Network Study Guides.com
CIT Answers

1. What show command would you issue to show tech support routers condition?
   - ❑ Show version
   - ❑ Show buffers
   - ❑ Show memory
   - ❑ **Show tech-support**

2. What is the proper pin-out for an ISDN RJ45 connector on the TE end?
   - ❑ Pin1 - TX, Pin 2 - TX, Pin 3 - RX, Pin 4 -RX
   - ❑ **Pin4 - TX, Pin 5 - RX, Pin 6 - RX, Pin 7 -TX**
   - ❑ Pin 4 - RX, Pin 5 -TX
   - ❑ Pin 4 –TX, Pin 5 – RX

3. Cisco IOS provides commands to troubleshoot ISDN BRI layer 2 & 3. First enter the command _____ for Layer 2 debug and the enter command _____ for Layer 3 debug
   - ❑ Debug isdn layer2 / debug isdn layer3
   - ❑ Show isdn datalink / show isdn transport
   - ❑ Debug isdn q219 / debug isdn q319
   - ❑ **Debug isdn q921 / debug isdn q931**
   - ❑

Note The ISDN switch provides the network interface defined by Q.921. This debug command does not display data link layer access procedures taking place within the ISDN network (that is, procedures taking place on the network side of the ISDN connection).

4. When you issue a “show ipx traffic” you see that the router has a high number of packets with a “bad hop count” what does this mean? (choose 1)
   - ❑ Your network is experiencing a count to infinity problem.
   - ❑ **Packets were discarded because their hop count exceeded 16.**
   - ❑ You have disabled split horizon, and packets are looping.
   - ❑ Packets are being received without the hop count field set.

Explanation: A possible cause of this is a backdoor bridge between segments which could happen if you disabled spanning tree.

5. If a CSE asks for the output of the show stack which of the following does he/she suspect? (choose all that apply)
   - ❑ Misconfigure router
   - ❑ **Bad Ram**
   - ❑ Invalid boot prom
   - ❑ **Bad Flash**
   - ❑ **Corrupt IOS image**

Explanation: This was a trick question, in order to get a stack trace you must be able to get into bootstrap mode > so it isn’t a valid boot prom, and a poorly configured router doesn’t usually require a stack trace to figure out what’

6. What command can you use to view information specifically about the D channel of a BRI line?

- ❑ Show isdn status
- ❑ **Show controller bri**
- ❑ Show dialer 0
- ❑ Show int bri 0

Explanation: this is a trick question, the full answer is “show controllers bri”, but the command “show controller bri” will work just fine.

7. You are using a gigabit ethernet module on a Catalyst 2924M connected to a third party gigabit switch, during heavy loads you are continually having data overrun issues, what is the probable cause of this problem?

- ❑ The catalyst 2924M backplane can’t handle the full bandwidth
- ❑ You need to increase the amount of ram in the catalyst switch
- ❑ **You need to enable symmetric flow control**
- ❑ Ouji board says sunspots.

Explanation: Gigabit ports can use either assymetric (default) or symmetric flow control. In an assymetric model the local port to performs flow control of the remote port. If the local port is congested, it can request the remote port to stop transmitting. When the congestion clears, the local port requests that the remote port begin transmitting. In a symmetric model the the local port to perform flow control only if the remote port can also perform flow control of the local port. If the remote port cannot perform flow control, the local port also will not.

8. Which of the following are true about the ISL specification? (choose all that apply)

- ❑ **It contains three fields, the header, the original packet and the FCS at the end**
- ❑ It is supported by Ethernet, FDDI, token ring and ATM
- ❑ The virtual lan ID is a 15 bit number, which is different for each host on a vlan
- ❑ **ISL puts a CRC at the end of the frame which covers both the header and the encapsulated packet.**

Explanation: ISL is not directly supported by ATM, although you could use it in a ATM LANE configuration. The virtual lan ID is 15 bits, and is different for each VLAN. This 15 bit value is referred to as the COLOR of the VLAN.

9. What command will send debugging output to the console?

- ❑ In console configuration mode, “Logging console level”
- ❑ In line 0 configuration mode, “logging console level”
- ❑ **In global configuration mode, “logging console level”**

10. Which command tells you if there are problems with the packets on the ISL trunk being either misconfigured or being sent/received on the wrong ISL subinterface.

- ❑ Show vlan status
- ❑ Debug vlan ip
- ❑ **Debug vlan packet**
- ❑ Debug vlan isl

11. Which of the following devices will show no CDP information? (choose all that apply)

- ❑ A Cisco™ router configured as a bridge, with the statement “no ip route” in its configuration
- ❑ **An ATM interface on a Catalyst 5000**
- ❑ **A router with the statement “no cdp enable” on all interfaces**
- ❑ **A non Cisco™ switch**
- ❑ A serial interface with a misconfigured encapsulation

12. What command do you use to show current status of router? Date of Last reboot?

- ❑ Show memory
- ❑ Show status

- **Show version**
- Show running-config
- Show startup-information

13. What does the command “IPX ping-default Novell” accomplish? (choose all that apply)
- Configures the router to respond to all novell format IPX pings.
- **Configures the router to send to novell format IPX pings by default.**
- Sends an IPX ping packet of default size to the server name “Novell”.
- Configures the router to ignore Cisco™ pings.

14. Which of the following is true about FDDI? (choose all that apply)
- **FDDI supports both synchronous and asynchronous traffic management**
- Synchronous bandwidth is allocated using an 8 level priority scheme
- Devices that can only use Asynchronous bandwidth are guaranteed to have their data deliever in a timely fashion.
- **Synchronous devices may fully utilize the network, by using a reserved token**

Explanation: Asynchronous bandwidth is allocated using an 8 level priority scheme. Asychronous bandwidth is what is left over after all devices which have been allocated synchronous bandwidth are finished. Synchronous bandwidth is allocated to devices which need a continous stream of data, such as voice or video.

15. Which of the following are CCO bug toolkit resources?
- **Bug Navigator**
- Bug Finder
- **Bug Alert**
- Bug Hunter
- **Bug Watcher**
- Bug spray

Explanation: there are only three resources in the Bug Toolkit II which are Bug Navigator, Bug Alert, and Bug Watcher.

16. In Spanning Tree Protocol what happens to a port if no information has been received by the end of a forwarding delay?
- The port transitions to blocked state
- The port transitions to forward state
- **The port transitions to learning state**
- The port transitions to listening state
- The port becomes the root bridge

Explanation: As BPDU information is updated and/or timed-out, the Spanning Tree is recalculated and ports may transition from the blocked state to the forwarding state and vice versa. That is, as a result of new BPDU information, a previously blocked port may learn that it is now the root port or the designated port for a given segment. Rather than transition directly from the blocked state to the forwarding state, ports transition through two intermediate states: a listening state and a learning state. The bridge will remain in each state for a preset period of time, called the forwarding delay. In the listening state, a port waits for information indicating that it should return to the blocked state. If, by the end of the forwarding delay time, no such information is received, the port transitions to the learning state. In the learning state, a port still blocks the receiving and forwarding of frames, but received frames are examined and the corresponding location information is stored, as described above. At the end of a second forwarding delay time, the port transitions from the learning state to the forwarding state, thereby allowing frames to be forwarded and received at the port.

17. When you issue a “show ipx traffic” you see that the router has a high number of packets with a “packets pitched” what does this mean? (choose all that apply)
- A high number of packets were discarded due to high load
- **The router has received its own broadcast many times**
- Packets are being dropped due to their TTL being expired.
- **You probably have a loop somewhere on your network**

- ❑ The router is probably mistaking IPX for SPX
- ❑ You don't have the correct frame type selected.

Explanation: The packets pitched counter is the number of times a router has received its own broadcast packets.

18. What should you do if you are checking frame-relay PVC and only see local DCLI 0 DLCI 1023 come up?

- ❑ Check the LMI type
- ❑ Check the encapsulation
- ❑ **Check the Frame Relay mappings**
- ❑ Call your network service provider

Explanation: This is a trick question. Normally when testing a frame relay circuit you loop the local CSU on both ends and see if your local LMI goes active (1023 for Cisco™). However in this circuit your LMI is active, but the circuit is not necessarily looped which means you probably don't have your frame relay mappings correct, eg: your data link is working, but your layer 3 isn't configured properly.

19. What are the functions of the NetSYS tool?

- ❑ It allows you to determine the location of cable breaks, etc. throughout the network
- ❑ **It allows you to simulate network changes, in a virtual environment**
- ❑ It provides RMON capability and advanced debugging tools when used with CCO.
- ❑ It is an industry standard management platform, which supports the Cisco MIB definitions

20. Why is process switching slow?

- ❑ Every packet must be handled by three interfaces (incoming, internal, and external)
- ❑ **Each packet must be examined individually**
- ❑ Process switching is only available on older cisco ASICs.
- ❑ Process switching checks the CRC on the packet before forwarding it.

21. In what switching mode will the router use if you have debugging on?

- ❑ Netflow switched
- ❑ **Process switched**
- ❑ Distributed switched
- ❑ Fast Switched

22. What debug command would you issue to see if rip routing is operating properly?

- ❑ _____

Answer: debug ip rip

23. On the frame-relay DTE/DCE which configuration element will the router autosense?

- ❑ Frame Type
- ❑ Encapsulation
- ❑ Network layer protoocols (eg: ppp)
- ❑ **LMI type**

24. Which of the following scenarios could be solved by using an IPX static sap on a router? (choose all that apply)

- ❑ You want clients to ignore broadcasts from certain servers
- ❑ **You want clients to always use services of a particular server**
- ❑ You want clients to login to one server, in case another server might be down

- ❑ You want to remove the additional load of distributing saps from a server.

Explanation: Servers use SAP to advertise their services via broadcast packets. Routers store this information in the SAP table, also known as the Server Information Table (SIT). This table is updated dynamically. You might want to explicitly add an entry to the SIT so that clients always use the services of a particular server. Static SAP assignments always override any identical entries in the SAP table that are learned dynamically, regardless of hop count. If a dynamic route that is associated with a static SAP entry is lost or deleted, the router will not announce the static SAP entry until it relearns the route.

25. What are the two ways to configure a VLAN?

- ❑ By using a NMP in the switch
- ❑ **By using an RSM in the switch**
- ❑ By attaching a route to a VLAN trunking port using 802.1Q encapsulation
- ❑ **By attaching a router to a VLAN trunking port using ISL encapsulation**

26. If a VLAN is slow or non-operational, which of the following are possible causes of the problem?

- ❑ **Incorrect VLAN trunking protocol is configured**
- ❑ Incorrect encapsulation on the VLAN

27. Which of the following Cisco™ products can collect RMON information so engineers can analyze it later?

- ❑ Vlan director
- ❑ **TrafficDirector**
- ❑ **CiscoWorks for Switched Internetworks Campus**
- ❑ CiscoWorks 2000
- ❑ Netsys baseliner

Answer: TrafficDirector can collect RMON information, and traffic director is included inside of CiscoWorks for Switched Internetworks Campus.

28. Which utility performs decodes of a stack trace (show stack) and may be useful for Cisco™ TAC support?

- ❑ Bug navigator II
- ❑ Troubleshooting Assistant
- ❑ **Stack Decoder**
- ❑ Management Toolkit

Answer: The Stack decoder is a tool which can be found on CCO, paste in the output of a “show stack” command after an error has occurred and the stack decoder tool will comment the stack trace with meaningful comments.

29. What type of switching is supported on the 7500 series router with a VIP installed?

- ❑ Priority switching
- ❑ Fast switching
- ❑ Weighted fair switching
- ❑ **Distributed switching**
- ❑ ASIC based switching

Answer: The Cisco 7000 family Versatile Interface Processor (VIP) is based on a RISC engine optimized for I/O functions. Either one or two port adapters or daughter boards may be attached to a VIP, to provide the media- specific interfaces to the network. A key feature of the VIP technology is its ability to receive route information from the master RSP. Based on route data received from the RSP, a VIP is able to make its own autonomous, multilayer switching decisions, thereby providing distributed switching, which is just one of many features supported by the VIP technology. The VIP supports:
High port densities. As higher densities of the VIP technology become available, users will be able to cost-effectively add additional ports to either the Cisco 7000 or Cisco 7500 platforms.
Mixed Media. The port adapter design enables different media types to be deployed on the same VIP, which enables maximum chassis slot utilization.

Packet memory. Each VIP contains its own packet memory, thus distributing and greatly increasing the amount of packet memory available in the system. This is a particularly important feature in environments where there are large round-trip propagation delays (trans-Atlantic or trans-Pacific for example), bursty traffic conditions, or where there may be many high-speed media pointing to a small number of slower-speed media.
Feature Offload. Each VIP can run a subset of the Cisco IOS software. With Feature Offload, it will be possible to distribute some of the more processor-intensive functions from the RSP throughout the rest of the system.
Distributed switching. This is the "CiscoFusion in a box" feature that enables scalable switching performance.

