

NEW!

**CramSession**Comprehensive **Study Guides**

A+  
Adobe  
C++  
Cisco CCNA

**Your Trusted  
Study Resource  
for  
Technical  
Certifications**

Written by experts.  
The most popular  
study guides  
on the web.

In Versatile  
PDF file format

Check out these great features  
at [www.cramsession.com](http://www.cramsession.com)

> **Discussion Boards**

<http://boards.cramsession.com>

> **Info Center**

<http://infocenter.cramsession.com>

> **SkillDrill**

<http://www.skilldrill.com>

> **Newsletters**

<http://newsletters.cramsession.com/default.asp>

> **CramChallenge Questions**

<http://newsletters.cramsession.com/signup/default.asp#cramchallenge>

> **Discounts & Freebies**

<http://newsletters.cramsession.com/signup/ProdInfo.asp>

Cisco CCNP 2.0

# Certified Internetworking Troubleshooting

Version 3.0.0

Microsoft Office  
Microsoft Windows 2000  
Microsoft Windows XP  
Network Security  
Network+  
Networking  
Nortel Networks  
Novell  
Oracle  
Proxy Server  
Red Hat Linux  
SAIR Linux  
SANS  
SCO  
Server+  
SQL  
Sun Solaris  
Unix  
Visual Basic  
Web Design

**Notice:** While every precaution has been taken in the preparation of this material, neither the author nor Cramsession.com assumes any liability in the event of loss or damage directly or indirectly caused by any inaccuracies or incompleteness of the material contained in this document. The information in this document is provided and distributed "as-is", without any expressed or implied warranty. Your use of the information in this document is solely at your own risk, and Cramsession.com cannot be held liable for any damages incurred through the use of this material. The use of product names in this work is for information purposes only, and does not constitute an endorsement by, or affiliation with Cramsession.com. Product names used in this work may be registered trademarks of their manufacturers. This document is protected under US and international copyright laws and is intended for individual, personal use only.

For more details, visit our [legal page](#).



**CramSession**  
Prepare for Success!



## Cisco CCNP 2.0

# Certified Internetworking Troubleshooting

Version 3.0.0

**NOTICE:** Got the **NEWest Version?**  
Make sure by clicking here!

### Abstract:

This study guide will help you to prepare for Cisco exam 640-506, Cisco CCNP 2.0 Certified Internetworking Troubleshooting. Exam topics include Troubleshooting Processes for Routers and Routed Protocols, Campus Switch, VLAN and WAN.

Find even more help here:

- > **Feedback & Discussion Board for this exam**
- > Read & Write Reviews of this study guide
- > Rate this Cramsession study guide



## Contents:

General Network Management .....	3
Analyzing a Network Problem: .....	3
Typical Troubleshooting Commands for Router / Switch .....	3
Troubleshooting Tools .....	5
Sales Tool Central - Troubleshooting Assistance .....	7
Physical Router Hardware Problems .....	7
Configuration Issues .....	8
Counters and Measurements .....	10
Troubleshooting for Serial Lines.....	11
Troubleshooting for ISDN .....	11
Troubleshooting ATM .....	11
Troubleshooting Frame Relay .....	12
Troubleshooting FDDI .....	12
Troubleshoot VLAN .....	13
Troubleshooting AppleTalk.....	13
Troubleshooting IPX.....	14
Troubleshoot Transparent Bridges.....	15
Connectionless Network Service - CLNS.....	16



**General Network Management**

Criteria:

- Fault management
- Performance management
- Configuration and device management
- Accounting management
- Security management

SMT (Station Management: ANSI FDDI specification that defines how ring stations are managed) entity coordination/management states:

- Responsible for overlooking the operation of CEM (Configuration Management Elements, not to confuse with Cisco email Manager) and PCM (Physical Connection Management)
- Out – router is isolated from network
- In – router is connected to the network
- Trace – router tries to localize a stuck beacon
- Leave – router allows all connections to break before leaving the network
- Path\_test – router tests its internal paths
- Insert – router ready for optical bypass process to perform insert operation
- Deinsert – router ready for the optical bypass process to perform de-insert operation
- Check – ensures optical bypasses are switched correctly

**Analyzing a Network Problem:**

The first step is to make a clear problem statement indicating symptoms and potential causes. After defining the possibilities, gather facts by asking users questions and collecting information from sources such as network management systems, protocol analyzers, output from router diagnostic commands or software release notes, etc. Then isolate the problem to one device by changing only one variable at a time until the problem is resolved. If the changes made do not solve the problem then undo all the changes and redefine the problem statement.

