN Switching**: primarily hardware based. Many spanning-tree instances per switch. More ports per switch, (up to 100). Faster than a Bridge.

### Transmitting Frames through a Switch

- **Store-and-Forward** – copies entire frame into buffer, checks for CRC errors. Higher latency.
- **Cut-Through** – reads only the destination address into buffer, and forwards immediately. Low latency.
- **Fragment free** – (modified cut-through). Switch will read into the first 64 bytes before forwarding the frame. Collisions will usually occur within the first 64 bytes. (default for 1900 series).
- Full-Duplex Ethernet – can provide double the bandwidth of traditional Ethernet, but requires a single workstation on a single switch port, and NIC must support it. Collision free because there are separate send and receive

wires, and only one workstation is on the segment. Half-Duplex must provide for collision detection, therefore can only use 50% of bandwidth available. It sends and receives on the same set of wires.

**LAN Segmentation**: breaking up the collision domains by decreasing the number of workstations per segment.

**Fast Ethernet** (100bt) – provides 10 times the bandwidth of older 10bastT Ethernet. Must have Cat5 cable, no longer than 100meters, and Fast Ethernet NIC's and Hubs/Switches.

**Bridges** – examines MAC address, and forwards frames unless the address was local. Forwards to all other segments it is attached to. Forwards multicast packets, so broadcast storms can occur.
**Routers** – examines network address, and forwards using the best available route to destination network. Can have multiple active paths.

**Virtual LAN's** – sets different ports on a switch to be part of different sub-networks. Some benefits: simplify moves, adds, changes; reduce administrative costs; have better control of broadcasts; tighten security; and distribute load. Relocate the server into a secured location.

## TCP/IP Layers

**Application Layer**

File transfer, E-Mail, Remote Login, Network Management, Name Management.
**Transport Layer**

TCP (connection oriented), UDP(Connectionless).
Flow control provided by sliding windows. Reliability provided by sequence numbers and acknowledgements.
**Port Numbers**

Used to pass information to the upper layers.

**TCP**

- FTP – 21
- Telnet – 23
- SMTP – 25
- DNS –53

**UDP**

- DNS – 53
- TFTP – 69
- SNMP – 161
- RIP – 520

Numbers below 1024 are well known ports. Dynamically assigned ports are above 1024. Registered ports are for vendor specific applications: usually above 1024.

**Internet Layer** – Corresponds with OSI Network layer

- **IP** provides connectionless, best-effort delivery routing of datagrams
- **ICMP** provides control and messaging capabilities
- **ARP** determines the **data** link layer address for known IP address
- **RARP** determines network address when data link layer addresses are known

### IP Address Classes

| | | | | |
|---|---|---|---|---|
| Class A | Net.Node.Node.Node | 0 | 1 – 127 | 126 networks, 16M nodes |
| Class B | Net.Net.Node.Node | 10 | 128 – 191 | 16K networks 65K nodes |
| Class C | Net.Net.Net.Node | 110 | 192-223 | 2M networks 254 nodes |

### Subnetting Formulas

(Count the bits only from the Node portion of the address. Therefore, for a Class B address, the total masked bits+ unmasked bits = 16):

- Max # of Subnets: $2^{(\text{masked bits})}-2$
- Max # of Hosts (per subnet): $2^{(\text{unmasked bits})}-2$

## Routing

Routers must learn destinations that are not directly connected.

### Static (manual)

Uses a route that the network administrator enters manually. (Must be setup bi-directional)

- Enter the IP Route command in global configuration mode
- ip route {destination network} {mask} {port, on remote side, to get there}
- ip route 172.16.10.0 255.255.255.0 172.16.40.1

**Dynamic:** Uses a route that a network routing protocol adjusts automatically

- router rip
- network 172.16.0.0
- router igrp {autonomous system #}
- network 172.16.0.0
- < use monitor, To>sh ip route {rip / igrp)

## Routing Protocols

**Interior -** (within an autonomous system – AS –group of routers under the same administrative authority)

**Distance Vector** – understands the direction and distance to any network connection on the internet work. Knows how many hops (the metric) to get there. All routers w/in the internet work listen for messages from other routers, which are sent every 30 to 90 seconds. They pass their entire routing tables. Possible problems: Slow convergence, Routing Loops, Counting to Infinity (this is solved by maximum hop count). Solutions: Split Horizon(cannot send information back in the direction it was received);Hold-Downs(prevent regular update messages from reinstating a route that's gone down). Uses hop count for measurement.

- **RIP** – 15 hop count max
- **IGRP**– 255 hop count max, uses reliability factor (255 optimal), and bandwidth

**Link State** – understands the entire network, and does not use secondhand information. Routers exchange LSP's (hello packets). Each router builds a topographical view of the network, then uses SPF (shortest path first) algorithm to determine the best route. Changes in topology can be sent out immediately, so convergence can be quicker. Uses Bandwidth for measurement.

