



Cisco™ Internetwork Troubleshooting Study Guide

S.J. Iveson

Preface

This document is only relevant:

- **Up to version 12.05 of the Cisco IOS.**
- **To the CCNP v2.0 track.**
- **To the material taught on the CIT course.**
- **To exams 604-506 and 604-606**

This document cannot be used as a cheat to be memorised or learnt by rote in order to pass the relevant CCNP exam without attending a course or having any practical experience. This is generally not possible with Cisco exams anyway, due to their structure and depth.

This guide is intended to be a succinct on-the-job reference or last minute revision tool to be used by candidates who are due to take the exam after having taken a course and/or having had a fair amount of relevant practical experience. Some highly useful real-world information is also included.

These notes were created by the author while studying for the exam using the Cisco authorised course notes. The author passed exam 604-606 second time with a score of 867.

If you have any comments regarding this document please e-mail: sjiveson@routerzone.com or visit my website at www.routerzone.com.

Steven Iveson 2002

ALL INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED "AS IS" WITH ALL FAULTS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. STEVEN IVESON DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

STEVEN IVESON SHALL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR REVENUES, COSTS OF REPLACEMENT GOODS, LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT OR ANY PRODUCT FEATURED, DAMAGES RESULTING FROM USE OF OR RELIANCE ON THE INFORMATION PRESENT, EVEN IF STEVEN IVESON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This document is not sponsored by, endorsed by or affiliated with Cisco Systems, Inc.

CONTENTS

SECTION ONE: Support Resources	5
Physical Network Test Equipment.....	6
Network Monitors.....	6
Protocol Analysers.....	7
Network Management Systems (NMS).....	7
CiscoWorks.....	8
TrafficDirector™.....	8
CiscoWorks for Switched Internetworks (CWSI).....	9
Cisco Netsys.....	9
Cisco Connection Online (CCO).....	9
Cisco TAC.....	13
SECTION TWO: Troubleshooting Methods.....	14
The Cisco Problem-Solving Model.....	15
SECTION THREE: Identifying Troubleshooting Targets	16
Data-Link Troubleshooting Targets.....	17
Show Interfaces Commands.....	17
Show Interfaces Ethernet.....	18
Show Interfaces Tokenring.....	20
Show Interfaces ATM.....	21
Protocol Characteristics.....	22
Protocol Connection Troubleshooting Targets.....	23
TCP Connections.....	23
Novell Connections.....	24
AppleTalk Connections.....	25
SECTION FOUR: Troubleshooting Tools.....	27
Basic Router Architecture.....	28
Router Routing and Switching Processes.....	28
Using Debug.....	29
Logging.....	30
PING – IP.....	30
PING – IPX and AppleTalk.....	31
TRACE – IP.....	32
Information Required by Cisco TAC.....	33
SECTION FIVE: Campus Network Layer Problems	34
IOS TCP/IP Tools and Commands.....	35
TCP/IP Symptoms, Problems and Solutions.....	37
IOS IPX Tools and Commands.....	40
Novell IPX Symptoms, Problems and Solutions.....	42
IOS AppleTalk Tools and Commands.....	44
SECTION X: Glossary & Appendices.....	46
Glossary.....	47

SECTION ONE: Support Resources

Physical Network Test Equipment

Digital Multimeters & Volt-Ohm Meters:

- Low-end electrical test equipment
- Used to measure values such as AC and DC current and resistance
- **Test physical connectivity**

Cable Testers:

- Provide physical layer information
- Normally handheld
- Available for STP, UTP, 10BaseT, coaxial and twinax cables
- Can test cable conditions such as attenuation and noise
- High-end devices include traffic monitoring, wire map functions and limited layer 2 and 3 functionality and testing (network utilisation, MAC information and ping etc.)

Fibre Optic Cable Testers:

- Fibre Optic cable should be tested before and after installation due to it's high cost
- Test light sources provide light at wavelengths 850nm, 1300nm and 1550nm and are used with power meters that measure these wavelengths and test attenuation and return loss in the fibre

TDR's:

- Time Domain Reflectometers identify and locate shorts, opens, kinks, sharp bends and so on in metallic cables.
- Optical TDR's are used for fibre installations
- Both are expensive and used primarily by wiring contractors and telecom engineers

Network Monitors

Network monitors allow administrators to observe current network activity or previous activity over a specific timeframe. Monitors can collect information such as the number of packets, packet size, errors, bandwidth usage and specific host-to-host data flows.

This data can then be used in a variety of ways to analyse network performance, plan for expansion, find bottlenecks and under-utilised areas and establish network baseline performance.

Baselining is now an important tool for network administrators. Network activity is sampled over a specific time period and the statistics collected are used to establish normal network performance, (the baseline). This baseline is then used as a reference point to identify unusual network activity or plan network growth.

Alerts and alarms are used to inform administrators when pre-defined events occur, such as links failing or a high number of errors occurring on a network segment.

Most monitors use SNMP (Simple Network Management protocol) or RMON (Remote Monitoring) MIBs (Management Information Bases) to gather information and statistics from network devices.

REAL WORLD: Beware, SNMP traffic can consume large amounts of bandwidth

Protocol Analysers

Protocol analysers are used to collect, display and analyse network data and traffic. The information captured is decoded into a readable format detailing frame type, OSI layer and protocol information and function, (as well as application data).

Most allow filtering so you can collect and view specific protocol or source/destination traffic flows to aid troubleshooting of specific issues.

Some analysers also allow you to generate traffic to allow you to plan capacity or load test devices.

Network Management Systems (NMS)

Network managements systems generally include a large range of tools to ease the management and administration of large and/or complex networks and automate the execution of tasks that would be time consuming and laborious if performed manually.

The ISO have defined five areas of network management that an NMS should address:

- *Fault Management
 - Determine where faults have occurred and raise appropriate alerts
 - Isolation of failed areas from the rest of the network
 - Reconfiguration of the network to lower the impact of operating without failed components or areas
 - Repair or replacement of failed components
- Accounting Management
- *Configuration and Name Management
 - Control and modify the configuration of components
 - Ability to do so in response to faults or changes
- Performance Management
- Security Management

*Fault and configuration management are most relevant to troubleshooting.

CiscoWorks

CiscoWorks can be integrated with SunNet Manager, HP OpenView and IBM NetView for AIX

Cisco's 'flagship' NMS contains:

- Device level monitoring
- Configuration management tools
- Fault management tools

The CiscoView Product:

- Web based, graphical 'real-world' display and basic configuration of Cisco devices
- Monitoring functions
- Basic troubleshooting

The Cisco Resource Manager Product:

- Web based applications for inventory and configuration management and software distribution, the 4 applications are:
 - Inventory Manager
 - Availability Manager
 - Syslog Analyser
 - Software Image Manager
- Dynamically tracks device information, software versions and device configuration information

REAL WORLD: This product is now know as RME, Resource Manager Essentials

TrafficDirector™

TrafficDirector can be run on: NT, SunOS, Solaris, HP/UX and IBM-AIX

An RMON application, TrafficDirector analyses traffic within switched internetworks. "A common traffic analysis and performance application for managing the embedded RMON agents within Catalyst™ switches and standalone Cisco SwitchProbe™ products."

TrafficDirector Can:

- Quickly discover traffic utilisation, broadcast levels, error rates etc. on any port or group of ports
- Generate alerts when predefined thresholds are exceeded on Catalyst switch ports
- Use data collected by SwitchProbe products (network usage can be analysed at the link, network, transport and application layers)
- Remotely capture packets

TrafficDirector Can be Used To:

- Perform analysis of network traffic flows
- Troubleshoot protocol related issues
- Report long term traffic trends
- Generate proactive alarms prior to problems affecting users

CiscoWorks for Switched Internetworks (CWSI)

CWSI can be integrated with SunNet Manager, HP OpenView and IBM NetView for AIX.

The CWSI suite contains:

- VLANDirector™
- TrafficDirector™
- CiscoView

The VLANDirector™ Product:

- Topology mapping using an auto discovery function. This provides a view of Cisco switches and routers within the network and enables administrators to display logical VLAN information superimposed on the underlying physical network
- VLAN management (including drag and drop configuration)
- Automatic configuration of inter-switch links

Cisco Netsys

REAL WORLD: This network simulation and modelling tool is no longer developed by Cisco.

Cisco Netsys could be used to:

- Test new network designs
- Plan and test network reconfiguration or change plans
- Stress test a network topology
- Give a measure of the network performance you should expect in any the above cases

Cisco Connection Online (CCO)

Found at: www.cisco.com

There are two levels of access:

- Guest – For the general public, access to general company and product information
- Registered – Customers who have purchased a support contract or have been sponsored by a Cisco authorised partner. Access to additional in-depth information and advanced online applications and services.