**Typical Troubleshooting Commands for Router / Switch**

Show controllers Ethernet [interface number]	To display statistics like missing datagrams, memory errors, buffer errors, and overflow errors for an Ethernet interface on a Cisco router (Please note this command will not give you information on internal hardware errors)
Show flash	To display the router images stored in NVRAM



Show buffers	To display statistics for the buffer pools in router (Please note that the router has one pool of queuing elements and five pools of packet buffers of different sizes. Network server keeps counts of the number of buffers outstanding, the number of buffers in the free list, and the maximum number of buffers allowed in the free list for each pool)
Show processes	To display information about the active processes in a router
Show tech-support	To show tech support router conditions
Show version	To show current status of router
Debug ip rip	To check if RIP routing is operating properly
Show ip route	To display the entries in the routing table
Show version	To obtain a router's firmware version
Show running-config	To obtain a router's current configuration
Show interface fddi 3/0	To display an upstream neighbor value of 0000 0000 0000 for FDDI (Keep in mind that 0000 0000 0000 means the upstream neighbor is unknown, indicating that a physical problem is likely to have occurred)
Debug isdn q921 / debug isdn q931	To troubleshoot ISDN BRI layer 2 and 3
Show controller bri	To view information specifically about the D channel of a BRI line
Logging console level	To send debugging output to the consol
Show frame-relay	To obtain statistics about a PVC (Permanent Virtual Circuit) on all Frame Relay interfaces

#### Other commands

- The "trace" command works by using an error message generated by routers when a datagram exceeds its time-to-live value. It displays the router round-trip time for each probe.



## Certified Internetworking Troubleshooting

- The "service timestamps" command puts a date and time in the log in order to tell how much time has elapsed between events.

### **Troubleshooting Tools**

Break out boxes / BERTS (Bit Rate Error Testers) / Fox boxes	Troubleshoot peripheral interfaces by monitoring data line conditions, analyzing and trapping data, and diagnosing problems common to data communication systems
Volt Ohm meter	Measures the physical properties including current, resistance, capacitance, and cable continuity
Cable tester	Checks physical connectivity on STP, UTP, 10BaseT, coaxial, and a special cable type called twinax-cable
Time Domain Reflectors	Troubleshoots crimps, kinks, impedance, bends, and other defects in metallic cables by measuring how much time it takes the signal to reflect and calculating the distance to a fault
Optical Time Domain Reflectors	Troubleshoots optical cable
Network Monitors	Determines a baseline and establish trends in the networks
Network Analyzer	Decodes the various layers in a frame and presents them as summaries detailing which layer is involved
Traffic Director	Collects RMON information
Stack Decoder	Pastes in the output of a "Show stack" command after an error. The stack decoder tool will provide meaningful comments in the stack trace
Protocol analyzers	Display packet data



**Certified Internetworking Troubleshooting**

CCO bug toolkit resources	Bug Navigator, Bug Alert and Bug Watcher
Net SYS	Simulates network changes in a virtual environment
Cisco website	The site has a technical database, an open question-and-answer forum, a mailing-list archive, a troubleshooting assistant, a software bug toolkit, access path configuration tools, an IP subnet calculator, a stack decoder, a 3600 memory calculator, TAC Case instructions, and Cisco products for purchase online
Cisco Works	Internetwork management software that works with SNMP. It can monitor devices for environmental and interface statistics, display information about the health of a device, view data similar to the output of a "show exec" command, display and analyze the path between two devices, probe and extract data about the condition of the network, dynamically monitor and troubleshoot using graphs of device statistics and comprehensive configuration information, gather historical data for analysis, and create detailed maps which you can provide to Cisco TAC for assistance in debugging your network
Cisco Traffic Director	Remote monitoring tools to gather data, monitor activity on your network and find potential problems, and allows users to



	monitor all seven layers of the OSI model
VLAN Director	Provides an accurate representation of the physical network, has the capability to find discrepancy on conflicting ports, can quick detect changes in VLAN status and switch ports, and has user authentication and write protection security
Troubleshooting Engine	Provides simulations of failures and allows users to test possible solutions (CSEs (Customer Support Engineers) often connect to the Troubleshooting Engine to network hardware in the TAC (Technical Assistance Center) lab)