30. One way to check why line protocol Frame Relay is down, is to check for timing problems with myseq & myseen keepalive events, command to show:

- **debug serial interface**
- show interface serial
- show frame relay lmi
- debug frame-relay pvc

31. What is the true statement about embedded RMON Agent & SwitchProbe

- functions in Catalyst software
- SPAN is option of switch Probe function
- **functions use all RMON groups as well as RMON**
- function of switch probe offers an in-band link to network manager
- RFC 1757 RMON groups supported are statistics, events, history & alarms
- Functions can monitor segment as long as they use 10BaseT or 100BaseT

32. To check timeliness of ISDN events in a log/ debug filter, what command can configure router to indicate how many milliseconds have occurred between events displayed:

- _____

Answer: Use the command “service timestamps” puts a date and time in your log so you can tell how much time has elapsed between events. However this command SPECIFICALLY asks for MILLISECONDS between events so you would need to use the form “service timestamps log datetime msec”

33. What are the allowed encapsulation in the output of “show interface atm” command?

- **AAL5, PVC, SVC**
- VC, VPI, VCI
- SNAP, NSAP
- AAL5, AAL4, AAL1
- AAL4, AAL5, LANE
- None of the above

Answer: Valid encapsulations for ATM are AAL5, PVC and SVC.
Example:
Switch# show interface atm 1/0/0

ATM1/0/0 is up, line protocol is up
Hardware is oc3suni
MTU 4470 bytes, sub MTU 4470, BW 156250 Kbit, DLY 0 usec, rely 255/255, load 1/255

Encapsulation ATM, loopback not set, keepalive not supported

Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
527152 packets input, 27939056 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles

```
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    527246 packets output, 27944038 bytes, 0 underruns

  0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
Switch#
```

This should not be confused with the "show atm interface atm command" which gives the following output?

```
Switch# show atm interface atm 1/0/0
Interface:      ATM1/0/0       Port-type:      oc3suni

  IF Status:      UP             Admin Status:   up
Auto-config:    enabled        AutoCfgState:   completed
IF-Side:        Network        IF-type:        NNI
Uni-type:       not applicable  Uni-version:    not applicable
Max-VPI-bits:   8              Max-VCI-bits:   14
Max-VP:         255            Max-VC:         16383
ConfMaxSvpcVpi: 255            CurrMaxSvpcVpi: 255
ConfMaxSvccVpi: 255            CurrMaxSvccVpi: 255
ConfMinSvccVci: 33             CurrMinSvccVci: 33
Svc Upc Intent: pass           Signalling:     Enabled
ATM Address for Soft VC: 47.0091.8100.0000.0040.0b0a.2a81.4000.0c80.8000.00
Configured virtual links:
  PVCLs SoftVCLs   SVCLs   TVCLs   PVPLs SoftVPLs   SVPLs Total-Cfgd Inst-Conns
     4       0       0       0       0       0       0         4         4
Logical ports(VP-tunnels):     0

  Input cells:    528135         Output cells:   528235

  5 minute input rate:           0 bits/sec,       0 cells/sec

  5 minute output rate:          0 bits/sec,       0 cells/sec

  Input AAL5 pkts: 344844, Output AAL5 pkts: 344878, AAL5 crc errors: 0
Switch#
```

34. Which is not cause for complete interface reset?

- ❑ problem with clocking signal
- ❑ problem with Frame relay
- ❑ hardware problem with router interface
- ❑ **interface counters cleared with clear interface**
- ❑ packets sequenced for transmission are not send for several ms
- ❑ router restart interface due to persistent line protocol

Answer: The following are causes for interface resets: Congestion on link (typically associated with output drops), Bad line causing CD transitions, Possible hardware problem at the CSU, DSU, or switch

35. Which is NOT one of IOS defined functional area of network management?

- ❑ fault management
- ❑ security management
- ❑ accounting management
- ❑ Quality of service management
- ❑ **Configuration & name management**

Explanation: Cisco defines five network management functional areas which include: fault management, performance management, configuration management (which includes device management), accounting management (which is included in performance management applications), and security management. Configuration management does not include name management.

36. When you see the Link LEDs flash orange during Catalyst 5000 power-up sequence, what is indicated?

- ❑ **A module was not correctly inserted into slot, or has failed**
- ❑ power-up sequence is underway & not yet completed
- ❑ more than 1 fan, power supply or supervisor clock is disabled
- ❑ network management autodiscovery process us underway
- ❑ traffic testing process of interface loopback has not yet completed

Answer: When dealing with the Link light, If the port is operational, the LED is green. If the link has been disabled by software, the LED is orange. If the link is bad and has been disabled due to a hardware failure, the LED flashes orange. If no signal is detected, the LED is off.

37. Because it moves packets, frames or cells from buffer to buffer with simpler determination of traffic source & destination switching is

- ❑ not performed in routers
- ❑ able to use more intensive processing
- ❑ part of protocol's best path decision
- ❑ moving data to its ultimate destination
- ❑ **affected by lower latency than routing**

38. where are special processes like debug packet filtering, sending error log entries to a syslog server & SNMP processing done?

- ❑ **route switch processor**
- ❑ Netflow error processor
- ❑ Si switch processor
- ❑ Autonomous switch processor
- ❑ CxBus diagnostic processor

39. For troubleshooting cables, which test helps to eliminate uncertainties about cable breaks, cable plant & punch down connections?

- ❑ change ports used on switch & determine if problem goes away
- ❑ check cable length, impedance and continuity with a network monitor
- ❑ replace network adapter card at user device end & retest
- ❑ Visually inspect cable connectors., the adapter (and/ interface port & punchdown block termination)
- ❑ **replace cable with an external cable known to be good**

40. When do you need to set a default gateway in a UNIX environment?

- ❑ When the hosts are connected to an internetwork
- ❑ When the hosts are running routed
- ❑ **When the hosts are not running routed**
- ❑ When the hosts are acting as a firewall?

Explanation: A Unix host running routed will learn its default gateway through RIP. If the host is not running routed then you will need to set its default gateway.

41. Which of the following are tools of Cisco Support online?

- ❑ **Troubleshooting Assistant**
- ❑ **TAC Assistance**
- ❑ **Software Bug Toolkit II**
- ❑ **Online Ordering**

Explanation: The Cisco website offers many helpful features including the ability to search technical database , an open question and answer forum, a mailing list archive, a troubleshooting assistant, a software bug toolkit, accesspath configuration tools, ip subnet calculator, stack decoder, 3600 memory calculator, tac case instructions, the ability to open and update TAC cases, and the ability to order cisco products online in the “Cisco™ Marketplace” area of the CCO website. Cisco™ Marketplace is the name of the area where you may perform online ordering.

42. Which command would you use to display statistics such as missed datagrams, memory errors, buffer errors, and overflow errors for the first ethernet interface on a Cisco router?

- ❑ Show interface ethernet 0
- ❑ **Show controllers ethernet 0**
- ❑ Show ethernet 0 errors
- ❑ Show interface ethernet 0 errors

Explanation: While the show interface ethernet 0 will give you a certain amount of errors it will not give you any errors which actually occurred on the interface (meaning internal hardware errors). Memory errors indicate you may have a hardware problem with your router.

43. Which command would you use to display the router images stored in NVRAM?

- ❑ Show internal memory
- ❑ **Show flash**
- ❑ Show nvram
- ❑ Show eprom

Explanation: the show flash displays the contents of the system flash memory, these images can be used to boot from. Here is a sample output:

```
Router1>show flash
System flash directory:
File  Length   Name/status
  1   1898550  4000ios-11.16.bin
[1898616 bytes used, 2295688 available, 4194304 total]
4096K bytes of processor board System flash (Read/Write)
```

44. Which command displays statistics for the buffer pools in router?

- ❑ Show memory
- ❑ **Show buffers**
- ❑ Show pools
- ❑ Show memory buffers

Explanation: Use the show buffers EXEC command to display statistics for the buffer pools on the network server. The router has one pool of queuing elements and five pools of packet buffers of different sizes. For each pool, the 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.

```
show buffers [type number]] | all]
show buffers [interface [type number]] [alloc [dump]]

CS# show buffers
Buffer elements:
        421 in free list (500 max allowed)
        409 hits, 0 misses, 0 created
     Public buffer pools:
    Small buffers, 104 bytes (total 50, permanent 50):
        50 in free list (20 min, 150 max allowed)
        277 hits, 0 misses, 0 trims, 0 created
    Middle buffers, 600 bytes (total 25, permanent 25):
        24 in free list (10 min, 75 max allowed)
        19 hits, 0 misses, 0 trims, 0 created
    Big buffers, 1524 bytes (total 50, permanent 50):
        50 in free list (5 min, 40 max allowed)
        4 hits, 0 misses, 0 trims, 0 created
    Large buffers, 5024 bytes (total 0, permanent 0):
       0 in free list (0 min, 10 max allowed)
        0 hits, 0 misses, 0 trims, 0 created
    Huge buffers, 18024 bytes (total 0, permanent 0):
        0 in free list (0 min, 4 max allowed)
        0 hits, 0 misses, 0 trims, 0 created
     Interface buffer pools:
    Fddi buffers, 5024 bytes (total 256, permanent 256):
        0 in free list (0 min, 256 max allowed)
        256 hits, 0 misses
```

256 max cache size, 110 in cache
14 buffer threshold, 0 threshold transitions
Ethernet0 buffers, 1524 bytes (total 64, permanent 64):
16 in free list (0 min, 64 max allowed)
48 hits, 0 misses
16 max cache size, 16 in cache
Ethernet1 buffers, 1524 bytes (total 64, permanent 64):
16 in free list (0 min, 64 max allowed)
48 hits, 0 misses
16 max cache size, 16 in cache
Serial0 buffers, 1524 bytes (total 64, permanent 64):
16 in free list (0 min, 64 max allowed)
48 hits, 0 misses
16 max cache size, 16 in cache
Serial1 buffers, 1524 bytes (total 64, permanent 64):
16 in free list (0 min, 64 max allowed)
48 hits, 0 misses
16 max cache size, 16 in cache
0 failures (0 no memory)

45. Which command displays information about the active processes in a router?

- ❑ Show utilitization
- ❑ **Show processes**
- ❑ Show threads
- ❑ Show system processes
- ❑ Show system threads

Explanation: Use the show processes EXEC command to display information about the active processes. Syntax: show processes [cpu]

cs# show processes
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%

PID	Q	T	PC	Runtime (ms)	Invoked	uSecs	Stacks	TTY	Process
1	M	T	40FD4	1736	58	29931	910/1000	0	Check heaps
2	H	E	9B49C	68	585	116	790/900	0	IP Input
3	M	E	AD4E6	0	737	0	662/1000	0	TCP Timer
4	L	E	AEBB2	0	2	0	896/1000	0	TCP Protocols
5	M	E	A2F9A	0	1	0	852/1000	0	BOOTP Server
6	L	E	4D2A0	16	127	125	876/1000	0	ARP Input
7	L	E	50C76	0	1	0	936/1000	0	Probe Input
8	M	E	63DA0	0	7	0	888/1000	0	MOP Protocols
9	M	E	86802	0	2	0	1468/1500	0	Timers
10	M	E	7EBCC	692	64	10812	794/1000	0	Net Background
11	L	E	83BBC	0	5	0	870/1000	0	Logger
12	M	T	11C454	0	38	0	574/1000	0	BGP Open
13	H	E	7F0E0	0	1	0	446/500	0	Net Input
14	M	T	436EA	540	3435	157	737/1000	0	TTY Background
15	M	E	11BA9C	0	1	0	960/1000	0	BGP I/O
16	M	E	11553A	5100	1367	3730	1250/1500	0	IGRP Router
17	M	E	11B76C	88	4200	20	1394/1500	0	BGP Router
18	L	T	11BA64	152	14650	10	942/1000	0	BGP Scanner
19	M	*	0	192	80	2400	1714/2000	0	Exec

46. Which commands of the following commands is accomplished by sending a packet with the TTL set to 1 then sends lots of packets while incrementing the TTL every 3 packets.

- ❑ Ping
- ❑ Echo
- ❑ **Trace**
- ❑ maproute

Explanation: The trace command works by using the eorrr message generated by routers when a datagram exceeds it time-to-live (TTL) value. First, probe datagrams are sent with a TTL value of 1. This causes the first router to discard the probe datagrams and

send back “time exceeded” error messages. The trace command then sends several probes and displays the route round-trip time for each. After every third probe, the TTL is increased by one.

47. Which of the following Cisco tools can be used to monitor a network using Simple Network Management (SNMP)?

- ❑ **CiscoWorks**
- ❑ TrafficDirector
- ❑ VLANDirector
- ❑ VlanWorks

Explanation: CiscoWorks is an internetwork management software, and a set of Simple Network Management Protocol (SNMP) based tools. Cisco Works includes the ability to monitor devices for information such as environmental and interface statistics, display information about the health of a device, view data similar to the output of a show exec commands, 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 last but not least create detailed maps which you can provide to Cisco TAC for assistance in debugging your network.

48. Which of the following Cisco tools lets you gather data, monitor activity on your network and find potential problems?

- ❑ CiscoWorks
- ❑ **TrafficDirector**
- ❑ VlanDirector
- ❑ VlanWorks

Explanation: Cisco TrafficDirector RMON application, a remote monitoring tools that enables you to gather data, monitor activity on your network and find potential problems. TrafficDirector advanced packet filters allow users to montor all 7 layers of the OSI model. Traffic Director threshold monitoring enables users to implement a proactive management environment.

49. Which of the following Cisco is used to manage switches, and also has the ability to provide an accurate picture of your VLANs?

- ❑ CiscoWorks
- ❑ TrafficDirector
- ❑ **VlanDirector**
- ❑ VlanWorks

Explanation: VLAN director switch offers many features for network administrators including an accurate representation of the physical network and vlan design, the capability to find discrepancy on conflicting ports, quick detection of changes in VLAN status and switch ports, user authentication and write protection security.

50. Which of the following would allow you to measure parameters such as AC and DC voltage, current, resistance, capacitance, and cable continuity for testing physical connectivity?

- ❑ **Volt Ohm meter**
- ❑ TDR
- ❑ Breakout Box
- ❑ Network Monitor
- ❑ Network Anaylzer

Explanation: Volt Ohm Members, digital multimeters and cable testers are all used to measure physical properties such as current, resistance, capacitance, and cable continuity. Cable testers (also called Cable scanner) let you check physical connectivity on STP, UTP, 10BaseT, coaxial, and twinax cable. Some cable testers might also be able to test and report on near end cross talk (NEXT), attenuation, and noise, perform TDR and traffic monitoring and wire map functions, and display MAC information.

51. Which of the following works by bouncing a signal off the other end of the cable.

- ❑ Volt Ohm meter
- ❑ **TDR**
- ❑ Breakout Box
- ❑ Network Monitor
- ❑ Network Analyzer

Explanation: Time Domain Reflectors are used to trouble shoot crimps, kinks, impedance, bends, and other defects in metallic cables. Optical Time Domain Reflectors (OTDR) are used to troubleshoot optical cable. A TDR works by bouncing a signal off the end of the cable. Opens, shorts, and other problems reflect the signal back at different amplitudes, depending on the problem. A TDR measures how much time it takes the signal to reflect and calculates the distance to a fault.

52. Which of the following would you use to measure the digital signals present at PCs, printers,modems and CSU/DSU's?

- ❑ Volt Ohm meter
- ❑ TDR
- ❑ **Breakout Box**
- ❑ Network Monitor
- ❑ Network Anaylzer

Explanation: A breakout box, also called a fox boxe and bit/block error rate testers (BERT or BLERT) are tools used for testing digital interfaces to measure the digital signals present on interfaces commonly found on printers, PC's, etc. These devices cannot test media signals such as ethernet, token ring or fddi.

53. Which device continuously tracks packets crossing a network, providing an accurate picture of historical network activity?

- ❑ Volt Ohm meter
- ❑ TDR
- ❑ Breakout Box
- ❑ **Network Monitor**
- ❑ Network Anaylzer

Explanation: Network monitors are useful for determining a baseline (a baseline is the normal amount of traffic on a network at certain points throughout the day, and is used to help troubleshoot network problems). Monitors collect information such as packet sizes, the number of packets, overall usage of a connection, number of error packets, the number of hosts on a network as well as many other items.

54. Which device decodes the various protocol layers in a recorded frame and presents summary information about them?

Volt Ohm meter
TDR
Breakout Box
Network Monitor
Network Anaylzer

Explanation: A network analyzer, also called a protocol analyzer decodes the various layers in a frame and presents them as summaries detailing which layer is involved. Most network analyzers can perform the following actions: filter traffic captured based on specific criteria, time stamp captured data, present protocol layers in readable format, generate frames and transmit them onto network, offer solutions based on a information it receives to determine what possible problems may be occuring.

