



Exam : 642-831

Title : Cisco Internetwork Troubleshooting (CIT)

Ver : 10.02.07

QUESTION 1

When troubleshooting a network, what are the advantages of using a logically layered network model?

- A. Focus on physical, data link and network layers to isolate a problem.
- B. Focus on specific elements to isolate a problem.
- C. Focus on physical layers to isolate a problem
- D. Focus on transport and application layers to isolate a problem.
- E. None of the above.

Answer: B

Explanation:

When troubleshooting any network issue, it is best to utilize the seven-layer OSI model and troubleshoot issues systematically from layer one (physical) all the way to the application layer. Since every layer relies on the layers below it in order to work properly, it is best to start verify the layers individually. Working from the bottom-up, you should focus on specific elements in order to most effectively isolate and correct the problem.

QUESTION 2

Your junior administrator is in the midst of a troubleshooting assignment. You observe him: gathering symptoms, isolating network problems, and then correcting the problem. What general troubleshooting methodology is he using?

- A. Proactive
- B. Reactive
- C. Standards-based
- D. Cisco proprietary

Answer: A

Explanation:

The word proactive means to act in advance, to use anticipation when dealing with a difficulty. In this sense, a troubleshooter should prepare a network in advance for a loss of availability. In this case, symptoms of network problems are being collected in advance of network issues. Here, these symptoms are being used to proactively isolate and correct problems before major network outages occur. A network administrator that waited until a complete network outage occurs before taking any corrective steps would be indicative of a reactive methodology.

QUESTION 3

The general troubleshooting process is composed of three essential stages. What are these three steps in the general troubleshooting process? (Choose three)

- A. Isolate Symptoms
- B. Isolate the problem
- C. Correct the problem
- D. Identify the problem
- E. Gather Symptoms
- F. Document the problem
- G. Research Solutions

Answer: B, C, E

Explanation:

Each school of thought and each manufacturer has a different troubleshooting process, and these processes change every few years. (Even Cisco had different troubleshooting steps five years ago). As of right now, for your exam the troubleshooting process consists of three steps.

- * Gathering symptoms
- * Isolating the problem
- * Correcting the problem

Gathering symptoms is all about comparing the status of the current model relative to the standard level of performance indicated on the baseline. This involves listening to the complaints of end-users, sub-administrators, and the statistics of general show commands.

Isolating the problem is an attempt to find the root of the problem. Your first priority is to find out what OSI layers the problem is effecting then what specific equipment and part of the equipment.

Correcting the problem is reconfiguring the affected portion/component, testing it to make sure it worked, then documenting your changes in your log book and if necessary updating your network configuration tables and topologies.

Reference:

http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac224/about_cisco_packet_department0900aecd800b198

QUESTION 4

You're a network administrator, and while you were gone in vacation; your junior administrator installed a new router. Since then, response time for end users on the network has degraded to the point of concern. To begin troubleshooting you start by examining the routing protocol operations, and then check the physical connections on the affected devices. What is the name of this troubleshooting method?

- A. Bottom-up
- B. Experience based
- C. Top-down
- D. Divide-and-conquer
- E. None of the above.

Answer: D

Explanation:

Since we started troubleshooting at the routing protocol layer (layer3) we have started our troubleshooting process by using the divide and conquer method.

Incorrect Answers:

A, C: The "top" and "bottom" refers to the different layers of the OSI model. Since the routing protocol operation was checked first, this means that layer 3 connectivity was being checked. The physical connections reside on the physical layer of the OSI model, which is layer 1. In this example, since layer 3 was checked first, and then layer 1, the model used here was the top-down method.

QUESTION 5

Is the following statement true or false?

The Cisco troubleshooting model is based on a rigid framework.

- A. False, it should instead be flexible
- B. False, as it is a software product, not a framework
- C. True
- D. False, as it is a proprietary slogan, not a framework

Answer: A

Explanation:

Cisco illustrates the process flow for the general problem-solving model. This process flow is not a rigid outline for troubleshooting an internetwork; it is a foundation from which you can build a problem-solving process to suit your particular environment. This process is a methodology, a framework, but not a software product.

QUESTION 6

Network trobleshooters are like detectives, sometimes they have to bring in network users for questioning in order to determine what the problem is. In which troubleshooting step does this happen?

- A. Verifying the information
- B. Defining the problem
- C. Isolating the problem
- D. Gathering facts
- E. Logging the trouble ticket
- F. None of the above.

Answer: D

Explanation:

You do not rely on the staffs telling you the problem. Instead, you gather the facts and then determine the problem using your judgment and analysis. The best source for

problem-related information is often from the actual end users that are impacted by the network issue.

QUESTION 7

Is the following statement true or false?

Systematic approaches are very effective when troubleshooting networks.

- A. True only when you are running IOS to manage the network gears.
- B. False
- C. True only when CWSI is in use.
- D. True
- E. True only when all network gear is Cisco based

Answer: D

Explanation:

When you're troubleshooting a network environment, a systematic approach works best. An unsystematic approach to troubleshooting can result in wasting valuable time and resources, and can sometimes make symptoms even worse. Define the specific symptoms, identify all potential problems that could be causing the symptoms, and then systematically eliminate each potential problem (from most likely to least likely) until the symptoms disappear. This method is true regardless of the network hardware that is being used.

QUESTION 8

According to Cisco's problem-solving model, what should a network troubleshooter do after they have resolved a problem?

- A. Gather facts about the problem.
- B. Call TAC to have the case closed.
- C. Document the changes that were made.
- D. Try the same solution on another router to verify the fix.

Answer: C

Explanation:

If the symptoms have disappeared and you are confident that the problem has been solved, you proceed to the next step: Report the problem as solved and document the results. It is always important to document the changes that were made, so that if other problems arise as a result of the changes that was made to the network.

Incorrect Answers:

- A: This is an initial step.
 - B: Not all troubleshooting tasks are reported to the Technical Assistance Center (TAC).
 - D: It might not be possible to recreate the original problem on another router. Furthermore, problems are not always related to routers.
-

QUESTION 9

When analyzing a network problem; in what terms should a network troubleshooter define the problem?

- A. Symptoms and root causes
- B. Root causes and root benefits
- C. Benefits and ROI
- D. Causes and benefits
- E. Symptoms and potential causes

Answer: E

Explanation:

When analyzing a network problem, make a clear problem statement. You should define the problem in terms of a set of symptoms and potential causes. To properly analyze the problem, identify the general symptoms and then ascertain what kinds of problems (causes) could result in these symptoms. For example, hosts might not be responding to service requests from clients (a symptom). Possible causes might include a misconfigured host, bad interface cards, or missing router configuration commands.

QUESTION 10

DRAG DROP

Match the correct network documentation procedure stage on the left side to its description on the right.

Stage	Place description here	Select from these
Login in	place here	discover relevant information about the device
Interface Discovery	place here	transfer any information from the network configuration table
Document	place here	log in to an undocumented neighboring device
Diagram	place here	use information to build the network configuration table
Device Discovery	place here	determine if any neighboring devices are undocumented

Answer:

Stage	Place description here	Select from these
Login in	log in to an undocumented neighboring device	
Interface Discovery	discover relevant information about the device	
Document	use information to build the network configuration table	
Diagram	transfer any information from the network configuration table	
Device Discovery	determine if any neighboring devices are undocumented	

Explanation:

To properly create network documentation the following steps are necessary:

- * Login: to gain access to any undocumented neighboring device.
- * Interface discovery: once logged in, you can determine the connections to the network to enable you to construct a cogent theory
- * Document: If you have this then you are in good shape and can "see" a network diagram but for a lot of areas you must do this yourself and the result will be a more thorough understanding of the issues and the processes to solve them.
- * Diagram: When focusing on new elements you will need to add any new info to the current (if any) diagrams you have.
- * Device discovery: This applies to my previous answer in that Device discovery: To check out any relevant devices that pertain to the issue is always a necessary step. But after seeing that you have inadequate documentation you may want to proceed to get this situation together ASAP. So this is ALWAYS a necessary step, even if you do not have any issues at all this should have been done.

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps2246/prod_troubleshooting_guide_chapter09186a00800ea

QUESTION 11

Which of the following is a network process characterized by the following: Log in, Interface discovery, and Device discovery?

- A. Network testing
- B. Network documentation
- C. Network configuration
- D. Network troubleshooting
- E. All of the above

Answer: B

Explanation:

In order to properly create network documentation the following steps are necessary:

1. Login: log in to an undocumented network device
2. Interface discovery: discovery relevant information about the device

3. Document: Use information to build the network configuration table.
 4. Diagram: Transfer any information from the network configuration table.
 5. Device discovery: Determine if any neighboring devices are documented.
-

QUESTION 12

Documenting the network is important for any network administrator. In which three ways is documentation beneficial? (Select three)

- A. Annual review
- B. Managed access
- C. Revision history
- D. Guaranteed accuracy
- E. Distribution efficiency

Answer: A, C, D

Explanation:

Proper network documentation can be useful for many reasons, including periodic reviews, a history of any changes that were made, and in order to guarantee the accuracy of any document via supporting documentation.

Incorrect Answers:

B: Managing the actual access to devices is a security measure, not a documentation measure.

E: The process of network documentation alone will not improve the efficiency or performance of the network.

QUESTION 13

What can you find in the Cisco Documentation CD-ROM that is provided from Cisco?

- A. Information on the most popular topics only
- B. A search facility to go directly to the needed information
- C. Similar information to the CCO web site but it is not in HTML format
- D. Command references and command summaries, but not product catalog information
- E. None of the above

Answer: B

Explanation:

The Cisco Documentation CD-ROM is actually a 2 CD set that contains an entire library of relevant information.

Navigating through the Documentation CD-Rom is facilitated by the online help, a table of contents, hypertext links, a search engine, book marking, and the history window.

1. Cisco IOS release notes, configuration guides, command references, and command summaries

2. Debug command reference and system error messages
3. Cisco Management Information Base (MIB) User Quick Reference and Access Services Quick Configuration Guide
4. Cisco product catalogue
5. Router and hub installation and configuration guides
6. Switch installation and configuration guides, switch command references guides and switch MIB reference guides
7. Client/server software installation guides
8. Configuration notes for memory upgrades, network interface cards, rack-mount kits, and other field upgrade products.

Reference:

CCNP Support Exam Certification Guide Amir S. Ranjibar, page 16, Cisco Press 2001, ISBN 0-7357-09955-5

QUESTION 14

When creating standards for network diagrams; which document characteristic should you use primarily?

- A. Icons
- B. Inventory
- C. Configuration
- D. Command syntax
- E. None of the above.

Answer: A

Explanation:

If you use any standardized diagrams or symbols to represent anything, use consistency and keep a guide so another troubleshooter can interpret them. A leading example of icons that are used is the stencils that are found in the Visio application.

QUESTION 15

Having a library of standardized symbols and templates contributes to which network documentation guideline?

- A. Document objectives
- B. Document accessibility
- C. Document scope
- D. Document consistency
- E. Document maintenance

Answer: D

Explanation:

Chapter 1 of the Cisco CIT Book offers the following guidelines for creating documentation for networks:

Table 1-7. Guidelines for Creating Network Documentation

Guideline	Explanation
Determine the scope.	Know which devices are part of your domain of responsibility.
Know your objective.	Collect data that is relevant to your objective and provide sufficient detail information. Avoid extraneous data because it renders the documentation difficult to use.
Be consistent.	Use consistent terminology, abbreviations, and style. Use templates when possible, and keep a library of symbols and graphics icons that you can reuse.

QUESTION 16

What is true regarding network documentation?

- A. For security reasons, all network documentation should be stored at on off-site location.
- B. For security reasons, all network documentation should be kept on-site.
- C. Copies of the network documentation should be stored in both on-site and off-site locations.
- D. The documentation should be completely open to allow anyone to make changes without having to go through any administrative channels and thus slowing the process.

Answer: C

QUESTION 17

You've just been hired as the new senior systems administrator at the Certkiller Corporation and although the network is working perfectly and efficiently the previous system administrator left no network documentation. In order to create a network baseline, what three steps should you take in creating this initial baseline? (Choose three)

- A. Determine all the variables in the network and record them.
- B. Determine the scope of the domain responsibility.
- C. Record the baseline data for the first two months.
- D. Determine the network performance goals.
- E. Start the baseline network model with the access layer.

F. Identify the devices and ports of interest.

Answer: B, D, F

Explanation:

When creating network documentation, don't bite off more than you can chew. Limit your energies to the scope of your domain. All of the variables outside of your domain are worthy to be known about, but not to be written about by you.

It is also good to determine the performance goals of your network, relative to the strength and capabilities of your equipment versus the number of users. This is especially important when creating your initial baseline.

Each device in your network that's within your domain should be identified, and every junction of interest needs particular attention.

QUESTION 18

While a network performs at an acceptable level, what should you do in order to create a snapshot of a network configuration?

- A. Establish a baseline
- B. Configure snapshot routing
- C. Use Netsys Baseliner
- D. Use Netsys Analyzer
- E. None of the above.

Answer: A

Explanation:

When your network is performing at the exact level you're comfortable with it performing at, use that as your benchmark for establishing a baseline. If our network performance drops as a result of doing anything, you'll have documentation to tell you what normal is, and you'll be quickly able to proactively monitor the network for any performance issues.

Incorrect Answers:

B: Snapshot routing is normally used on DDR situations such as ISDN in order to keep dial costs down but it will not help in this scenario.

Snapshot routing is useful in two command situations:

1. Configuring static routes for DDR interfaces
2. Reducing the overhead of periodic updates sent by routing protocols to remote branch offices over a dedicated serial line

C, D: Using third party tools can be useful in establishing a baseline or for monitoring the performance of the network, but using any single tool will not be sufficient in this example.

QUESTION 19

Which of the following guidelines should you adhere to if you wanted to ensure proper network documentation as network devices and conditions change? (Choose

four)

- A. Be consistent
- B. Know your objective
- C. Document everything
- D. Keep the documents accessible
- E. Establish new baselines weekly
- F. Maintain the documentation

Answer: A, B, D, F

Explanation:

Consistency is the key to good documentation, as slow response is a relative term.

When you know your objective, you'll be more efficient in reaching your goal, and you'll know exactly what brought you to your goal.

Keep the documents accessible where you can find them, your supervisor can find them, and your subordinate can find them. You should be able to tell somebody you've never met before over the phone or email where to find your documents. The documents themselves should be well organized and easy to read.

Maintain the documentation consistently every time the network changes, so you can go over it and study the networks evolution like a historian, pinpointing cause and effect.

Incorrect Answers:

C: You don't have to document absolutely everything. The more time you spend documenting menial data, the more clutter you're going to have in your notes, and the longer it is going to take you to go through all that clutter when you have to fix a problem when time is of an essence.

E: You should not change your baselines on a weekly basis or as a result of any event on a calendar. There will be times when you will go weeks without changing anything, and you won't need to waste your time. There will be other times, when you'll have to make major changes on your network numerous times in a single week.

QUESTION 20

You work as a network administrator at Certkiller .com. You are establishing a topology diagram as part of a baseline strategy for troubleshooting.

Which three components should you include? Select three.

- A. IP addresses
- B. VLANs
- C. duplexes
- D. STP states
- E. routing protocols

Answer: A, B, E

QUESTION 21

Which two types of documentation use network information captured from a

baseline? Select two.

- A. a layered networking model
- B. network configuration tables
- C. topology diagrams
- D. a troubleshooting model
- E. end-system user guides

Answer: B, C

QUESTION 22

Which step of the troubleshooting model may require that affected users be contacted and that network baselines be checked?

- A. gather symptoms
- B. isolate the problem
- C. correct the problem
- D. verify the problem resolution

Answer: A

QUESTION 23

When a network baseline is first being established, which router CLI command will display information about the operational status, IP addresses, media type, and interface name for all interfaces?