**Sales Tool Central - Troubleshooting Assistance**

- <http://www.cisco.com/warp/public/779/smbiz/service/troubleshooting/ts.htm>
- Online resources for troubleshooting Internetworks

**Physical Router Hardware Problems**

Green LED	Port is operational
Orange LED	Link disabled
LED flashes orange	Hardware failure
Off LED	No signal

- Cabling: to eliminate possible cable breaks or cable plant & punch down connections, try to replace cable with a good external cable.
- Dialing: if the incorrect cable is used, the router may never attempt to dial; if the speed is configured incorrectly, the router will dial but not connect.
- Power system: power supply + wiring + system cables (including all external cables that connect to the router) + cooling system + blower assembly. Note that some models have power supply redundancy, and some are even hot swappable.



## Certified Internetworking Troubleshooting

- Emulator traps: the processor has executed an illegal instruction, caused by either the software taking illegal branches or by hardware failures
- Connection: misconfigured CHAP allows connection but not authentication; misconfigured route does not allow traffic to reach the remote end.
- Processor timers: guard against certain types of system hangs. The watchdog timer must be periodically reset, or a trap will occur (i.e. something wrong).
- Input errors: error occurred while the data was in transit.
- Parity errors: internal hardware error checks failed, likely to be a hardware problem.
- Bus errors: processor tries to use a device or a memory location that either does not exist or does not respond properly.
- Address errors: software tries to access data on an incorrectly aligned boundary.

### **Configuration Issues**

- Bad hop count: when there is a high number of packets with a bad hop count (i.e., packets were discarded because their hop count exceeded 16), a possible cause is a backdoor bridge between segments (when Spanning Tree was disabled).
- Asymmetric VS symmetric flow control: in an asymmetric model the local port performs flow control of the remote port. If the local port is congested, it can request the remote port to stop transmitting until the congestion is clear. In a symmetric model, the local port will perform flow control only if the remote port can perform flow control.
- Spanning Tree Protocol: if no information has been received by the end of a forwarding delay, the port returns to a learning state. As a result of new BPDU information, a previously blocked port may now be the root port or the designated port for a given segment. Rather than move directly from the blocked state to the forwarding state, ports go through two intermediate states – the listening state and then the learning state. At the end of a second forwarding delay time, the port switches from the learning state to the forwarding state, thereby allowing frames to be received and forwarded at the port.
- Booting: a ROM IOS image is relatively old, so is not desirable. Net booting is acceptable only if the server is reliable. Booting from Flash is the fastest, but you still need an alternate boot path setup in the event that your flash becomes corrupt. The recommended order to boot images is: Flash, network, ROM.
- IRDP (ICMP Router Discovery Protocol): IRDP uses router advertisements and router solicitation messages to discover the addresses of routers on directly attached subnets. Sometimes a host will receive an ICMP redirect to another destination if the host uses a router with a poor metric to reach a destination.