55. Which of the following are valid ways of netbooting a Cisco router:

MOP
TFTP

RCP
FDDI
DHCP

Explanation: routers can boot from a server using Trivial File Transfer Protocol (TFTP), the DEC Maintenance Operation Protocol (MOP), or Remote Copy Protocol (RCP) across any media such as token ring, ethernet and FDDI

56. Which is the recommended order to boot images from:

Rom, flash, network
Network, rom, flash
Flash, network, rom
Network, flash rom

Explanation: Typically the ROM IOS image is very old, so it should only be used in a pinch, netbooting is acceptable however a down server can cause a router not to boot, booting from flash is the fastest, however you may want to have an alternate boot path setup in the event that your flash becomes corrupt. The recommended order for booting is: Flash, Network, Rom. Here is a sample configuration that you may want to use:

Router1(config)#boot system flash ios-11.2

Router1(config)#Boot system ios-11.2 192.168.1.1

Router1(config)#Boot system rom

57. Which symbol is used to represent a successful receipt of a packet during netboot?

! (exclamation)
* (asterisk)
. (period)
O (Letter O)

Explanation: During a netboot you may receive out of order packets which are indicated by a “o” while missed packets are represented by a . (period). Here is some example output showing a few missed and out of order packets. Please keep in mind while receiving an out of sequence packet or a missed packet is not optimal, the protocol will generally retry and the router may perform normally after the full image has been received.
Booting ios-11.2 from 192.168.1.1 !..!oo!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

58. Which of the following things should occur when powering up a Cisco 7500 series router?

The AC (or DC) OK LED should go on and then turn off once the router is completed is power up sequence.
The blower will not operate unless the router is overheating
The RSP and front panel Normal LED’s should go on, the CPU HALT lite should be off
The enabled LED on each interface should go off to indicate that the RSP has assumed master control

The system banner should be displayed on the console port

Explanation: During book the AC OK led should go on and stay on as long as the system is receiving power, the blower should always be operating, the LEDS for the Route Switch Processor (RSP) which is located on the supervisor board should go and stay on during normal system operation, the CPU HALT lite should stay off during normal operation. The Enabled LED on each interface processor should go on to indicated that the RSP has completed initialization of the interface processor. After all this has been completed the system banner message will be displayed

59. Which of the following are valid subsystems on all Cisco 2000, 2500, 3000, and 4000 series routers?

Power subsystem
Network processor modules
System cables
Cooling subsystem
Network Interfaces

Explanation: Cisco defines troubleshooting subsystems for each piece of equipment, common to all Cisco series routers is the power system which includes power supply and wiring, the system cables which includes all external cables that connect to the router, and the cooling system which includes the blower assembly. The Network Processor Modules are boards installed in a 4000 chassis, the 4000 series routers do not have any network interfaces installed in them by default.

60. Which of the following are true about the power up sequence in a 5000 series startup?

PS1 and PS2 leds on the supervisor engine faceplate should be green
PS1 and PS2 leds on the supervisor engine faceplat should be orange
The status led on the supervisor engine, and all interfaces should be orange
The status led on the supervisor engine, and all interfaces should be green

Explanation: During a normal 5000 series bootup, the PS1 and PS2 leds located on the supervisor engine faceplate should be green, the supervisor engine module and all interfaces should be orange. In addition the system fan assembly should be operating and the fan led on the supervisor engine module should come on. Once the system has been started the fan, the supervisor engine and all modules, should turn and stay green.

61. True/False: 802.3 does not provide a logical link control protocol?

True
False

Explanation: IEEE 802. Specifies the physical layer (layer 1) and the channel access portion of the link layer (layer 2), but does define a local link control protocol. IEEE 802.3 is usually implemented in hardware. IEEE 802.3 specifies several different phyiscal layers, whereas Ethernet defines only one. Each IEEE 802.3 phyiscal layer protocol has a name that summaries its characteristicss. The coded components of an IEEE 802.3 physical layer are names such as 10Base2 and 10BaseT.

62. True/False: The 802.2 frame specifies a type whereas 802.3 frame specifies a length

True
False

Explanation: 802.2 frames specifies a protocol type, whereas 802.3 is more generic and simple specifies a length.

63. Which of the following counters accumulates the number of packets that are discarded because theya re smaller than the mediums minims packet size?

Giants
Overrun
Runts
Underruns
Mini

Explanation: The Runts is the number of packets which are discarded because they are smaller than the mediums minimum packet size. For instance, any Ethernet packet that is less than 64 bytes is considered to be a runt.

64. Which of the following counters accumulates the number of times the transmitter has been running faster than router can handle?

Giants
Runts
Overruns
Underruns
Catch ups

Explanation: The number of underruns is the number of the times the transmitter has been running faster than the router can handle. This counter may never be incremented on some interfaces.

65. Which of the following counters counts the number of packets which were ignored because of a low amount of internal buffers?

Giants
Runts
Overruns
Underruns
Ignored

Explanation: The ignored counter holds the number of received packets ignore by the interface because the interface interface ran low on buffers. The ignored counter only tracks packets ignored due to internal buffers, which are different than system buffers (kept in the buffer counter). Typically this counter is incremented by broadcast storms and bursts of noise.

66. Which of the following scenarios will cause a interface reset?

Heavy bursts of packets which overrun all system buffers
Packets queued for transmission were not sent within several seconds
High CRC errors on a particular interface
Malfunctioning modem that is not supply the transmit clock signal
The system notices that the carrier detect line of a serial interface is up

Explanation: The interface reset counter accumulates the number of times the interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line interface resets are caused by a malfunctioning modem that is not supplying a transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.

67. Which of the following is a 100mbps token passing, dual ring LAN using fiber optic transmission medium?

100baseTX
100baseFL
Token Ring b100
FDDI

Explanation: FDDI is a 100mbps, token passing, dual ring LAN using a fiber optic transmission medium. FDDI defines a physical layer and media access portion of the link layer, and is roughly analogous to IEEE 802.3 and IEEE 802.5 in its relationship to the Open System Interconnection (OSI) reference model.

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55773.htm

68. Which of the following are legal FDDI specifications?

MAC, PHY, LLC, PMD
MAC, PHY, PMD, SMT
PHY, MAC, LLC, PMD
PHY, MAC, PMD, SMT

Explanation: FDDI is defined by four separate specifications. MAC defines how the medium is access including frame format, and methods for error detection (CRC) and error correction. PHY (Physical Layer Protocol) defines data encoding and decoding procedures, clocking requirements, and framing. PMD (Physical Layer Medium) defines the transmission medium characteristics including the power levels, bit error rates (BER), and optical components and connectors. SMT (Station Management) defines the FDDI station & ring configuration, and ring control features such as station insertion and removal, initialization, fault isolation and recovery, scheduling, and collection of statistics.

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55773.htm

69. Which type of FDDI station would a PC or other device which frequently powers on or off be classified as?

RAS
DAS
SAS
PAS

Explanation: FDDI specifies two rings with data traveling in opposite directions. Physically the rings consist of two or more point to point connections between adjacent stations. One of the two FDDI rings is called the primary ring the other is (obviously) the secondary ring. The primary ring is used for data transmission while the secondary is used for backup. A Dual Attached Station (DAS) is a device which is essiential to the operation of the network, while a Single Attached Station (SAS) is a device which is frequently powered up an down such as PC.

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55773.htm

70. FDDI defines two traffic types, what are they?

Bitwise, counter bitwise
Synchronous, asynchronous
Serial, parallel
Priority, non priority

Explanation: FDDI provides real time allocation of network bandwidth by using two traffic types synchronous and asynchronous. Synchronous can consume a portion of the 100mbps and asynchronous can consume the rest. Synchronous is best suited for high demand, low latency applications such as voice and video while asynchronous is useful for the rest. Asynchronous bandwidth is assigned using a 8 level priority scheme, each station is assigned a asynchronous priority level, in addition FDDI also permits extended dialogs which allows stations to temporarily use all available asynchronous traffic.

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55773.htm

71. Which term is used to describe what happens in a FDDI ring when a failure occurs?

Loopback
Wrapping
Fail Safe
Relay

Explanation: If a station on the dual ring fails or is powered down or if the cable is damanage the dual ring is automatically "wrapped" (doubled back on itself) into a single ring. As a FDDI gets larger the changes for a multiple failure occurs in which case the FDDI network wraps in multiple areas creating isolated rings which cannot talk to eachother.

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55773.htm

72. Which device can be used to prevent ring segmentation by eliminating failed stations from the ring?

DAS
SAS
Optical bypass switch

Explanation: Optical bypass switches can be used to prevent ring segmentation by eliminating failed stations from the ring.

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55773.htm

73. Which FDDI neighbor state(s) indicates that the connection management process has established a connection with a DAS neighbor?

A
S
B
M
Unk

Explanation: A FDDI port status of 'A' indicates that the FDDI station has determined that its upstream neighbor is a Physical A type DAS or concentrator that attaches to the primary ring IN and the secondary ring OUT. A FDDI port status of 'B' indicates that the FDDI station has determined that its upstream neighbor is a Physical B type DAS.

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55773.htm

74. Which FDDI neighbor state indicates that the connection management process has established a connection with a SAS neighbor?

A
S
B
M
Unk

Explanation: A FDDI port status of 'S' indicates that a FDDI station has determined that its upstream neighbor is a Physical A type SAS.

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55773.htm

75. Which FDDI neighbor state indicates the connection management process has established a connection with a neighbor and determined that it is a concentrator, serving as a master.

A
S
B
M
Unk

Explanation: A FDDI neighbor state of M indicates that the connection management process has determined that its neighbor is a physical M type concentrator serving as a master to a connection station or concentrator.

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55773.htm

76. Which of the following are valid states of a FDDI station which has NOT established connection with its neighbor?

A
S
B
M
Unk

Explanation: A FDDI status of UNK indicates that the network server has not completed the CMT process and, as a result does not know about its neighbor.

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55773.htm

77. Which of the following are valid states for a Physical A or Physical B connection?

Off
linked

Active
Trace
Reset

Explanation: Valid FDDI states of the Physical A or Physical B interface are Off, Active, Trace, Connect, Next, Signal, Join, Verify, or Break.

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55773.htm

78. Which are the two types of frames defined by token ring?

Tokens
Controls
Delimiters
Data/command

Explanation: The two types of frames defined by Token Ring are tokens and data/command frames. Each token is 3 bytes in length and consists of a start delimiter, access control byte, and end delimiter. Data/command frames vary in size depending on the size of the information field. A token is not a frame type (rather it is the type of frame).

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55773.htm

79. Which of the following are valid uses of the ICMP protocol?

Echo and reply message to test node reachability
Used by source to perform route tracing by incrementing the TTL
Redirect message to stimulate more efficient routing
Reliable transport protocol for some applications

Explanation: ICMP can be used for echo and reply messages, to redirect messages to assist more efficient routing. When a packet reaches a destination after the TTL (Time to Live) has been exceeded ICMP is used to send time exceeded messages to inform the sources the datagram has exceeded its allocated time to exist. Last but not least router advertisement and solicitation messages to determine the addresses of routers on directly attached networks. Although it is conceivable that an application use ICMP as a transport protocol, any reliability would be implemented at the application layer instead of a of the transport layer (eg: ICMP is NOT reliable even if the application sends a ICMP response to ensure receipt of information)

80. Which protocol is used to discover the addresses of routers on directly attached subnets?

ICMP
IDRP
TCP
UDP

Explanation: IDRP (ICMP Router Discovery Protocol) uses routers advertisements and router solicitation messages to discover the addresses of routers on directly attached subnets. If a host supports IDRP and uses a router with a poor metric to reach a destination then it will receive a ICMP redirect to another destination.

81. Which of the following are valid ways of IP multicasting?

Spanning Tree Protocol

UDP flooding
Subnet Broadcast
Internet Group Membership Protocol
Multicast Membership Protocol

Explanation: Multicasting is used when a single packet is needed to be sent to multiple destinations, it is used instead of sending a unicast packet to each destination. There are three ways that multicasting is accomplished. UDP flooding depends on the spanning tree algorithm to place interfaces in the forwarding and blocking states for multicast information, this is very useful for optimal flow of traffic throughout an internetwork. Subnet broadcast (RFC 922) supports the sending of packets to all the subnets of a particular network number, however packet duplication may occur where there are alternative paths to a destination. IGMP (Internet Group Membership Protocol - RFC 1112) relies on class D IP address for the creation of multicast groups, by using specific class D address an individual host dynamically registers itself in a multicast group.

82. Which of the following multicast methods requires that a host dynamically register itself in a multicast group?
UDP Flooding
Subnet Broadcast
IGMP
DVMRP

Explanation: Multicasting is used when a single packet is needed to be sent to multiple destinations, it is used instead of sending a unicast packet to each destination. There are three ways that multicasting is accomplished. UDP flooding depends on the spanning tree algorithm to place interfaces in the forwarding and blocking states for multicast information, this is very useful for optimal flow of traffic throughout an internetwork. Subnet broadcast (RFC 922) supports the sending of packets to all the subnets of a particular network number, however packet duplication may occur where there are alternative paths to a destination. IGMP (Internet Group Membership Protocol - RFC 1112) relies on class D IP address for the creation of multicast groups, by using specific class D address an individual host dynamically registers itself in a multicast group.

83. Distance Vector Multicast Routing Protocol uses reverse path flooding, with reverse path flooding…
The router floods the packet out all interfaces except the one the packet arrived from
The router floods the packet out all paths include the one it arrived from
The router floods the packet out all paths except the path that leads back to the source

Explanation: With DVMRP (Distance Vector Routing Protocol) the router floods all multicast packets out except the path that leads back to the destination (usually the one the packet arrived on, but not always).

84. Which of the following situations would cause a route to be learned through the wrong interface?
Invalid registration in the multicast registration group
Split horizon has been disabled on the interface
Routes are being distributed through the wrong protocol

Explanation: Though sometimes in a multipoint WAN environment it is desirable to leave split horizon disabled. Since Split horizons only allow routes to be propagated through interfaces other than the one it came from, thereby ensuring that routers are learned from the proper interface. Steps should be taken to ensure that routes are not learned from the wrong interface, in these situations you should use route filtering.

85. True/False: You are troubleshooting a down FDDI Ring, you get a pattern of all zeros in either address field for both neighbors, so you can safely assume there is a physical connection problem?

True

False

Explanation: When troubleshooting a FDDI ring first issue a "show interfaces fddi" command to see the status of the upstream and downstream neighbors. In the event that both neighbors appear as normal use a ping to test connectivity, if either neighbor shows all zeros in the address field then the problem is probably physical and you should use an OTDR or light meter to test for connectivity.

86. Which of the following are common problems that occur when a upstream neighbor has failed and a bypass switch has been installed?