CCO's CD and web based tools enable you to:

- Prevent and correct problems
- View resources on how to design, order, configure, support and provide spares for Cisco products
- Detect, identify, track and resolve bugs

CCO Documentation

Found at: <http://www.cisco.com/univercd/home/home.htm>

Available online and on CD CCO documentation includes:

- Cisco IOS™ and CatOS release notes, configuration guides and command references
- Debug command references and system error message information
- Cisco MIB quick reference
- Quick configuration guides
- The Cisco product catalogue
- Hardware installation guides
- Client/server software installation guides
- General configuration notes for upgrades, NICs, rack-mount kits and other field upgrade products

CCO MarketPlace Product Centre

Found at: <http://www.cisco.com/go/marketplace/> - registration is required

The Cisco MarketPlace allows the purchase of Cisco software product over the Internet.

The IPeXchange is used for immediate download of software orders.

The IPC (Internetworking Products Centre), is used for products shipped in the traditional manner.

MarketPlace utilities and services include:

- Status Agent
 - Allows tracking of order progress and status
- Pricing Agent
 - Access to the online product price lists including the option to download locally
- Configuration Agent
 - Search of configurable products and online product configuration
- Service Order Agent
 - Real-time access to service order status
 - Service Order Submit
 - Service Order Status
 - Service Parts Agent (Field replaceable parts)
- Service Parts Agent

CCO Software Center

Found at: <http://www.cisco.com/public/sw-center/> - registration is required

Previously known as the software library.

Software Center utilities and services include:

- Obtain major upgrades and maintenance releases of Cisco software
- Obtain selected demonstration and beta distributions for the latest products
- Use of Software Upgrade Planners which include literature, release information etc.
- Checksum and MD5 values for software integrity checking
- Use Software Checklists to ensure current availability and compatibility of software for various platforms
- Obtain custom software such as custom or critical fixes

CCO Bug Navigator, Alert and Watcher

Found at: <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl> - registration is required

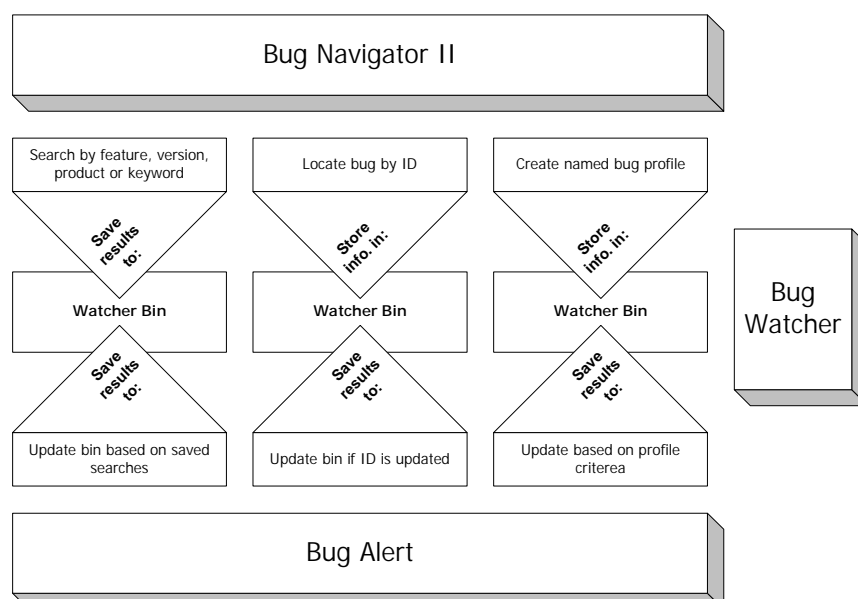
REAL WORLD: Now known as the Bug Toolkit

Bug Navigator II:

- Search for known bugs based on software version, feature set or keyword
- Locate information on bugs if you know the ID no.
- Search results can be saved in Watcher Bins and you can also create Alert Agents to update bins with new bug alerts, based on criteria you specify

Bug Watcher:

- Allows the creation of multiple Watcher Bins which can be used to 'watch' the status of pre-selected bugs
- You can also create Alert Agents to update bins with new bug alerts, based on criteria you specify



CCO Troubleshooting Engine

Found at: <http://te.cisco.com/SRVCS/cgi-bin/webcgi.exe?New,KB=TE> - registration is required

REAL WORLD: Now known as the Troubleshooting Assistant

- Automated software for solving common and/or simple problems
- You select a problem area and you will then be prompted for more and more specific information until a list of suggested possible resolutions can be found
- Even if a specific answer cannot be found, links to suitable troubleshooting and informational documents are presented to assist you further
- Not suitable for issues requiring debugging etc.

CCO Stack Decoder

Found at: <http://www.cisco.com/cgi-bin/Support/Stackdecoder/stackdecoderinput.pl>
- registration is required

Used to troubleshoot stack traces, which are generated when a device encounters conditions it has not been designed to expect, such as a hardware failure.

Use the **show stack** command to display stack traces.

Stack Decoder decodes the stack trace that you provide and provides a list of likely diagnosis, normally including bug ID's and/or hardware diagnostics.

CCO Open Forum

Found at:

This forum allows you to:

- Browse the Q&A database, which contains answers to common technical questions
- Enter a natural language question that is parsed and submitted to a search engine
- Send questions to the Open Forum, allowing real-time communication with other Open Forum users

Cisco TAC

Found at: <http://www.cisco.com/tac>

The Cisco Technical Assistance Center (TAC) provides warranty, contracted and chargeable support for all Cisco products.

The TAC recommend you do all you can to troubleshoot an issue prior to contacting them.

If you do need to open a case you should do the following prior to doing so:

1. Gather all relevant facts to define the issue. This includes obtaining output from the **show tech-support** command on all relevant devices, relevant **debug** output and any other relevant information
2. Gather all relevant information regarding your support contract or warranty. This should include serial and model no's for affected devices
3. Decide on the priority of your issue:
 - 1 – Network down
 - 2 – Network severely degraded
 - 3 – Network performance degraded
 - 4 – Information required on product capabilities, installation or configuration

When you log a case with the TAC a Customer Support Engineer (CSE) will assign a case number to the issue, your case will then be passed to an appropriate Customer Engineering Response Team (CERT).

A service action plan will be created to resolve your issue.

CCO Case Management Toolkit

Found at:

This tool allows you to:

- Open a new TAC case - Case Open
- Check the status of outstanding cases - Case Query
- Add your own notes to an outstanding case - Case Update