## Certified Internetworking Troubleshooting

- Multicasting: used when a single packet needs to be sent to multiple destinations. Three ways to multicast are UDP flooding (useful for optimal traffic flow throughout an Internetwork), subnet broadcast (may lead to packet duplication), and IGMP (relies on class D IP addresses for the creation of multicast groups).
- Routing: a route is learned through the wrong interface is caused by a disabled split horizon. Split horizon allows routes to be propagated through interfaces other than the one it came from.
- Serial line over utilization: controlling how the router uses buffers can (to a certain extent) resolve the problem. Cisco routers allocate different size buffers. When a buffer is needed and no existing buffer is available in the free list, a new buffer is created. The count created by the show buffers keeps track of the number of newly created buffers. Of course, a buffer is a limited resource, so if the usage is really too heavy, no matter how you adjust it, the buffer problem will still exist.
- When a router crashes, obtain a full copy of the core dump and let your technical support representative identify the cause.
- Critical error messages: displayed to console. If you set "no logging on" – this will disable logging to all other destinations.
- Access lists: must be put in place intentionally. Other possibilities to an access-list problem are addressing and sub-netting problems. If connection attempts to certain applications succeed while others fail, try the "show running-config" command and determine which access lists cause the problems. Finally, disable the troublemakers.
- Novell servers: use an internal IPX network number that is unique throughout the entire Internetwork. Novell servers auto detect network numbers and frame types during installation. Problems may arise when a Novell server is moved from one segment to another. By default Cisco routers use 802.3 encapsulation for IPX. Watch out for incorrect encapsulation type settings.
- SNMP: causes significant impact on the network due to its almost continuous amount of traffic to the management station.
- LOOPBACK test: to troubleshoot a HDLC (High-level Data Link Control) or PPP (Point-to-Point Protocol) link, put the CSU/DSU in loop-back mode and issue a "show interfaces serial" exec command. This command will check whether the line status changes from "line protocol is down" to "line protocol is up (looped)" or if it remains down. The bottom line is the keep-alive counter should increment. Keep in mind though, there is no loop back in X.25 or Frame-Relay packet- switched networks.
- System image corruption troubleshooting steps:
  - Power cycle the router
  - Press the break key within 60 seconds of booting



## Certified Internetworking Troubleshooting

- In ROM monitor enter "o/r 0x1" to set the configuration register to boot from ROM (1 to reinitialize the router and obtain the correct system image via TFTP)
- Fix the configuration as necessary
- Enter "boot system flash" to change the configuration register to boot from flash memory instead of ROM
- Modem configuration: If you are using IOS Release 11.1 or later, configure your Cisco router to communicate with and configure your modem automatically (use the modem "auto configure discovery line" configuration command). To display the list of modems for which the router has entries, use "show modemcap modem-name." If you want to change a modem value, use "modemcap edit modem-name attribute value line" configuration command.

### **Counters and Measurements**

- Runt: the number of packets discarded because they are smaller than the medium's minimum packet size.
- Under runs: the number of times transmitter has been running faster than the router can handle.
- Ignored - number of received packets ignored by the interface because the interface ran low on internal buffers (not system buffer). The usual causes are broadcast storms and bursts of noise.
- Interface reset: the number of times the interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds, if a serial line a malfunctioning modem is not supplying a transmit clock signal, or if there is a cable problem. Sometimes interface resets can occur when an interface is looped back or shut down.
- Packets pitched: the number of times a router has received its own broadcast packets
- CRC (Cyclic Redundancy Check): the number of times the interface receives packets that fail the Cyclic Redundancy Checksum. On a LAN this usually indicates noise, transmission problems, or a station transmitting bad data.
- Transition counter: the number of times the ring made a transition from up to down or vice versa. A large number indicates a problem with the ring or the interface.
- Switching mode and Cisco 7000 series VIP (Versatile Interface Processor):
  - When debugging is on, the mode is process switched
  - Based on RISC engine
  - One or two port adapters or daughter boards may be attached to a VIP
  - Able to receive route information from the master RSP
  - Able to make its own autonomous, multiplayer-switching decisions for distributed switching



- Supports mixed media

### **Troubleshooting for Serial Lines**

- Show interfaces serial - displays information specific to serial interfaces.
- Show controllers - for serial interfaces on Cisco 7000 series routers use "show controllers cbus." For the Access series products use "show controllers." For the AGS, CGS, and MGS, use "show controllers mci."
- Incorrect DSU or CSU configuration can lead to clocking problem. You can examine the interface and see if CRC, framing errors, and aborts are exceeding an approximate range of 0.5% to 2.0% of traffic.
- Excessively high bandwidth utilization (over 70%) results in reduced performance and possible intermittent failures. Before increasing the bandwidth, you can adjust the router data buffer to help temporarily.

### **Troubleshooting for ISDN**

- Commands:
  - DEBUG DIALER – debug dial-on-demand routing information.
  - DEBUG ISDN EVENT – debug ISDN activity occurring on the user side of the ISDN interface.
  - DEBUG ISDN Q931 – debug information about call setup and teardown of ISDN network connections between local router and network.
  - DEBUG ISDN Q921 – debug data link layer (Layer 2) access procedures that take place at the router on D-channel.
  - DEBUG PPP NEGOTIATION – debug negotiation of Point-to-Point Protocol options and Network Control Protocol parameters.
  - DEBUG PPP AUTHENTICATION - exchange of Challenge Authentication Protocol and Password Authentication Protocol packets.
- Note: in North America, all ISDN lines are connected to the ISDN switch at the local Central Office via a U interface, while in Europe you need an S/T interface.