Ring does not fail over correctly and becomes stuck in transitive sync

Bypass switches cause degradation and bring the ring down

The upstream neighbor sends a electrical pulse while it is going down which requires a manual reset on the bypass switch

Collisions occur on the FDDI ring

Explanation: When the upstream neighbor goes down and the FDDI ring fails over to a bypass switch you may encounter problems since bypass switches do not actually repeat signals, like a normal FDDI transceiver does.

87. Capturing appletalk packets with your sniffer with your encounter the following counter: 279 frames accepted. What is the meaning of this field?

the analyzer has transmitted 279 well formed packets

the analyzer has seen 279 well formed packets

279 packets have met the routers access list criteria

the router has received 279 packets that met the capture filter criteria

the analyzer has seen 279 packets with its address as the destination

Explanation: The packet sniffer only accepts frame which match its filter criteria, other frames are simply discarded. Once a frame has been accepted it is then recorded in the packet sniffer for review.

88. Identify the correct order to resolve a incorrect or corrupted image on a Cisco 2500 series router?

A. Power cycle router
B. at the > prompt enter o/r 0x1,
C. obtain a new system image via TFTP
D. press break key within 60 seconds
E. enter I to reinitialize the router

A, B, C, D, E

A, C, D, B, E

E, D, C, A, B

A, D, B, E, C

Explanation: in the event that your system image becomes corrupt on a Cisco 2500 series you should power cycle the router, and press the break key within 60 seconds of booting which will enter ROM monitor. At the ROM monitor prompt (>) enter o/r 0x1 to set the configuration regsiter to boot from ROM. Enter I to reinitialize the router, obtain the correct system image via TFTP, then fix the configuration as necessary and finally enter the "boot system flash" to change the configuration register to boot from flash memory instead of ROM.

89. Which word is used to describe the alternating pattern of ones and zeros at the front of an ethernet frame?

Header
FCS
Preamble
SOF
FCS

Explanation: The preamble is 7 bytes (or 8 if you count the last 8 bits which are technically the SOF – Start of Frame) which is used as a frame delimiter. The preamble is an alternating patter of 1's and 0's except for the last two bits which are 1's, these are used by the ethernet receiver to acquire bit synchronization.

90. Which word is used to describe the last 4 bytes of an 802.3 frame?

Header
FCS
Preamble
SOF
FCS

Explanation: The FCS is a 32 bit CRC calculated using the AUTODIN II polynomial (you don't need to know that for the exam). This field is normally generated by the chip and is used to determine if the data arrived in tact.

91. What is the longest and shortest ethernet frames (not including the preamble)?

48/1514
48/1600
60/1514
60/1600

Explanation: Ethernet frame format:
Preamble: 8 bytes (we don't actually count this in the frame size though)

Destination Ethernet Address: 6 bytes
Source Ethernet Address: 6 bytes

Length or Type: 2 bytes

Data: minimum of 46 bytes (padded if there is less data), maximum of 1500 bytes

FCS: 4 bytes

So the the shortest frame is 6 + 6 + 2 + 46 = 60 bytes, the longest frame is 6 + 6 + 2 + 1500 = 1514 bytes
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55773.htm

92. How do you tell the difference between an Ethernet II and a 802.3 ethernet frame?

Ethernet II does not have a FCS algorithm
Ethernet II implements a type, whereas 802.3 implement a length
Both formats use a difference sequencing algorithm
There is no noticable difference between the two formats

Explanation: Ethernet II uses the length field as a TYPE field, the TYPE code for IP is 0x800, while in IEEE 802.3 the same two bytes are used to specify a length of the frame. All Ethernet II type codes are > 1500 so that both frame formats can coexist peacefully on the same wire.

93. What is the 802.3 type code for the IP protocol?

0x006
0x800
0x100
0x001
There is no type code for IP

Explanation: This was a trick question, Remember 802.3 implements a length field whereas Ethernet II implements a type field. If we had asked what the type code for IP using Ethernet II was, the correct answer would have been 0x0800.

94. Which of the following FDDI specifications handles addressing, token handling, and error recovery?

SMT
MAC
PHY
PMD
NFS

Explanation:
Media Access Control (MAC)---Defines how the medium is accessed, including frame format, token handling, addressing, algorithm for calculating a cyclic redundancy check value, and error recovery mechanisms.
Physical Layer Protocol (PHY)---Defines data encoding/decoding procedures, clocking requirements, framing, and other functions.
Physical Layer Medium (PMD)---Defines the characteristics of the transmission medium, including the fiber-optic link, power levels, bit error rates, optical components, and connectors.
Station Management (SMT)---Defines the FDDI station configuration, ring configuration, and ring control features, including station insertion and removal, initialization, fault isolation and recovery, scheduling, and collection of statistics.
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55773.htm

95. Which of the following FDDI specifications handles defines data encoding/decoding, clocking requirements and framing?

SMT
MAC
PHY
PMD
NFS

Explanation:
Media Access Control (MAC)---Defines how the medium is accessed, including frame format, token handling, addressing, algorithm for calculating a cyclic redundancy check value, and error recovery mechanisms.
Physical Layer Protocol (PHY)---Defines data encoding/decoding procedures, clocking requirements, framing, and other functions.
Physical Layer Medium (PMD)---Defines the characteristics of the transmission medium, including the fiber-optic link, power levels, bit error rates, optical components, and connectors.
Station Management (SMT)---Defines the FDDI station configuration, ring configuration, and ring control features, including station insertion and removal, initialization, fault isolation and recovery, scheduling, and collection of statistics.

96. Which of the following FDDI specifications defines the characteristics of the transmission medium such as power levels, bit error rate, and optical components?

SMT
MAC
PHY
PMD
NFS

Explanation:
Media Access Control (MAC)---Defines how the medium is accessed, including frame format, token handling, addressing, algorithm for calculating a cyclic redundancy check value, and error recovery mechanisms.
Physical Layer Protocol (PHY)---Defines data encoding/decoding procedures, clocking requirements, framing, and other functions.
Physical Layer Medium (PMD)---Defines the characteristics of the transmission medium, including the fiber-optic link, power levels, bit error rates (BER), optical components, and connectors.
Station Management (SMT)---Defines the FDDI station configuration, ring configuration, and ring control features, including station insertion and removal, initialization, fault isolation and recovery, scheduling, and collection of statistics.
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55773.htm

97. Which of the following FDDI specifications handles FDDI stations configuration, ring configuration and ring control features including insertion and removal?

SMT
MAC
PHY
PMD
NFS

Explanation:
Media Access Control (MAC)---Defines how the medium is accessed, including frame format, token handling, addressing, algorithm for calculating a cyclic redundancy check value, and error recovery mechanisms.
Physical Layer Protocol (PHY)---Defines data encoding/decoding procedures, clocking requirements, framing, and other functions.
Physical Layer Medium (PMD)---Defines the characteristics of the transmission medium, including the fiber-optic link, power levels, bit error rates, optical components, and connectors.
Station Management (SMT)---Defines the FDDI station configuration, ring configuration, and ring control features, including station insertion and removal, initialization, fault isolation and recovery, scheduling, and collection of statistics.
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55773.htm

98. Which of the following protocols would you use to establish and maintain full duplex data streams between sockets in a Appletalk network.

ASP
ADSP
PAP
AFP

Explanation: AppleTalk Data Stream Protocol (ADSP) establishes and maintains full-duplex data streams between two sockets in a AppleTalk network. ADSP is a reliable protocol in that it guarantees that data bytes are delivered in the same order as sent and that they are not duplicated. ADSP numbers each data byte to keep track of the individual elements of the data stream. ADSP also specifies a flow-control mechanism. The destination can essentially slow source transmissions by reducing the size of its advertised receive window. ADSP also provides an out-of-band control message mechanism.
Attention packets are used as the vehicle for moving out-of-band control messages between two AppleTalk entities. These packets use a separate sequence number stream to differentiate them from normal ADSP data packets. ADSP is a session layer protocol.

99. Which Appletalk protocol is used to establish and maintain sessions between clients and servers?

ASP
ADSP
PAP
AFP

Explanation: The AppleTalk Session Protocol (ASP) establishes and maintains sessions (logical conversations) between an AppleTalk client and a server. ASP is considered a session layer protocol.

100. Which of the following protocols is a connection oriented protocol that establishes connections between clients and servers?

ASP
ADSP
PAP
AFP

Explanation: AppleTalk's Printer Access Protocol (PAP) is a connection-oriented protocol that establishes and maintains connections between clients and servers. (Use of the term printer in this protocol's title is part of its legacy though it has no relevance to the current implementation.) PAP is considered a session layer protocol

101. Which Appletalk protocol is used to help clients share files across a network?

ASP
ADSP
PAP
AFP

Explanation: The AppleTalk Filing Protocol (AFP) helps clients share server files across a network. The Appletalk Filing Protocol maps to the Application and Presentation layers of the OSI model.

102. Which of the following Appletalk protocols are part of AppleTalk’s transport layer?

RTMP
AFP
AURP
ASP

Explanation: AppleTalk's transport layer is implemented by several protocols: Routing Table Maintenance Protocol (RTMP), AppleTalk Update-Based Routing Protocol (AURP), AppleTalk Echo Protocol (AEP), AppleTalk Transaction Protocol (ATP), and Name Binding Protocol (NBP).

103. AppleTalk's primary network-layer protocol is the ____

AARP
RTMP
ZIP
DDP
NBP

Explanation: AppleTalk's primary network-layer protocol is the Datagram Delivery Protocol (DDP). DDP provides connectionless service between network sockets. Sockets can be assigned either statically or dynamically.

104. Which of the following are valid Appletalk Addresses?

10.1.1.1
10.1.1
10.1
10

Explanation: AppleTalk addresses, which are administered by the DDP, consist of two components: a 16-bit network number and an 8-bit node number. The two components are usually written as decimal numbers, separated by a period (for example, 10.1 means network 10, node 1). When an 8-bit socket identifying a particular process is added to the network number and node number, a unique process on a network is specified.

105. Which protocol used to tunnel Appletalk packets through a non appletalk network?

RTMP
ZIP
AURP
ATP

Explanation: AppleTalk Update-Based Routing Protocol (AURP) allows a network administrator to connect two or more AppleTalk internetworks through a foreign network (such as Transmission Control Protocol/Internet Protocol [TCP/IP]) to form an AppleTalk wide-area network (WAN). The connection is called a tunnel, which functions as a single, virtual data link between the AppleTalk internetwork
AURP uses the principle of split horizons to limit the propagation of routing updates. For that reason, an exterior router sends routing information about only the networks that comprise its local network to other exterior routers connected to the tunnel. Remember that split horizons states that it is never useful to send information about a route back in the direction from which the information came)

106. Which FDDI ECM state means the router is allowing time for the optical bypass switch to join into the ring?

CHECK
INSERT
TRACE
PATH_TEST

Explanation: there are 8 SMT entity coordination management states, which overlook the operation of CFM and PCM. The ECM state can be on of the following:
Out – router is isolated form the network.
In – router is actively connected tot he network. This is the normal state for a connected router.
Trace – router is trying to localize a stuck beacon condition.
Leave – router is allowing time for all connections to break before leaving the network.
Path_test – router is testing its internal paths
Insert – router is allowing time for the optical bypass to insert
Check – router is making sure optical bypasses switched correctly
Deinsert – router is allowing time for the optical bypass to deinsert

107. Which of the following is true about a Appletalk Node?

A node can belong to a single zone
A node can belong to multiple zones

A node can belong to multiple zones as long as it is a server

Explanation: Zones are defined by the AppleTalk network manager during the router configuration process. Every node in an AppleTalk network belongs to a single specific zone. However Appletalk phase II implements the concept of an extended network which can have multiple zones. Nodes on extended networks can belong to any single zone associated with the extended network.

108. Which Appletalk protocol is a transport protocol which is transmitted reliably?

ARTP
AARP
ATP
ZIP

Explanation: ATP is suitable for transaction-based applications such as those found in banks or retail stores. ATP transactions consist of requests (from clients) and replies (from servers). Each request/reply pair has a particular transaction ID. Transactions occur between two socket clients. ATP uses exactly once (XO) and at-least-once (ALO) transactions. XO transactions are used in situations where performing the transaction more than once would be unacceptable. Banking transactions are examples of transactions that, if performed more than once, would result in invalid data. ATP is capable of most important transport-layer functions, including data acknowledgment and retransmission, packet sequencing, and fragmentation and reassembly. ATP limits message segmentation to 8 packets, and ATP packets cannot contain more than 578 data bytes.

109. Which protocol is used to associate an Appletalk address with a particular media address?

NBP
AARP
FLAP
ZIP

Explanation: The AppleTalk Address Resolution Protocol (AARP) is used to associate AppleTalk addresses with particular media addresses. AARP associates protocol addresses with hardware addresses. When either AppleTalk or any other protocol stack must send a packet to another network node, the protocol address is passed to AARP. AARP checks its address cache to see if the relationship between the protocol and the hardware address is already known. If so, that relationship is passed up to the inquiring protocol stack. If not, AARP sends a broadcast or multicast message inquiring about the hardware address for the protocol address in question. If the broadcast reaches a node with the specified protocol address, that node replies with its hardware address. This information is passed up to the inquiring protocol stack, which uses the hardware address in communications with that node.

110. Select the correct order for Appletalk node address assignment

1. Conflicting address sends a conflict message indicating a problem
2. Node chooses a new address
3. Chooses its first network address
4. Chooses a network protocol
5. Checks to see if a network address is in use

4, 3, 5, 1, 2

Explanation: To ensure minimal network administrator overhead, AppleTalk node addresses are assigned dynamically. When a Macintosh running AppleTalk starts up, it chooses a protocol (network-layer) address and checks to see whether that address is currently in use. If not, the new node has successfully assigned itself an address. If the address is currently in use, the node with the conflicting address sends a message indicating a problem, and the new node chooses another address and repeats the process

111. Which of the following are valid Appletalk Link Layer protocols? (1)

ADSP, ZIP, ASP

TDSP, TASP, PAP, NBP
ELAP, LLAP, TLAP, FLAP
NBP, ADSP, ZIP, PAP

Explanation: Apple refers to AppleTalk over Ethernet as EtherTalk, to AppleTalk over Token Ring as TokenTalk, and to AppleTalk over FDDI as FDDITalk. The link-layer protocols that support
AppleTalk over these media are EtherTalk Link Access Protocol (ELAP), LocalTalk Link Access Protocol (LLAP), TokenTalk Link Access Protocol (TLAP), and FDDITalk Link Access Protocol (FLAP). For more information about the technical characteristics of Ethernet, Token Ring, and FDDI

112. What is the maximum speed and node count of a local talk network?

230.4 kbps / 32 nodes
512 kbps / 64 nodes
1 mbps / 128 nodes
10 mbps / 256 nodes

Explanation: LocalTalk is Apple's proprietary media-access system. It is based on contention access, bus topology, and baseband signaling, and runs on shielded twisted-pair media at 230.4 kbps. The physical interface is EIA/TIA-422 (formerly RS-422), a balanced electrical interface supported by EIA/TIA-449
(formerly RS-449). LocalTalk segments can span up to 300 meters and support a maximum of 32 nodes.