- A. show ip interface
- B. show interface
- C. show ip interface brief
- D. show interface status

Answer: C

QUESTION 24

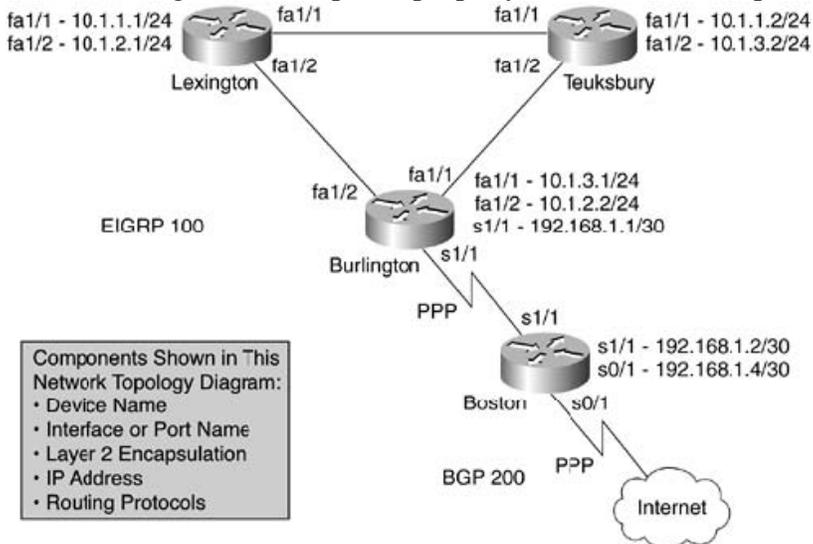
Which of the following items should you include in a network topology diagram?
(Choose two)

- A. Individual end user systems.
- B. Location of configuration files.
- C. Illustrations of each network device.
- D. Representations of logical and physical connections.
- E. Speed and duplex of individual switch ports.

Answer: C, D

Explanation:

The following is an example of properly drawn network topology diagram:



A network topology diagram shows all the devices and how they are physically and logically connected. The device name, interface or port name, IP address, and routing protocol(s) are a few of its important components.

QUESTION 25

In order to be more proactive in the management of the Certkiller network, an action plan was created. What step should an administrator take while in the process of implementing an action plan?

- A. Document the topology of the network.
- B. Delete access lists on routers to isolate traffic.
- C. Create troubleshooting steps as needed during the process.
- D. Restore your network to a known previous state if the action item does not solve the problem.
- E. None of the above.

Answer: C

Explanation:

General Problem-Solving Model

The following steps detail the problem-solving process:

Step 1 When analyzing a network problem, make a clear problem statement. You should define the problem in terms of a set of symptoms and potential causes.

To properly analyze the problem, identify the general symptoms and then ascertain what kinds of problems (causes) could result in these symptoms. For example, hosts might not be responding to service requests from clients (a symptom). Possible causes might include a misconfigured host, bad interface cards, or missing router configuration commands.

Step 2 Gather the facts that you need to help isolate possible causes.

Ask questions of affected users, network administrators, managers, and other key people. Collect information from sources such as network management systems, protocol

analyzer traces, output from router diagnostic commands, or software release notes.

Step 3 Consider possible problems based on the facts that you gathered. Using the facts, you can eliminate some of the potential problems from your list.

Depending on the data, for example, you might be able to eliminate hardware as a problem so that you can focus on software problems. At every opportunity, try to narrow the number of potential problems so that you can create an efficient plan of action.

Step 4 Create an action plan based on the remaining potential problems. Begin with the most likely problem, and devise a plan in which only one variable is manipulated.

Changing only one variable at a time enables you to reproduce a given solution to a specific problem. If you alter more than one variable simultaneously, you might solve the problem, but identifying the specific change that eliminated the symptom becomes far more difficult and will not help you solve the same problem if it occurs in the future.

Step 5 Implement the action plan, performing each step carefully while testing to see whether the symptom disappears.

Step 6 Whenever you change a variable, be sure to gather results. Generally, you should use the same method of gathering facts that you used in Step 2 (that is, working with the key people affected, in conjunction with utilizing your diagnostic tools).

Step 7 Analyze the results to determine whether the problem has been resolved. If it has, then the process is complete.

Step 8 If the problem has not been resolved, you must create an action plan based on the next most likely problem in your list. Return to Step 4, change one variable at a time, and repeat the process until the problem is solved.

Reference: Troubleshooting Overview:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1901.htm

QUESTION 26

Network Topology Diagrams and Network Configuration Tables share two similarities. What are they? (Choose two)

- A. Both share few components.
- B. Both share many of the same components.
- C. Both define physical memory components.
- D. Both are used for troubleshooting.
- E. Both use lines and symbols to represent network components.

Answer: B, D

Explanation:

Network Topology Diagrams and Network Configuration Tables basically do the same thing; they are used to help the trouble shooter understand the network. A topology diagram uses lines, symbols, and pictures to help someone understand the way a network is built and operates. A network configuration table has a table of facts and stats to give details about the network. For visually orientated people a topology diagram is better, for auditory oriented people a configuration table is better, for some jobs a topology diagram is best, and for others a network configuration table is better. Regardless, both are excellent troubleshooting tools.

QUESTION 27

What is true about the characteristics of a network topology diagram? (Choose all that apply)

- A. It is a detailed report about the capabilities of the network.
- B. It is an illustration of how each network is connected to the Internet.
- C. It contains the components that the network configuration table does not contain.
- D. It illustrates how each device in a network is connected.
- E. It is defined by the aspects of its logical architecture.

Answer: D, E

Explanation:

A network topology diagram shows all the devices and how they are physically and logically connected. The device name, interface or port name, IP address, and routing protocol(s) are a few of its important components.

Incorrect Answers:

- A: A Topology diagram is used as a high-level view of the network, not as a detailed report.
- B: This is not necessarily true, as many networks and network diagrams do not include Internet access circuits.
- C: The diagram shares much of the same information that can be found in the configuration table, except that it is displayed using a different format.

QUESTION 28

The Topology Builder is a network tool that is included with which of the following?

- A. Router Configuration File Loader
- B. Connectivity Baseline
- C. Connectivity Solver
- D. Topology Builder
- E. Diagnostic Report Generator

Answer: B

Explanation:

The Connectivity Tools currently have two components; the Connectivity Baseline and the Connectivity Solver. The Connectivity Baseline is a pre-requisite of the Connectivity Solver. As such, the additional functionality of the Connectivity Solver is used in conjunction with the Connectivity Baseline. The functionality provided is:

- Connectivity Baseline
- Router Configuration File Loader
- Diagnostic Report Generator
- Topology Builder
- Connectivity Solver

Connectivity Requirements Analyzer
Scenario "what-if" Simulator
Delta IOS command generation

QUESTION 29

A Certkiller network documentation file contains the following:

1. Hardware and software installed
2. Device hostnames and locations
3. Data link & network layer addresses
4. VLANs
5. ACL configurations

What is the proper name of this type of network documentation?

- A. Network configuration table
- B. Network topology diagram
- C. End-system configuration table
- D. End-system topology table.

Answer: A

Explanation:

A network configuration table contains the physical, data link, and network configuration elements as shown below:

Physical - Contains the CPU type, Flash memory, DRAM, MAC address, media type, Speed, Duplex, and Trunk Status

Data Link - Contains the Device name, model (and IOS version) MAC address, Duplex, port identifier, STP status, etc.

Network - IP address, subnet mask, IP routing, access lists, VLANs, Interface name, IP information

Incorrect Answers:

B: The topology diagram does not include Access List information.

Reference:CCNP CIT Exam Certification Guide Page No. 12

Second Edition ISBN: 1-58720-081-3

QUESTION 30

Which of the following documentation traits have to be addressed when creating network diagram standards?

- A. Inventory
- B. Abbreviations
- C. Configurations
- D. Command syntax
- E. None of the above

Answer: B

Explanation:

The *network topology diagram* is the second piece of documentation (after the network configuration table), and it is considered an essential part of any network baseline. This diagram is a graphical representation of the network that must illustrate all the devices and how they are connected. Physical and logical detail about the network are revealed using consistent notations and symbols. Figure 1-1 is an example of a network topology diagram. In Figure 1-1, you can see a network cloud symbol with the title *Internet*. A network cloud symbol is often used to represent a network that is under control of another group (or company, or autonomous system, and so on). At times, the network cloud symbol is used within a network topology diagram to show an area whose detail is outside the scope of the diagram.

Reference:

CCNP CIT Exam Certification Guide Page No. 14
Second Edition ISBN: 1-58720-081-3

QUESTION 31

Which one of the following is the leading cause of lost network availability?

- A. Natural disasters
- B. Operational errors
- C. Network device software failures
- D. Network device outage at single points of failure in the topology
- E. End user error

Answer: D

Explanation:

Network device outages from single points of failure are much more common than the other choices. The power supply of a single device can fail, a plug can be pulled out, a fuse can blow, a device can overheat, fall from its rack, a cable could be loosened, a cord can be severed, and if there is a problem on a higher layer that's the result of an administrator making a bad configuration it will happen on a single device, or bottleneck.

Incorrect Answers:

A: Natural disasters are rare and aren't as likely to result in a loss network availability as we may expect. If they do happen, then usually they equally affect the competition and they happen on the end of the WAN service provider (therefore it is normally their responsibility to fix).

B, E: Operational errors from end users usually only damage the individual user workstations, operational errors from systems administrators are usually brief and easily reversible, since configurations happen line by line.

C: Network device software failure is very rare, especially with Cisco devices. The Cisco IOS has a lot of built in redundancy, and even if damaged or bugged will usually continue operating.

QUESTION 32

Which of the following components should you include in an End-System Topology Diagram? (Choose all that apply.)

- A. Device illustration
- B. Operating system
- C. IP routing protocol
- D. Connection to the network
- E. Device name
- F. VTP domain

Answer: A, B, D, E

Explanation:

The following table lists the different information pieces that should be included in a network topology end-system diagram:

Table 2-2 End System Configuration Table Components Classified Based on the TCP/IP Protocol Stack Layers

Layer	Information
Physical/data link	Physical location Manufacturer/model CPU type/speed RAM Storage Device name Device function or purpose Access VLAN MAC address
Network	IP address Subnet mask Default gateway DNS address WINS address
Application	Operating system/version Network applications High-bandwidth applications Latency-sensitive applications Business-critical applications

Reference: CCNP CIT Exam Certification Guide Second Edition ISBN: 1-58720-081-3

QUESTION 33

Which of the following pieces of information are relevant to an end-system network configuration table? Select four.

- A. network media type
- B. DNS server address
- C. default gateway address
- D. routing protocol characteristics
- E. operating system and version
- F. IP address and subnet mask

Answer: B, C, E, F

Explanation:

The following table lists the different information pieces that should be included in a network end-system configuration table:

Table 2-2 End System Configuration Table Components Classified Based on the TCP/IP Protocol Stack Layers

Layer	Information
Physical/data link	Physical location Manufacturer/model CPU type/speed RAM Storage Device name Device function or purpose Access VLAN MAC address
Network	IP address Subnet mask Default gateway DNS address WINS address
Application	Operating system/version Network applications High-bandwidth applications Latency-sensitive applications Business-critical applications

Reference:

CCNP CIT Exam Certification Guide Page No. 32 Second Edition ISBN: 1-58720-081-3

QUESTION 34

What categories of information should you take into consideration when you document the properties of a router for a Network Configuration Table? (Choose three)

- A. STP state
- B. interface IP address
- C. routing protocol information
- D. EtherChannel configuration
- E. management IP address
- F. interface types

Answer: B, C, E

Explanation:

Table 1-3 below shows an example of a network configuration table for routers. In Table 1-3, the following information is recorded for each of the shown routers:

* Device name and model

- * Interface name
- * MAC address (or other Layer 2 address)
- * IP address (and subnet mask)
- * IP routing protocol(s)

Table 1-3. Example of a Network Configuration Table for a Router

Device Name, Model	Interface	MAC Address	IP Address /Subnet Mask	IP Routing Protocol(s)
Long Island, Cisco1760-V	fa0/0	0007.8500.a159	10.2.3.1/16	EIGRP 100
fa0/1	0007.8500.a160	10.0.1.1/16	EIGRP 100	
s0/1	HDLC	192.168.34.1/24	OSPF 100	
s1/1	PPP	172.18.1.1/16	EIGRP 100	
New York, Cisco2611XM	s0/1	FR DLCI 200	192.168.34.2/24	OSPF
s1/0	HDLC	172.18.2.1/16	EIGRP 100	

QUESTION 35

In which step of network documentation would it be beneficial to know a domain of responsibility?

- A. Establishing document objectives
- B. Establishing document scope
- C. Establishing document troubleshooting steps
- D. Establishing document consistency

Answer: B

Explanation:

<i>Table 1-7. Guidelines for Creating Network Documentation</i>	
Guideline	Explanation
Determine the scope.	Know which devices is part of your domain of responsibility.
Know your objective.	Collect data that is relevant to your objective and provide sufficient detail information. Avoid extraneous data because it renders the documentation difficult to use.
Be consistent.	Use consistent terminology, abbreviations, and styls. Use templates when possible, and keep a library of symbols and graphics icons that you can reuse.
Keep the documents accessible.	Store the network documentation in a location where it is readily available on the job; keep another copy of it in a secure location off-site.
Maintain the documentation.	As the network undergoes changes, modify the network documentation accordingly to keep it accurate and up to date. Note: Many organizations have deployed a formal process called <i>change control</i> . This process enforces reporting of network changes, maintaining version control, and assigning responsibility for modifying and distributing updated documents.

QUESTION 36

Information relating to a Certkiller switch is displayed below:

```
Port      Mode      Encapsulation      Status      Native vlan
Fa5/9     desirable n-isl               trunking    1
```

```
Port      Vlans allowed on trunk
Fa5/9     1-1005
```

```
Port      Vlans allowed and active in management domain
Fa5/9     1-6,10,20,50,100,152,200,300,303-305,349-51,400,500,521,524,570, 801-802,850,917,999,1002-1005
```

```
Port      Vlans in spanning tree forwarding state and not pruned
Fa5/9     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570, 801-802,850,917,999,1002-1005
```

Your junior administrator is in the midst of gathering information on this Layer 2 switch for the sake of creating a network configuration document. From the output above, what command did he enter?

- A. show spanning-tree
- B. show vlan
- C. show interfaces capabilities
- D. show interfaces trunk

E. show etherchannel summary

Answer: D

Explanation:

The following example displays the output of a "show interfaces trunk" command when issued on a switch.

```
Certkiller 1#show interfaces trunk
Port Mode Encapsulation Status Native vlan
Gi0/1 desirable 802.1q trunking 1
Gi0/2 desirable 802.1q trunking 1
Port Vlans allowed on trunk
Gi0/1 1-4094
Gi0/2 1-4094
Port Vlans allowed and active in management domain
Gi0/1 1-3,10
Gi0/2 1-3,10
Port Vlans in spanning tree forwarding state and not pruned
Gi0/1 1-3,10
Gi0/2 1-3,10
```

Reference:

http://www.cisco.com/en/US/tech/CK3_89/CK8_15/technologies_configuration_example09186a008015f17a.shtml#v

QUESTION 37

To what three destinations can a Cisco router send its logging processes and error messages to? (Choose three)

- A. Message directory
- B. External syslog server
- C. Logging buffer
- D. Terminal lines
- E. History file
- F. Configuration file

Answer: B, C, D,

Explanation:

The destination options for logging are:

- * Console
- * internal buffer
- * a virtual terminal session (telnet)
- * syslog server

Incorrect Answers:

A, E: Message directories and history files aren't terms used in the exam since Cisco routers do not retain these types of information files

F: The configuration file doesn't show a history of error messages; it only reflects the current configuration.

QUESTION 38

Which command could you use to copy debug messages to your current terminal display?

- A. logging monitor
- B. logging terminal
- C. terminal monitor
- D. monitor terminal

Answer: C

Explanation:

The terminal monitor command copies debug command output and system error messages to the current terminal as well as to the console terminal.

Note: When you telnet into a Cisco device, by device this command is not enabled. However, when connected via the console cable, this is enabled by default.

QUESTION 39

When you enter a debug command, or if the system has to display an error message, by default where is the output sent?

- A. Output goes to the remote console if logging is off.
- B. Output is sent to the console terminal.
- C. Error logging automatically invokes debug output to the designated TFTP server.
- D. Output configuration requires a TFTP server to write files.
- E. Output is written to a Syslog server.

Answer: B

Explanation:

By default, a debug or a system error message will show up on the console terminal. This is very apparent when you log into a router via the console for the first time in order to initially configure the router.

Tip: Use the "logging synchronous" command to keep this console information from interfering with the configuration and show commands as they are being typed in.

Incorrect answers:

A: This is a distracter answer, because it uses the correct term 'console'; but if logging is turned off, the messages won't go to the remote console.

C, D: Answers C and D are both incorrect because a TFTP server isn't necessary to view the system debug and error outputs.

E: Although this information can be written to an external syslog server and although it is good practice to keep a syslog server to store error and debug messages this is an option that requires extra configuration that does NOT happen by default.

QUESTION 40

Which IOS command could you use to keep track of the exact time and date that a debug output occurred at or the duration of events?

- A. debug all
- B. service timestamps
- C. access list
- D. debug events
- E. terminal monitor

Answer: B

Explanation:

The service timestamps command configuration determines the format of the "Last Time" column in the show logging command output. Use the service timestamps command to configure the time-stamp format in the "Last Time" column.