- **OSPF** – decisions based on cost of route (metric limit of 65,535)
- **EIGRP** – hybrid protocol (has features of Distance Vector and Link State protocols), Cisco proprietary

**Exterior**

- EGP (Exterior Gateway Protocol)
- BGP (Border Gateway Protocol)

## Counting to Infinity

- Define a limit on the number of hops to prevent infinite loops
- Split Horizon (never sends information about a route back the same direction in which it was received)
- Route Poisoning (Routers set the distance of routes that have gone down to infinity. Used with hold-down timers)
- Hold-Down Timers (Router keeps an entry for the network possibly down state, allowing time for other routers to re-compute for this topology change)
- Poison Reverse(overrides split horizon. Informs the sending router that the destination is inaccessible)
- Triggered Updates (Sends updates when a change in its routing table occurs. Does not wait for the prescribe time to expire

## IOS / Routing / Network Security

- Cisco IOS (operating system) is stored in flash memory (EEPROM)
- IOS configuration is stored in NVRAM

**User Mode** –ordinary tasks – checking status, etc. Need password depending on how you're entering (Virtual Terminal pw for telnet session, Auxiliary pw for aux port, Console pw for console port)

- conf t
- line vty 0 {line aux 0} {line con 0}
- login
- password letmein

**Privileged Mode**

- conf t
- enable password letmein

**Banner**

- conf t
- banner motd #

**Hostname**

- conf t
- hostname MyRouter

**Editing**

- CTRL+A – beginning of line
- CTRL+E – end of line
- <>show history

TAB completes command

**Help**

- Press ? after any command for a list of what comes next

**Router Elements/Configuration**

- <>show startup-config
- <>show running-config
- <>copy running-conifg startup-config
- erase startup-config
- setup
- reload
- boot system {flash / tftp}
- copy flash tftp< to OR server) tftp software IOS(backup>
- <>copy tftp flash
- copy run tftp < configuration to tftp OR server)(backup>
- copy tftp run
- <>show proc
- show mem
- show buff
- show flash
- show cdp

## Network Security / Access Lists

**Standard IP access list**

Check the source address of packets that could be routed. Permits or denies output for an entire protocol suite.

- Filters based on source
- Permit or deny entire TCP/IP protocol suite
- Range is 1 through 99
- Place close to the destination
- access-list {number} {permit / deny} {source address}
- access-list 10 permit 172.16.30.2

## Extended IP access list

Check for both source and destination packet address. Can also check for specific protocols, port numbers, and other parameters, which allows administrators more flexibility in describing what checking the access list will do.

- Filter based on Source and destination
- Specifies a particular IP protocol and port number
- Range is 100 though 199
- Place lists close to the source
- access-list {number} {permit / deny} {protocol}{source} {destination} {port}
- access-list 110 permit tcp host 172.16.50.2 host 172.16.10.2 eq8080
- Access lists may be applied to:
    - Inbound access lists. Saves overhead of routing lookups if the packet is to be discarded because it is denied by the filtering tests.
    - Outbound access lists. Packets are routed to the outbound interface and then processed through the outbound access lists.
    - An access list can be applied to multiple interfaces. However, there can be only one access list per protocol, per direction, per interface.

**Wildcard masks** – use masks to identify insignificant bits, eg

- access-list 11 permit 172.16.30.0 0.0.0.255
- (permits anybody with 172.16.30.x)
- Note: you can use 0.0.0.0 as the mask to limit to that specific host, or prefix it with 'host'
- Applying the list to an interface (use access-group on the interface):
    - <>
    - int e0
    - ip access-group 110 out

## IPX Access lists

- Standard: access-list {number} {permit/deny} {source}{destination}
- Extended: access-list {number} {permit/deny} {protocol} {source}{socket} {destination} {socket}
- access-list 810 permit 30 10
- int e0
- ipx access-group 810 out

## IPX SAP Filters

- access-list {number} {permit/deny} {source} {service type}
- To apply – on interface: ixp input-sap-filter {number}

- access-list 1010 permit 11.0000.0000.0001 0
- int e0
- ipx input-sap-filter 1010

**Access list Numbers allowed:**

| | |
|---|---|
| 1-99 | IP Standard |
| 100-199 | IP Extended |
| 800-899 | IPX Standard |
| 900-999 | IPX Extended |
| 1000-1099 | IPX SAP |

**To Monitor Access Lists**

- <>
- Show access-list

# WAN

**Layer 1 Connection Types**

- **Leased Lines** – "point-to-point" or" dedicated connection". Pre-established WAN path from customer through ISP to remote network.
- **Circuit Switching** – Dedicated circuit path must exist between sender and receiver for the duration of the "call." Used with ISDN. Used when customer doesn't need a 24/7 connection, but needs a reliable connection
- **Packet Switching** – Network devices share a single point-to-point link to transport packets from a source to a destination across a carrier network. They use virtual circuits that provide end-to-end connectivity.