113. Which Appletalk protocol is used to establish and maintain routing tables?

ZIP
NBP
RTMP
AURP

Explanation: The protocol that establishes and maintains AppleTalk routing tables is called the Routing Table Maintenance Protocol (RTMP). RTMP routing tables contain an entry for each network that a datagram can reach. Each entry includes the router port that leads to the destination network, the node ID of the next router to receive the packet, the distance in hops to the destination network, and the current state of the entry (good, suspect, or bad). Periodic exchange of routing tables allows the routers in an internetwork to ensure that they supply current and consistent information.

114. Which protocol is the Appletalk counterpart to TCP/IP’s DNS server?

RTMP
NBP
ASP
AURP

Explanation: AppleTalk's Name Binding Protocol (NBP) associates AppleTalk names (expressed as network-visible entities, or NVEs) with addresses. An NVE is an AppleTalk network-addressable service, such as a socket. NVEs are associated with one or more entity names and attribute lists. Entity names are character strings such as printer@net1, while attribute lists specify NVE characteristics.

115. What term is used to describe the following table:

1. Marketing
2. Accounting
3. Engineering

ZIP
ZIT
ZONE MAP
ZONE LIST

Explanation: ZIP maintains network number to zone name mappings in zone information tables (ZITs). ZITs are stored in routers, which are the primary users of ZIP, but end nodes use ZIP during the startup process to choose their zone and to acquire internetwork zone information. ZIP uses RTMP routing tables to keep up with network topology changes. When ZIP finds a routing table entry that is not in the ZIT, it creates a new ZIT entry.

116. When troubleshooting a problem connecting a modem to a router which of the following is a useful diagnostic step?

Use the show line command to verify adequate buffering
Issue the show line command to check modem state
Show serial s0 queue to monitor traffic on the port
Upgrade to the latest modem drivers

Explanation: use the show line exec command on the access serer or router. The output for the auxiliary port should show inout or RiisCD in the modem column. This indicates that modem control is enabled on the line of the access server or router.

117. The follow lines are part of the output from a show interfaces command:
Ethernet 0 is up, Line protocol is up
Hardware is MCI Ethernet aa00.0040.0134 BIA 0000.0c00.4365
Ethernet address 131.0.8.11 subnet 255.255.255.0

Which hardware address will this station respond to

0000.0c00.4365
Aa00.0040.0134
131.0.8.11
255.255.255.0

Explanation: the hardware address is aa00.0040.0134, while the BIA (Burned In Address) is 0000.0c00.4365 it has been overridden to aa00.0040.0134

118. What does the SNAP mean in the following packet dump:
FC: LLC Frame PFC
Attention Code = none
FS addr recognized indicator –0
Frame copied indicator 00
Destination = station cisco a05903
Source = station ibm 0a8591
Llc header
dsap ==aa
Source sap = aa
Command unnumbered frame relay
Dsap header type 0x800

subnetwork access protocol
super non application process
serial network application
second node appearance

Explanation: Sub-Network Access Protocol (SNAP) is similar to 802.2, with LLC parameters, but with expanded LLC capabilities. Ethernet SNAP can support IPX/SPX, TCP/IP, and AppleTalk Phase 2 protocols.

119. Capturing appletalk packets with your sniffer with you encounter the following counter:
5024 frames received
What is the meaning of this field ?

the analyzer has transmitted 5024 well formed packets
the analyzer has seen 5024 well formed packets
5024 packets have met the routers access list criteria
the router has received 5024 packets that met the capture filter criteria
the analyzer has seen 5024 packets with its address as the destination

Explanation: What the analyzer receives and what the analyzer accepts are two different values. Just because a frame was received does not necessarily mean it matched the frame/packet filter criteria. If a frame doesn't match the criteria then it is simply discarded.

120. Which problem will cause an increasing number of transitions occurred when you do a show interface token ring

Broadcast storms
The ring is repeatedly going down and coming back up
Malformed packet arriving on the token ring interface
Excessive ring poll processes on the network

Explanation: The transition counter holds the number of times the ring made a transition from up to down, or vice versa. A large number of transitions indicates a problem with the ring or the interface.

121. Which FDDI ECM state means the router is allowing time for the optical bypass to remove itself from the ring?

CHECK
DEINSERT
TRACE
PATH_TEST

Explanation: there are 8 SMT entity coordination management states, which overlook the operation of CFM and PCM. The ECM state can be on of the following:
Out – router is isolated form the network.
In – router is actively connected tot he network. This is the normal state for a connected router.
Trace – router is trying to localize a stuck beacon condition.
Leave – router is allowing time for all connections to break before leaving the network.
Path_test – router is testing its internal paths
Insert – router is allowing time for the optical bypass to insert
Check – router is making sure optical bypasses switched correctly
Deinsert – router is allowing time for the optical bypass to deinsert

122. Which problem will cause an increasing number of CRC errors occurred when you do a show interface token ring

Broadcast storms
The ring is repeatedly going down and coming back up
Malformed packet arriving on the token ring interface
Excessive ring poll processes on the network

Explanation: The CRC counter increases when the interface receives packets that fails the Cylic Redundancy Checksum. The cylic redundancy checksum (CRC) is generated by the originating LAN station or far-end device and should match the checksum calculated from the data received by the interface. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of a station transmitting bad data.

123. Which tool is best suited for testing signals across a PC / Modem interface?

Network monitor
Breakout box
Time domain reflectometer
Null modem cable

Explanation: break out boxes, BERTS (Bit Rate Error Testers) and fox boxes are useful for troubleshooting problems in peripheral interfaces. These devices can monitor data line condiditions, analyze and trap data, and diagnose problems common to data communication systems.

124. After capturing a variety of IPX traffic from your network, you want to view only the packets using the 802.3 frame type, what is the easiest way to accomplish this?

Set a router access list that prevent other frame types on the network
switch the analyzers connection to thin ethernet
configure a display filter
set the interface card in the analyzer to accept on the ethernet II frame type

Explanation: You've already received the packets, so the only correct answer is the configure a display filter.

125. What tool is useful for certification of your Lan infrastructure?

a bert/wart
cable tester
packet driver
network management system

Explanation: cable testers enable you to check phyiscal connectivity. Cable testers are available for most types of cable. A cable tester might be able to test and report on cable connections included NEXT (Near end crosstalk), perform TDR

126. You have noticed a few of your IPX clients on a serverless segment are having a problem connecting to their router since you've updated your router from an older IOS version to the newest version. What action can you take to resolve this problem

enable old style novell broadcasts
issue the ipx gns-round-robin
increase the ipx-gns-reponse-delay time on the router
enable gns on the cisco router
turn off gns on the novell server

127. What command displays the entries in the routing table

Show ip route
Show ip protocol
Show ip arp
Ping

128. You are on a network with a large variety of traffic, you only want to accept the packets using the 802.3 frame type, what is the easiest way to accomplish this?

Set a router access list that prevent other frame types on the network
switch the analyzers connection to thin ethernet
configure a display filter
set the interface card in the analyzer to accept only the desired frame type

Explanation: The analyzer will only receive whatever traffic the network card sends it, by configuring the frame type to only accept 802.3 then you will prevent the analyzer from seeing other frame types.

129. Based on the output of the show processes command what problem is currently affecting the router,:

```
Router1>show processes
CPU utilization for five seconds: 100%/90%; one minute: 79%; five minutes: 59%
PID QTy       PC Runtime (ms)    Invoked   uSecs    Stacks TTY Process
  1 Mwe   15AD82    420354636  232519845    1807 1816/3000   0 IP-EIGRP Router
  2 Lst    7520A    584387348    4922340  118726 1780/2000   0 Check heaps
  3 Mst    9D35E           0          2       0 1768/2000   0 Timers
  4 Lwe    F68D8     23212148   17455578    1329 1084/2000   0 ARP Input
  5 Lwe   110B42           0          1       0 1764/2000   0 Probe Input
  6 Mwe   1104BE       64736     189362     341 1712/2000   0 RARP Input
  7 Hrd   1021A8    258473500  222795846    1160 2828/4000   0 IP Input
  8 Mwe   12B99A       196784    8186013      24 1056/2000   0 TCP Timer
  9 Lwe   12D764         1220        503    2425 3204/4000   0 TCP Protocols
 10 Mwe   17A406     10036532    8521505    1177 1440/2000   0 CDP Protocol
```

Several ospf and iso protocols have stopped running
The tcp timer has expired
Excessive high network bandwidth utilization
high cpu utilization

Explanation: the CPU utilization is extremely high, the 100% and 79% show the overall cpu usage and the overhead caused by interrupts respectively.

130. What command can you use to obtain a routers firmware version?

Show config
Show version
Show controller
Show system

Explanation:

Router1>show version
Cisco Internetwork Operating System Software
IOS (tm) 4000 Software (XX-IN-M), Version 11.0(17), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Thu 04-Sep-97 15:02 by richv

Image text-base: 0x00012000, data-base: 0x003C0FA0

ROM: System Bootstrap, Version 4.6(4), SOFTWARE

City_Hall uptime is 67 weeks, 1 day, 17 hours, 49 minutes
System restarted by reload at 23:16:51 PST Wed Nov 5 1997
System image file is "4000ios-11.16.bin", booted via flash

cisco 4000 (68030) processor (revision 0xA0) with 16384K/4096K bytes of memory.
Processor board ID 5037838
G.703/E1 software, Version 1.0.
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
2 Ethernet/IEEE 802.3 interfaces.
6 Serial network interfaces.
128K bytes of non-volatile configuration memory.
4096K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

131. What is an advantage of a connectionless protocol?

high reliability
preferrable and lengthy exchanges of data
less network traffic
fast error recovery and flow control

Explanation: Since connectionless protocols do not require the extra overhead of sending back an acknowledgement they require much less traffic. Examples of connectionless protocols include UDP and IPX.

132. What is a common term Cisco systems uses when referring to the frame type Novell describes as ethernet 802.3
choose (1)

e2

arpa
ethernet_ii
snap
ethernet_snap
etherner_802.2
novell-ether
sap
ISO 1

Explanation: the keyword for Novell's 802.3 encapsulation is novell-ether

133. What problem is likely to result in a users inability to see zones or services outside their own network?

clients are not configured with a default gateway
phase 1 / phase ii incompability
incorrect appletalk encapsulation
too many zones configured for a single network

Explanation: Since appletalk networks automatically detect their gateways, the most probable cause is a phase I / phase II incompatibility, however we should also point out that in the few remaining appletalk networks, there is little to no chance of finding this particular problem!

134. The results of a show controllers token command on one of the token ring interfaces on your router includes the information that the interface is "bridge capab1e" what does this mean?

the ring bridge has passed the ring bridge self test
source bridge routing is enabled
the interface is bridge capable but not configured for bridging
the router has source route bridging buffers available

Explanation: show controllers token is the command, bridge capable means that it could, but it isn't right now.

135. Which FDDI ECM state means the router is isolated from the network?

IN
OUT
TRACE
LEAVE
DEINSERT

Explanation: there are 8 SMT entity coordination management states, which overlook the operation of CFM and PCM. The ECM state can be on of the following:
Out – router is isolated form the network.
In – router is actively connected tot he network. This is the normal state for a connected router.
Trace – router is trying to localize a stuck beacon condition.
Leave – router is allowing time for all connections to break before leaving the network.
Path_test – router is testing its internal paths
Insert – router is allowing time for the optical bypass to insert
Check – router is making sure optical bypasses switched correctly
Deinsert – router is allowing time for the optical bypass to deinsert

136. What command can you use to obtain a routers configuration for your tech support engineer

Show firmware
Show controllers
config
Show running-config

Explanation: Show running-config lists your current running configuration, which is the configuration that the system is using right now, this is the most useful information when debugging your router.

137. What does IPX internal network command do?

Set the ipx interface as non seed
Adds an additional network address to an interface
Assigns the address for IPX when it is tunneled over IP network
Assigns the address that is advertised by NLSP and IPX wan on all router interfaces

Explanation: Every novell server uses an internal IPX network number which is uses to forward packets between networks. Every network number must be unique throughout the entire Novell IPX internetwork. A duplicate network number will prevent packets from being forwarded properly.

138. You configured your Novell server to use 802.2 encapsulation, you check your router sap table and notice it is empty, what is a possible problem?

SAP is not supported on 802.2
Mismatched frame type
IPX does not work correctly with 802.2

Explanation: By default Cisco routers use 802.3 encapsulation (otherwise known as novell-ether)

139. show interface fddi 3/0 displays an upstream neighbor value of 0000 0000 0000 what is the significance of this address?

it is the software address of the upstream neighbor
it is the hardware address of the upstream neighbor
there is probably a physical problem
the address upstream neighbor is illegal

Explanation: A value of 0000 0000 0000 means the upstream neighbor is unknown, and that there is a good chance a physical problem has occurred.

140. Which step of the troubleshooting process involves asking questions of affected users, and collecting information from network management systems.

logging the trouble ticket
verifying the information
gathering facts
defining the problem
isolating the problem to the device level

Explanation: After defining the problem, you should gather facts by asking questions of affected users and network administrators. Collect information from sources such as network management systems, protocol analyzers traces, output from router diagnostic commands or software release notes.

141. Which step of the troubleshooting process dictates that you should contact affected users and check network management tools.

verifying the information
gathering facts
defining the problem
isolating the problem to the device level

Explanation: After defining the problem, you should gather facts by asking questions of affected users and network administrators. Collect information from sources such as network management systems, protocol analyzers traces, output from router diagnostic commands or software release notes.

142. Which step of the troubleshooting process contains changing one variable at a time to allow you to reproduce a given situation

logging the trouble ticket
verifying the information
gathering facts
defining the problem
isolating the problem to the device level

Explanation: After defining the problem, and gathering information, you should isolate the problem to one device, to do this you should change only one variable at time until the problem is resolved.

143. Which FDDI ECM state means the router is actively participating in the network?

CHECK
INSERT
OUT
IN
LEAVE

Explanation: there are 8 SMT entity coordination management states, which overlook the operation of CFM and PCM. The ECM state can be on of the following:
Out – router is isolated form the network.
In – router is actively connected tot he network. This is the normal state for a connected router.
Trace – router is trying to localize a stuck beacon condition.
Leave – router is allowing time for all connections to break before leaving the network.
Path_test – router is testing its internal paths
Insert – router is allowing time for the optical bypass to insert

Check – router is making sure optical bypasses switched correctly
Deinsert – router is allowing time for the optical bypass to deinsert

144. Which step of the troubleshooting process contains identifying a set of symptoms and associated causes?

logging the trouble ticket
verifying the information
gathering facts
defining the problem
isolating the problem to the device level

Explanation: The first in analyzing a network problem is to make a clear problem statement. You should define the problem in terms of a set of symptoms and potential causes.