Benefits:

1. Provides detailed information regarding system messages, including the most recent time the message occurred.
2. Alerts you to a potential problem with the system if you see the same error message occurring repeatedly.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087ca9.html

Explanation #2: The service timestamps commands:

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

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

add time stamps to debugs in the format MMM DD HH:MM:SS, indicating the date and time according to the system clock.

Reference: Important Information on Debug Commands

http://www.cisco.com/warp/public/793/access_dial/debug.html

Incorrect Answers

A: This command enables all debugging.

B, C: These are not valid IOS commands.

D: The terminal monitor command copies debug command output and system error messages to the current terminal as well as to the console terminal.

QUESTION 41

Which of the following IOS commands could you use to verify network connectivity on upper levels (Layers 4-7) of the OSI model? (Select two)

- A. Traceroute
- B. Telnet
- C. Ping
- D. Show interfaces
- E. Show arp

F. Show ip traffic

Answer: A, B

Explanation:

Cisco Traceroute test up to layer four using UDP as the transport protocol. In a Cisco traceroute, the TTL for the initial User Datagram Protocol (UDP) datagram probe is set to 1 (or the minimum TTL, as specified by user in the extended traceroute command).

The destination UDP port of the initial datagram probe is set to 33434 (or as specified in the extended traceroute command output). Telnet is an actual application, so a successful telnet session would mean that all layers (1-7) of the OSI model is functioning correctly.

Note: Microsoft Tracert only tests up to layer three by using ICMP. If the question asked for only a single answer, then the correct answer would be

A. For additional information

on the traceroute function, see the following:

<http://www.cisco.com/warp/public/105/traceroute.shtml>

Incorrect Answers:

C: The Ping utility will only test up to layer three (network layer) through the use of ICMP packets.

D: This command will only display the status of the interface, so it could be used to test the physical and data link layers.

E: ARP is used by ethernet hosts at layer 2.

F: IP is a layer 3 protocol.

QUESTION 42

Which of the following protocols can you use with the trace (aka traceroute) command? (Choose all that apply)

- A. IP
- B. AppleTalk
- C. VINES
- D. CLNS2
- E. Only A and B
- F. None of the above

Answer: A, B, C, D

Explanation:

Although IP is the default protocol, the other protocols that traceroute can be use for are: Appletalk, CLNS, Novell (IPX), Apollo, Banyan vines, Decnet, and XNS.

QUESTION 43

You are a resident network troubleshooter and one of your clients has told you that they are unable to reach the mail server host to access their email. What would be one of your first steps in isolating this problem?

- A. Run debug on the local host.
- B. Ping other hosts in the network.
- C. Check the local host configuration.
- D. Telnet to other hosts in the network.

Answer: B

Explanation:

As a first step in this troubleshooting process, you should check to see if the client can reach other nodes within the network. This step would help to isolate the problem. The problem may in fact be with the host itself, and not the email server. Of the choices given, this step will test connectivity to the lowest level (in this case layer 3 with ping) of the OSI model. As a general rule, it is best to test at the lower layers first.

QUESTION 44

You are the administrator of a large switched network. A group of users (who are all connected to the very same switch) are all experiencing issues with their connectivity. Your competent junior administrator went to check the physical connection, and he reports that all appears to be normal. What should you do next do verify connectivity?

- A. Check downstream connections.
- B. Check the counters and status of the switch's ports.
- C. Check the software version for bugs.
- D. Reload the switch to clear up any potential problems.

Answer: B

Explanation:

Incorrect Answers:

C: This is one of the last things that should be checked, since it is very time consuming and troublesome to diagnose software bugs. In this example, numerous end users are experiencing down time and their connectivity needs to be restored as soon as possible.

D: Although this may also be useful, simply rebooting a network device can often times cause outages for additional users. Doing this can also make finding the root cause of the outage difficult if not impossible.

QUESTION 45

At the Certkiller Corporation you've been hired on to a help desk position. On your first day, your phone is flooded with users complaining that they're unable to browse the Internet. What could you do to determine whether or not the clients are resolving the correct address to the Internet web sites from the DNS server?

- A. Ping the DNS server
- B. Run a trace route to the DNS server

- C. Browse to the IP address of the web server
- D. Release and renew the DHCP address on the client

Answer: C

Explanation:

If it is possible to browse the web site by IP address and not by host name, we would know that we have a name resolution problem.

Incorrect Answers:

A: Pinging the DNS server only checks if the DNS is reachable, not whether the client has the correct name resolution configuration.

B: A trace route to the DNS server will only check if the DNS server is reachable (and which route was used), not whether the client has the correct name resolution configuration.

D: Renewing the IP configuration on the client would not help in this scenario. This method would help determine DHCP server issues, but not DNS server problems.

QUESTION 46

DRAG DROP

Drag and drop the devices on the left to their corresponding slot on the right:

Select from these		Place here
BERT	Locate Cable Faults	
Cable Tester	Profile LAN Traffic	
Modeling Software	Examine DTE to DCE	
Network Monitor	Analyze Network Design	
Protocol analyser	Capture and Decode Packets	
TDR	Locate Cross Talk	

Answer:

Select from these		Place here
	Locate Cable Faults	TDR
	Profile LAN Traffic	Network Monitor
	Examine DTE to DCE	BERT
	Analyze Network Design	Protocol analyser
	Capture and Decode Packets	Modeling Software
	Locate Cross Talk	Cable Tester

Explanation:

Cable Tester:

A cable tester contains a Time Domain Reflectometer (TDR) and perhaps additional test circuits. A TDR sends sonar-like pulses through the cable. The TDR detects the reflections, analyzes them and displays the result.

A cable tester typically can tell you:

- * The length of a cable
- * Whether the cable is correctly wired internally (pin-to-pin wire mapping)
- * Whether the cable contains a short circuit (wires touching each other through damaged or missing insulation)
- * Whether the cable contains a broken wire (called an "open")
- * Whether the cable suffers from electrical cross talk (interference).

TDR is used to locate cable faults

<http://www.hma.tierranet.com/mcse/nettools.html>

Network Diagnostic Tools

Network Tool	Function
Digital Volt Meters (DVM)	Measures voltage passing through a resistance. Primarily used for network cable troubleshooting.
Network Monitor	Examines packet types, errors and traffic to and from each computer on a network.
Oscilloscope	Measures amount of signal voltage per unit of time. Displays crimps, shorts, opens, etc.
Protocol Analyzer	Look inside the packet to determine cause of problem. Contains built in Time-Domain Reflector. Gives insights to many problems including connection errors, bottlenecks, traffic problems, protocol problems, etc.
Time-Domain Reflectors (TDRs)	Sends sonar-like pulses to look for breaks, shorts or crimps in cables. Can locate a break within a few feet of actual fault.

QUESTION 47

Which command would you enter if you wanted a router to send out an ICMP message if it has to resend a packet out the same interface that it received the package from?

- A. ip porxy-arp
- B. ip routing
- C. ip redirects
- D. ip mroute-cache
- E. ip address dhcp
- F. ip split-horizon

Answer: C

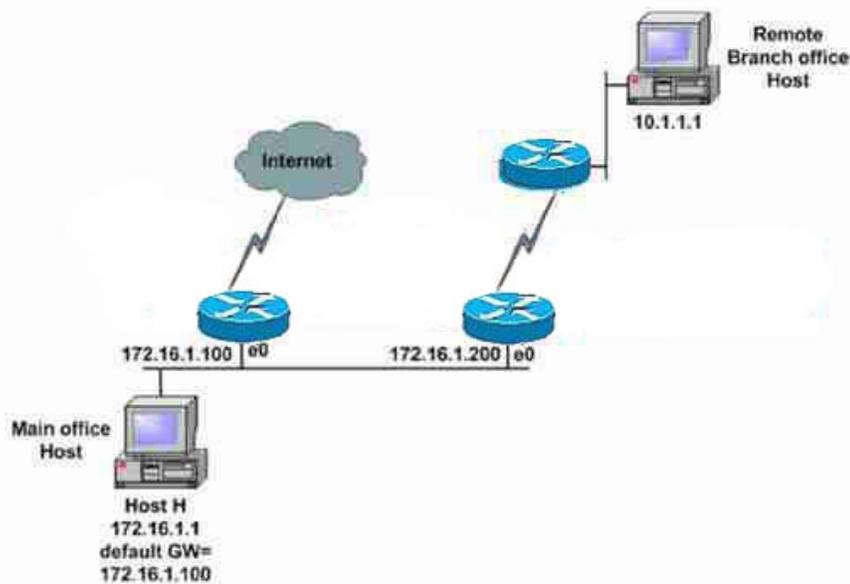
Explanation:

ICMP Redirects - How it works?

ICMP redirect messages are used by routers to notify the hosts on the data link that a better route is available for a particular destination. For example, there are two routers, R1 and R2, connected to the same Ethernet segment as IP host H, and host H is

642-831

configured to use R1 as its default gateway. Host H sends a packet to R1 to reach the destination host 10.1.1.1. R1, after consulting its routing table, finds that the next-hop to reach 10.1.1.1 is R2. Now R1 must forward the packet out the same Ethernet interface on which it was received. Router R1 forwards the packet to R2 and also sends an ICMP redirect message to host H, informing the host that the best route to reach 10.1.1.1 is by way of router R2. Host H will now forward all the subsequent packets destined for 10.1.1.1 to router R2.



The following debug message shows router R1, as in the above diagram, sending an ICMP redirect message to host H (172.16.1.1).

```
R1#debug ip icmp
```

```
ICMP packet debugging is on
```

```
ICMP: redirect sent to 172.16.1.1 for dest 10.1.1.1, use gw  
172.16.1.200
```

```
R1#
```

Router R1 (172.16.1.100) is sending a redirect to host H (172.16.1.1) to use router R2 (172.16.1.200) as the gateway to reach the destination 10.1.1.1.

When Are ICMP Redirects Sent?

Cisco routers send ICMP redirects when all of the following conditions are met:

The interface on which the packet comes into the router is the same interface on which the packet gets routed out.

The subnet or network of the source IP address is the same subnet or network of the next-hop IP address of the routed packet.

The datagram is not source-routed.

The kernel is configured to send redirects. (By default, Cisco routers send ICMP redirects. The interface subcommand `no ip redirects` can be used to disable ICMP redirects.)

Note: ICMP redirects are disabled by default if Hot Standby Router Protocol (HSRP) is configured on the interface. For example, if a router has two IP addresses on one of its interfaces:

Interface ethernet 0

Ip address 171.68.179.1 255.255.255.0

Ip address 171.68.254.1 255.255.255.0 secondary

If the router receives a packet that is sourced from a host in the subnet 171.68.179.0 and destined to a host in the subnet 171.68.254.0, the router does not send an ICMP redirect because only the first condition is met, not the second. The original packet for which the router sends a redirect still gets routed to the correct destination.

QUESTION 48

To a troubleshooter, what are the advantages of looking at a network from the perspective of the logical layered model? (Choose two)

- A. Identifies the applications being used in the network.
- B. Divides the problem into manageable parts.
- C. Provides a general troubleshooting process.
- D. Minimizes the complexity of a problem.
- E. Identifies the equipment being used in the network.

Answer: B, D

Explanation:

When you look at a problematic network from the perspective of the logical layered model you divide the problem into manageable parts. Once broken down, you can designate others to troubleshoot different layers (ie. One person checks the physical layer connections, another person checks the application layer from the user end systems) and you can track your progress.

When a problem is isolated to a few layers the complexity is also minimized because each layer only has a limited number of things that can go wrong, with a more exact set of diagnostic tools to use. With less time spent thinking on the possibilities, a troubleshooter can spend more time working on the details, and eliminating the potential problem causes systematically.

QUESTION 49

A problem at which of the following layers of the OSI model would result in the following console messages? (Choose two.)

Router#

Mar 23 12:10:20 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1, changed state to down

Mar 23 12:10:20 %DUAL-5-NBRCHANGE: IP-EIGRP 101: Neighbor 172.21.177.1 (Serial1/0) is down: interface down

- A. Data link
- B. Physical
- C. Session
- D. Network
- E. Application

F. Transport

Answer: A, B

Explanation:

The line and the interface are both down, so there are problems at the physical and data link layers. Although the EIGRP message would relate to a layer 3 issue, the EIGRP neighbor became unreachable only because of the interface status changing to a downed state. Therefore, the problems could only have occurred as a result of a physical or data link problem.

QUESTION 50

While performing your battery of routing network tests on the Certkiller networks, you come across a remote router that is NOT routing packets to the central router by way of its point-to-point link. To begin troubleshooting, you enter the command "show ip interface brief" and to your surprise you see that the interface status is UP/UP. Taking this information in consideration, which TCP/IP model layer should you begin your troubleshooting efforts?

- A. Application
- B. Internet
- C. Network interface
- D. Transport
- E. Network

Answer: B

Explanation:

As with the OSI model, the TCP/IP suite uses a layered model. The OSI model has seven layers, the TCP/IP model has four or five - depending on who you talk to and which books you read. Some people call it a four layer suite - Application, Transport, Internet and Network Access, others split the Network Access layer into its Physical and Datalink components. In this example, since the physical access layer (Network Access) layer is functioning properly, the next layer that should be examined is the Internet layer. More information on the different layers of the TCP/IP model is displayed below:

Layer 5 - Application

This layer is broadly equivalent to the application, presentation and session layers of the OSI model. It gives an application access to the communication environment. Examples of protocols found at this layer are Telnet, FTP (File Transfer Protocol), SNMP (Simple Network Management Protocol), HTTP (Hyper Text Transfer Protocol) and SMTP (Simple Mail Transfer Protocol).

Layer 4 - Transport

The transport layer is similar to the OSI transport model, but with elements of the OSI session layer functionality. This layer provides an application layer delivery service. The two protocols found at the transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). Either of these two protocols are used by the application

layer process, the choice depends on the application's transmission reliability requirements.

Layer 3 - Internet

This layer is responsible for the routing and delivery of data across networks. It allows communication across networks of the same and different types and carries out translations to deal with dissimilar data addressing schemes. IP (Internet Protocol) and ARP (Address Resolution Protocol) are both to be found at the Internet layer.

Layers 2 and 1 - Network Access

The combination of data link and physical layers deals with pure hardware (wires, satellite links, network interface cards, etc.) and access methods such as CSMA/CD (carrier sensed multiple access with collision detection).

Reference: <http://burks.bton.ac.uk/burks/pcinfo/hardware/ethernet/tcpip.htm>

QUESTION 51

You are a network administrator and you've got a predicament on your hands. Your users can't connect to the email server and calendar system on their network; but they can access web pages located on the same server. Where in the TCP/IP model layer would you begin troubleshooting the problem?

- A. Transport
- B. Internet
- C. Network Interface
- D. Application
- E. Messaging
- F. Data Link
- G. None of the above

Answer: D

Explanation:

The application layer of the TCP/IP suite maps to the session (Layer 5), presentation (Layer 6), and application (Layer 7) layers of the OSI model. Therefore, issues that are related to any of these layers should be referred to as application layer problems within the TCP/IP framework. You can categorize a problem as a pure application layer problem if you can prove that all the lower layers up to the transport layer are in good working condition. Application layer problems might be rooted at the application server devices, client hosts, firewalls, routers, or multilayer switches. Typical symptoms of a failure/problem at the application layer can include one or more of the following:

- * Resources are unreachable or unusable, while the physical, data link, network, and transport layers are functional.
- * Operation of a network service or application does not meet a user's normal expectations.
- * Applications generate error messages or report lack of functionality.
- * Users complain that the network is slow or that their network applications are not functioning, are unavailable, or are too slow.

- * Console messages indicate abnormal events; system log file messages report errors.
 - * Management system alarms deliver unexpected news.
-

QUESTION 52

On what OSI layers would a switch be most likely to be operating at?

- A. Network
- B. Transport
- C. Physical
- D. Data Link
- E. Application

Answer: D

Explanation:

Switches connect Ethernet end stations together and operate at layer 2 of the OSI model.

Note: Some switches operate at higher layers, most notably the network layer. These switches are generally termed layer 3 switches since they perform routing functions.

There are also application-level switches, which is a marketing term for application aware switches that use port and flow based information to switch traffic. Although these switches can indeed operate at layers 2-7, it is more precise to say that all switches operate at layer 2, the data link layer, since not all switches are capable of layer-3 and above functionality. Therefore, D is clearly the single best choice even though a case could be made for any of the other choices.

QUESTION 53

During routine maintenance on the network you noticed that packets are being delivered to incorrect destinations.

Which protocol layer is most likely place to encounter problems?