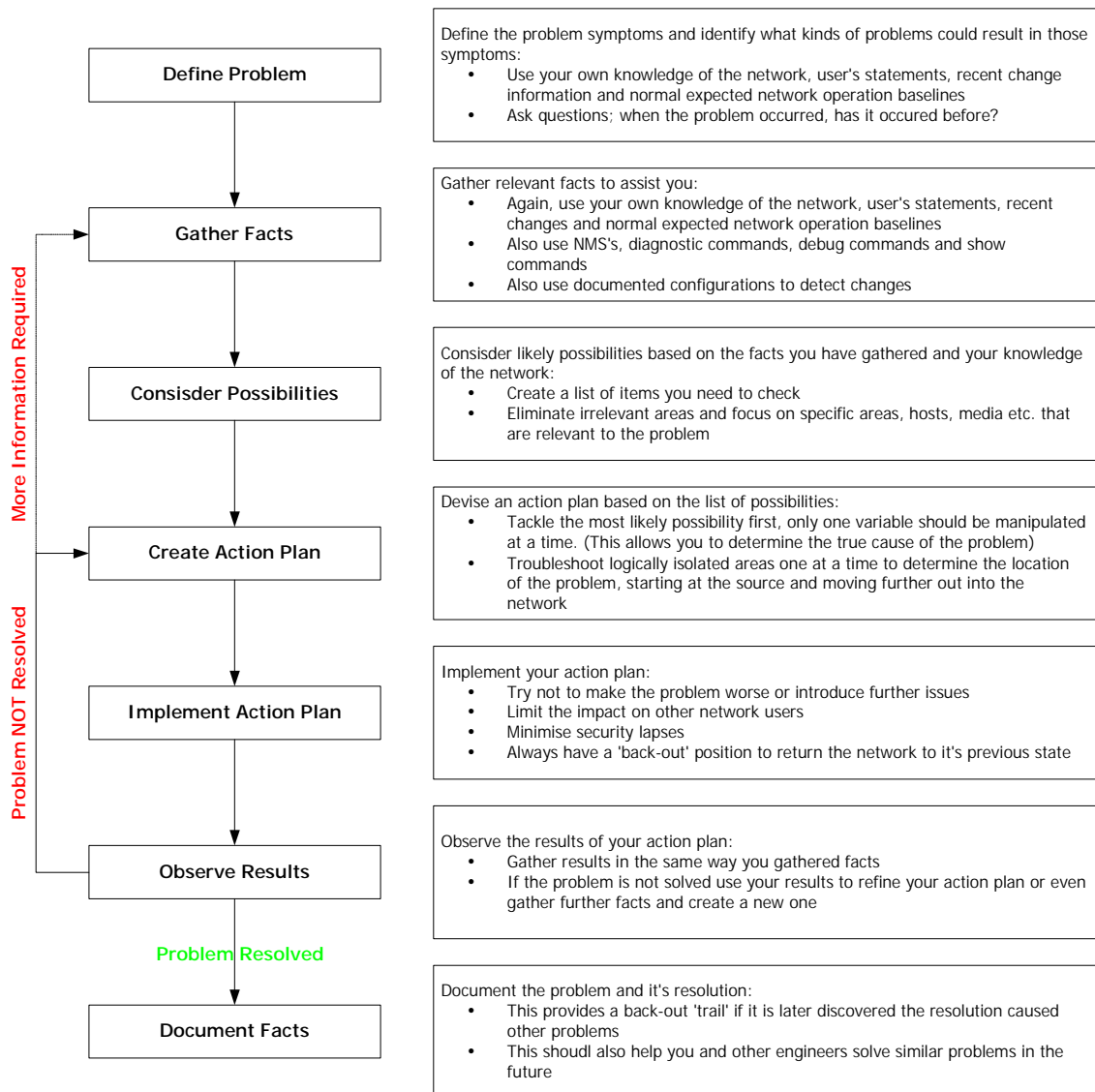
SECTION TWO: Troubleshooting Methods

The Cisco Problem-Solving Model

Cisco encourage the use of troubleshooting models such as this one.

If you use your own troubleshooting model, Cisco do not expect you to stop using it in favour of this model.

If your knowledge allows you to bypass part or all of a model, for instance because you have experienced a particular issue before, do so.



SECTION THREE: Identifying Troubleshooting Targets

Failures at lower layers in the OSI model normally affect and cause issues with higher layers, therefore always start your troubleshooting efforts at the lowest appropriate layer.

Data-Link Troubleshooting Targets

Data-Link troubleshooting targets consist of physical device connections between interfaces, the interfaces themselves and layer 2 protocols.

Data-Link troubleshooting relies on the assumption that physical layer connections are operating correctly, this may require hands-on checking.

Data-Links can be divided into two parts, the hardware and logical or software portion.

Hardware:

- Physical layer functioning
- Interfaces operation

Software:

- Keep-alives
- Hello messages

Show Interfaces Commands

To diagnose hardware, interface problems statistical counters can be highly useful.

To view interface counters use the command:

To see when the counters were last cleared:

```
router#show interfaces
```

To diagnose an existing issue reset the counters using the command:

```
router#clear counters
```

Show Interfaces Ethernet

On a Cisco 7000 router you must specify a slot/port argument when using this command otherwise information on all interfaces will be displayed.