### **Troubleshooting ATM**

- Allowed encapsulation methods: AAL5, PVC, SVC.
- ISL contains header, original packet, and FCS fields.
- ISL not directly supported by ATM, but can be implemented in ATM LANE configuration.
- Virtual LAN ID (called the COLOR) is 15 bits, which is different for each VLAN.
- Packets on the ISL trunk use: Debug vlan packet.



## **Troubleshooting Frame Relay**

- Typical problems: frame relay link is down, cannot ping remote router, or cannot ping end-to-end.
- Output from "show interfaces serial" can show if the interface and line protocol are down or that the interface is up and the line protocol is down.
- Ensure that both Cisco devices are using IETF encapsulation method - check it out with the "show frame-relay map" command.
- Ensure proper frame relay address mapping by using "show frame-relay map."

## **Troubleshooting FDDI**

- FDDI has two rings with data traveling in opposite directions. One ring is called the primary ring while the other is the secondary ring:
- Primary ring for data transmission, and
- Secondary ring for backup.
- Physical architecture: two or more point-to-point connections between adjacent stations.
- Four separate specifications:
- MAC (Media Access Control) - how the medium is accessed including frame format, methods for error detection (CRC), and error correction.
- PHY (Physical Sub-layer) - data encoding and decoding procedures, clocking requirements, and framing.
- PMD (Physical Medium Dependent) - transmission medium characteristics including power levels, bit error rates and optical components and connectors.
- SMT (Station Management) - defines FDDI station, ring configuration, and ring control.
- Ring control functions include station insertion and removal, initialization, fault isolation and recovery, scheduling, and collection of statistics.
- Supports both synchronous and asynchronous traffic management:
- Synchronous - fully utilizes the network by using a reserved token, best suited for high-demand, low-latency applications such as voice and video.
- Asynchronous - bandwidth is allocated using an eight-level priority scheme and using what is left over after all devices have been allocated synchronous bandwidth. Usually used for continuous stream of data. Please note that FDDI permits extended dialogs to allow stations to temporarily use all available asynchronous traffic.
- Dual ring: if a station on the dual ring fails the dual ring is automatically doubled back on itself into a single ring. The problem for a big FDDI is multiple failures occur in multiple areas and will create isolated rings that cannot talk to each other.
- Optical bypass switches can prevent ring segmentation by eliminating failed stations from the ring.
- FDDI port statuses:



## Certified Internetworking Troubleshooting

- `A` - upstream neighbor is a Physical A type DAS.
  - `B` - upstream neighbor is a Physical B type DAS.
  - `S` - upstream neighbor is a Physical A type SAS.
  - `M` - neighbor is a physical M type concentrator serving as a master to a connection station or concentrator.
  - `UNK` - network server has not completed the CMT process – cannot find out about its neighbor.
- Valid states of the Physical A or Physical B interface are Off, Active, Trace, Connect, Next, Signal, Join, Verify, or Break.
  - To troubleshoot FDDI ring use the command "show interfaces fddi." If both neighbors appear as normal, use ping to test connectivity. If either neighbor has only zeros in the address field, then try using an OTDR (Optical Time Domain Reflectometer) or light meter to test for physical connectivity.
  - A fail-over to a bypass switch: bypass switches do not actually repeat signals.
  - Frames: tokens and data/command frames. A token is not a frame type, but a "field" within a frame. Each token is three bytes in length with a start delimiter, an access control byte, and end delimiter. Data / command frames vary in size.

### **Troubleshoot VLAN**

- To configure a VLAN use RSM in the switch or attach a router to a VLAN trunking port using ISL encapsulation.
- Incorrect VLAN trunking protocol configuration will cause a VLAN to be slow or non-operational. When a line protocol Frame Relay is down, check for timing problems with myseq and my seen keep-alive events, command to show: debug serial interface.