- A. Physical
- B. Network
- C. Data Link
- D. Transport
- E. Application

Answer: B

Explanation:

Following are some common symptoms of network layer problems:

- * No component on the failing link appears to be functional above the network layer.
- * The network is functional but is operating either consistently or intermittently at a lower capacity (speed, response, or throughput) than the baseline level.
- * No connectivity on the link is seen from the transport layer.
- * Pings succeed only part of the time.

- * Routing tables are empty, inconsistent, or incomplete.
- * Routing behavior is unexpected.
- * Packets are delivered to incorrect destinations. (Correct Answer)
- * Various console messages report failures and problems.
- * System log-file messages report failures/problems.
- * Management system alarms indicate problems/failures.

QUESTION 54

Excessive flooding on a single VLAN (on an access switch) is associated with the _____ layer of the OSI model.

- A. physical
- B. data link
- C. network
- D. transportation
- E. application

Answer: B

Explanation:

Access layer switch works on data link layer and when an unknown Unicast or broadcast message comes to an access-layer switch, it floods the message to the computers in that particular vlan.

References:

www.cisco.com/warp/public/473/53.shtml

www.cisco.com/warp/public/473/62.shtml

QUESTION 55

Which layer(s) of connectivity is tested with the ping command?

- A. Layer 1
- B. Layer 2
- C. Layer 3
- D. Layer 1-2
- E. Layer 1-3
- F. Layer 1-4

Answer: E

Explanation:

Ping works by sending out ICMP packets and waiting for an echo. This happens on the network layer (layer 3), so if ping works then we know that level 3 is functional, therefore the lower layers (1 & 2) are functional as well. Remember, each layer of the OSI model functions only if the underlying layers are also functioning.

QUESTION 56

Encryption and tunneling protocols that work with PAT (Port/Address Translation) sometimes have problems. At which OSI level do PAT problems exist at?

- A. Data Link Layer
- B. Network Layer
- C. Transport Layer
- D. Presentation Layer
- E. Physical Layer

Answer: C

Explanation:

PAT (port/address translation) is a form of dynamic NAT (network address translation) that maps multiple unregistered IP addresses to a single registered IP address by way of using different ports. TCP/UDP ports are associated with the transport layer of the OSI model.

QUESTION 57

While addressing a connectivity problem between two hosts you administer 'ping' and achieve success. What OSI layer should you troubleshoot next?

- A. Data link
- B. Physical
- C. Network
- D. Transport
- E. Session
- F. Internet

Answer: D

Explanation:

A successful ping means that the network layer is operating properly, so layers 1-3 are functional. The next step in the troubleshooting process is to advance to the next layer of the OSI model, which is the Transport layer (layer 4).

QUESTION 58

For troubleshooting a connection-orientated protocol such as TCP, what things should you focus on? (Choose all that apply.)

- A. Verify protocol numbers
- B. Verify time-to-live fields
- C. Verify sequence numbers
- D. Verify acknowledgment numbers

Answer: C, D

Explanation:

In a sliding window protocol like TCP, the sequence number allows both TCP stacks to know what packets have been received and which ones have not. The Acknowledgment Number works by acknowledging the sequence number as sent by the remote host. The local host's Acknowledgement Number is a reference to the remote machine's Sequence number, and the local machine's sequence number is related to the remote machine's acknowledgement number.

When problems arise from a connection oriented protocol, the first steps that should be taken are verifying that the protocol is sending sequence numbers correctly, as well as receiving the associated acknowledgement numbers from the host.

QUESTION 59

In the encapsulated data flow process; how many total stages are there?

- A. 5
- B. 4
- C. 2
- D. 3
- E. 1
- F. 7

Answer: B

Explanation:

The stages of the encapsulated data flow process are:

1. Encapsulation
2. Transmission
3. Forwarding/Filtering
4. Decapsulation

QUESTION 60

Host CK1 wants to initiate a TCP connection to host CK2 . To do this, what kind of packet will CK1 first send out in the connection sequence?

- A. ARP packet
- B. Synchronization packet
- C. SYN packet
- D. TCP ACK packet
- E. ARPA initiate packet

Answer: C

Explanation:

In the TCP three way connection, the three packet types used are SYN, SYN/ACK, and ACK.

Connection Establishment and Termination

Connection establishment is the last TCP function reviewed in this section, but it occurs before any of the other TCP features can begin their work. Connection establishment refers to the process of initializing sequence and acknowledgment fields and agreeing to the port numbers used. Figure 5-7 shows an example of connection establishment flow.

Figure 5-7 TCP Connection Establishment



This three-way connection establishment flow must complete before data transfer can begin. The connection exists between the two sockets, although there is no single socket field in the TCP header. Of the three parts of a socket, the IP addresses are implied based on the source and destination IP addresses in the IP header. TCP is implied because a TCP header is in use, as implied by the protocol field value in the IP header. Therefore, the only parts of the socket that need to be encoded in the TCP header are the port numbers.

Two single-bit portions of the flags field of the TCP header are used to signal the three-step process for connection establishment. Called the SYN and ACK flags, these bits have a particularly interesting meaning. SYN means, "Synchronize the sequence numbers," which is one necessary component in initialization for TCP. The ACK field means "the acknowledgment field is valid in this header." Until the sequence numbers are initialized, the acknowledgment field cannot be very useful. Also notice that in the initial flow in Figure 5-7, no acknowledgment number is shown—this is because that number is not valid yet. Because the ACK field must be present in all the ensuing segments, the ACK bit will continue to be set until the connection is terminated.

QUESTION 61

While troubleshooting an FTP server, you realize that the 'get' commands are failing but the 'put' commands are working. What do you suspect is the cause of the problem?

- A. Incorrect MTU on a link.
- B. Timeout on TCP connections.
- C. No route to the FTP server destination address.
- D. Default gateway of host not correctly configured.
- E. All of the above are possible reasons.

Answer: A

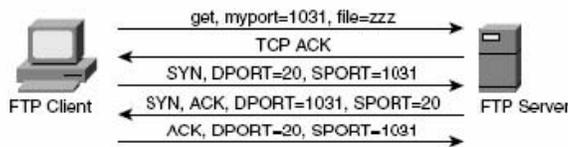
Explanation:

Over some IP paths, a TCP/IP node may send small amounts of data (typically less than 1500 bytes) with no difficulty, but transmission attempts with larger amounts of data hang, then time out. The behavior is generally only experienced in one direction. When attempting to send large amounts of data, transfers may succeed in one direction but fail in the other direction. This problem is likely caused by a PMTUD failure, different LAN media types, or defective links. For a detailed paper describing this problem, go here:

http://www.netopia.com/en-us/support/technotes/hardware/NIR_067.html?print=yes
Generally, when downloading from an FTP server, large packet sizes are used. When using the "put" command, smaller packet sizes are needed. Since the packet sizes vary during the FTP process, the problem could be that the MTU settings are incorrect.
Note:

At this point, the user has a variety of commands available to enable settings for transfer, change directories, list files, and so forth. However whenever a `get` or a `put` command is entered (or `mget` or `mput`—`m` is for *multiple*) or the equivalent button is clicked, then a file is transferred. The data is transferred over a separate *TCP data connection*. Figure 5-16 outlines the FTP data connection process.

Figure 5-16 FTP Data Connection



Incorrect Answers:

B, C, D: If any of these were true, a connection to the FTP server could not be made, and the "put" command would not work.

Reference:

http://www.netopia.com/en-us/support/technotes/hardware/NIR_067.html?print=yes

QUESTION 62

You are a mobile troubleshooter and you arrive to a jobsite.

The users are complaining that they have trouble viewing files on the internet. After some investigation you find out that there's a good network layer path between client and server and back. What should you check next?

- A. Buffer underruns
- B. Retransmissions
- C. Switching topology
- D. Routing topology
- E. Buffer overruns

Answer: B

Explanation:

Causes of retransmissions including bit errors, alignment errors, and FCS errors which will all contribute to higher retransmission rates elevating traffic levels. The presence of a large number of retransmissions could be indicative of errors on one of the links between the end user and the Internet server.

Incorrect Answers:

C, D: A problem with these two choices would most likely mean that the Internet server would not be reachable at all.

A, E: A problem with the buffer levels of the routers would most likely mean that users would be experiencing problems with all of their connections, and not just the Internet files.

QUESTION 63

Host CKA and CKB both reside on the same IP subnet. What two sequences of events have to occur for these hosts to establish a connection with the other host on an Ethernet? (Choose two)

- A. TCP SYN
- B. TCP ACK
- C. TCP ARP
- D. ARP reply
- E. ARP request

Answer: D, E

Explanation:

ARP is used to locate the ethernet address associated with a desired IP address. When a machine has a packet bound for another IP on a locally connected ethernet network, it will send a broadcast ethernet frame containing an ARP request onto the ethernet. All machines with the same ethernet broadcast address will receive this packet. [1] If a machine receives the ARP request and it hosts the IP requested, it will respond with the hardware address on which it will receive packets for that IP address An ARP reply will be used.

QUESTION 64

Host CK1 is having difficulties sending UDP data streams to host CK2 . Which of the following are possible reasons for this?

- A. Sequence numbers
- B. Flow control and window sizes
- C. Connection-oriented upper layers
- D. The unplanned transmission of data
- E. Multiple retransmission of data segments

Answer: D

Explanation:

Choice D is the only logical choice, since the other choices are functions of connection-oriented protocols such as TCP, not connectionless protocols such as UDP. TCP is a connection oriented protocol that establishes a virtual circuit before it sends data. It is designed to ensure that we have a connection to the destination before we send data just as you do with a telephone conversation. When large amounts of data are exchanged, TCP is normally used. TCP uses sequence numbers and acknowledgements to ensure that no data is lost.

TCP establishes a virtual circuit connection whereas UDP sends connectionless datagrams

UDP is a connectionless protocol that provides a datagram service. Data is sent and no acknowledgement is required. It provides a best-effort service and does not retransmit

lost data. It is used for sending small amounts of data and broadcasts where loss of data is not a serious problem. It is like sending junk mail, where if the junk mail is lost, you will be sent another message in the near future.

TCP Window Size

Traditionally network protocols exchanged information and acknowledgements in a pin-pong fashion. Although the data get through, delays accumulate and performance is poor. TCP supports the transfer of more than one packet for each acknowledgement through a process known as a sliding window. The bigger the window size the fewer acknowledgements are sent. If the window is too large, there will be too much unnecessary traffic after a server failure. In general, a smaller window size is appropriate for slow WAN Wide-Area Networks, and a larger window size should be used for high speed LANs.

To optimize the TCP Window Size, use Network Monitor to observe typical network traffic. If the number of replies fills the TCP windows, then your performance is limited by the TCP window size and it should be increased. If the number of replies is less than the TCP window size, then increasing the size will have no benefit.

Connection-Oriented means that when devices communicate, they perform handshaking to set up an end-to-end connection. The handshaking process may be as simple as synchronization such as in the transport layer protocol

TCP, or as complex as negotiating communications parameters as with a modem.

Connection-Oriented systems can only work in bi-directional communications environments. To negotiate a connection, both sides must be able to communicate with each other. This will not work in a unidirectional environment.

Connectionless means that no effort is made to set up a dedicated end-to-end connection. Connectionless communication is usually achieved by transmitting information in one direction, from source to destination without checking to see if the destination is still there, or if it is prepared to receive the information. When there is little interference, and plenty of speed available, these systems work fine. In environments where there is difficulty transmitting to the destination, information may have to be re-transmitted several times before the complete message is received.

Reference: <http://teamapproach.ca/trouble/Protocols.htm>

QUESTION 65

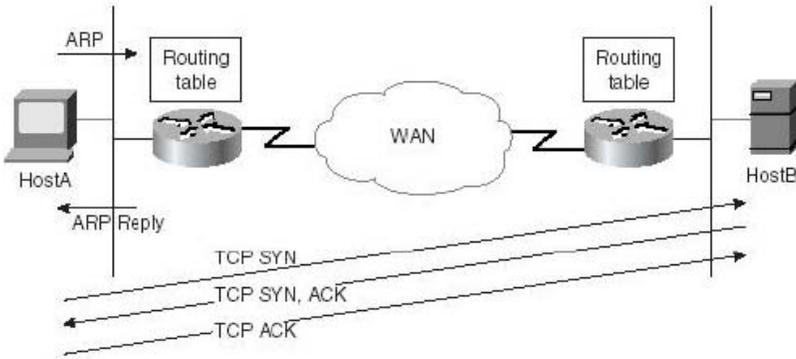
Your junior administrator is studying for his CCNA examination and asks you if you know what kind of connection sequence TCP uses. How would you answer?

- A. Five-way SYN
- B. Three-way SYN
- C. Five-way handshake
- D. Three-way handshake
- E. None of the above.

Answer: D

Explanation:

The TCP connection is established through a three-way handshake.



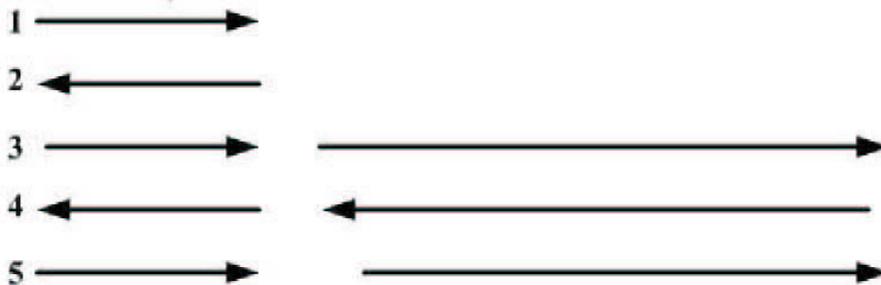
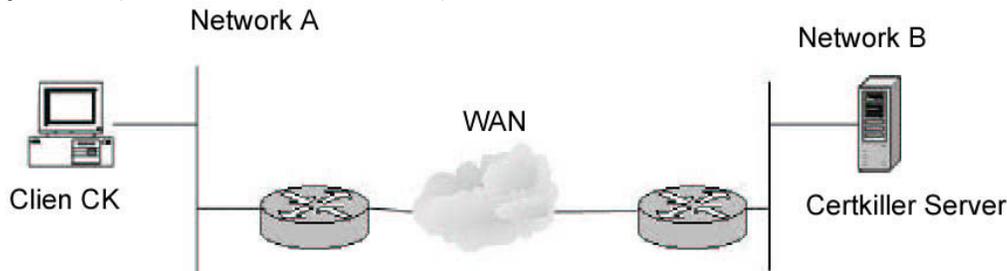
Incorrect Answers

- A: Only a three-way handshake is used.
- B: Only two SYNs are used, including the SYN/ACK.
- C: Only a three-way handshake is used.

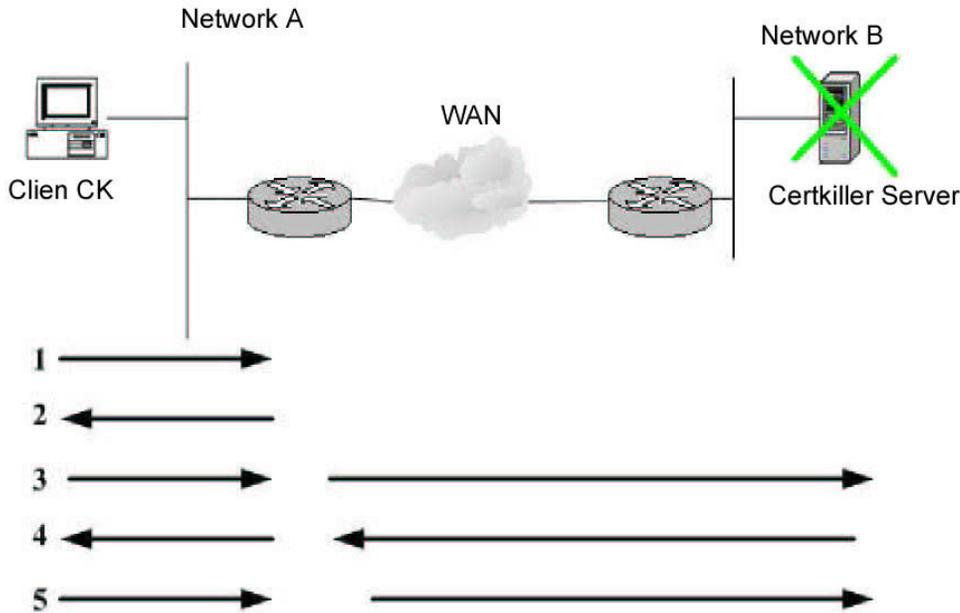
QUESTION 66

HOTSPOT

On the Certkiller network shown below, client CK initiates a TCP data session to the Certkiller Server. Based on the diagram below, which device will send a SYN ACK packet? (Choose the device below).