router#**show interfaces Ethernet 1**

```
Ethernet1 is up, line protocol is up
  Hardware is Am79c970, address is 0000.0c5c.c364 (bia 0000.0c5c.c364)
  Description: To BHSwitch3 po 16 cab A9 comms room 2
  Internet address is 149.191.0.137/26
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 1w4d
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 375 drops
  5 minute input rate 28000 bits/sec, 29 packets/sec
  5 minute output rate 19000 bits/sec, 10 packets/sec
    11143775 packets input, 193886024 bytes, 39 no buffer
    Received 5276742 broadcasts, 0 runts, 0 giants, 375 throttles
    7 input errors, 7 CRC, 6 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    3986967 packets output, 801596896 bytes, 0 underruns
    0 output errors, 7574 collisions, 0 interface resets
    0 babbles, 0 late collision, 13130 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

Output fields include:

Ethernet x is up down administratively down	Indicates if hardware is active or not or if it has been 'forced' down by an administrator
Line protocol in up down	Indicates if the software processes that handle the line protocol consider the interface usable, i.e. if keepalives are successful. If the interface misses 3 successive keepalives the line protocol is considered down
Keepalive	Whether keepalives are set
Output queue, input queue and drops	Number of packets in the input and output queues, size of the queue and the no. of packets dropped due to a full queue
No buffers	Number of received packets discarded due to a lack of software (system) buffer space. Ethernet broadcast storms are often responsible for these events
Received broadcasts	Number of broadcast or multicast packets received. This should ideally be under 20% of the total number of received packets
Runts	Packets discarded because they are smaller than the minimum Ethernet packet size of 64bytes. Usually caused by collisions, more than 1 runt per million bytes received should be investigated
Giants	Packets discarded because they exceed the MTU. Packets greater than 1518 bytes are

	giants
CRC	The Cyclical Redundancy Checksum generated does not match that calculated from the data received. Usually indicates noise or transmission problems on a LAN interface. A large no. of CRC errors may be caused by collisions or a host transmitting bad data. More than 1 CRC per million bytes received should be investigated
Frame	Number of packets received with a CRC error and a noninterger no. of octets. Normally due to collisions or a malfunctioning device
Overrun	Number of times the interface was unable to pass received data to a hardware buffer because the input rate exceeded the interfaces ability to handle the data
Ignored	Number of packets ignored because the interface ran low on internal hardware buffers. Caused by broadcast storms and bursts of noise
Collisions	Messages retransmitted due to a collision. Usually caused by malfunctioning NIC's or over extended LAN segments. Collisions should ideally account for less than 0.1% of output packets. A packet that collides is only counted once in output packet statistics
Resets	Can occur if packets queued for transmission are not sent within a few seconds. Can also occur when an interface is shut down or looped back
Restarts	Number of times a type 2 controller was restarted because of errors

Show Interfaces TokenRing

On a Cisco 7000 router you must specify a slot/port argument when using this command otherwise information on all interfaces will be displayed.

router#**show interfaces tokenring 0/1**

Output fields include: (See the Ethernet section for other common fields not listed here. Remember that collisions cannot occur on a Token Ring).

TokenRing x is up down administratively down	Indicates if hardware is active or not or if it has been 'forced' down by an administrator