### **Troubleshooting AppleTalk**

- Debug apple events EXEC command: displays information about AppleTalk special events or to find out if neighbors become reachable/unreachable or interfaces go up/down.
- AppleTalk Data Stream Protocol: guarantees that data bytes are delivered in the same order as they are sent and that they are not duplicated.
- AppleTalk Session Protocol: establishes and maintains logical conversations between an AppleTalk client and a server. ASP is considered a session layer protocol.
- AppleTalk Printer Access Protocol: a connection-oriented protocol responsible for establishing and maintaining connections between clients and servers.
- AppleTalk Filing Protocol: allows a client to share server files across a network.



## Certified Internetworking Troubleshooting

- AppleTalk Update-Based Routing Protocol: allows network administrator to connect two or more AppleTalk Internetworks through a foreign network.
- Datagram Delivery Protocol - provides connectionless service between network sockets that can be assigned statically or dynamically. AppleTalk addresses are administered by the DDP and are made up of two components: a 16-bit network number and an 8-bit node number.
- AppleTalk's Name Binding Protocol (NBP): associates AppleTalk names with addresses. AppleTalk's node addresses are assigned dynamically. When a Macintosh starts up it will choose a network layer protocol address and try to find out whether that address is currently in use. If it cannot the new node will assign itself an address.
- AppleTalk's transport layer consists of:
  - Routing Table Maintenance Protocol (RTMP)
  - AppleTalk Update-Based Routing Protocol (AURP)
  - AppleTalk Echo Protocol (AEP)
  - AppleTalk Transaction Protocol (ATP)
  - Name Binding Protocol (NBP).
  - EtherTalk: AppleTalk over Ethernet.
  - TokenTalk: AppleTalk over Token Ring.
  - FDDITalk: AppleTalk over FDDI.
  - LocalTalk: AppleTalk's proprietary media-access system based on contention access, bus topology, and baseband signaling running on shielded twisted-pair media at 230.4kbps. Maximum span of up to 300 meters and support up to 32 nodes.
- Zones: defined by the AppleTalk network manager during the router configuration process. Every node belongs to a single specific zone.
- AppleTalk phase II: extended network having multiple zones.
- Debug apple zip: command to report the discovery of new zones.

### **Troubleshooting IPX**

- NetWare specifies the upper five layers of the OSI reference model.
- Remote access transparent to user through remote procedure calls.
- LAN - runs on Ethernet/IEEE 802.3, Token Ring/IEEE 802.5, Fiber Distributed Data Interface (FDDI), and ARCnet.
- WAN - Point-to-Point Protocol.
- IPX uses RIP to route packets in an Internetwork.
- SAP allows nodes that provide services to advertise their addresses and the services they provide.
- Supports IBM logical unit (LU) 6.2 network addressable units (NAUs) for peer-to-peer connectivity across IBM communication environments.
- SPX - transport layer protocol, reliable and connection-oriented.



## Certified Internetworking Troubleshooting

- Internet Protocol is supported in the form of User Datagram Protocol.
- NCP - services provided include file access, printer access, name management, accounting, security, and file synchronization.
- NetBIOS session-layer interface specification is supported!
- Typical problem for IPX network: Misconfigured client or server, not enough user licenses, mismatched network numbers (all servers on the same LAN must have the same external network number if they use the same frame type).
- Other common problems are:
  - Router interface is down (use show interfaces)
  - Mismatched Ethernet encapsulation methods (use show ipx interface)
  - Ring speed specification mismatch (use the show interfaces token command)
  - Duplicate node numbers on routers (use ipx routing node)
  - Duplicate network numbers (use show ipx servers and show ipx route), and
  - Backdoor bridge between segments (use show ipx traffic).
  - If you are using NetWare 3.12 or above and you have LIPX enabled, a client and server could conceivably negotiate a packet size larger than a router could support, causing intermediate routers to drop packets.
  - RIP timer-value mismatches between routers and servers can cause connectivity problems – use show ipx interfaces to view the state of IPX interfaces. Timer values configured on servers and routers should be the same across the whole IPX network, so use the “ipx update-time” interface configuration command to change the RIP timer interval.
  - When Novell SAP packets are not forwarded through a router running IPX RIP, it may be due to a timer mismatch or a server problem / access list misconfiguration.