**Wan Service Providers**

- **Customer premises equipment (CPE) -** Devices physically located at subscriber's location.
- **Demarcation (or demarc)** - The place where the CPE ends and the local loop portion of the service begins. (Usually in the "phonecloset").
- **Local loop** - Cabling from the demarc into the WAN service provider's central office.

- **Central Office switch (CO)** - Switching facility that provides the nearest point of presence for the provider's WAN service.
- **Toll network** – The switches and facilities,(trunks), inside the WAN provider's "cloud."

**Layer 2 Encapsulation Protocols**

- **High-Level Data Link Control (HDLC)** – Default encapsulation type on point-to-point, dedicated links, and circuit switched connections. Used for communications between two Cisco devices.
- Point-to-Point Protocol (PPP) – Provides router-to-router and host-to-network connections over synchronous and asynchronous circuits.
- Uses PAP or CHAP authentication.
- Int s0, encapsulation PPP
- **Serial Line Internet Protocol (SLIP)** – Standard protocol for use with TCP/IP. It has, for the most part, been replaced by PPP.
- **X.25/Link Access Procedure, Balanced (LAPB) –** Standard that defines how connections between DTE and DCE are maintained.
- **Frame Relay** – Industry standard, switched data linklayer protocol that handles multiple virtual circuits. (Replaces X.25). Shared bandwidth over public network. Virtual circuits are identified by **DLCI**'s.
- **DLCI** - (Data Link Connection identifiers). **LMI**(Local Management Interface), co-developed in 1990 by Cisco, provides message information about current DLCI values (global or local significance), and the status of virtual circuits. **Subinterfaces** allow you to have multiple virtual circuits on a single serial interface. You must **map** an IP device to the DLCI (using the frame-relay map command or the Inverse-ARP function)
  - int s0
  - encapsulation frame-relay {ietf}
  - *Note: if you don't specify ietf, it uses cisco bydefault*
  - frame-relay interface-dlci {#}
  - frame-relay lmi-type {cisco, ansi, q933a}

**Subinterfaces:**

- int s0.x {multipoint / point-to-point}
- Mapping:
- int s0
- inverse-arp *or*
- frame-relay map ip x.x.x.x #

**Monitoring:**

- show frame {pvc / ip / lmi / traffic / etc.}

**Asynchronous Transfer Mode (ATM)** – International standard for cell relay while using multiple services (voice, video, data)

**Frame Relay PVC Connection**

Uses the Data Link and Physical Layer of OSI model.

- Local access Rate – Clock speed of the connection to the Frame Relay cloud
- Virtual Circuit (VC) Logical circuit created to ensure communication between two devices.
- PVC – Virtual circuit that is permanent. Saves bandwidth by not having to establish circuits each time it is used.
- SVC– Virtual circuit that is established "on-demand" and is disconnected when no longer needed.
- Data-link connection identifier (DLCI) -A number which identifies the logical circuit between the router and the Frame Relay Switch.
- Committed Information Rate (CIR) – The rate that the Frame relay switch agrees to transfer data (in bits per second).
- Inverse Address resolution Protocol (Inverse ARP) – Method of dynamically associating a network layer address with a DLCI.
- Local Management Interface(LMI) – Signaling standard between the router device and the Frame Relay Switch.
- Backward Explicit Congestion Notification (BECN) – When congestion occurs, a BECN is sent from the receiving Frame Relay switch to reduce the rate of sending date.

**ISDN**

ISDN - digital service that runs over existing telephone networks
Normally used to support applications requiring high-speed voice, video, and data communications for home users, remote offices, etc.

**ISDN Terminal Equipment Types**

- TE1 – understand ISDN standards
- TE2 – predate ISDN standards, require a TA (terminal adaptor)
- NT1 – Converts BRI signals into a form used by the ISDN digital line.
- NT2 – ISDN PBX
- TA– Terminal Adapter, converts V.35, and other signals into BRI signals.

**Reference Points describe the point between**

- R – non-ISDN and TA
- S – user terminals and NT2
- T– NT1 and NT2 devices
- U – NT1 and line termination

**ISDN Protocols**

- E – on existing telephone network
- I – concepts, terminology, and services
- Q – switching and signaling
- ISDN BRI (Basic Rate Interface): 2 64K B channels, plus 1 16K D channel
- ISDN PRI (Primary Rate Interface):
  23 64K B channels, plus 164K D channel (North America & Japan)
  30 64K B channels, plus 1 64K D channel (Europe & Australia)
- Configuration example:
  - config t
  - isdn switch-type basic-dms100
  - int bri0
  - encap ppp
  - isdn spid1 775154572
  - isdn spid1 455145664

Special thanks to
Dale Long
for contributing this
Cramsession.