TokenRing is Reset	A hardware error has occurred
TokenRing is initialising	In the process of inserting into the ring
Line protocol in up down	Indicates if the software processes that handle the line protocol consider the interface usable, i.e. if keepalives are successful. If the interface misses 3 successive keepalives the line protocol is considered down
Keepalive	Whether keepalives are set
Ring Speed	4 or 16 Mbps
Single ring multiring node	Whether this node is enabled to collect and use source-routing (RIF) information for routable Token Ring protocols
Group Address	A multicast address, maximum of one
Resets	Resets can be performed manually or automatically when errors occur. An increasing value points to a loose cable failure.
Transitions	Number of times the ring has gone up or down. A large number indicates problems with the ring or interface

Show Interfaces ATM

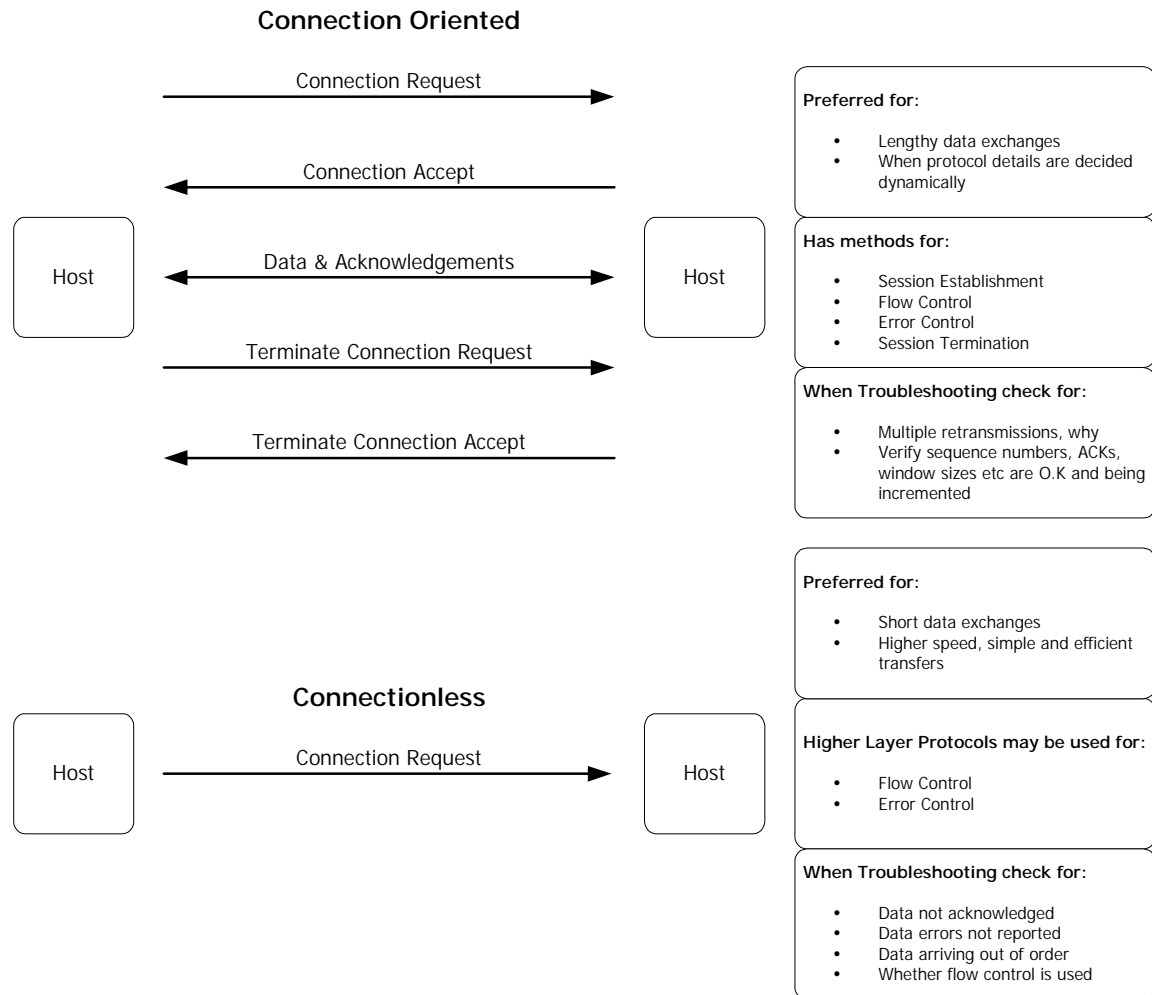
router#show interfaces atm 3/1

Output fields include: (See the Ethernet section for other common fields not listed here).

ATM x is up down administratively down	Indicates if hardware is active or not or if it has been 'forced' down by an administrator
Line protocol in up down	Indicates whether the software processes that handle the line protocol think the line is usable
NSAP Address	The prefix provided by the ATM switch followed by an End System Identifier (ESI) address
Encapsulation	AAL5, PVC or SVC mode
Signalling vc, vpi, vci	Number of signalling PVC's, virtual path identifiers and virtual channel identifiers
Output hang	Time since the interface was last reset because of a transmission that took too long

Protocol Characteristics

High-level information about routed and routing protocols can be displayed using the `router#show protocol traffic` command



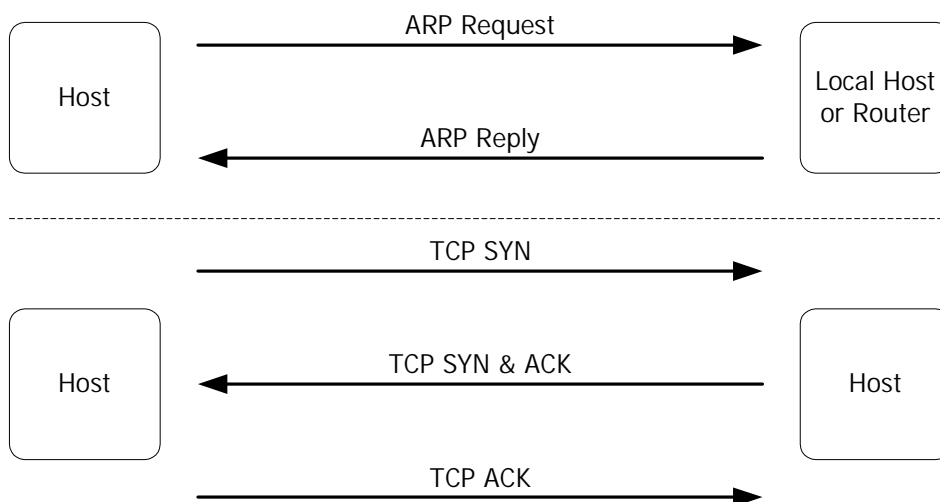
Protocol Connection Troubleshooting Targets

Routed and Routing Protocol Connection Sequences:

TCP/IP	ARP, SYN, ACK
Novell NCP	GNS, SAP, RIP
AppleTalk	RTMP, ZIP, NBP and ATP

TCP Connections

Connection oriented, using a 3-way handshake



ARP is used to resolve TCP/IP addresses to layer 2 addresses

When troubleshooting TCP/IP connection issues use the command:

`router#show ip arp` to view the ARP cache entries on a device. Check for anomalies and/or if a specific host is present in the cache.

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	149.191.9.35	1	0050.dad0.2a1d	ARPA	Vlan82
Internet	149.191.11.33	2	0050.dae4.d4cb	ARPA	Vlan84
Internet	149.191.10.32	3	0050.dafd.cdeb	ARPA	Vlan83
Internet	149.191.4.46	25	0050.8bdc.d983	ARPA	Vlan41

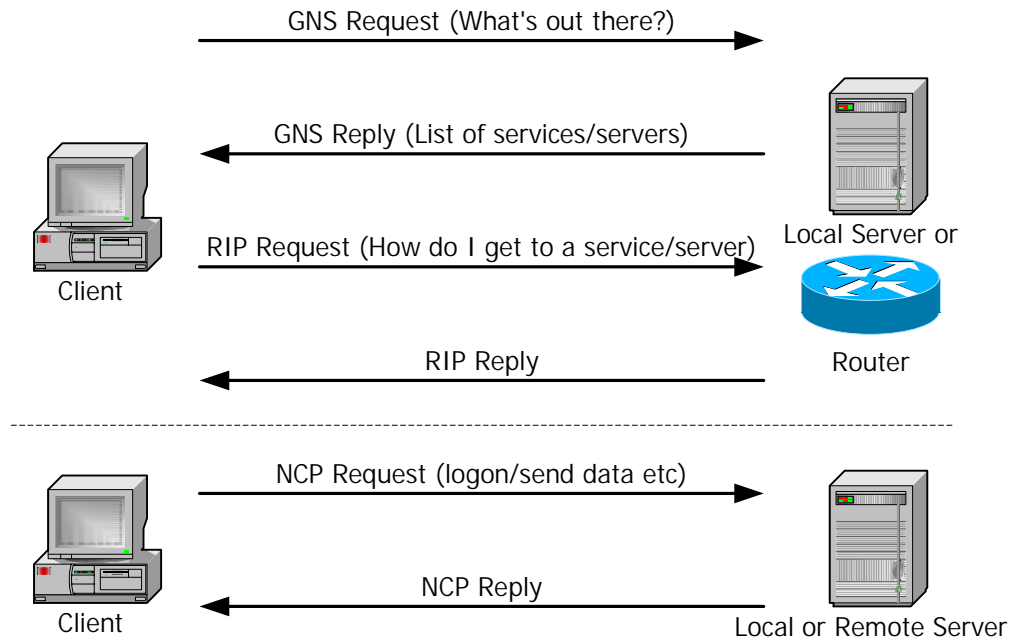
Type = Encapsulation Type (ARPA, SNAP or SAP (802.3))

The following additional input can also be used to refine output:

<code>router#show ip arp 0080-6A9C-55E1</code>	View the entry for a specific MAC address
<code>router#show ip arp 170.161.10.12</code>	View ARP entries for a specific IP address
<code>router#show ip arp hostname</code>	View ARP entries for a specific host
<code>router#show ip arp ethernet0</code>	View all ARP entries learned on this interface

Novell Connections

NCP (Novell Core Protocol) is connection orientated



When troubleshooting Novell IPX connection issues use the command:

router#**show ipx traffic** to view IPX traffic and error statistics.

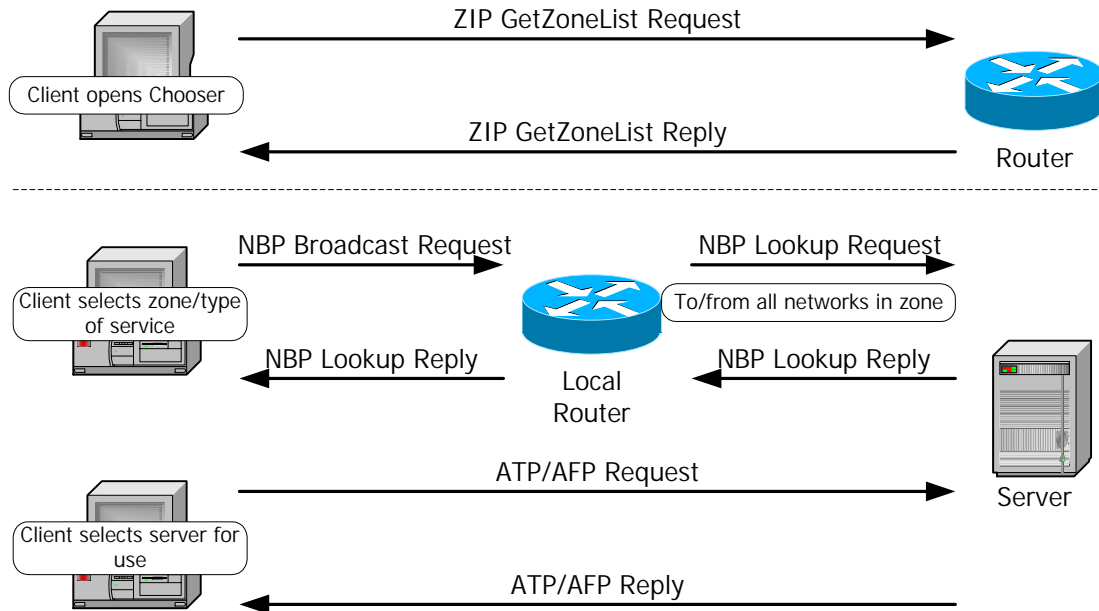
Output fields include:

Format Errors	Increments whenever a bad packet (e.g. corrupted header) is detected. Can suggest an encapsulation mismatch
Bad Hop Count	Increments when a packet's hop count exceeds 16. Can suggest a backdoor bridge
Encapsulation failed	Increments when the router is unable to encapsulate a packet. Can be due to unsupported encapsulation types or and interface hardware problem