145. Which FDDI ECM state means the router is actively trying to reclaim a stuck beacon?

CHECK
INSERT
TRACE
PATH_TEST

Explanation: there are 8 SMT entity coordination management states, which overlook the operation of CFM and PCM. The ECM state can be on of the following:
Out – router is isolated form the network.
In – router is actively connected tot he network. This is the normal state for a connected router.
Trace – router is trying to localize a stuck beacon condition.
Leave – router is allowing time for all connections to break before leaving the network.
Path_test – router is testing its internal paths
Insert – router is allowing time for the optical bypass to insert
Check – router is making sure optical bypasses switched correctly
Deinsert – router is allowing time for the optical bypass to deinsert

146. which tool can be used to verify cable length? (2)

ethernet analyzer
tdr
snmp agent
volt/ohm meter

Explanation: Time Domain Reflectors are used to trouble shoot crimps, kinks, impedance, bends, and other defects in metallic cables. Optical Time Domain Reflectors (OTDR) are used to troubleshoot optical cable. A TDR works by bouncing a signal off the end of the cable. Opens, shorts, and other problems reflect the signal back at different amplitudes, depending on the problem. A TDR measures how much time it takes the signal to reflect and calculates the distance to a fault.

147. Which line in the partial display of the tcp packet header listed below indicates available space for incoming data below:

tcp: source port = 1339
tcp: destination port = 23

tcp: initial sequence number = 0
tcp: data offset = 20 bytes
tcp: flags = 20
tcp: 0 = no urgent point
tcp: 0 = no acknowledge
tcp: 0 = no push
tcp: 0 = no reset
tcp: 1 sent
tcp: 0 = no fin
tcp: tcp window = 512
tcp: checksum = e43e correct
tcp: no options

Explanation: the TCP window indicates how many packets can be sent or received before an acknowledgement must be sent.

148. What is the source of a common novell network error referred to as "Configuration mistmatch"

routers do not contain support for proprietary novell frame types
servers or routers have assigned different network addresses to a common network
inconsistent frame types used by the clients and servers
netware servers on the same network using different frame types

Explanation: Since Novell servers will often autodetect network numbers, and frame types during installation, when a novell server is moved from one cable segment to another great care should be taken to change the network numbers or else the server will not be able to communicate with other servers on the same segment. Since clients issue a Get Nearest Server (GNS) they may attach to the new server and then be isolated from the rest of the network.

149. what command reports the discover of new zones?

Debug apple errors
Debug apple zip
Debug apple routing
Show apple interfaces

Explanation: Zone information protocol is used to keep track of zones, debug apple zip shows any changes in the zone table.

150. when diagnosing a problem the output of the show interfaces serial command includes the following line:
serial s0 is administratively down, line protocol is down
what does this mean?

the serial line is in an idle state
the interface has been taken down by an administrator
the remote router is down
the interface is in an idle dial on demand link

Explanation: anytime and interface is administratively down, it means that somebody issued a "shutdown" while in interface configuration mode.

151. Regarding the following frame which statements are true? (choose 2)

Ipx: ipx header
Ipx: no align
Ipx: checksum = ffff
Ipx: length = 224
Ipx: transport control = 00
Ipx: 0000 = reserved ipx
Ipx: ….. 0000 = hop count
Ipx : dest network.node = 1000.ffffffffffff socket = 1106 (sap)
Ipx: src network.node = 100.02.60 c2 fc 79 socket = 1106 (sap)

This is a broadcast packet
This frame uses a snap format
This is uses a novell ether frame
This a portion of a network layer protocol
The ipx portion is a connection oriented protocol

Explanation: this must be a novell ethernet frame since it has a length, rather than a type field. This is a broadcast packet because the destination network node is ffff ffff ffff and because it's a SAP.

152. A show interfaces serial command indicates a high number of ignored frames, what is the significance of the interface ignore counter?

The amount of frames received which where too large for the interface buffers
The number of times the hardware interface discarded frames because it ran low on internal buffers
The amount of frames received which could not be saved due to congestion on the routers backplane
The number of times the hardware interface could not save data to its internal buffer due to high traffic rates
The number of times the physical media dropped frames due to improper buffering

Explanation: Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.

153. An IP ping command displays a series of five exclamation points in the output. What is the significance of the exclamation points.

Network unreachable
a level five error was returned
indicates a wait time before a reply was received
five replies were received
five receive buffers available.

Explanation: a ! (exclamation) is used to show that a packet was received, while a . (period) is used to show that a packet was not received.

154. Which of the following protocols are always connectionless (choose 3)

1. IP
2. Tcp

3. Arp
4. 802.3
5. 802.2

Explanation: This is a trick question. Typicallky Link layer protocols such as 802.3 are not reliable (expect in certain WAN environments such as X.25) however 802.2 includes a type 2 version which is reliable. ARP (Address Resolution Protocol) is also not transmitted reliably since there is no guarantee that you'll ever get a response back. IP includes TCP, it is also sometimes transmitted reliably (however IP also supports UDP and ICMP for transport, which are not reliable). The answer to this question requires that you have read the the Appendix A in Cisco CIT v4.0 book it says that 802.2 have a type 2 which is connection oriented, it also says that IP is connectionless.

155. What is the show buffers command used for?

Showing trends that indicate the link is a bottleneck
Baseline application performance
Proof of interface functionality
Verifying that all protocols are operational

Explanation: Use the show buffers EXEC command to display statistics for the buffer pools on the network server and the interfaces on the system. Once again, many answers here could seem correct however in the Cisco CIT book says "If the situation is bad enough, you must increase the bandwidth of the link, however increasing the bandwidth might not be necessary or immediately practical. One way to resolve marginal serial line over utilization problems is to control how the router users buffers."

156. What type of device is typically used to test physical connectivity?

protocol analyizer
digital multimeter
breakout box
packet driver

Explanation: Volt Ohm Members, digital multimeters and cable testers are all used to measure physical properties such as current, resistance, capacitance, and cable continuity. Cable testers (also called Cable scanner) let you check physical connectivity on STP, UTP, 10BaseT, coaxial, and twinax cable. Some cable testers might also be able to test and report on near end cross talk (NEXT), attenuation, and noise, perform TDR and traffic monitoring and wire map functions, and display MAC information.

157. Which tool is most useful for analysis of redesign, reconfiguration, or stress testing?

network analyzer
network management system
simulation and modeling tools
network monitor

Explanation: While each of the tools listed is helpful when planning a redesign, reconfiguration or stress test, you need to know the official Cisco answer.
From the CIT 4.0 book, page 2-17 "Simulation/modelling software is useful for purposes such as initial network design, analysis of a network reconfiguration or redesign, and stree-testing a network."

158. what type of protocol requires the application to request retransmission of lost, missing or corrupt packets?

connectionless

connection oriented
host to host
client/server

Explanation: connection oriented protocols such as SPX or TCP require that the packet be received, and acknowledged or that the sender should resend the packet.

159. which step follows isolating a problem isolating a problem to a specific device (router)
swapping out the router and observe the result
run a diagnostic on all interfaces and observe the result
isolate the likely problem source to a single variable
upgrade all software to the current release levels?

Explanation: swapping out the device is likely to isolate the problem to a device, if you replace the device and the problem remains then the device is not your problem, check cabling and configuration.

160. A show interfaces serial command indicates a high number of overruns, what is the significance of the interface overrun counter?
The amount of frames received which where too large for the interface buffers
The amount of frames received which could not be saved due to congestion on the routers backplane
The number of times the hardware interface could not save data to its internal buffer due to high traffic rates
The number of times the physical media dropped frames due to improper buffering

Explanation: The overrun counter keeps track of the number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.

161. Where should you first look for errors when troubleshooting a serial wan problem?
the physical connections by checking the cable interface connections
the protocol operation by viewing a packet trace of link traffic
interface operation with the show interface command
network host reachability with the ping utility?

Explanation: Using the show interface exec command is the first step in troubleshooting wan connections. It will give you one of 5 error states: serial x is down, line protocol down; serial x is up, line protocol is down; serial x is up, line protocol is up (looped); Serial x is up, line protocol is up (disabled); Serial x is administratively down, line protocol is down. Notice that the serial interface is never down while the line protocol is up, this is a common trick on the CIT exam.

162. Where are the output of the debug and system error messages sent by default?
output configuration requires a tftp server to put files
console
output is written to a syslog server
error logging automatically invokes debug output to a designated ftp server

Explanation: Error messages are sent to the console port by default. By connecting a PC or Macintosh to the console port of the router and log all output to a disk file (using a terminal emulation program). The exact procedure varies depending on the communication package used with the system.

163. What is the troubleshooting engine?

the report generator for cisco debug commands
the name of the cisco documentation cd
a customer engineered tool that uses case based reasoning to solve common problems
a cisco road show highlighting internetwork troubleshooting solutions

Explanation: Cisco has developed the Troubleshooting Engine, which provides simulations of failures and allows users to test possible solutions. Customers and CSEs use this tool to learn how to diagnose and repair failures in a variety of different network configurations. The TAC constantly updates the Troubleshooting Engine, with new configurations and regular testing. For some configurations, CSEs have connected the Troubleshooting Engine to network hardware in the TAC lab to allow diagnosis on actual hardware, rather than being limited to software simulation.

164. A show interfaces serial command indicates a high number of interface resets, what is the significance of the interface resets counter?

the router restart several times
key packets were not sent within several seconds time
there have been several attempts to restart the interface with the protocol down but the interface up
this counter reflects the number of times the reset button the back of the router was pushed

Explanation: The interface reset counter keeps the number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.

165. Which command should you use on an appletalk network if you suspect problems and want to monitor neighbors becoming reachable or unreachable and interfaces coming up or down.

show apple rtmp
debug apple traffic
protocol apple verbose
debug apple events

Explanation: Use the debug apple events EXEC command to display information about AppleTalk special events, neighbors becoming reachable/unreachable, and interfaces going up/down. Only significant events (for example, neighbor and route changes) are logged. The no form of this command disables debugging output. The other commands listed do not exist, however if the command “debug apple routing” had been listed it would also be correct.

166. When should you use the write core command?

to obtain a core dump after a router has crashed?
To write a backup of the configuration to the routers memory
To obtain a memory image of a malfunctioning router
to write the os image to nvram

Explanation: When a router crashes, it is sometimes useful to obtain a full copy of the memory image (called a core dump) to identify the cause of the crash. Core dumps are generally only useful to your technical support representative.

167. The show Ipx traffic displays the pitched count increasing and the routes disappear and reappear often. Which of the problems is likely a source of the symptoms?

increased routing throughput
better error recovery with redundant links
routes unpredictably appearing and disappearing
the router is sending broadcasts on a network with spanning tree disabled
non routable protocols could not reach remote destinations.

Explanation The pitched packets counter measures the number of times the router received its own broadcast packet. When spanning tree is disabled packets have the possibility of looping endlessly across bridges, thereby causing a single broadcast packet to be received more than once.

168. When troubleshooting a wan connection what command displays hardware type and version information for each module in a Cisco router?

Show interfaces serial
Show version
Show controller
Show running-config

Explanation: The “show controllers” (short version is show controller) command displays the current internal status information for the interface controller cards.
Syntax: show controllers [e1 | ethernet | fastethernet | fddi | serial | t1 | token]

169. When placing your CSU/DSU in loopback which of the following should happen:

The keepalive counters will increment
The show interface serial x should say that it is looped
The error lite on the remote CSU should be activated
The green lite on the interface should turn to orange

Explanation: One of the steps to perform while troubleshooting a HDLC or PPP link is to put the CSU/DSU in loopback mode. Once you put the CSU/DSU in loopback mode you should issue a “show interfaces serial” exec command to determine whether the line status changes from “line protocol is down” to “line protocol is up (looped),” or if it remains down. Since any traffic sent out, is automatically received back you should see the keepalive counter increment (which is why the interface should come up)

170. When a CSU/DSU is in loopback, the line protocol should be:

Up
Down
Either up or down
Transitive

Explanation: depending on the problem (local or remote) the results of the “show interfaces serial” exec command will display that the interface is up (indicating a problem on the remote end) or the interface is down (indicating a problem with the local interface or cable). There is no such thing as a transitive state.

171. True/False: The best way to troubleshoot a frame relay connection is to put the CSU/DSU in loopback mode?

True

False

Explanation: Because there is no concept of a loopback in X.25 or Frame Relay packet switched network (PSN) environment, loopback tests do not apply.

172. The output of show buffers indicates an increasing trend under very big buffers what does this indicate?

too many frames are being sliced because the receive buffer is too small
outgoing frames are being truncated because the very big buffer size is too small
the number of very big output buffers is being reduced
there are no buffers in the free list
Unused very big buffers are being reduced to smaller buffers

Explanation: Cisco routers allocate different sized buffers, when a buffer is needed and none exist in the freelist then a new buffer is created. The created count from the show buffers keeps track of the number of new buffers created to satisfy buffer allocation attempts when the available buffers in the pool have already been allocated.

173. You have begun implementing an action plan to resolve a problem. What should your next action be if your previous action did not solve the problem?

gather additional facts
undo the changes that didn't work
repeat the process modifying additional variables till a solution is reached
evaluate the problem definition for validity

Explanation: According to cisco you should only change one variable at a time, if the changes you make do not solve the problem then you should undo the changes.

174. What is the purpose of the debug arp command?

Determines if the router is sending and receiving arp requests?
displays the arp cache contents
send an arp request to all attached router neighbors
place a new list of ip hardware address pairs for all stations on attached segments into the routers cache.

Explanation: Use the debug arp EXEC command to display information on Address Resolution Protocol (ARP) transactions. The no form of this command disables debugging output. Use this command when some nodes on a TCP/IP network are responding, but others are not. It shows whether the router is sending ARPs and whether it is receiving ARPs. Example:
router# debug arp
IP ARP: sent req src 172.16.22.7 0000.0c01.e117, dst 172.16.22.96 0000.0000.0000
IP ARP: rcvd rep src 172.16.22.96 0800.2010.b908, dst 172.16.22.7
IP ARP: rcvd req src 172.16.6.10 0000.0c00.6fa2, dst 172.16.6.62
IP ARP: rep filtered src 172.16.22.7 aa92.1b36.a456, dst 255.255.255.255 ffff.ffff.ffff
IP ARP: rep filtered src 172.16.9.7 0000.0c00.6b31, dst 172.16.22.7 0800.2010.b908

175. How do you use the show processes command to see when processes are causing an excessive load on the router?

issue the command at select time throughout the workday to note the variations in the values over time

issue the command multiple times because the fast clock of the router does not provide an accurate snapshot of the router with a single invocation

redirect output to a file since the high number of processes running on a router results in multiple screens of information

issue the command several times on a busy router because high utilization spikes truncate the output of the command.