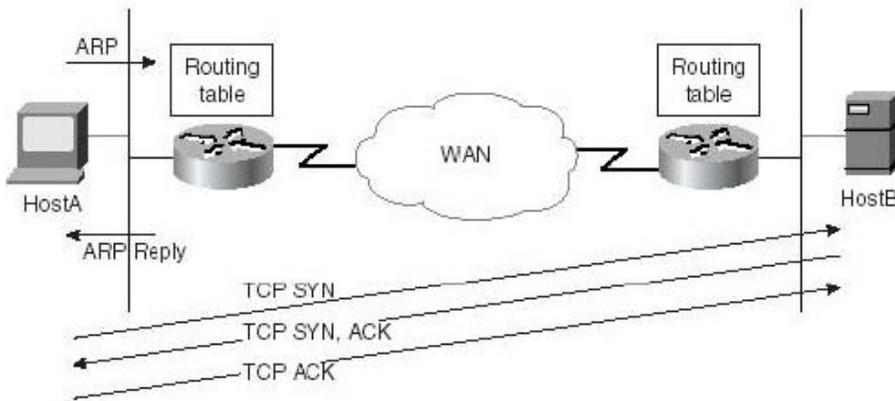


Answer:



Explanation:

The Certkiller server sends a TCP SYN ACK during the TCP connection sequence (see below)



QUESTION 67

Which of the following protocols are connectionless? (Choose all that apply)

- A. IP
- B. ATM
- C. TCP
- D. UDP
- E. Novell IPX

Answer: A, D, E

Explanation:

IPX, UDP, and IP are connectionless, unreliable transport. Traffic sent using these

protocols are delivered on a best effort basis, and they rely on higher layer protocols or the application itself to inform the sender if any data needs to be retransmitted.

QUESTION 68

When a client on the Certkiller network wants to start a connection with a server it sends a greeting packet, if the server is ready to continue it sends a reply packet. What is this reply packet called?

- A. NACK
- B. ACK
- C. SYN/ACK
- D. SYN

Answer: C

Explanation:

The reply packet has both the SYN and ACK bits set. When a TCP connection is first established, a SYN packet is sent from the host initiating the session. The receiver then replies with a SYN/ACK packet to acknowledge the original sequence packet. Finally, the sender completes the three way handshake with an ACK packet back to the host that sent the SYN/ACK.

QUESTION 69

During the establishment of a TCP connection; how do hosts choose their initial sequence?

- A. Both hosts start at sequence 1.
- B. Both hosts start at sequence 1024.
- C. Host A starts at sequence N and host B starts at N+1.
- D. Both hosts start at a randomly chosen sequence number.

Answer: D

Explanation:

To use reliable transport services, TCP hosts must establish a connection-oriented session with one another. Connection establishment is performed by using a "three-way handshake" mechanism.

A three-way handshake synchronizes both ends of a connection by allowing both sides to agree upon initial sequence numbers. This mechanism also guarantees that both sides are ready to transmit data and know that the other side is ready to transmit as well. This is necessary so that packets are not transmitted or retransmitted during session establishment or after session termination.

Each host randomly chooses a sequence number used to track bytes within the stream it is sending and receiving. Then, the three-way handshake proceeds in the following manner:

Incorrect Answers:

C: The first host (Host A) initiates a connection by sending a packet with the initial sequence number (X) and SYN bit set to indicate a connection request. This initial sequence number is a randomized number. The second host (Host B) receives the SYN, records the sequence number X, and replies by acknowledging the SYN (with an ACK = X + 1). So, the reply is N+1, but not the initial sequence number.

Reference: Internet Protocols

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

QUESTION 70

Which troubleshooting method should an administrator use, if they were troubleshooting a routing protocol issue?

- A. Top-down
- B. Bottom-up
- C. Divide-and-conquer
- D. Knowledge-based search

Answer: C

Explanation:

Since the root of the problem is already known to the network administrator (Routing protocol issue) the best approach would be to focus on the network layer using the Divide and Conquer method. A summary of the troubleshooting methods is displayed in the following table:

<i>Table 6-2. Summary of Troubleshooting Approaches</i>			
Troubleshooting Approach	How It Operates	Cases It Is Suitable For	Advantages/Disadvantages
Bottom-up	Always starts at the physical layer and works its way up until it finds a faulty layer.	More suited for complex cases.	It is a slow, but solid approach. When the problem is application (or upper layer) related, this approach can take a long time.
Top-down	Always starts at the application layer and works its way down until it finds a faulty layer.	More suitable for simpler problems or those that are suspected to be application/user or upper-layer related.	If the problem turns out to be related to lower layers, you have wasted a lot of time and effort at the upper or application layers.
Divide-and-conquer	Based on the circumstances (reported issues) and your experience, you might decide to start at any layer and work up or down the OSI stack.	Most suitable when you are experienced and the problem has precise symptoms.	It approaches the layer of the culprit faster than the other approaches. You need experience to use this approach effectively.

QUESTION 71

You've noticed the following console message while logged into router CK1 :
Feb 27 10:13:32 %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial 0/0, changed state to down

What would an experienced troubleshooter do to address the problem?

- A. Use a top-down troubleshooting exercise.
- B. Use a divide-and-conquer troubleshooting exercise.
- C. Use the LEDs on the affected device to gather symptoms.
- D. Use a show interface command on the affected interface.

Answer: B

Explanation:

The divide and conquer method is best for experienced troubleshooters, handling problems that are either familiar or localized. In this example, the problem is already known (serial interface is down) and so it would be best to focus on this particular problem.

Incorrect Answers:

C: This is incorrect because the line protocol is at a higher layer than the physical layer.

D: This is not necessarily the best option, as we already know that the status of the interface is down, and the errors that are shown on the counters may have occurred long ago.

QUESTION 72

What troubleshooting approach should you use if your router is receiving excessive CRC (cyclic redundancy check) and FCS (frame check sequence errors)?

- A. Top-down
- B. Divide and conquer
- C. Trial and error
- D. Bottom-up

Answer: D

Explanation:

Start from the physical layer, and work your way up. If you're experiencing a problem with excessive CRC's and FCS's then your problem is more likely to reside at the lower layers. CRC and FCS errors are usually the result of physical layer problems.

QUESTION 73

You're a network administrator and one of your users is having problems with her browser. You interview other users on the network and you find a handful of other users who are experiencing similar problems. You start your troubleshooting by pinging the user workstations, and the ping is successful. What type of troubleshooting method should you use to continue?

- A. Forward-first
- B. Divide and conquer
- C. Top-up
- D. Top-down
- E. Conquer through force
- F. Bottom-up

Answer: D

Explanation:

Since the problem is not related to layers 1-3 (as proven by the successful pings) the issue can be isolated to the higher layers. Because of this, a top-down approach would be best. The following table describes the various troubleshooting methodology.

<i>Table 6-2. Summary of Troubleshooting Approaches</i>			
Troubleshooting Approach	How It Operates	Cases It Is Suitable For	Advantages/Disadvantages
Bottom-up	Always starts at the physical layer and works its way up until it finds a faulty layer.	More suited for complex cases.	It is a slow, but solid approach. When the problem is application (or upper layer) related, this approach can take a long time.
Top-down	Always starts at the application layer and works its way down until it finds a faulty layer.	More suitable for simpler problems or those that are suspected to be application/user or upper-layer related.	If the problem turns out to be related to lower layers, you have wasted a lot of time and effort at the upper or application layers.
Divide-and-conquer	Based on the circumstances (reported issues) and your experience, you might decide to start at any layer and work up or down the OSI stack.	Most suitable when you are experienced and the problem has precise symptoms.	It approaches the layer of the culprit faster than the other approaches. You need experience to use this approach effectively.

QUESTION 74

What is the name of the troubleshooting approach that begins with the checking of the routing table?

- A. Bottom-up troubleshooting
- B. Divide and Conquer Troubleshooting
- C. OSI Troubleshooting
- D. Top-Down Troubleshooting
- E. None of the above

Answer: B

Explanation:

Since checking the routing table means first focusing on layer 3, neither the top-down or bottom-up approach is being used. Focusing first on a specific issue is the divide and conquer method.

Table 6-2. Summary of Troubleshooting Approaches			
Troubleshooting Approach	How It Operates Cases It Is Suitable	For	Advantages/Disadvantages
Divide-and-conquer circumstances	Based on the (reported issues) and your experience, you might decide to start at any layer and work up or down the OSI stack.	Most suitable when you are experienced and the problem has precise symptoms.	It approaches the layer of the culprit faster than the other approaches. You need experience to use this approach effectively.

QUESTION 75

When troubleshooting a very complex problem, what is the most appropriate troubleshooting approach to take?

- A. Top-down
- B. Bottom-up
- C. Split-difference
- D. Divide-and-conquer
- E. None of the above

Answer: B

Explanation:

This is the Cisco recommended technique for troubleshooting any type of problem. It is

the most time efficient way to get to the root of the problem, especially for complex issues.

Table . Summary of Troubleshooting Approaches

Troubleshooting Approach	How It Operates Cases It Is Suitable	For	Advantages/Disadvantages
Bottom-up	Always starts at the physical layer and works its way up until it finds a faulty layer.	More suited for complex cases.	It is a slow, but solid approach. When the problem is application (or upper layer) related, this approach can take a long time.

QUESTION 76

You are tasked with solving a problem on the Certkiller network. System users experience slow response times when they try to access files on the Certkiller database server; but when they go to access their email (on a server that resides on the same network segment) there are problems only intermittently. At which OSI layer should you start your troubleshooting efforts?

- A. Physical
- B. Data link
- C. Network
- D. Transport
- E. Application
- F. Any of the above.

Answer: A

Explanation:

This is a complex problem, so it calls for a bottom-up approach, which begins at the bottom (the physical layer) and works itself up.

Table 6.2. Summary of Troubleshooting Approaches

Troubleshooting Approach	How It Operates Cases It Is Suitable	For	Advantages/Disadvantages
Bottom-up	Always starts at	More suited for complex	It is a slow, but

	the physical layer and works its way up until it finds a faulty layer.	cases.	solid approach. When the problem is application (or upper layer) related, this approach can take a long time.
--	--	--------	---

QUESTION 77

It is a very important for an administrator to _____ before implementing a plan of action.

- A. Create troubleshooting steps as needed during the process.
- B. Delete access lists on routers to isolate traffic.
- C. Document the topology of the network.
- D. Restore your network to a known previous state if the action item does not solve the problem.

Answer: C

Explanation:

It is always advisable to document the network before making any changes, and certainly before implementing a plan of action.

Incorrect Answers:

- A: The troubleshooting steps should be well thought out before implementing a plan of action. It is not advisable to create them in the middle of a plan unless absolutely necessary, since these steps may not get properly documented.
- B: Usually, access lists are in place for a reason (traffic control, security) and it is generally not advised that they be removed unless there is a good reason for it.
- D: Although this is true, this step should be taken after the action plan has failed to correct the problem, and not before.

QUESTION 78

You are a junior network administrator, and your CTO has given you a proper trouble shooting plan to fix a network bug. Sadly, your efforts were unsuccessful. What should you do next?

- A. Stop making changes and return to the Gathering Symptoms stage.
- B. Continue to make changes, documenting each change as it is made until the problem is corrected.
- C. Undo all changes, returning the device to their known initial state.
- D. Perform a core dump to send to Cisco technical support for analysis.

Answer: C

Explanation:

If you tried a plan and it failed, you should restore the device back to where you started, and document your unsuccessful attempt. Only then should another attempt at correcting the problem be taken.

If you try a change, on top of a change, on top of a change, you'll be more likely to get lost and if by chance you do solve the problem, you won't be able to truly confirm the source of the problem for your documentation and you'll have finished without learning anything.

QUESTION 79

What should the Certkiller administrator do after successfully implementing and testing a network change?

- A. Gather statistics
- B. Identify the affected network layer
- C. Compare the result to the baseline
- D. Document the solution
- E. None of the above

Answer: D

Explanation:

The last step in the troubleshooting process is to document your work. This will save you and others a lot of time and effort in the future. You and your colleagues will want to understand what you have changed and why you did it. You may also want to document any recommendations and tips and lessons learned that you think might be useful to those parties involved.

Reference:

CCNP Support Exam Certification Guide page 41, Amir S. Ranjibar, Cisco Press 2001
ISBN 0-7357-09955-5

QUESTION 80

Is the following statement true or false?

Network professionals should always gather facts before analyzing a network problem.

- A. False, you should first contact TAC for assistance
- B. False, you should define the problem first.
- C. False, you should first define the alternative solutions
- D. True
- E. False, you should first open a case via CCO
- F. There is not enough information to determine the answer

Answer: B

Explanation:

According to the technical documentation at CCO:

When analyzing a network problem, make a clear problem statement. You should define the problem in terms of a set of symptoms and potential causes. To properly analyze the problem, identify the general symptoms and then ascertain what kinds of problems (causes) could result in these symptoms. For example, hosts might not be responding to service requests from clients (a symptom). Possible causes might include a misconfigured host, bad interface cards, or missing router configuration commands.

QUESTION 81

The Certkiller corporate building you work in was hit by a lightning bolt during a thunderstorm. As a result of the strike, your network experiences a power outage, and as a result of the power outage, many users from all segments of the network are experiencing connectivity problems. What should you do first, to resolve the connectivity problem?

- A. Interview the end-users.
- B. Test for connectivity on critical network segments.
- C. Reboot routers on critical network segments.
- D. Use show commands to isolate any configuration changes.
- E. None of the above.

Answer: A

Explanation:

Before you go around testing for connectivity on critical network segments (gathering facts) you should first truly define the problem. The best way of defining a problem is by interviewing the network users who are experiencing the problem. Once you know what they're suffering from, then you'll be able to form a few hypothesis and then when you do go to test connectivity you'll know exactly where to test and be more perspective as what to look for.

QUESTION 82

A Certkiller end user has been trying to attempt a TFTP session but has been unsuccessful. You do some troubleshooting and find out that there is a network layer path from client to server and back. What three troubleshooting steps should you perform next? (Choose three.)

- A. Check to see if data are arriving out of order
- B. Check to see if the TFTP requests are acknowledged
- C. Check to see if there are errors in the segment headers
- D. Check to see if the TCP sequence and acknowledgement numbers are aligned
- E. Reboot all network devices that reside between the client and the server

Answer: A, B, C

Explanation:

We could check if data is arriving out of order, if TFTP requests are acknowledged, or if there are errors in the segment headers. Systematically troubleshooting each individual function of the TFTP process is the best method for solving this problem.

Incorrect Answers:

D: TFTP uses UDP, not TCP. TFTP is a connection-less protocol that does not use acknowledgements.

E: This solution would only cause additional outages for other network users.

QUESTION 83

You work as a network administrator at Certkiller .com. You have identified two IP routers that have connectivity but are not exchanging routing information. You issue the following command: show cdp neighbors

You are able to see the directly connected router in the question.

Which troubleshooting approach would be the most sufficient to use?

- A. bottom-up
- B. divide and conquer
- C. top-down
- D. determine the scope
- E. gather the symptoms

Answer: B

QUESTION 84

At which troubleshooting stage must the troubleshooter identify characteristics of problems at the logical layers of the network in order to determine the most likely cause?

- A. when symptoms are gathered
- B. when the problem is isolated
- C. when the problem is corrected
- D. when the scope is determined

Answer: B

QUESTION 85

You work as a network administrator at Certkiller .com. You receive reports that a group of users is unable to connect to a server on another subnet. You have seen these symptoms before and you decide to perform the following command on the local router to learn additional information and begin the troubleshooting process.

Command: show ip route

Which troubleshooting approach are you using?

- A. top-down
- B. divide-and-conquer
- C. bottom-up

- D. knowledge-based search
- E. none of the above

Answer: B

QUESTION 86

For the sake of supporting problem detection and problem resolution; what should you include in a network documentation system? (Choose three)

- A. logical topology diagram,
- B. network operations budget
- C. physical topology diagram
- D. device configuration table
- E. application deployment schedule
- F. documentation maintenance schedule

Answer: A, C, D

Explanation:

In any good network documentation set, the logical and physical topology diagrams should be included, along with the configuration table of each individual device. Some of the items that should be included in the diagrams, based on OSI layer, are shown in the table below:

Table 2-4. End System Topology Diagram Components Classified Based on the TCP/IP Protocol Stack	
Layers	Information
Physical	Physical location
Network/data link	IP address Subnet mask Default gateway Device name Device purpose Access VLAN MAC address
Application	Operating system/version Network applications

QUESTION 87

What form of network documentation would you expect to find a list of high-bandwidth applications?