Unknown	Increments when packets are encountered that the router is unable to forward. (This could be due to a bad helper-address or no route available)

The command router#**show ipx interface** can also be used to ensure the correct router interfaces and line protocols are up.

AppleTalk Connections

ATP (AppleTalk Transaction Protocol) is connection orientated



When troubleshooting AppleTalk connection issues use the command:

router#**show appletalk traffic** to view IPX traffic and error statistics.

Output fields include:

Checksum Errors	Packets directed to the router that were discarded because their DDP checksum was incorrect. The DDP checksum is not verified for forwarded packets.
Bad Hop Count	Increments when a packet's hop count exceeds 15.
Encapsulation Failed	Increments when the router is unable to encapsulate a packet. Can be due to DDP packet encapsulation failure or because AppleTalk ARP resolution failed
ZIP receives, sent and netinfo	ZIP packets the router received and sent and the number of packets that requested port configuration via ZIP GetNetInfo requests. If ZIP requests are greater than 10 and increasing a ZIP storm is probably occurring
Unknown	Packets discarded because they had the wrong encapsulation, i.e. nonextended AppleTalk packets were on an extended Appletalk network and/or vice versa

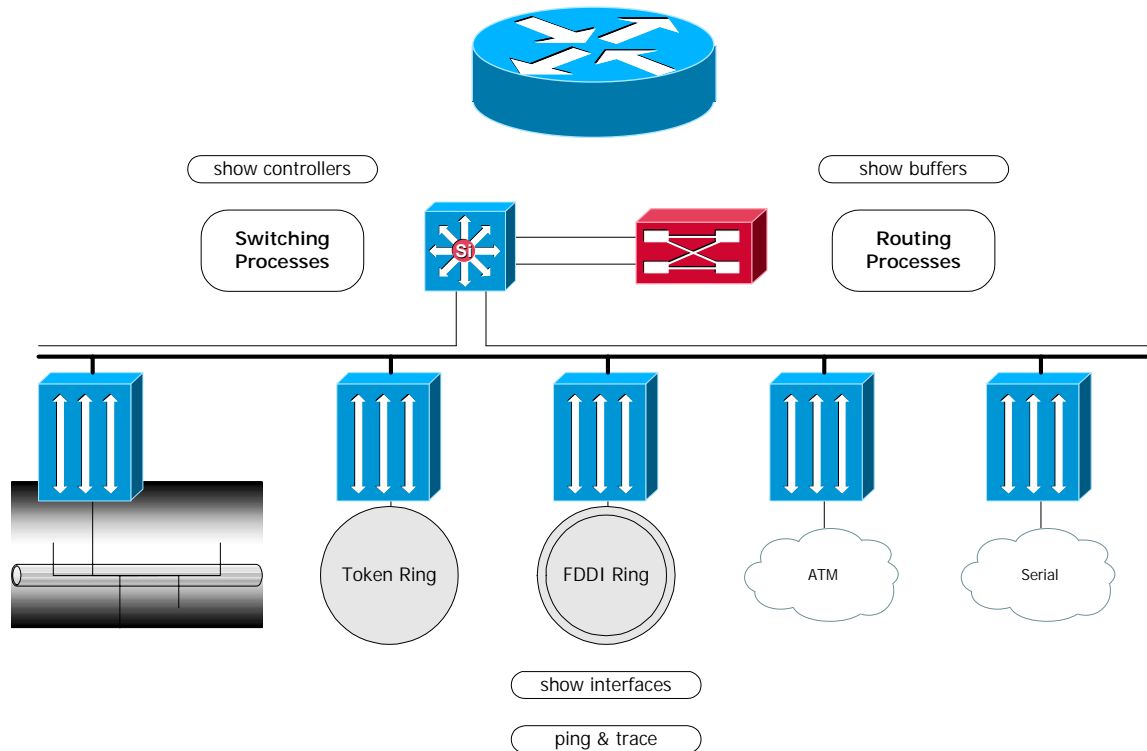
The command `router#show appletalk interface` can also be used to ensure the correct router interfaces and line protocols are up.

This command will also display configuration mis-matches which occur if all the routers on a given cable do not agree on the cable configuration, (network number, cable range, zone name or zone list).

SECTION FOUR: Troubleshooting Tools

Basic Router Architecture

This diagram displays the basic architecture of a Cisco 7000 router:



Router Routing and Switching Processes

Routing Functions:

- Identify the best path traffic should take to a destination over an interface
- Processor intensive

Switching Functions:

- Moves packets, frames or cells between interfaces
- Less processor intensive

Both types of functions occur within a router.

There are several types of routing and switching that a router may use (dependant on hardware).

Switching Types:

- Process Switching
 - Slowest type of switching
 - Always used when initialising
 - Always used with broadcasts, routing updates etc, debugging, error logging, SNMP, protocol translation, tunnelling, custom and priority queuing, keepalives and link compression
 - Available on all models
- Silicon Switching
- Autonomous Switching
- Fast Switching
 - Available on the 2000, 3000 and 4000 series
- Optimum Switching
 - Available on the 7500 series

Using Debug

Debugging a data flow will force the device to use process switching for that data flow.

A router will give debugging processes a higher priority than other packet data flow.

Use the router#**show processes cpu** command to access how loaded a router is before using debug commands. With over 50% utilisation you should consider using event rather than packet debugging

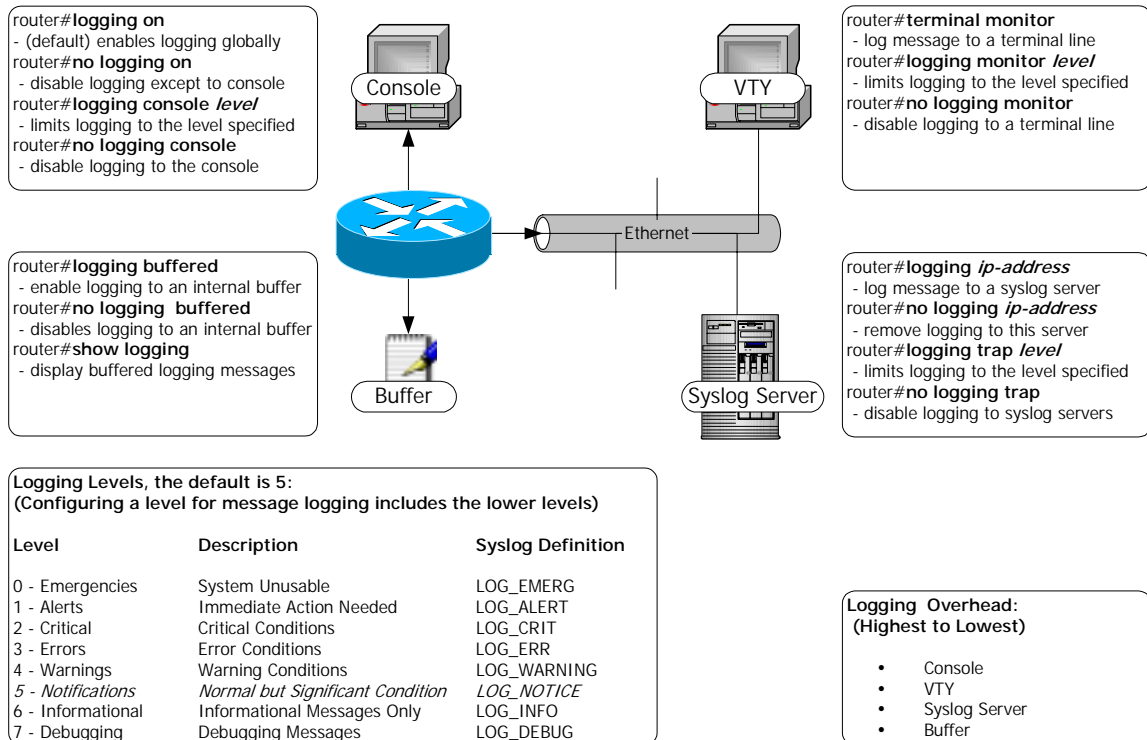
```
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID  Runtime(ms)   Invoked  uSecs   5Sec   1Min   5Min  TTY  Process
  1         0           33870    0      0.00%  0.00%  0.00%  0  Load Meter
  2      11728       482990   24      0.00%  0.00%  0.00%  0  OSPF Hello
  3     104256       17210   6057    0.00%  0.07%  0.05%  0  Check heaps
  4         0             1        0      0.00%  0.00%  0.00%  0  Chunk Manager
.....
```

It is recommended you use the router#**service timestamps [type][time format]** command to put a time stamp on debug and log message. This is useful for determining when events occur and the time period between events.