Explanation: the show processes command (or more specifically the show processes cpu) should be used to establish a baseline for each process throughout the day. This way when a problem occurs you will be able to better determine if the process load is normal.

176. Which type of troubleshooting tool is commonly used to display packet data?

Digital multimeter

Network monitor

Fox box

Protocol analyzer

Explanation: While network monitors are useful for establishing trends in networks, the protocol analzyers are generally used exclusively for displaying packet data. It should be mentioned though that some network monitors can display packet data.

177. which command restricts logging to the console only?

no logging on

log console

logging monitor only

logging monitor

Explanation: all critical error messages are displayed to console, regardless if there is anything connected. So no logging on would disable logging to all other destinations.

178. if users can access some hosts on a local and remote host on some segment but not others what is the likely cause of the problem?

router failures

access list configuration

addressing and subnet mask problems

high utilization

overloaded hosts

Explanation: since access-lists must be put in place intentionally, the most likely problem (at least according to cisco) is that addressing and subnet problems on either the host, or the server could be causing the problem. A good thing to check is if the server is listening to a routing protocol such as RIP which does not carry any subnet information in it.

179. Regarding the following show interfaces command output which of the following statements is true?

2200000 packets input, 200000000 bytes 0 no buffer

192000 broadcasts, 134 runts, 0 giants

3 input errors, 390 crc, 0 frame, 0 overrun, 0 ignore, 0 abort

0 input packets with dribble condition detected

23000230 packets output 30239203 bytes 0 no buffers
output packets: 436000 collisions

the network attached is experiencing broadcast storms
the network exceeds router capacity
the network is experiencing excessive collisions
malformed packets are causing router degradation

Explanation: According to cisco (and pretty much any network technician you'll meet) the total number of collisions with respect to the total number of output packets should be around 0.1% or less. So we have 436,000 divided by 23,000,230 which equals 0.0018 which is greater than 0.1%

180. what command should you use to display debugging information about ip packets?
debug ip packet
show ip buffers
show ip access
debug ip traffic

Explanation: Use the debug ip packet EXEC command to display general IP debugging information and IP security option (IPSO) security transactions. The no form of this command disables debugging output. If a communication session is closing when it should not be, an end-to-end connection problem can be the cause. The debug ip packet command is useful for analyzing the messages traveling between the local and remote hosts. IP debugging information includes packets received, generated, and forwarded. Fast-switched packets do not generate messages. IPSO security transactions include messages that describe the cause of failure each time a datagram fails a security test in the system. This information is also sent to the sending host when the router configuration allows it.

router# debug ip packet
IP: s=172.16.13.44 (Fddi0), d=10.125.254.1 (Serial2), g=172.16.16.2, forward
IP: s=172.16.1.57 (Ethernet4), d=10.36.125.2 (Serial2), g=172.16.16.2, forward
IP: s=172.16.1.6 (Ethernet4), d=255.255.255.255, rcvd 2
IP: s=172.16.1.55 (Ethernet4), d=172.16.2.42 (Fddi0), g=172.16.13.6, forward
IP: s=172.16.89.33 (Ethernet2), d=10.130.2.156 (Serial2), g=172.16.16.2, forward
IP: s=172.16.1.27 (Ethernet4), d=172.16.43.126 (Fddi1), g=172.16.23.5, forward
IP: s=172.16.1.27 (Ethernet4), d=172.16.43.126 (Fddi0), g=172.16.13.6, forward
IP: s=172.16.20.32 (Ethernet2), d=255.255.255.255, rcvd 2
IP: s=172.16.1.57 (Ethernet4), d=10.36.125.2 (Serial2), g=172.16.16.2, access denied

181. Which of the following error logging methods produces the lowest overhead
console
remote terminal
syslog server

Explanation: From the CIT book, page 5-28 "NOTE: Be aware that the logging destination you use affects system overhead. Logging to the Console produces very high overhead, whereas logging to a virtual terminal produces less overhead. Logging to a syslog server produces even less, and logging to an internal buffer produces the least overhead of any method"

182. which device commonly uses the rmon mib for internetwork troubleshooting
protocol analyzer
network monitor
cable tester
packet driver

Explanation: Network monitors are useful for determining a baseline (a baseline is the normal amount of traffic on a network at certain points throughout the day, and is used to help troubleshoot network problems). Monitors collect information such as packet

sizes, the number of packets, overall usage of a connection, number of error packets, the number of hosts on a network as well as many other items. Network monitors use SNMP.

183. The global statistics screen of a internetwork analyzer says that there is a large amount of SNMP traffic. What is the significance of SNMP?

The routers are exchanging large routing tables
The management overhead constitutes a large portion of the link traffic
A lot of email is exchanged across the link
A remote device is informing the management console that there is a problem with the link.

Explanation: SNMP (Simple Network Management Protocol) is used to monitor the network, however SNMP can also have a significant impact due to its almost continuous amount of traffic that must be sent to a management station.

184. What will be indicated in the show interfaces command output if more than 3 consecutive keepalives have been missed by the s0 interface?

Serial 0 is up, line protocol down
Serial 0 is down, line protocol is up
Serial 0 is up, line protocol is down
Serial 0 is not responding
Serial 0 is down

Explanation: The line protocol is brought down after three keepalives have been missed.

185. Which is the possible cause of a host being unable to access on other networks

the local host and a remote station have the same address
the router between different hosts uses the same frame type
no default gateway specified
incompatible link type between the local host and remote router

Explanation: The default gateway is used to reach hosts that are not on the local subnet.

186. What tool is used to verify a optical fiber installation?

Protocol analyzer
Volt/ohm meter
Network monitor
Otdr
Digital multimeter

Explanation: Optical Time Domain Reflectors (OTDR) are used to troubleshoot optical cable. A TDR works by bouncing a signal off the end of the cable. Opens, shorts, and other problems reflect the signal back at different amplitudes, depending on the problem. A TDR measures how much time it takes the signal to reflect and calculates the distance to a fault.

187. What is the purpose of the debug ip icmp command?

verbose explanation of icmp ping results

display if the router is sending or receiving icmp messages
troubleshoot problems with icmp protocol stack
send icmp packets to all neighboring routers

Explanation: Use the debug ip icmp EXEC command to display information on Internal Control Message Protocol (ICMP) transactions. The no form of this command disables debugging output. This command helps you determine whether the router is sending or receiving ICMP messages. Use it, for example, when you are troubleshooting an end-to-end connection problem.
router# debug ip icmp
ICMP: rcvd type 3, code 1, from 10.95.192.4
ICMP: src 10.56.0.202, dst 172.16.16.1, echo reply
ICMP: dst (10.120.1.0) port unreachable rcv from 10.120.1.15
ICMP: src 172.16.12.35, dst 172.16.20.7, echo reply
ICMP: dst (255.255.255.255) protocol unreachable rcv from 10.31.7.21
ICMP: dst (10.120.1.0) port unreachable rcv from 10.120.1.15
ICMP: dst (255.255.255.255) protocol unreachable rcv from 10.31.7.21
ICMP: dst (10.120.1.0) port unreachable rcv from 10.120.1.15
ICMP: src 10.56.0.202, dst 172.16.16.1, echo reply

188. The show Ipx traffic displays the bad hop count increasing and the routes disappear and reappear often. Which of the problems is likely a source of the symptoms?

increased routing throughput
better error recovery with redundant links
routes unpredictably appearing and disappearing
non routable protocols could not reach remote destinations.

Explanation: The bad hop count measures the number of packets discarded because their hop count exceeded 16 (that is, the packets timed out). Since routers appearing and disappearing could potentially generate loops this is the most likely solution to the problem.

189. Which of the problems can cause problems when attempting to forward BOOTP or other UDP broadcasts packets

Invalid routes appearing in the routing table
Invalid arp cache entries
Heavy traffic on segment
Missing or Misconfigured ip helper-address

Explanation: The IP helper address is used to forward UDP or BOOTP broadcast packets. To solve this problem use the debug ip udp privledged exect command on the router which should be forwarding the packets to verify if they are being received. Then use a show running-config to verify that the ip helper address is configured correctly.

190. If certain TCP/IP host connections fail, and other succeed what is a likely cause of the problem? (choose all that apply)

- ❑ **Misconfigured subnet mask or addresses on hosts or router**
- ❑ IP Authentication options are not configured correctly
- ❑ **Misconfigured access list**
- ❑ High broadcasts causing frames to be discarded
- ❑ ICMP redirects are not supported by some hosts
- ❑ **No default gateway specified on remote host**

191. Invalid routes appearing in the routing table

Misconfigured access lists
Invalid arp cache entries
Heavy traffic on a segment

Explanation: connection attempts to some applications are successful, but attempts using other applications fail. For instance you may be able to ping one host, but not telnet. To solve this problem use the show running-config and then determine which access lists may be causing the problem and use the no form of them to disable them.

192. If certain RIP or IGRP routes are missing from the routing table, what is a likely cause of this problem? (two answers)

Other routing protocols causing conflicts
Variable length subnet mask
Heavy network traffic causes information to be discarded
Missing network router configuration command

Explanation: Routers will only redistribute routes for which they are told to. Use the "network" command in the router configuration mode. Also since RIP and IGRP do not carry subnet information, it can also potentially cause problems on complex networks.

193. What is the function of the debug apple events command?

display router errors
monitors route aging advertisements and acquisition
starts a log of all appletalk traffic
starts a log of NBP traffic

Explanation: Use the debug apple events EXEC command to display information about AppleTalk special events, neighbors becoming reachable/unreachable, and interfaces going up/down. Only significant events (for example, neighbor and route changes) are logged. The no form of this command disables debugging output.

194. What is kept in the route descriptor field of a RIF?

Ring numbers of the last/next ring
Mac addresses of the last/next router
Bridge numbers of the last/next bridge
Bridge numbers and the last/next ring

Explanation: The route descriptor field, of which there can be more than one. Each router descriptor field carries a ring number/bridge number pair that specifies a portion of a route. Routes, then are simply alternating sequences of LAN and bridge numbers that start and end with LAN numbers.

195. Which of the following is most likely caused by a classfull subnet mask?

Excessive broadcast traffic
Non functioning helper address
Invalid RIP or IGRP routes
Unwanted debugging information to console

Explanation: since RIP and IGRP do not carry subnet information non-classfull (e.g.: variable length subnet masks) subnet masks can also potentially cause problems on complex networks.

196. Which of the following is caused when the processor has executed an invalid instruction?

Bus error
Address error
Watchdog timeout
Parity error
Emulator trap

Explanation: Emulator traps indicate the processor has executed an illegal instruction. Emulator traps can be caused by either software taking illegal branches or by hardware failures, notably ROM failures.

197. The length field in the RIF frame format covers the

Header
Payload
Payload + header
There is no such field

Explanation: the length subfield in the RIF frame covers the payload + header.

198. How many route descriptor fields can there be in a single RIF frame?

None, RIF's do not have route descriptor fields
Only 1
More than 1

Explanation: The route descriptor field, of which there can be more than one. Each router descriptor field carries a ring number/bridge number pair that specifies a portion of a route. Routes, then are simply alternating sequences of LAN and bridge numbers that start and end with LAN numbers.

199. What is the direction bit (D) used for in a token ring RIF frame?

To indicate if the frame has been bridged
To indicate if a frame is coming or going
To indicate if the frame contains source route information
To indicate if the frame has been returned to the source with an error

Explanation: The D bit indicates the direction of a frame (forward or reverse).

200. Which type of SDLC frame carry upper layer information and some control information?

I frames
U frames
S frames
FCS frames

Explanation: The Information (I) frames carry upper-layer information and some control information. Send and receive sequence numbers and the poll final (P/F) bit perform flow and error control. The send sequence number refers to the number of the frame to be sent next. The receive sequence number provides the number of the frame to be received next. Both the sender and the receiver

maintain send and receive sequence numbers. The primary uses the P/F bit to tell the secondary whether it requires an immediate response. The secondary uses this bit to tell the primary whether the current frame is the last in its current response.

201. During an attempted ISDN call, the attempt to connect is successful, however attempts to ping or otherwise communicate fail, what are possible problems?

Incorrect cable
Speed setting mismatch
CHAP misconfigured
No route to remote host

Explanation: If the incorrect cable is used then the router will never attempt to dial, and if the speed is configured incorrectly the router will still dial but not connect. If chap is misconfigured (eg: wrong username or password) then you will connect but not be able to authenticate. If there is no route setup, then obviously traffic will not reach the remote end.

202. Which command would you use to determine if a DLCI is assigned to the wrong interface?

Show frame-relay dlci
Show frame-relay pvc
Show interface dlci
Show interface frame-relay

Explanation: To obtain statistics about PVCs on all Frame Relay interfaces, use this command with no arguments.The following is sample output from the **show frame-relay pvc** command:

```
Router1# show frame-relay pvc
   PVC Statistics for interface Serial (Frame Relay DCE)
DLCI = 22, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial3/1:1.1
              input pkts 9             output pkts 300008     in bytes 2754
              out bytes 161802283      dropped pkts 0         in FECN pkts 0
              in BECN pkts 1           out FECN pkts 0        out BECN pkts 0
              in DE pkts 0             out DE pkts 0
              outbcast pkts 0          outbcast bytes 0
  Shaping adapts to ForeSight   in ForeSight signals 1304
  pvc create time 1d05h, last time pvc status changed 00:11:00
```

203. Which type of SDLC frame are used to request control information?

I frames
U frames
S frames
FCS frames

Explanation: The supervisory (S) frames, provide control information. They request and suspend transmission, report on status and acknowledge the receipt of I frames. They do not have an information field.

204. Which of the following is caused when the system hangs?

Bus error
Address error

Watchdog timeout
Parity error
Emulator trap

Explanation: Cisco processors have timers that guard against certain types of system hangs. The CPU periodically resets a watchdog timer. If the timer is not reset, a trap will occur. Failure to service the watchdog timer indicates either a hardware or software bug.

205. By default how often are keepalive messages sent on a frame relay interface?
1 seconds
3 seconds
5 seconds
10 seconds

Explanation: Enter the "show interfaces" exec command to find out whether keepalives are configured. If you see a line that says "keepalives not set" then keepalives are not configured. Use the "keepalive seconds" interface configuration command to configure keepalives. The default value for this command is 10 seconds.

206. Which of the following are possible reasons why an ISDN router will not dial? (2)
Incorrect cable
Misconfigured dialer map
Speed setting mismatch
Misconfigured access-list

Explanation: Possible reasons why a ISDN router will not dial include interface down, missing or misconfigured dialer map, dialer lists, access lists, or not dialer group configured, in addition the router may be missing the pri-group command. If the incorrect cable is used then the router will never attempt to dial, if the speed is configured incorrectly the router will still dial but not connect.