- A. A network topology diagram

- B. A network configuration table
- C. An end-system topology diagram
- D. An end-system configuration table

Answer: D

Explanation:

The types of applications that take up the most bandwidth (file sharing programs, streaming movies, online video conferencing, and internet applications) are all end user applications. Since the programs are located on the end systems hard drive and used by the end system user, it would be natural for it to be classified with the end system. Since it's easier to list an application's name on a table than it is to draw an application on a diagram the correct answer is end-system configuration table.

QUESTION 88

What is a primary goal when constructing end-system network configuration documentation?

- A. Device responsibility
- B. Objective documentation
- C. Rapid discovery of specific information about end-systems
- D. Documentation maintenance
- E. All of the above

Answer: D

Explanation:

The guidelines for creating these types of documentation are described in the following table:

Guidelines for Creating End System Network Configuration Documentation	
Guideline	Explanation
Determine the scope.	Find out exactly which end systems you are responsible for and focus your effort on those.
Know the objective.	Collect relevant data only. Make sure you provide sufficient detail but avoid extraneous information because that can make the documentation difficult to use.
Be consistent.	Use consistent terminology, abbreviations, and style. Make sure

	the documents are well organized and easy to understand. Use templates and keep a library of symbols and graphics icons that you can reuse.
Keep the documents accessible.	Store the network documentation in a location where it is readily available and accessible to the appropriate personnel on the job. Keep a copy of the documentation in a secure location off-site.
Maintain the documentation.	Modify your network documentation as conditions and devices in the network change. Keeping network documentation up to date is especially important.

QUESTION 89

When the Certkiller administrator documents the properties of a router; what kind of information is documented? (Choose all that apply.)

- A. IP address
- B. Processing type
- C. Device name
- D. IP routing protocols
- E. MAC address
- F. Interface cache

Answer: A, C, D, E

Explanation:

When documenting the properties of a router, the IP address, device name, IP routing protocols and MAC addresses of a router are all good because their values can change with subsequent network configurations and alterations and it is always good to have these addresses documented.

Incorrect Answers:

B, E: The processing type and the memory of the interface cache on the other hand don't

really need to be documented since these values are generally not vital networking information pieces.

QUESTION 90

What should you consider as a guideline for creating network documentation?

- A. Device discovery
- B. Interface discovery
- C. Security policy
- D. Maintenance schedule
- E. Consistent terminology

Answer: E

Explanation:

The guidelines for creating these types of documentation are described in the following table:

Guidelines for Creating End System Network Configuration Documentation	
Guideline	Explanation
Determine the scope.	Find out exactly which end systems you are responsible for and focus your effort on those.
Know the objective.	Collect relevant data only. Make sure you provide sufficient detail but avoid extraneous information because that can make the documentation difficult to use.
Be consistent.	Use consistent terminology, abbreviations, and style. Make sure the documents are well organized and easy to understand. Use templates and keep a library of symbols and graphics icons that you can reuse.
Keep the documents accessible.	Store the network documentation in a location where it is readily available and accessible to the appropriate

	personnel on the job. Keep a copy of the documentation in a secure location off-site.
Maintain the documentation.	Modify your network documentation as conditions and devices in the network change. Keeping network documentation up to date is especially important.

Reference: CCNP CIT Exam Certification Guide Page No. 20 Second Edition ISBN: 1-58720-081-3

QUESTION 91

If you wanted to create network documentation for general problem detection and correction, which of the following stages would you require?

- A. Fault analysis
- B. Budget allocation
- C. Network detection
- D. Interface discovery
- E. Security enforcement

Answer: D

Explanation:

The Interface Discovery stage is the second stage of the network documentation process as shown in the table below:

Table 1-6 Explanation for Each Stage of the Network Documentation Process

Stage	Description
1. Login	You must log in to the device and switch to the privileged mode; then you can type the commands necessary for network discovery.
2. Interface Discovery	Discover the necessary information about the device so that you can complete the network configuration table.
3. Document	Document/record the discovered information in the network configuration table and determine whether you need to record any of it in the network topology diagram. If you must record any information in the network topology diagram, proceed to Stage 4; otherwise, move to Stage 5.
4. Diagram	Transfer the necessary information about the device from the network configuration table to the network topology diagram. If you need to document more information about the device, return to Stage 2; otherwise, move to Stage 5.
5. Device Discovery	Determine whether any neighboring device is undocumented; if there is one, go to Stage 1. Otherwise, if there are no undocumented network devices, it means that network documentation is completed.

Reference: CCNP CIT Exam Certification Guide Page No. 19 Second Edition ISBN: 1-58720-081-3

QUESTION 92

What should you do to ensure good network documentation as devices and conditions on your network change? (Choose all that apply)

- A. Be consistent
- B. Keep the documents accessible
- C. Establish new baselines weekly
- D. Maintain the documentation
- E. Know your objective
- F. Document everything

Answer: A, B, D, E

Explanation:

The purpose of this section is to provide guidelines on creating good end system network configuration documentation. Good documentation provides up-to-date, sufficient, and accurate information about the end systems' network configuration. The guidelines are listed and explained in Table 2-9.

Table 2-9. Guidelines for Creating End System Network Configuration Documentation	
Guideline	Explanation
Determine the scope.	Find out exactly which end systems you are responsible for and focus your effort on those.

Know the objective.	Collect relevant data only. Make sure you provide sufficient detail but avoid extraneous information because that can make the documentation difficult to use.
Be consistent.	Use consistent terminology, abbreviations, and style. Make sure the documents are well organized and easy to understand. Use templates and keep a library of symbols and graphics icons that you can reuse.
Keep the documents accessible.	Store the network documentation in a location where it is readily available and accessible to the appropriate personnel on the job. Keep a copy of the documentation in a secure location off-site.
Maintain the documentation.	Modify your network documentation as conditions and devices in the network change. Keeping network documentation up to date is especially important. Note: Many organizations have deployed a formal process called change control. This process enforces reporting of network changes, maintaining version control, and assigning responsibility for modifying and distributing updated documents.

QUESTION 93

What should you remember to include when developing a document control plan for maintenance and distribution of your network documentation? (Choose three)

- A. Access documentation
- B. Correct syntax
- C. Security documentation
- D. Maintenance of the documentation
- E. Equipment inventory

Answer: B, C, D

Explanation:

Syntax is very important because the wording, terms, and nomenclature of the documentation needs to be consistent.

A problem that all networks experience at one time or another is forgotten passwords. It'd be wise, to have a book with all the passwords, but at the same time this password book needs to be secure so it can't get into the wrong hands.

Finally, network documentation needs to be maintained and updated whenever a change takes place.

QUESTION 94

You are in charge of the network documentation of the Certkiller network. Which of the following methods could you use to achieve maximum performance at minimal costs? (Choose two)

- A. Have the documentation stored offsite.
- B. Have the documentation stored near end-systems.
- C. Have the documentation stored near administrative systems.
- D. Ensure that the documentation is changed with system changes.
- E. Make available documentation that represents all network devices.

Answer: B, D

Explanation:

The purpose of this section is to provide guidelines on creating good end system network configuration documentation. Good documentation provides up-to-date, sufficient, and accurate information about the end systems' network configuration. The guidelines are listed and explained in Table 2-9.

Table 2-9. Guidelines for Creating End System Network Configuration Documentation	
Guideline	Explanation
Determine the scope.	Find out exactly which end systems you are responsible for and focus your

	effort on those.
Know the objective.	Collect relevant data only. Make sure you provide sufficient detail but avoid extraneous information because that can make the documentation difficult to use.
Be consistent.	Use consistent terminology, abbreviations, and style. Make sure the documents are well organized and easy to understand. Use templates and keep a library of symbols and graphics icons that you can reuse.
Keep the documents accessible.	Store the network documentation in a location where it is readily available and accessible to the appropriate personnel on the job. Keep a copy of the documentation in a secure location off-site.
Maintain the documentation.	Modify your network documentation as conditions and devices in the network change. Keeping network documentation up to date is especially important. Note: Many organizations have deployed a formal process called change control. This process enforces reporting of network changes, maintaining version control, and assigning responsibility for modifying and distributing updated documents.

QUESTION 95

How should administrator group information on a network configuration table for maximum efficiency and simplicity?

- A. OSI model
- B. Physical location
- C. Purpose
- D. IP address
- E. None of the above

Answer: A

Explanation:

We're taught to visualize how a network works by thinking in terms of the 7-layered OSI model, so it'd be natural to think of how a network can break using a layered approach. In order to maximize the efficiency and simplicity of the network table used during the documentation process, it is best to organize information based on the layers within the OSI model.

QUESTION 96

When should Network Topology Diagrams and Network Configuration Tables be updated?

- A. At the end of the year.
- B. Before making any changes.
- C. At the end of the day.
- D. At the time changes are applied.
- E. At the end of the month.

Answer: D

Explanation:

As the network undergoes changes, modify the network documentation accordingly to keep it accurate and up to date. It is best to always document these changes as they occur, rather than at a set time such as at the end of the day or week. This will ensure that no changes that were made will be forgotten and left undocumented.

Note: Many organizations have deployed a formal process called change control. This process enforces reporting of network changes, maintaining version control, and assigning responsibility for modifying and distributing updated documents

QUESTION 97

Which of the following components should an administrator include in a network device configuration table? (Choose three)

- A. Device name
- B. WINS server address

- C. DHCP server address
- D. Configured access lists
- E. MAC addresses
- F. DNS sever IP address
- G. Default gateway

Answer: A, D, E

Explanation:

Network configuration tables store accurate information about the hardware and software components of a network. Recording data into these tables, referring to these tables to look up information, and maintaining the accuracy of these tables are easier and more pleasant than using documentation that is composed of massive amounts of text and configuration printouts. Network configuration tables should hold essential information about the network devices and not be cluttered with unimportant data. The following is a list of important information that a network configuration table should include about each networking device:

1. Device name and model, as well as IOS name and version
2. Data link layer addresses and implemented features
3. Network layer addresses and implemented features
4. Important information about the physical aspects of the device
5. Other information that someone who is familiar with the network or has experience troubleshooting it considers important to the document

Layer	Information
Physical	CPU type Flash memory DRAM MAC address Media type Speed Duplex Trunk status
Data link	Device name Device model (+ IOS version) MAC address Duplex Port identifier STP status Port Fast Ether Channel Username/password

QUESTION 98

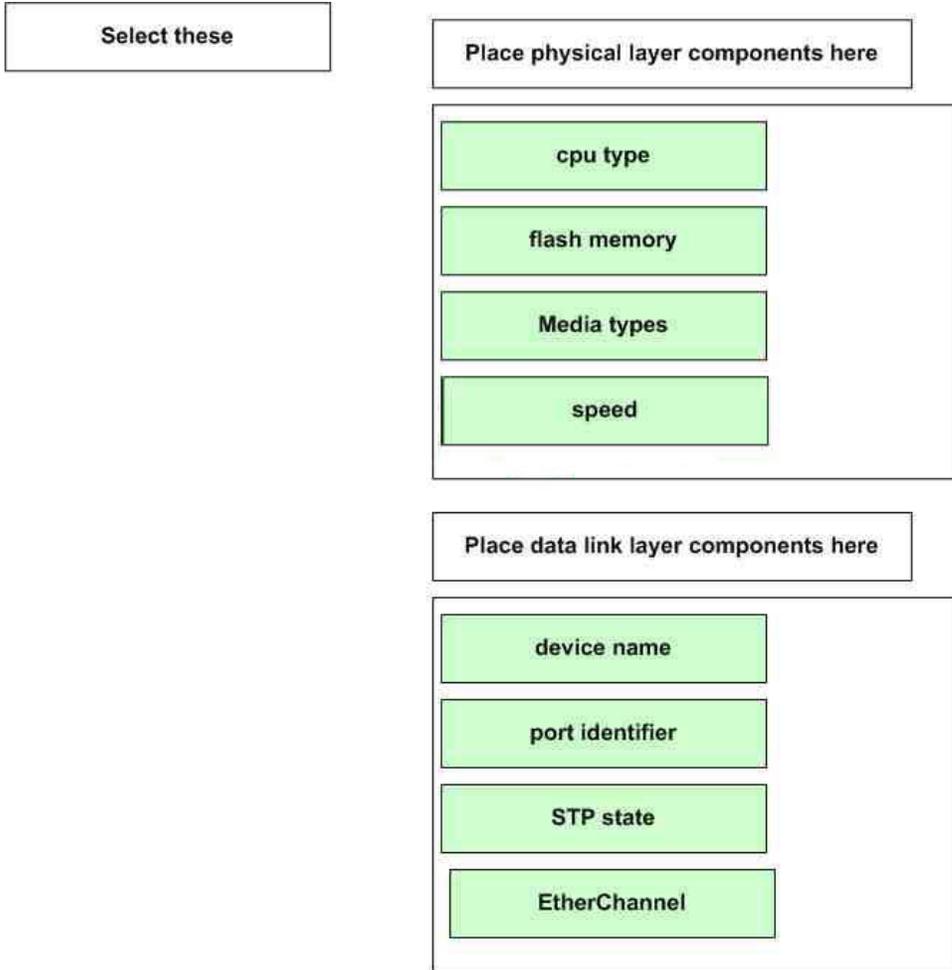
DRAG DROP

642-831

Drag and drop the troubleshooting components into their proper categories.

Select these	Place physical layer components here
device name	
speed	
port identifier	
cpu type	
STP state	Place data link layer components here
flash memory	
EtherChannel	
Media types	

Answer:



Explanation:

Table 1-2. Elements/Components of Network Configuration Table (Classified)

Layer	Information
Physical	CPU type Flash memory DRAM MAC address Media type Speed Duplex Trunk status
Data link	Device name Device model (+ IOS version) MAC address Duplex Port identifier STP status Port Fast

QUESTION 99

What is the first step the Certkiller network administrator should undertake when creating a network baseline?

- A. Determining the performance characteristics of networked applications
- B. Creating a network configuration inventory table
- C. Determining the scope of the administrator's domain responsibility
- D. Creating a network topology diagram.
- E. None of the above

Answer: B

Explanation:

A baseline is a process for studying the network at regular intervals to ensure that the network is working as designed. It is more than a single report detailing the health of the network at a certain point in time. The following describe the different steps in creating a network baseline:

Baseline Procedure

Step 1: Compile a Hardware, Software, and Configuration Inventory

Step 2: Verify that the SNMP MIB is supported in the Router

Step 3: Poll and Record Specific SNMP MIB Object from the Router

Step 4: Analyze Data to Determine Thresholds

Step 5: Fix Identified Immediate Problems

Step 6: Test Threshold Monitoring

Step 7: Implement Threshold Monitoring using SNMP or RMON

Reference: http://www.cisco.com/warp/public/126/HAS_baseline.html

QUESTION 100

You have been tasked with creating a network baseline for the Certkiller network. What is the rationale behind building a network baseline model?

- A. It is to determine if the current network status is approaching the breakpoint
- B. It is to find and resolve current network issues.
- C. It is to determine network traffic utilization between two and devices on the network
- D. It is to submit network devices and links to a stress test
- E. None of the above.

Answer: B

Explanation:

The elements of a network can be classified into two groups:

- Networking devices, such as routers and switches
- End systems, such as servers and workstations

The *network baseline* must include information on both of these groups. The network baseline and network configuration documentation can serve as a troubleshooting tool to diagnose a problem and, more importantly, to correct it. The network baseline information (about network devices) is recorded in network configuration tables and topology diagrams. These documents help to restore the network devices and components to their normal configuration, operation, and performance. This chapter identifies the components of a network configuration table and topology diagram, explains how to discover and record (document) network configuration information, and provides guidelines on best practices while creating network documentation.

Reference: CCNP CIT Exam Certification Guide Page No. 5 Second Edition ISBN: 1-58720-081-3

QUESTION 101

You are about to leave on vacation and you need to leave your junior administrator in charge of the network. Which document should you leave behind in order to help your junior save time learning the structure and configuration of the network and to have a guide to know normal network operations in case of a mishap?

- A. Design document
- B. Baseline document
- C. Network summary
- D. Design summary

Answer: B

Explanation:

A baseline is a process for studying the network at regular intervals to ensure that the network is working as designed. It is more than a single report detailing the health of the network at a certain point in time. By following the baseline process, you can obtain the following information:

- * Gain valuable information on the health of the hardware and software
- * Determine the current utilization of network resources
- * Make accurate decisions about network alarm thresholds
- * Identify current network problems
- * Predict future problems

Reference: Baseline Process: Best Practices White Paper Document ID: 15112

http://www.cisco.com/warp/public/126/HAS_baseline.html#what

QUESTION 102

What is the concept behind a 'self-healing network'?

- A. Embedding a network performance measurement agent in Cisco IOS software.
- B. Preventing interruptions to applications and end users after failures occur in the network.
- C. Analyzing network elements and attempting to predict failures and MTBF before failures occur.
- D. Distributing policy-based decision methodology which derives configurations and determines network behaviors.