```
router(config)#service timestamps debug datetime
router(config)#service timestamps log datetime
```

Use the commands: router#**no debug [argument | all]** or router#**undebug all** to turn off debugging.

Logging



PING – IP

PING uses the echo and reply functions of ICMP.

Router>**ping** *hostname* or *ip-address*

Returned characters and their meanings follow:

!	Receipt of a reply
.	Timeout
U	Destination Unreachable
N	Network Unreachable
P	Protocol Unreachable
Q	Source Quench
M	Could not fragment
A	Administratively Prohibited
?	Unknown Packet Type

Commands: **router#show ip icmp** and **router#debug ip icmp** traffic may be useful when used in conjunction with PING.

Extended options are available when in privileged mode, these can be accessed with the command: **router#ping** [ENTER]

PING – IPX and AppleTalk

IPX:

Router>**ping ipx address**

Because Cisco developed an IPX ping before Novell, Novell devices may not respond to an IPX ping from a Cisco device.

If they do not, use the command: **router#ipx ping-default novell**, or use the extended privileged mode ping and answer yes to the Novell Standard Echo prompt.

REAL WORLD: You cannot use this command to ping a router from itself, except on the 7000

Returned characters and their meanings follow;

!	Receipt of a reply
.	Timeout
U	Destination Unreachable PDU was received
C	A congestion experience packet was received
I	User interrupted the test
?	Unknown packet type
&	Packet lifetime exceeded

AppleTalk:

Router>**ping appletalk address**

REAL WORLD: You cannot use this command to ping a router from itself except on Ethernet interfaces that support hearing themselves

Returned characters and their meanings follow;

!	Receipt of a reply
.	Timeout
B	A bad or malformed echo was received from the target address
C	An echo with a bad DDP checksum was received
E	Transmission of an echo packet failed
R	Transmission of an echo packet failed due to no route to the target

Trace

router>**trace** *hostname* or *ip-address*

The trace command sends probe datagrams with a TTL of 1 to the first router used to reach the destination host. This probe causes the router to discard the datagrams and return 'time exceeded' error messages. The trace command then sends several further probes and displays the round trip time for each.

After every third probe the TTL is increased by one and therefore the next router on the path to the destination is 'tested'. The command only terminates when the destination responds, when the maximum TTL is exceeded or when the user interrupts the trace.

Returned characters and their meanings follow:

1	Sequence number of the router in the path to the host
Hostname.domain-name	Hostname of a router
Address	IP address of a router
10msec 9msec 8msec	Round trip time for each of the three probes sent
*	The probe timed out
?	Unknown packet type
Q	Source quench
P	Protocol unreachable
N	Network unreachable
U	Port unreachable
H	Host unreachable

If a host appear multiple times a routing loop could be present in the network

Extended options are available when in privileged mode, these can be accessed with the command: router#**ping** [ENTER]

Information Required by Cisco TAC

When placing a call with Cisco TAC you will be expected to provide the following information depending on the issue:

Note: Most of these commands are now included in the **show tech-support** command

<p>General Information:</p> <p>Problem History & Symptoms #show version</p> <p>A detailed network diagram</p>	<p>Gives details of:</p> <p>Software versions, bootstrap version, boot date, router uptime, log of how the system was last restarted - this could be an error message, boot location, configuration register</p>
<p>Crash or Hang Issues:</p> <p>#show stacks</p> <p>#write core</p> <p>#exception dump ip-address</p>	<p>Gives details of:</p> <p>Gives reason for the last system restart, used by TAC to identify bugs etc. Generated when a router encounters a set of conditions it has not been programmed to handle</p> <p>Useful if the router is malfunctioning but has not crashed. Used by TAC. The core dump (memory image) is written to a file <i>hostname-core</i> on a specific TFTP server you specify</p> <p>Sets the router to automatically write a core dump to the TFTP server you specify, when a crash occurs</p>
<p>Lost Data or Performance Issues:</p> <p>#show interfaces</p> <p>#show buffer</p> <p>#show memory</p> <p>#show process</p> <p>#show protocol</p> <p>#show protocol traffic</p>	<p>Gives details of:</p> <p>Shows various interface details and statistics</p> <p>Displays statistics for the memory buffer pools on a router</p> <p>Displays statistics about a routers memory, including free pools</p> <p>Displays information about active processes, it is recommended you take snapshots of this output at least one minute apart and then compare them to see which processes are invoked most often. Use keywords cpu or memory to show specific details</p> <p>Displays routed and routing protocol information</p> <p>Displays detailed routed and routing protocol traffic statistics</p>
<p>Loss of Functionality Issues:</p> <p>#show interfaces</p> <p>#show protocol</p> <p>#show protocol traffic</p>	<p>Gives details of:</p> <p>Shows various interface details and statistics</p> <p>Displays routed and routing protocol information</p> <p>Displays detailed routed and routing protocol traffic statistics</p>
<p>Optional Information:</p> <p>Debug captures</p> <p>Protocol analyser output</p>	<p>Gives details of:</p> <p>Shows various interface details and statistics</p> <p>Displays routed and routing protocol information</p> <p>Displays detailed routed and routing protocol traffic statistics</p>

SECTION FIVE: Campus Network Layer Problems

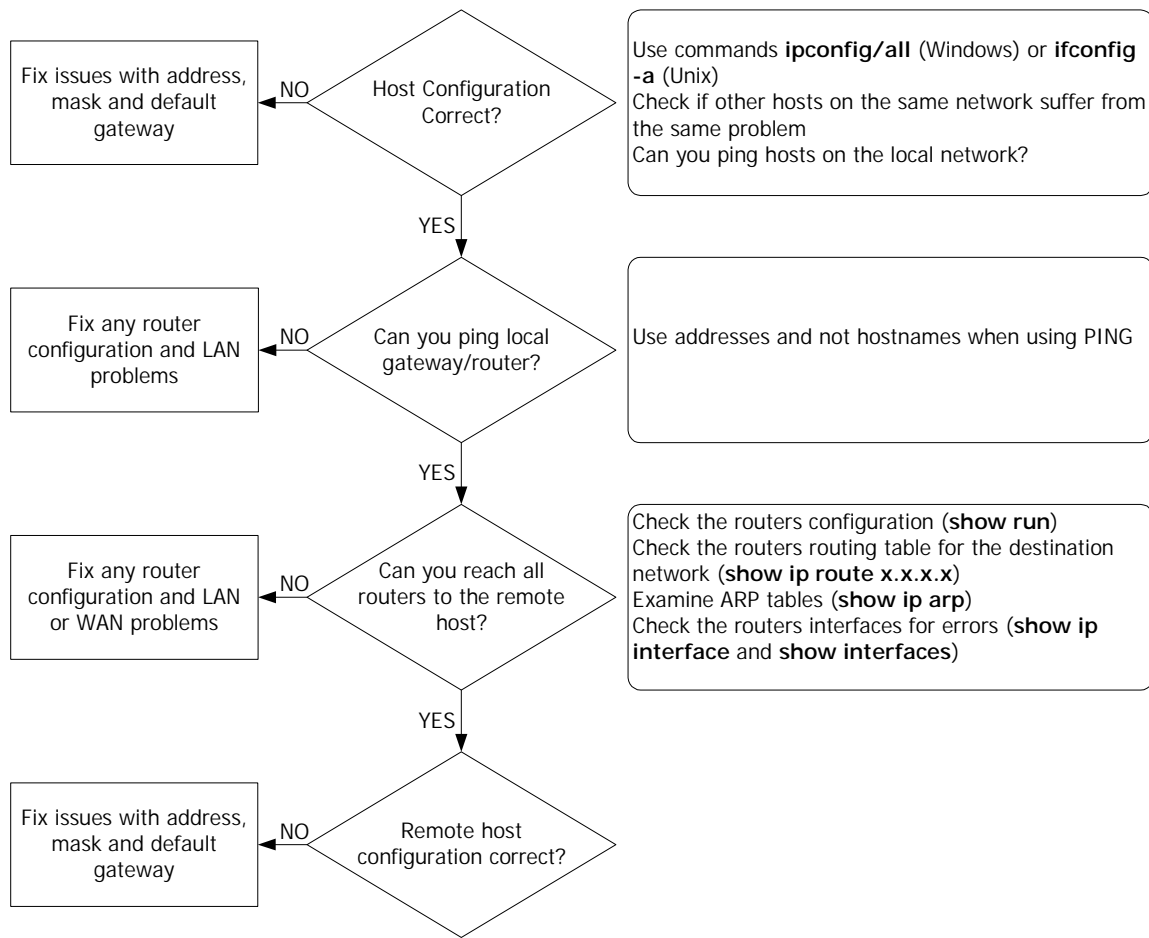
IOS TCP/IP Tools and Commands

Useful troubleshooting **show** commands include:

#ping	Tests connectivity to a host
>show ip interface	Displays IP related configuration of specified interfaces Check if interfaces are up Check addressing and masks are correct
>show ip protocols	Displays parameters and the state of all active routing protocols Check update intervals and administrative distances Check if access-lists are used and redistribution taking place
>show ip route	Displays the routing table
>show ip traffic	Displays statistics on IP protocol process and traffic Check for errors
>trace	Tests the route used to reach a host
>show ip access-list	Displays the contents of access lists and how many matches have been made
>show ip arp	Displays the routers ARP cache

Useful troubleshooting **debug** commands include:

#debug ip eigrp	Displays EIGRP packets sent and received on an interface
#debug ip icmp	Displays ICMP messages Useful for troubleshooting end-to-end connectivity
#debug ip igrp events	Displays summary information on IGRP routing messages including the source and destination of updates Useful for when the network is busy and there are too many networks in your routing table
#debug ip packet	Displays the flow of IP packets transmitted between local and remote hosts An access-list-number argument lets you limit the scope and load placed on the router by this command Useful for troubleshooting end-to-end connectivity
#debug ip rip	Displays RIP packets sent and received on an interface Useful for investigating Windows 95/NT issues as RIP is one of the default routing protocols used
#debug arp	Displays ARP transactions Useful for checking if the router and other hosts are sending and receiving ARPs Useful for situations where some hosts on a network are responding but some are not



Things to check for when you encounter issues with Windows based clients:

Inaccurate or incomplete resolution of non-IP entities into IP addresses (name resolution)

, Check:

- LMHosts file
- Hosts file
- WINS and DNS servers

Inappropriate sources for browser update information on the network, i.e. too many master browsers

TCP/IP Symptoms, Problems and Solutions

Symptom	Problem
Hosts cannot access remote hosts through a router	No default gateway configured on local hosts
	Misconfigured subnet mask configured on local hosts
	Router between hosts is down
Hosts cannot access certain networks through router	No default gateway configured on local hosts
	Misconfigured access list
	Discontiguous network due to poor design or link failure
Users can access some hosts but not others	Misconfigured subnet mask configured on local hosts
	Misconfigured access list
	No default gateway configured on remote host
Some services are available but others are not	Misconfigured extended access list
Users cannot connect when one redundant path is down	Discontiguous network due to link failure
	Routing has not converged
	Misconfigured access list or other routing filters
Router sees duplicate routing updates or packets	Bridge or hub in parallel with router
Certain protocols are being routed, others are not	Misconfigured access list
Routers or hosts cannot reach certain parts of their own network	Subnet mask configuration mismatch between router and host
	Misconfigured access list
	No default gateway specified
Routing is not working when redistribution is used	Missing redistribute or default-metric command
	Problem with default administrative distance

Unix Host Issues

Problem	Solution
No default gateway configured on local or remote host	Check routing table of host using netstat - rn
	If there is no default use the route add default address 1 command where address is the address of the default gateway
	To boot with a default gateway already configured specify the default gateway in host file /etc/defaultrouter