### **Troubleshoot Transparent Bridges**

- First developed by DEC.
- Their presence and operation are transparent to network hosts.
- Learn network's topology by analyzing the source address of incoming frames from all attached networks.
- Sees its table as the basis for traffic forwarding.
- Without a bridge-to-bridge protocol, the transparent bridge algorithm fails when there are multiple paths.
- Use “show bridge” to see whether there is a connectivity problem and to make sure that the bridging table includes the MAC addresses of attached end nodes.



- Use "debug spanning-tree" to see whether spanning-tree hello frames are being exchanged.

### **Connectionless Network Service - CLNS**

- Implemented by using the Connectionless Network Protocol (CLNP) and Connectionless Network Service (CLNS).
- ISO 8473 standard.
- CLNP - network-layer protocol to carry upper-layer data and error indications over connectionless links. It is the interface between the Connectionless Network Service (CLNS) and the upper layers.
- CLNS – does not perform connection setup or termination, as paths are determined independently for each packet. It works on best-effort delivery basis only.
- Does not exchange control information (*handshake*) to establish end-to-end connection before transmitting data.
- Other transport-layer protocols will have to take care of error detection and correction.
- IP is a connectionless protocol! It relies on protocols in other layers to establish the connection if connection-oriented services are required.
- IPX specifies a connectionless datagram similar to the IP packet of TCP/IP networks.
- IOS supports packet forwarding and routing for ISO CLNS on networks using data link layers: Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), and serial.
- CLNS routing on serial interfaces is possible with High-Level Data Link Control (HDLC), Point-to-Point Protocol (PPP), Link Access Procedure, Balanced (LAPB), X.25, Switched Multimegabit Data Service (SMDS), or Frame Relay encapsulation.
- The ISO-developed IS-IS routing protocol and Cisco's ISO Interior Gateway Routing Protocol (IGRP) are designed to include support for dynamic/static routing of ISO CLNS.
- ISO CLNS Addressing - addresses in the ISO network architecture are referred to as NSAP addresses and network entity titles (NETs). Each node in has one or more NETs as well as many NSAP addresses. Cisco's implementation supports all NSAP address formats that are defined by ISO 8348/Ad2.
- Key difference between ISO-IGRP and IS-IS NSAP addressing schemes is in area- addresses definition: ISO-IGRP NSAP address includes three separate levels for routing: the domain, area, and system ID, while IS-IS address includes only two fields: a single continuous area field comprising the domain and area fields defined for ISO-IGRP and the system ID.



- The following link has information on troubleshooting CLNS: [http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg\\_v1/tr1912.htm#xtocid27250](http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1912.htm#xtocid27250)
- High-Level Data Link Control - HDLC
- Bit-oriented synchronous data-link layer protocol.
- Developed by ISO.
- Derived from SDLC (Synchronous Data Link Control).
- Specifies data encapsulation method on synchronous serial links using frame characters and checksums.
- Corresponds to Layer 2 and is responsible for the error-free movement of data between network nodes.
- Perform flow control to ensure that data is transmitted only as fast as the receiver can receive it.
- Two distinct HDLC implementations: HDLC NRM (also known as SDLC) and HDLC Link Access Procedure Balanced (LAPB).
- LAPB:
  - Complete data transparency in full-duplex point-to-point operation.
  - Supports peer-to-peer without the need for permanent master station (NRM does need designated permanent master station).
  - Very efficient.
  - Frame window is used to send multiple frames before receiving confirmation that the first frame has been correctly received.
- Three categories of frames:
  - Information frames -transport data across the link and may encapsulate the higher layers.
  - Supervisory frames -perform flow control and error recovery.
  - Unnumbered frames -provide link initialization and termination.
- Maximum frame size depends on the number of CRC bytes at the end of the frame.
- Usually used by [X.25](#).
- Cisco router supports point-to-point software compression on serial interfaces that use HDLC encapsulation to reduce size of a HDLC frame via loss less data compression, using Stacker (LZS) algorithm.
- CiscoMC3810 multiservice access concentrator supports Voice over High-Level Data Link Control (VoHDLC), a variation of HDLC.



Special Thanks to [Michael Yu](#) for contributing material for this Cramsession. Make sure to visit his site at:  
<http://michaelyu.freesevers.com>