Answer: B

Explanation:

A self-healing network is a concept used to describe putting a resilient, redundant network in place in order to minimize the impact to the end users. By eliminating single points of failures within the network and by utilizing redundant techniques, application uptime can be maximized. This term describes the concept of the network automatically routing traffic around single faults within the network, in a way that is transparent to the end users.

Incorrect Answers:

- A: This would describe an element of network management, not of a self healing network.
- C: This describes pro-active management.
- D: This refers to a network administrative policy.

QUESTION 103

In most applications, bandwidth utilization over _____% leads to intermittent failures.

- A. 80%
- B. 70%
- C. 60%
- D. 50%

Answer: B

Explanation:

When the short term average load on an Ethernet LAN passes the 70% threshold of the total bandwidth, a network will experience performance degradation as a result of more collisions and deferred transmissions. This in turn can easily consume the remainder of the bandwidth, and cause an intermittent failure. In addition, when utilization reaches this level, some TCP transmissions can become lost, which will lead to re-transmissions, which will lead to increased utilization. This is true for any network type.

QUESTION 104

You've been promoted to network help desk, and on your first day on the job you get a call from a user who's experiencing poor network performance when she browses the web and checks her email. You go to the user's workstation and you

ping other devices with intermittent success and failure messages along the way. You then issue a traceroute to the corporate Internet gateway and you notice high latency and occasional timeout messages. From what you know so far, what troubleshooting approach should you take?

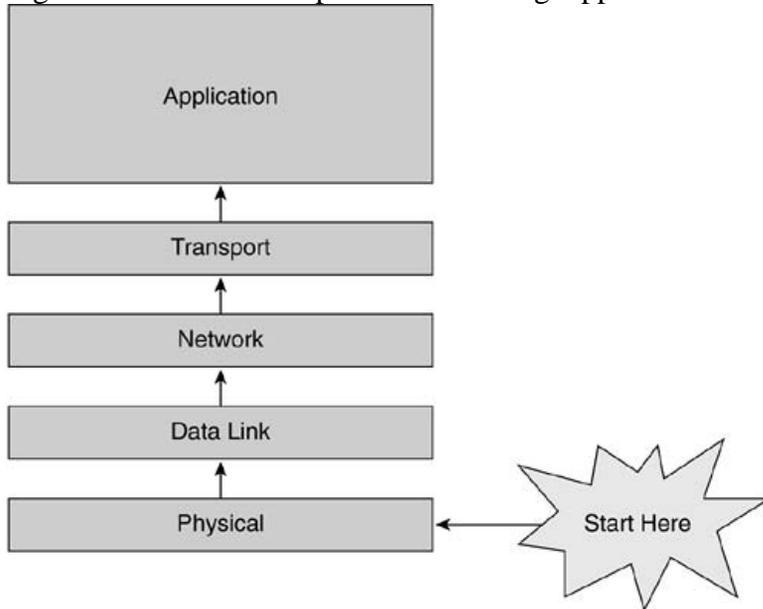
- A. bottom-up approach
- B. divide and conquer approach
- C. top-down approach
- D. random access approach

Answer: A

Explanation:

The bottom-up approach to troubleshooting a networking problem starts with the physical components of the network and works its way up the layers of the OSI model. If you conclude that all the elements associated to a particular layer are in good working condition, you inspect the elements associated with the next layer up until the cause(s) of the problem is/are identified. Figure 6-1 shows the bottom-up troubleshooting approach.

Figure 6-1. A Bottom-Up Troubleshooting Approach



Bottom-up troubleshooting is an effective and efficient approach for situations when the problem is suspected to be physical. Most networking problems reside at the lower levels, so implementing the bottom-up approach often results in effective and perhaps fast results. When faced with a complex troubleshooting case such as the one described in this question, the bottom-up approach is usually favored. That is because after you ascertain that the elements associated with a particular OSI layer are in good working condition, you can shift your focus on the next layer above, and so on, until you identify the faulty layer.

QUESTION 105

Which troubleshooting approach should you take if you suspect a problem with a

piece of physical media in the Certkiller network?

- A. Top-down
- B. Divide and conquer
- C. Bottom-up
- D. Isolate and solve
- E. Random

Answer: C

Explanation:

These problems are related to the physical layer (Layer 1) of the OSI reference model. This layer is located at the bottom of the OSI model, so it would make sense to start with this approach in order to find the root cause of the problem as quickly as possible.

QUESTION 106

The _____ approach to troubleshooting was used when the process begins with the issuing of the show controllers command.

- A. OSI troubleshooting
- B. Top-down
- C. Divide and conquer
- D. Bottom-up

Answer: D

Explanation:

The show controller command provides hardware-related information useful to troubleshoot and diagnose issues with Cisco router interfaces. Since this approach starts at the physical interface, this is a bottom up approach.

QUESTION 107

Which of the following devices/actions/tools can you use to gather facts before taking an action when managing and troubleshooting a network? (Choose three)

- A. Cable tester/protocol analyzer
- B. Network management systems
- C. Documented diagnostics commands
- D. Confirm your DHCP server configuration
- E. Review the entries in the hosts file on your server

Answer: A, B, C

Explanation:

- A: A protocol analyzer could be use to study network traffic.
- B: Network management systems, such as System Monitor in Windows 2000, can be

helpful in locating network performance issues.

C: IOS diagnostics commands can be useful in gathering network performance data.

Incorrect Answers:

D: The DHCP server does not impact network performance in any significant way. This choice would only apply if there was a specific problem with the DHCP settings or the server itself.

E: The hosts file is used for name resolution and does not normally impact the performance of a network.

QUESTION 108

When troubleshooting a problem on the Certkiller network; which problem should you deal with first?

- A. All problems simultaneously
- B. The least likely problem
- C. The most likely problem
- D. None of the choices.
- E. Based on user inputs

Answer: C

Explanation:

According to the technical documentation at CCO:

You should create an action plan based on the remaining potential problems. Begin with the most likely problem, and devise a plan in which only one variable is manipulated. Changing only one variable at a time enables you to reproduce a given solution to a specific problem. If you alter more than one variable simultaneously, you might solve the problem, but identifying the specific change that eliminated the symptom becomes far more difficult and will not help you solve the same problem if it occurs in the future. This troubleshooting method will resolve the problem in the most timely manner the majority of the time.

QUESTION 109

On a Cisco router; what kind of logging uses the LEAST amount of system overhead?

- A. Logging to the console
- B. Logging to a syslog server
- C. Logging to an internal buffer
- D. Logging to a dynamic buffer
- E. Logging to a virtual terminal over a WAN

Answer: C

Explanation:

Because debugging output is assigned high priority in the CPU process, it can render the

system unusable. For this reason, only use debug commands to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

Be aware that the debugging 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.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_command_reference_chapter09186a00800

7

QUESTION 110

You have been tasked with generating a solution template for the Certkiller network. When would it be wise to create a solution template?

- A. For low risk solutions that will be deployed more than once
- B. For low risk solutions that will be deployed once
- C. For high risk solutions that will be deployed more than once
- D. For high risk solutions that will be deployed once

Answer: C

Explanation:

Solution Templates

You can use solution templates to define standard modular network solutions. A network module may be a wiring closet, a WAN field office, or an access concentrator. In each case you need to define, test and document the solution to help ensure that similar deployments can be carried out in exactly the same way. This ensures that future changes occur at a much lower risk level to the organization since behavior of the solution is well defined.

Create solution templates for all higher-risk deployments and solutions that will be deployed more than once. The solution template contains all standard hardware, software, configuration, cabling, and installation requirements for the network solution. Specific details of the solution template are shown as follows:

1. Hardware and hardware modules including memory, flash, power, and card layouts.
2. Logical topology including port assignments, connectivity, speed, and media type.
3. Software versions including module or firmware versions.
4. All non-standard, non device-specific configuration including routing protocols, media configurations, VLAN configuration, access lists, security, switching paths, spanning tree parameters, and others.
5. Out-of-band management requirements.
6. Cable requirements.
7. Installation requirements including environmental, power, and rack locations.

Reference:

http://www.cisco.com/en/US/tech/CK8_69/CK7_69/technologies_white_paper09186a008014f924.shtml#topic8

QUESTION 111

When you issue a debug command on router CK1 you are inundated with messages. What could you do to minimize the output of a debug command?

- A. Apply an access list to contain the focus.
- B. Configure the router to run optimum switching.
- C. Only debug packets when using this command.
- D. Debug only received packets.
- E. Apply service timestamps to sort messages.

Answer: A

Explanation:

Access lists can be used to minimize debug output by filtering on appropriate conditions. This is an effective method for filtering out the unwanted information, and focusing on specific debug information. It is possible to use extended access lists so that only the debug output that is permitted by the access list will be seen.

QUESTION 112

A smart network trouble shooter will schedule a maintenance time window when they perform network troubleshooting. Why do they do this?

- A. To maximize potential business ROI
- B. To maximize potential business performance
- C. To minimize potential business impacts
- D. To maximize potential business efficiency
- E. To enhance network TCO (Total cost of ownership)

Answer: C

Explanation:

During the process of network troubleshooting, the network is expected to exhibit abnormal behavior. Therefore, it is always a good practice to set up a maintenance time window for troubleshooting to minimize any business impact. The window is normally after hours, so if anything goes wrong the impact to the end users is minimized or even eliminated. Always document any changes being made so that it is easier to back out if troubleshooting has failed to identify the problem within the maintenance window.

QUESTION 113

While logged into router CK1 , you wish to limit the amount of debug information that you see. What command could you use to filter debugging information on a particular interface? (Type in answer below)

Answer: debug list

Explanation:

According to the technical documentation at CCO:

To filter debugging information on a per-interface or per-access list basis, use the debug list privileged EXEC command. The no form of this command turns off the list filter. The debug list command is used with other debug commands for specific protocols and interfaces to filter the amount of debug information that is displayed. This is a good way to filter out the unwanted information, and to focus on specific debug information. It is possible to use extended access lists so that only the debug output that is permitted by the access list will be seen.

QUESTION 114

Under what circumstances would it be beneficial to debug events rather than packets?

- A. When you suspect that certain packets may be triggering multiple events
- B. When the "show cpu" command displays CPU utilization greater than 50%
- C. When the "show processes cpu" command displays CPU utilization greater than 50%
- D. When you experience an extremely slow response after entering a "debug all" command

Answer: C

Explanation:

Debugging specific events uses much less processor overhead than debugging all packets. If CPU utilization is greater than fifty percent, debugging the packets could put the processor on the verge of being overwhelmed.

Incorrect Answers:

- A: If this were true, simply debugging the packets alone would not allow you to correlate them to specific events.
- B: This is an invalid command. The correct syntax is "show processes cpu"
- D: It is normal for any production router to become extremely slow after issuing the debug all command. This command should never be used in a production environment as it will almost certainly cause problems due to the CPU load.

QUESTION 115

Debug commands are notorious for the heavy toll they take on network resources. You want to begin troubleshooting router CK1 using debugs due to some issues it has been having. When is a good time to start debug troubleshooting? (Select two)

- A. When network traffic is low.
- B. When there are fewer users.
- C. When traffic is operating normally.
- D. When the router is fast-switching mode.
- E. When protocol baselines need to be established.

Answer: A, B

Explanation:

Debug commands substantially lower a router's performance. Therefore they must be used selectively, properly, and temporarily. The debug command should be used during periods when network traffic is low and fewer critical business applications are active, i.e. few users are online. Ideally, it is done after hours when the service impact is the lowest.

QUESTION 116

You wish to increase the level of availability to the Certkiller end users on the network. What is the fundamental principle behind increasing a network's level of availability?

- A. Increase MTTR and increase MTBF.
- B. Increase MTTR and decrease MTBF.
- C. Decrease MTTR and increase MTBF.
- D. Decrease MTTR and decrease MTBF.

Answer: C

Explanation:

This question is very simple if you know the definitions of the acronyms.

MTTR stands for mean time to repair; the amount of time it'd usually take for an administrator to fix a down network. Assuming a network isn't functional while its being repaired, the faster you can fix a network problem, the more availability you'll have.

MTBF stands for mean time before failure; the amount of time a network can go before something fails. The longer you can go without a failure, the less a time a network has to be unavailable or repairs.

QUESTION 117

The _____ command can be used to verify router connectivity between the physical and application layers.

- A. Telnet
- B. Ping
- C. Trace
- D. FTP
- E. All of the above.

Answer: A

Explanation:

Telnet functions at the application layer of the OSI model.

Telnet is an IOS EXEC command used to verify the application layer software between source and destination and is the most complete test mechanism available. It is an

application that uses TCP port 23, so using the telnet program ensures connectivity all the way to layer 7.

Incorrect Answers:

B: The ping command uses ICMP packets and will only test through layer 3 (network layer).

C: The Trace route command uses UCP and will only ensure connectivity through layer 4 (transport layer).

D: Although FTP is also an application using TCP ports 20 and 21, Cisco routers use TFTP, not FTP so there is no way to connect to another router using FTP.

QUESTION 118

Router CK1 is configured as a DHCP server on the Certkiller network. Which command line would you use to report duplicate address assignments on CK1 ?

- A. debug ip dhcp server events
- B. show dhcp lease
- C. show ip dhcp binding
- D. debug chip

Answer: C

Explanation:

The show ip dhcp binding command displays address bindings on a DHCP server, and the show dhcp lease command lists the addresses leased from a server. The debug ip dhcp server events command reports DHCP server events, such as address assignments and database updates (the router is the DHCP server), and the debug ip dhcp server packets command reports on packet activities.

QUESTION 119

Router CK1 is being configured for IP multicast. The command _____ can be used to verify the IP routes contained in a multicast routing table?

- A. show ip mroute
- B. show ip route multicast
- C. show ip msdp sa-cache
- D. show ip route summary | include multicast

Answer: A

Explanation:

To display the contents of the IP multicast routing table, use the show ip mroute command in EXEC mode.

showip mroute [group-name | group-address] [source] [summary] [count] [active kbps]
Syntax Description

group-name group-address	(Optional) IP address, name, or interface of the multicast group as defined in the DNS hosts table.
source	(Optional) IP address or name of a multicast source.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the IP multicast routing table.
count	(Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bits per second.
active kbps	(Optional) Displays the rate that active sources are sending to multicast groups. Active sources are those sending at a rate of kbps or higher. The kbps argument defaults to 4.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_r/xrfscmd6.htm#wp1056899

QUESTION 120

Sometimes when troubleshooting, you will encounter two devices using the same IP address. Which command line could you use to determine whether or not duplicate IP addresses are in use? (Choose two)

- A. debug arp
- B. show ip traffic
- C. show ip protocol
- D. show ip arp/clear arp-cache

Answer: A D

Explanation: In order to find the duplicate IP addresses we should study the MAC to IP address mapping.

A: The debug arp command is used to the to display information on Address Resolution Protocol (ARP) transactions.