Misconfigured subnet mask on local or remote host or router	Check host file /etc/netmasks and /etc/rc.local
	Check host configuration with ifconfig -a
	Check router configuration with show ip interface
Router between hosts is down	Ping outwardly until problem area located
	Check and fix router configurations
	Check and fix intermediate LAN or WAN problems
Misconfigured access list or other filter	Use ping and trace to isolate router with misconfigured list
	Check routing table – show ip route
	Check protocol exchanges (i.e. debug ip eigrp events)
	Temporarily disable access lists (no ip access-group)
	Debug access lists that cause problems
Discontiguous network due to poor design or network failure	Check routes and how they are learned (show ip route)
	Use ping or trace to determine where traffic stops
	Fix topology or reassign addressing (assign segments to same major network)
	If backup path exists, assign secondary address
	If Discontiguous network due to link failure, fix link

Windows Host Issues

Problem	Solution
Unable to reach target using an IP address	Ping loopback address
	Ping local ip address
	Ping router
	Ping DNS server
	Ping default gateway address
	Ping WINS server
	Ping remote target address
	Use trace and tracert
No default gateway specified on local or remote host	Check routing table of host using netstat and route commands
	If no default, use the route add default address command
	To boot with default gateway already configured, specify it in ??????
Misconfigured IP address on local or remote hosts or router	Check network control panel
	Check host configuration with ipconfig
	Check router configuration with show ip route and host configuration with route command
Local host can access remote hosts using an IP address but not using non-IP addresses or a NetBIOS name	NBT not set up correctly
	DNS configuration wrong
	Hosts file incorrect
	Incorrect Lmhosts file on server
	WINS configuration wrong
	Winsock proxy incorrect or nonfunctional

IOS IPX Tools and Commands

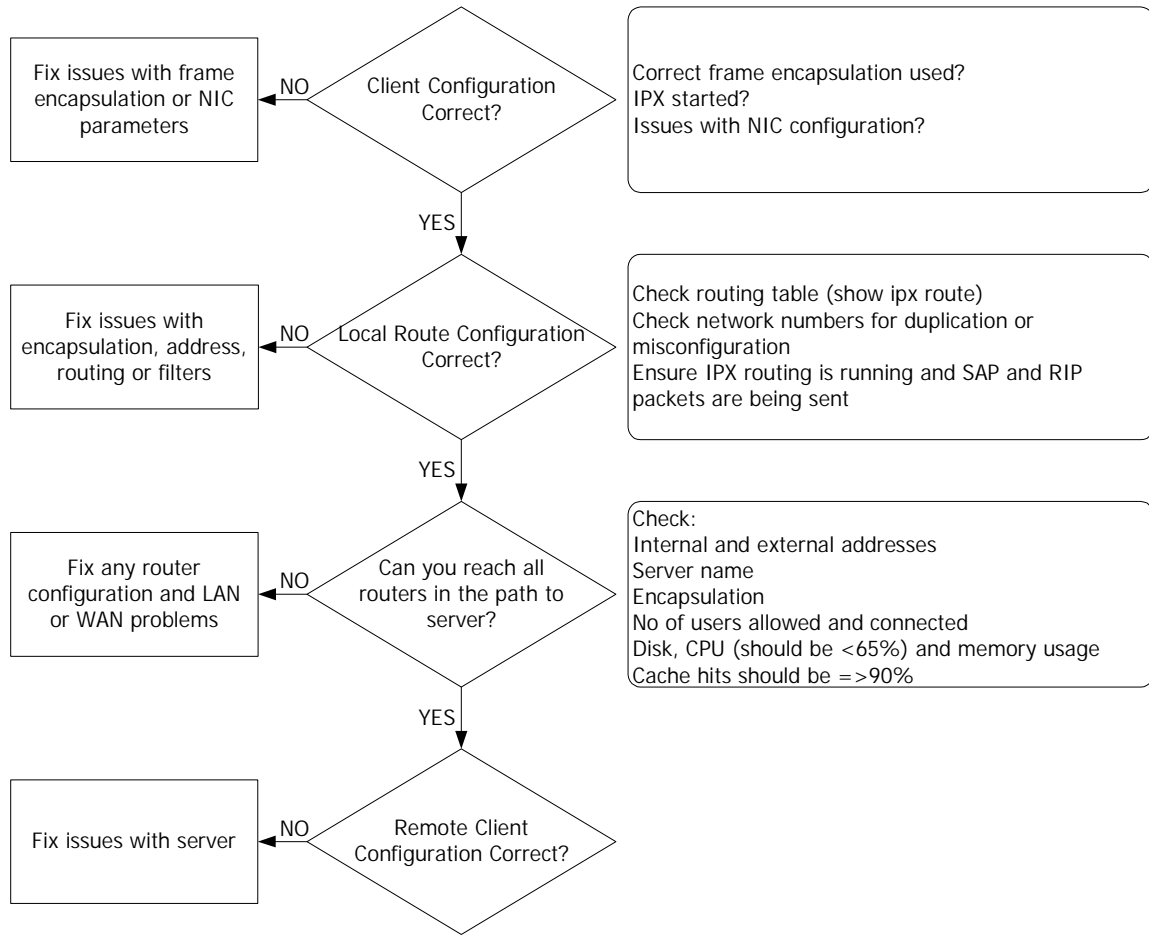
Useful troubleshooting **show** commands include:

#ipx ping-default novell	Use Novell pings, not Cisco proprietary
#ping	Tests connectivity to a host
>show ipx eigrp topology	Displays the IPX EIGRP topology table
>show ipx eigrp neighbors	Display neighbours discovered by EIGRP
>show ipx interface	Displays IPX related configuration of specified interfaces
>show ipx nlsr database	Display entries in the link state database
>show ipx route	Displays the IPX routing table
>show ipx servers	Displays IPX servers discovered via SAP advertisements
>show ipx traffic	Displays statistics on IPX protocol process and traffic Check for errors

Useful troubleshooting **debug** commands include:

To debug IPX packets you are required to disable fast switching on the router, to do so enter the command: **router#no ipx route-cache**

#debug ipx wan	Displays information for interfaces configured to use IPXWAN Check startup negotiations between routers running IPX over a WAN, produces output only during state changes or startup
#debug ipx packet	Displays the flow of IPX packets transmitted between local and remote hosts
#debug ipx routing	Displays information about IPX routing packets that the router sends and receives
#debug ipx sap [events]	Displays information about IPX SAP packets that the router sends and receives. Use the events parameter to limit output or use the activity parameter to view more detailed information



Novell IPX Symptoms, Problems and Solutions

Symptom	Problem
Client cannot communicate with local server	Client or server is not on the network
	Client is not configured for correct frame encapsulation
Client cannot communicate with remote server	Router interface not functional
	Configuration mismatch
	Duplicate network numbers
	Misconfigured access list or other filter
	Client or router is not configured for correct frame encapsulation
	GNS reply from router too quick for slow client
SAP updates are not being propagated by router	Server is not sending SAP updates
	Misconfigured access list or other filter
	Configuration mismatch
	Duplicate network numbers
	Server cannot keep up with SAPs from router
SAP or RIP timers mismatch	
Client or server is not on network	Use a protocol analyser to check the source address of the client and server (assuming on same network)
	Look for an excessive number of collisions or other lower layer errors
	Check NIC configuration parameters
Client or router is not configured for correct frame encapsulation	Check client configuration files
	On router use show running config to check IPX encapsulation
Router interface not functional	Check operation of the router with the show interface command
	Check the cable connections from the router
Configuration mismatch	Verify the router network number agrees with the other routers or servers on this segment using the show ipx interface command
Duplicate network numbers	Use the show ipx servers and show ipx interface commands to look for duplicate network numbers. Modify configurations accordingly.

Misconfigured access list or other filter	Use ping to isolate the router with the Misconfigured list
	Check routing tables (show ipx routing)
	Check protocol exchanges (i.e. debug ipx sap)
	Temporarily disable access lists one by one and test accordingly. Debug access lists that cause connectivity problems
Backdoor bridge between segments	Look for 'bad hop count' with the show ipx traffic command
	Use a protocol analyser to check for packet loops
	Look for known remote network devices that show up on the local network with a remote MAC address
Server is not sending SAP updates	Check for SAP updates with a protocol analyser
	Check frame encapsulation for SAP updates
Server cannot keep up with SAPs from a router	Look for missing services with the show ipx servers command on the router and the slist command on a client
	Use the ipx output-sap-delay command to specify the delay between packets in a multi-packet SAP update
SAP or RIP timer mismatch	Bring the timer values on routers and servers to within 3 minutes of each other

IOS AppleTalk Tools and Commands

Useful troubleshooting **show** commands include:

#ping	Tests connectivity to a host
>show appletalk interface	Displays AppleTalk related configuration of specified interfaces
>show appletalk route	Display entries in the AppleTalk routing table
>show appletalk zone	Displays entries in the AppleTalk zone information table
>show appletalk access-lists	Displays the contents of all AppleTalk access lists
>show appletalk adjacent-routes	Displays routes to networks that are directly connected or one hop away
>show appletalk arp	Displays the contents of the AppleTalk ARP cache (AARP)
>show appletalk globals	Displays AppleTalk settings and parameters
>show appletalk name-cache	Displays the routers cache of local names and services
>show appletalk traffic	Display AppleTalk traffic statistics

Useful troubleshooting **debug** commands include:

#debug apple arp	Displays AARP information Check when a node has problems communicating on the local network
#debug apple errors	Displays errors such as configuration mismatch problems, incorrect encapsulation and so on
#debug apple events	Displays information about Appletalk special events, such as neighbors becoming reachable or unreachable and interfaces going up or down. When making configuration or topology changes use this command to monitor any possible errors. This command will not return information in a stable network.
#debug apple nbp	

SECTION X: Glossary & Appendices

Glossary

AFP	AppleTalk Filing Protocol (Layer 3)
AARP	AppleTalk ARP
ARP	Address Resolution Protocol (Resolved TCP/IP addresses to layer 2 addresses, a layer 2 protocol)
ATM	
ATP	AppleTalk Transaction Protocol
CCO	Cisco Connection Online Website (Online Cisco website and resource)
CERT	Customer Engineering Response Team (Deal with TAC case resolution)
CRC	Cyclical Redundancy Checksum
CRM	Cisco Resource Manager (Part of the CiscoWorks NMS – Web Based)
CSE	Customer Support Engineer (Engineers who deal with TAC cases)
CWSI	CiscoWorks for Switched Internetworks
DDP	Datagram Delivery Protocol (Provides connectionless services between network sockets) (AppleTalk – Network Layer)
ESI	End System Identifier (ATM interfaces)
GNS	GetNearestServer (Novell)
IPC	Internetworking Products Centre (Part of the CCO MarketPlace allowing ordering and purchasing of Cisco software which is physically shipped to you)
IPeXchange	Internetworking Products Exchange (Part of the CCO MarketPlace allowing ordering, purchasing and downloading of Cisco software over the Internet)
ISO	International Organisation for Standardisation
MAC	Media Access Control (Layer 2)
MIB	Management Information Base (Information file used by SNMP and RMON applications)
NBP	Name Building Protocol (AppleTalk)
NCP	Netware Core Protocol
NIC	Network Interface Card
NMS	Network Management System(s)
PAP	Printer Access Protocol (AppleTalk)
PING	Packet Internet Groper
PVC	Permanent Virtual Circuit (Frame Relay/ATM)
RIF	Routing Information Field (Source-routing information contained in a Token Ring frame)
RIP	Routing Information Protocol
RME	Resource Manager Essentials (Part of the CiscoWorks NMS – Web Based) (Previously called CRM)
RMON	Remote Monitoring
RTMP	Routing Table Maintenance Protocol (AppleTalk)
SAP	Service Advertising Protocol (Novell)
SNMP	Simple Network Management Protocol (TCP/UDP Port Assignments: 161 and 162)
SVC	
TAC	Technical Assistance Center (Cisco service and support)
TTL	Time to Live
VC	
VLAN	Virtual LAN
ZIP	Zone Information Protocol (AppleTalk)
ZIT	Zone Information Table (AppleTalk)

--	--