207. Which command would you use to check if there is a chat script running?
Debug chat
Debug modem chat
Debug line chat
Debug all

Explanation: Use the debug chat privileged exec command to check whether there is a chat script running. If there is no chat script running, use the start-chat privileged exec command or another appropriate command to start the chat script on the line.

208. What should the status of the show line exec command on a cisco access server show, in order for you to be able to perform a reverse telnet? (choose all that are correct)
inout
ready
RIisCD
Waiting
Online

Explanation: Use the show line exec command on the access server or router. The output for the auxiliary port should show inout or RIisCD in the Modem column. This indicates that the modem control is enabled on the line of the access server or router.

209. Which command would you use to view the status of the auxiliary port attached to a cisco 2516 (the 2516 has 16 serial ports connected to it)

Show line 1
Show line aux
Show line 17
The status auxiliary port cannot be viewed

Explanation: On a cisco router, port 01 is the auxiliary port. On a cisco access server, the auxiliary port is another last_tty+1, so on a 16 port access server, the auxiliary port is port 17. Use the show line exec command to make certain you are working with the correct line.

210. Which of the following is not a problem which can occur on a serial interface?

CRC errors
High number of collisions
Data underruns
Interface in loopback

Explanation: Serial interfaces cannot experience collisions.

211. Which command would you use to verify which interfaces have OSPF running with the IP protocol on them?

Show interfaces ospf ip
Show ospf ip interfaces
Show ip ospf interfaces
Show interfaces ip ospf

Explanation The following is sample output from the show ip ospf interface command when Ethernet 0 is specified:
Router1# show ip ospf interface ethernet 0
Ethernet 0 is up, line protocol is up
Internet Address 131.119.254.202, Mask 255.255.255.0, Area 0.0.0.0
AS 201, Router ID 192.77.99.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State OTHER, Priority 1
Designated Router id 131.119.254.10, Interface address 131.119.254.10
Backup Designated communication server id 131.119.254.28, Interface addr 131.119.254.28
Timer intervals configured, Hello 10, Dead 60, Wait 40, Retransmit 5
Hello due in 0:00:05
Neighbor Count is 8, Adjacent neighbor count is 2
Adjacent with neighbor 131.119.254.28 (Backup Designated Router)
Adjacent with neighbor 131.119.254.10 (Designated Router)

212. The show interface fddi 3/0 displays a status value of LSU what doe this mean?

It was caused by because all other line states are unknown
It was caused by the occurance of 16 potential noise events that did not satisfy the criteria for entering into any other line state.
It was caused by the receipt of eight or nine HQ or QH symbol pairs
It was caused by four or five idle symbols

Explanation: this is state is used when no other state is known or can be determined.

213. Identify the true statements about the frame relay frame format?

The flags field delimit the beginning and end of a frame
Four bytes are reserved for the DLCI value
The frame is a fixed length
Each frame can be flagged as Discard Eligible.

Explanation: There is one byte at the front and end of each frame which is used for flags, there are 10 bits currently used for the DLCI however two bytes are reserved. There is a bit called the DE bit, which allows certain frames to flagged as discard eligible.

214. Which of the following are mandatory for a implementation of LMI for any device participating in a frame relay network?

Virtual Circuit Status messages
Multicasting
Global addressing
Simple flow control

Explanation: Only virtual circuit status messages are mandatory for all frame relays devices to implement, the rest are completely optional.

215. What is the result when a host and router have a subnet mismatch?

Excessive broadcast traffic
Packets not routed properly
Unwanted debugging information to console

Explanation: When hosts and routers disagree on the length of subnet mask, packets are not routed properly.

216. Which type of SDLC frames are not sequenced and are used exclusively for control purposes?

I frames
U frames
S frames
FCS frames

Explanation: Unnumbered (U) frames are not sequenced. They are used for control purposes such as initializing secondaries. Depending on the function of the unnumbered frame, its control field is 1 or 2 bytes. Some unnumbered frames have an information field.

217. What is a possible result when OSPF routers do not properly establish neighbors?

Excessive broadcast traffic
Non functioning helper address
Networks become unreachable
Unwanted debugging information to console

Explanation: When OSPF routers do not properly establish neighbors the result is router information is not exchanged between routers, therefore networks becoming unreachable. The best command to issue in this situation is use the "show ospf interfaces" to

determine which interfaces have ospf enabled. Then use the show running-config to verify configuration, then make sure that the "network" router configuration commands are specified for each interface on which OSPF should be run.

218. Which Cisco product works with sun net manager and hp openview?

cisco netmanager
cisco works
cisco rmon manager
cisco traffic manager

Explanation: Ciscoworks integrates with both sun net manager and hp openview.

219. What counter in the show interfaces serial command output indicates a modem or line problem exists?

input errors
carrier transitions
queue overruns
keepalive set

Explanation: input errors means that an error occurred while the data was in transit. All of the other messages relate to things that happen inside the router.

220. Which of the following occurs when a hardware error check fails. This problem is almost always due to hardware failure.

Bus error
Address error
Watchdog timeout
Parity error
Emulator trap

Explanation: Parity errors indicate that internal hardware error checks have failed. A parity failure is almost always due to a hardware problem.

221. Which of the following is caused when the processor tries to use a device or memory location that does not exist?

Bus error
Address error
Watchdog timeout
Parity error
Emulator trap

Explanation: The system encounters a bus error wen the processor tries to use a device or a memory location that either does not exist or does not respond properly. Bus errors typically indicate either a software bug or a hardware problem. The address the processor was trying to access when the system crashed provides a key as to whether the failure is due to software or hardware.

222. Which of the following error types is generated when the IOS software tries to access data on incorrectly aligned boundaries?

Bus error
Address error
Watchdog timeout
Parity error
Emulator trap

Explanation: Address errors occur when the software tries to access data on an incorrectly aligned boundary. For example, 2- and 4-byte accesses are allowed only on even addresses. An address error usually indicates a IOS software bug.

223. Which of the following are reasons for periodic communication failures when using RSRB? (2)

Misconfigured T1 timers
Incorrect mapping of netbios names
Wan Link problems
Misconfigured source-bridge command

Explanation: If you are not using local acknowledgement then misconfigured T1 timers can cause period timeouts, of course a WAN link timeout can always cause all sorts of communication errors.

224. What command monitors RTMP route aging acquisition advertisements

Debug apple rtmp
Debug rtmp
Debug apple events
Debug events apple

Explanation: Use the debug apple events EXEC command to display information about AppleTalk special events, neighbors becoming reachable/unreachable, and interfaces going up/down. Only significant events (for example, neighbor and route changes) are logged. The no form of this command disables debugging output.

225. Which command would you use to determine if a target token ring station is visible to current router when attempting to debug and ethernet to token ring bridging scenario?

Show rif
Show span
Show rsrb
Show bridge

Explanation: use the show rif exec command to determine whether the target token ring station is visible on the internetwork.

226. Which command would you issue to send all logging results to an internal buffer to viewed later

Logging offline
Logging snmp
Logging buffered
Logging console

227. Which of the following commands would you use to troubleshoot a misconfigured ethernet to token ring address mapping?

Show e2t
Show irb
Show rsrb
Show span

Explanation: use the show spanning exec command to determine whether the ethernet port is in forwarding mode.

228. Which command will display information on ALL IP Routing Information Protocol (RIP), as well as all routing table updates and route-cache updates

Debug ip route-cache
Debug routing events
Debug ip routing
Debug rip router

Explanation: The only correct answer here is “debug ip routing” which displays all routing protocols, routing table updates, and route cache updates. IF you wanted to just display IP RIP received and sent messages then you use use the “debug ip rip”, but that would not display the all routing table and route cache updates.

229. Which of the following commands would allow you to output the traffic that matches access list 101.

Debug access-list 101
Debug access-list 101 events
Debug ip packet 101
Debug ip access-list 101

Explanation: Use the **debug ip packet** EXEC command to display general IP debugging information and IP security option (IPSO) security transactions. The **no** form of this command disables debugging output.

230. Select the command which would give you the output:

IP ARP: sent req src 131.108.22.7 0000.0c01.e117, dst 131.108.22.96 0000.0000.0000
IP ARP: rcvd rep src 131.108.22.96 0800.2010.b908, dst 131.108.22.7
IP ARP: rcvd req src 131.108.6.10 0000.0c00.6fa2, dst 131.108.6.62
IP ARP: rep filtered src 131.108.22.7 aa92.1b36.a456, dst 255.255.255.255 ffff.ffff.ffff
IP ARP: rep filtered src 131.108.9.7 0000.0c00.6b31, dst 131.108.22.7 0800.2010.b908

Debug arp
Debug ip arp
Debug arp all
Debug arp event

231. Select the command which would give you the output:

ICMP: rcvd type 3, code 1, from 10.95.192.4
ICMP: src 10.56.0.202, dst 172.16.16.1, echo reply
ICMP: dst (10.120.1.0) port unreachable rcv from 10.120.1.15
ICMP: src 172.16.12.35, dst 172.16.20.7, echo reply

Debug ip event
Debug ip icmp
Debug ip ping

Debug ip eigrp

232. Which command would you issue to send all logging results to the telnet session

Logging offline
Logging monitor
Logging buffered
Logging telnet

233. Which command would give you the following output:

Ether0: AT: Resetting interface address filters
%AT-5-INTRESTART: Ether0: AppleTalk port restarting; protocol restarted
Ether0: AppleTalk state changed; unknown -> restarting
Ether0: AppleTalk state changed; restarting -> probing
%AT-6-ADDRUSED: Ether0: AppleTalk node up; using address 65401.148
Ether0: AppleTalk state changed; probing -> acquiring
AT: Sent GetNetInfo request broadcast on Ether0

Debug apple nbp
Debug apple rtmp
Debug apple events
Debug apple zip

234. Which of the following commands would produce the output:

Ether0: AARP: Sent resolve for 4160.26
Ether0: AARP: Reply from 4160.26(0000.0c00.0453) for 4160.154(0000.0c00.8ea9)
Ether0: AARP: Resolved waiting request for 4160.26(0000.0c00.0453)
Ether0: AARP: Reply from 4160.19(0000.0c00.0082) for 4160.154(0000.0c00.8ea9)
Ether0: AARP: Resolved waiting request for 4160.19(0000.0c00.0082)
Ether0: AARP: Reply from 4160.19(0000.0c00.0082) for 4160.154(0000.0c00.8ea9)

Debug apple aarp
Debug apple arp
Debug apple nbp
Debug apple ZIP
Debug apple events

235. In the ARP conversation show below, what is the IP address for the station with the MAC address 0000.0c00.6fa2

IP ARP: sent req src 131.108.22.7 0000.0c01.e117, dst 131.108.22.96 0000.0000.0000
IP ARP: rcvd rep src 131.108.22.96 0800.2010.b908, dst 131.108.22.7
IP ARP: rcvd req src 131.108.6.10 0000.0c00.6fa2, dst 131.108.6.62
IP ARP: rep filtered src 131.108.22.7 aa92.1b36.a456, dst 255.255.255.255 ffff.ffff.ffff
IP ARP: rep filtered src 131.108.9.7 0000.0c00.6b31, dst 131.108.22.7 0800.2010.b908

131.108.22.7
131.108.22.96
131.108.6.10
131.108.6.62

236. In the AARP conversation show below, what was the MAC address for the host with the Appletalk address of 4160.26?
Ether0: AARP: Sent resolve for 4160.26
Ether0: AARP: Reply from 4160.26(0000.0c00.0453) for 4160.154(0000.0c00.8ea9)
Ether0: AARP: Resolved waiting request for 4160.26(0000.0c00.0453)
Ether0: AARP: Reply from 4160.19(0000.0c00.0082) for 4160.154(0000.0c00.8ea9)
Ether0: AARP: Resolved waiting request for 4160.19(0000.0c00.0082)
Ether0: AARP: Reply from 4160.19(0000.0c00.0082) for 4160.154(0000.0c00.8ea9)

0000.0c00.8ea9
0000.0c00.0453
0000.0c00.0082
not shown

237. In the ARP conversation show below, what is the MAC address for the station with the IP address 131.108.22.7
IP ARP: sent req src 131.108.22.7 0000.0c01.e117, dst 131.108.22.96 0000.0000.0000
IP ARP: rcvd rep src 131.108.22.96 0800.2010.b908, dst 131.108.22.7
IP ARP: rcvd req src 131.108.6.10 0000.0c00.6fa2, dst 131.108.6.62
IP ARP: rep filtered src 131.108.22.7 aa92.1b36.a456, dst 255.255.255.255 ffff.ffff.ffff
IP ARP: rep filtered src 131.108.9.7 0000.0c00.6b31, dst 131.108.22.7 0800.2010.b908

0000.0c01.e117
0000.0000.0000
0800.2010.b908
0000.0c00.6fa2
aa92.1b36.a456

238. In the AARP conversation show below, what was the MAC address for the host with the Appletalk address of 4160.19?
Ether0: AARP: Sent resolve for 4160.26
Ether0: AARP: Reply from 4160.26(0000.0c00.0453) for 4160.154(0000.0c00.8ea9)
Ether0: AARP: Resolved waiting request for 4160.26(0000.0c00.0453)
Ether0: AARP: Reply from 4160.19(0000.0c00.0082) for 4160.154(0000.0c00.8ea9)
Ether0: AARP: Resolved waiting request for 4160.19(0000.0c00.0082)
Ether0: AARP: Reply from 4160.19(0000.0c00.0082) for 4160.154(0000.0c00.8ea9)

0000.0c00.8ea9
0000.0c00.0453
0000.0c00.0082
not shown

239. In the ARP conversation show below, what is the MAC address for the station with the IP address 131.108.22.96
IP ARP: sent req src 131.108.22.7 0000.0c01.e117, dst 131.108.22.96 0000.0000.0000
IP ARP: rcvd rep src 131.108.22.96 0800.2010.b908, dst 131.108.22.7
IP ARP: rcvd req src 131.108.6.10 0000.0c00.6fa2, dst 131.108.6.62
IP ARP: rep filtered src 131.108.22.7 aa92.1b36.a456, dst 255.255.255.255 ffff.ffff.ffff
IP ARP: rep filtered src 131.108.9.7 0000.0c00.6b31, dst 131.108.22.7 0800.2010.b908

0000.0c01.e117
0000.0000.0000
0800.2010.b908
0000.0c00.6fa2
aa92.1b36.a456

240. Based on the output from the "debug apple zip" command below, what is the network number for the zone named US-Florida?

AT: Sent GetNetInfo request broadcast on Ether0
AT: Recvd ZIP cmd 6 from 4160.19-6
AT: 3 query packets sent to neighbor 4160.19
AT: 1 zones for 31902, ZIP XReply, src 4160.19
AT: net 31902, zonelen 10, name US-Florida

4160
19
31902
10