Sample output:

```
RouterCK# 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

D: The show ip arp command is used to display the Address Resolution Protocol (ARP) cache.

Sample output:

```
RouterCK# show ip arp
Protocol Address Age(min) Hardware Addr Type Interface
Internet 171.69.233.22 9 0000.0c59.f892 ARPA Ethernet0/0
Internet 171.69.233.21 8 0000.0c07.ac00 ARPA Ethernet0/0
Internet 171.69.233.19 - 0000.0c63.1300 ARPA Ethernet0/0
```

Incorrect Answers:

B: The show ip traffic is used to display statistics about IP traffic. It is not useful in this scenario.

C: The show ip commands display information about the configured and run-time IP parameters and IP routes. They can also show information about the status of the IP ARP cache and IP statistics. In particular, the show ip protocol command displays a summary of the configuration of each IP routing protocol.

Ensure that no two network devices are assigned the same IP address. If two network devices have the same IP address, you will encounter a duplicate IP address conflict, which will render one of your devices unusable.

QUESTION 121

You enter the following command on router CK1 :

```
show ppp multilink
```

What information can you expect to see?

- A. Bundle name
- B. Bundle flapping record
- C. Bundle idle time out
- D. Bundle disconnect reason
- E. None of the above

Answer: A

Explanation:

The show ppp multilink command displays information about the newly created multilink bundle which includes the bundle name.

Example:

The following is the output when a single Multilink PPP bundle (named Certkiller) is on a system:

```
Router# show ppp multilink
Bundle Certkiller , 3 members, first link is BRI0: B-channel 1
0 lost fragments, 8 reordered, 0 unassigned, sequence 0x1E/0x1E rcvd/sent
```

QUESTION 122

The telnet command is helpful tool in troubleshooting network connectivity. You

telnet to router CK1 from a remote host on the network. What can you conclude from this successful telnet connection?

- A. It gives a detailed view of information about the TCP/IP settings.
- B. It shows the path used to connect to a remote destination in a Windows environment.
- C. It shows that the TCP/IP protocol stack is available and functioning at the destination.
- D. It shows the information about the network configuration of an end-system.

Answer: C

Explanation:

Firstly, if you can telnet then you communicated via an application layer hence you do not have an application layer issue. Since the telnet program proves that there are no problems all the way to the application layer, the TCP/IP stack must also be functioning since the application relies on these lower layers in order to work.

QUESTION 123

The command _____ will let you know whether or not a router is receiving ARP requests and sending ARP replies.

- A. debug arp
- B. debug ip arp messages
- C. debug ip arp events
- D. debug ip arp packets
- E. debug ip arp

Answer: A

Explanation:

You should use the debug arp privileged EXEC command to display information on Address Resolution Protocol (ARP) transactions.

The following is sample output from the debug arp command:

Router CK1 # debug arp

IP ARP: sent req 172.16.22.7 0000.0c01.e117, dst 172.16.22.96 0000.0000.0000

IP ARP: rcvd rep 172.16.22.96 0800.2010.b908, dst 172.16.22.7

IP ARP: rcvd req 172.16.6.10 0000.0c00.6fa2, dst 172.16.6.62

IP ARP: rep filtered 172.16.22.7 aa92.1b36.a456, dst 255.255.255.255 ffff.ffff.ffff

IP ARP: rep filtered 172.16.9.7 0000.0c00.6b31, dst 172.16.22.7 0800.2010.b908

In the output, each line of output represents an ARP packet that the router sent or received.

Incorrect Answers:

B, C, D, E: These are all invalid commands. Note that the "show ip arp" command is valid, but not the "debug ip arp" command.

QUESTION 124

While troubleshooting a performance problem, your junior administrator isolated

the problem to above the data link layer. Assuming that it's a TCP/IP network, which command would you use to display information about TCP events like: retransmissions, duplicate packets, and state changes?

- A. debug ip tcp
- B. debug ip tcp packet access list
- C. show ip traffic
- D. debug ip tcp transactions

Answer: D

Explanation:

To display information on significant TCP transactions such as state changes, retransmissions, and duplicate packets, use the debug ip tcp transactions command in privileged EXEC mode. The following is sample output from the debug ip tcp transactions command:

```
Router# debug ip tcp transactions
TCP: sending SYN, seq 168108, ack 88655553
TCP0: Connection to 10.9.0.13:22530, advertising MSS 966
TCP0: state was LISTEN -> SYNRCVD [23 -> 10.9.0.13(22530)]
TCP0: state was SYNSENT -> SYNRCVD [23 -> 10.9.0.13(22530)]
TCP0: Connection to 10.9.0.13:22530, received MSS 956
TCP0: restart retransmission in 5996
TCP0: state was SYNRCVD -> ESTAB [23 -> 10.9.0.13(22530)]
TCP2: restart retransmission in 10689
TCP2: restart retransmission in 10641
TCP2: restart retransmission in 10633
TCP2: restart retransmission in 13384 -> 10.0.0.13(16151)]
TCP0: restart retransmission in 5996 [23 -> 10.0.0.13(16151)]
```

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801e9f2f.html

QUESTION 125

You've just entered the following command on router CK1 :

```
showclns neighbors
```

From this, you see that all of the neighbors in the output are in the INIT state.

What are three possible reasons why? (Choose three)

- A. Mismatched level 1 and level 2 interfaces.
- B. Mismatched MTU.
- C. Authentication problems.
- D. Incorrect IP subnet configuration.
- E. Transmitted hellos are being corrupted before reaching the neighbor(s).
- F. Duplicate system IDs in IS-IS area or backbone.
- G. This is the normal CLNS state.

Answer: B, C, E

Explanation:

An IS-IS adjacency can be in three different states, up, down, or INIT. If a neighbor is stuck in INIT there could be three possibilities:

The most common explanation is that the IS-IS authentication has been improperly configured. The next most common reason is an MTU (maximum transmission unit) mismatch between the two nodes. An MTU mismatch is shown in detail in this link:

http://www.cisco.com/warp/public/97/isis_mtu.html

The final cause could be that the hello packets are being corrupted. In such a scenario the command, debug isis adj-packets should be used to isolate the problem.

QUESTION 126

Which of the following Internet protocols can you use to discover all of the locally attached router addresses?

- A. IRDP
- B. IGMP
- C. UDP
- D. ICMP

Answer: A

Explanation:

IRDP: ICMP Router Discovery Protocol

ICMP Router Discovery Protocol (IRDP) enables a host to determine the address of a router that it can use as a default gateway. Similar to ES-IS but used with IP.

QUESTION 127

While conducting routine maintenance on router CK1 , you enter the "show buffers" command. To your surprise you notice a count of over runs. Where in the router would you most likely find the culprit of this problem?

- A. Shared NVRAM
- B. The router bus
- C. The route processor
- D. The processor
- E. The interface hardware

Answer: E

Explanation:

Overruns represent the number of times that the receiver hardware is unable to send received data to a hardware buffer because the input rate exceeds the receiver's ability to handle the data.

Reference:

http://www.cisco.com/en/US/products/ps5763/products_command_reference_chapter09186a00802a0172.html

QUESTION 128

The correspondence between network and LAN hardware addresses are kept in the ARP table. Which of the following show commands could you use to perform the following 2 functions?

1. Check whether or not the hosts are present in the table.
2. Check whether or not there are any duplicate addresses.

- A. show ip arp
- B. show ip addresses
- C. show ip hosts
- D. show ip interface
- E. show ip routes

Answer: A

Explanation:

The show ip arp command is used to display the Address Resolution Protocol (ARP) cache.

ARP establishes correspondences between network addresses (an IP address, for example) and LAN hardware addresses (Ethernet addresses). A record of each correspondence is kept in a cache for a predetermined amount of time and then discarded.

Examples

The following is sample output from the show ip arp command:

```
Router CK1 # show ip arp
```

```
Protocol Address Age(min) Hardware Addr Type Interface
Internet 171.69.233.22 9 0000.0c59.f892 ARPA Ethernet0/0
Internet 171.69.233.21 8 0000.0c07.ac00 ARPA Ethernet0/0
Internet 171.69.233.19 - 0000.0c63.1300 ARPA Ethernet0/0
Internet 171.69.233.30 9 0000.0c36.6965 ARPA Ethernet0/0
Internet 172.19.168.11 - 0000.0c63.1300 ARPA Ethernet0/0
Internet 172.19.168.254 9 0000.0c36.6965 ARPA Ethernet0/0
```

Incorrect Answers:

- B: The show ip route command is used to display IP routing table entries.
- C: The show ip protocol command displays the parameters and current state of the active routing protocols.
- D: The show ip interface command lists a summary of interface(s) IP information and status.

QUESTION 129

The following output was displayed on router CK1 :

```
-----  
Device ID: r6-2612  
Entry address(es):  
  IP address: 10.1.1.6  
Platform: cisco 2612, Capabilities: Router  
Interface: Serial0/1, Port ID (outgoing port): Serial0/1  
Holdtime : 147 sec  
  
Version :  
Cisco Internetwork Operating System Software  
IOS (tm) C2600 Software (C2600-JK9S-M), Version 12.2(3), RELEASE  
SOFTWARE (fcl)  
Copyright (c) 1986-2001 by Cisco Systems, Inc.  
Compiled Wed 18-Jul-01 15:28 by pwade  
  
advertisement version: 2
```

Which of the following commands is responsible for the output above? (Hint: it's used to troubleshoot data-link targets)

- A. show interfaces serial 0/1
- B. show cdp neighbor detail
- C. show interfaces serial 0/1 summary
- D. show cdp neighbor

Answer: B

Explanation:

The above output is from the show cdp neighbors detail command (although the entire command output isn't shown) and it is characterized by the presence of:

- * device name
- * device capabilities
- * hardware platform
- * port type and number
- * address

CCNP Support Exam Certification Guide, page 76, Amir S. Ranjibar, ISBN 0-7357-09955-5

QUESTION 130

While logged in to router CK1 you see "network unreachable" messages. Which of the following commands displays these messages seen by your router?

- A. debug ip packet
- B. debug ip icmp
- C. show ip events
- D. show ip statistics
- E. show ip rip

Answer: B

Explanation:

The debug ip icmp command is used to display information on Internal Control Message Protocol (ICMP) transactions. IP unreachable messages are used by ICMP.

Incorrect Answers:

A: This will not display unreachable messages.

B, C: In order to dynamically see the output in real time, a debug command must be issued, not a show command.

D: This command shows the aggregated TCP and UDP statistics of the unit, but not network unreachable messages.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a00800e9763.html#xto

QUESTION 131

While troubleshooting connectivity issues between your help desk location and a remote host, you get the remote user to send out a ping to your help desk computer. What command could you use to see the results of their ping?

- A. show icmp traffic
- B. debug icmp ip ping
- C. show icmp ip ping
- D. debug ip icmp
- E. None of the above

Answer: D

Explanation:

Use the "debug ip icmp" EXEC command to display information on Internal Control Message Protocol (ICMP) transactions. 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.

The following is sample output from the debug ip icmp command:

```
Router CK1 # 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
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
```

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_chapter09186a008007

QUESTION 132

Which of the following protocol is a layer 2, media independent, messaging protocol for Cisco devices to discover neighbors?

- A. ISL
- B. CDP
- C. VTP
- D. SPAN
- E. None of the above

Answer: B

Explanation:

Cisco Discovery Protocol (CDP) is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be used to show information about the interfaces your router uses. CDP is media and protocol-independent, and runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches.

Incorrect Answers:

A: ISL is the Inter Switch Link protocol, which is a trunking method used to pass VLAN information.

C: The VLAN Trunking Protocol (VTP) is a Layer 2 messaging protocol that manages the addition, deletion, and renaming of VLANs on a network-wide basis.

D: SPAN is the Switch Port Analyzer, which is used by switches to capture traffic for analysis, not for neighbor discovery.

QUESTION 133

Which of the following IOS commands could you use to check the characteristics of data-link functionality? (Choose three)

- A. traceroute
- B. show controller
- C. show ip route
- D. show cdp neighbor
- E. show interfaces
- F. ping
- G. tracert

Answer: B, D, E

Explanation:

The commands: show controller and show interface are all based on the data link layer (although a controller and an interface is a physical device). The command show cdp neighbor command is for checking the CDP (Cisco Discovery Protocol) which operates on the data link layer.

In some texts you'll read that the command show interfaces and show controllers are

associated with the physical layer. This is true, but these commands use the data link layer, to confirm the physical.

Incorrect Answers:

A, G. These commands are both trace routes, one is using the Cisco syntax, while choice G is the MS windows syntax, and they are used to verify connectivity up to the transport layer.

C: IP routing is a network layer function

F: The ping utility verifies connectivity though layer 3, the network layer.

QUESTION 134

While inspecting a Cisco 7000 series router name CK1 , you come to suspect a problem with the serial hardware. What show command would you use to confirm your suspicion?

- A. show hardware serial
- B. show serial hardware
- C. show controllers serial
- D. show serial controllers
- E. All of the above are acceptable

Answer: C

Explanation:

The show controllers serial command is used to display information that is specific to the interface hardware. This command also displays configuration information such as the framing, clock source, bandwidth limit, whether scrambling is enabled, the national bit, the international bits, and DSU mode configured on the interface. Also displayed are the performance statistics for the current interval and last 15-minute interval and whether any alarms exist.

Incorrect Answers:

A, B, D: There are no such commands.

QUESTION 135

While logged into router CK1 , you issue the "show interfaces serial" command.

What does this command accomplish? (Choose all that apply)

- A. It verifies that the ring is connected
- B. It verifies that the line protocol is up
- C. It views the router configuration
- D. It verifies that the ring is well connected
- E. It verifies the serial interface information

Answer: B, E

Explanation:

To display information about a serial interface, use the show interfaces serial command

in privileged EXEC mode. When using Frame Relay encapsulation, use the show interfaces serial command in user EXEC and privileged EXEC mode to display information about the multicast data-link connection identifier (DLCI), the DLCIs used on the interface, and the DLCI used for the Local Management Interface (LMI).

The following is sample output from the show interfaces serial command for a synchronous serial interface:

```
CK1 # show interfaces serial
Serial 0 is up, line protocol is up
Hardware is Certkiller Serial
Internet address is 192.168.10.203, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 0:00:07, output 0:00:00, output hang never
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 0 bits/sec, 0 packets/sec
16263 packets input, 1347238 bytes, 0 no buffer
Received 13983 broadcasts, 0 runts, 0 giants
2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
1 carrier transitions
22146 packets output, 2383680 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets, 0 restarts
```

Reference:

CCNP Support Exam Certification Guide, Amir S. Ranjibar, ISBN 0-7357-09955-5

QUESTION 136

From switch CK1 , You have entered the "show version" command and this is what you get:

```
Switch CK1 >show version
Cisco Internetwork Operating System Software
IOS(tm)C2950 Software(C2950-I6Q4L2-M), Version 12.1(11)EA1,
RELEASE SOFTWARE(fc1)
Copyright(c) 1986-2002 by cisco Systems, Inc.
Compiled Web 28-Aug-02 10:25 by antonino
Image text-base: 0x80010000, data-base: 0x80528000
ROM: Bootstrap program is CALHOUN boot loader
Switch uptime is 8 hours, 34 minutes
System returned to ROM by power-on
System image file is "flash:/c2950-i6q412-mz.121-11-EA1.bin"
cisco WS-C2950-24 (RC32300) processor (revision G0) with 20402K
bytes of memory.
Processor board ID FHK0645Z0TE
Last reset from system-reset
Running Standard Image
24 FastEthernet/IEEE 802.3 interface(s)
32K bytes of flash-simulated non-volatile configuration memory.
```

Base ethernet MAC Address: 00:0B:5F:4D:77:80
Motherboard assembly number: 73-5781-11
Power supply part number: 34-0965-01
Motherboard serial number: F0C064507AL
Power supply serial number: PHI0638059E
Model revision number: G0
Motherboard revision number: A0
Model number: WS-C2950-24
System serial number: FHK0645Z0TE
Configuration register is 0xF
Switch>

From the above command output, what can you determine about the switch configuration? (Choose all that apply.)

- A. Routing protocol version
- B. Model of the device
- C. MAC addresses of any interfaces or ports
- D. Spanning-tree version
- E. Installed memory
- F. Active routing protocol

Answer: B, C, E

Explanation:

The model number is mentioned twice in the command output:

Model number: WS-C2950-24

As is the amount and the type of installed memory:

cisco WS-C2950-24 (RC32300) processor (revision G0) with 20402K bytes of memory.

32K bytes of flash-simulated non-volatile configuration memory.

As is the address of the base Ethernet MAC address.

Base ethernet MAC Address: 00:0B:5F:4D:77:80

QUESTION 137

While troubleshooting data-link targets from one of the Certkiller routers you see the following output:

```
DeviceID: r6-2612
Entry address(es):
  IP address: 10.1.1.6
Platform: cisco 2612, Capabilities: Router
Interface: Serial0/1, Port ID (outgoing port): Serial0/1
Holdtime : 147 sec

Version :
Cisco Internetwork Operating System Software
IOS (m) C2600 Software (C2600-JK95-M), Version 12.2(3), RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 18-Jul-01 15:28 by pwade

advertisement version: 2
```

In regards to the last line:
advertisement version: 2
What is its significance?

- A. RIP advertisement version
- B. CDP advertisement version
- C. Cisco IOS mirror release version
- D. broadcast route summary version

Answer: B

Explanation:

The output shown in this example is the result of the "show cdp neighbor detail" command. The last line in this output indicates the version of CDP being used for CDP advertisements.

Reference: CDP Commands

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_r/frprt3/frd3001b.htm

QUESTION 138

What can you expect to achieve from debugging a serial line? (Choose all that apply)

- A. Provide diagnostic information relating to IP addresses
- B. Provide diagnostic information relating to protocol status
- C. Provide diagnostic information relating to station ID
- D. Provide diagnostic information relating to network activity

Answer: B, D

Explanation:

Debugging a serial line will ultimately tell you whether a protocol is up or down, and it

will give you information of what kind of traffic is going through the line.

Note: The output of the debug serial interface command can vary, depending on the type of WAN configured for an interface: Frame Relay, HDLC, HSSI, SMDS, or X.25. The output also can vary depending on the type of encapsulation configured for that interface. The hardware platform also can affect debug serial interface output.

Reference:

Please refer to the Cisco 606 Exam notes from examnotes.com for more information.

QUESTION 139

On the "netstat" command, what does the "-r" switch do when used at the end of the command (for example, netstat -r)?

- A. Reverse lookups on known network
- B. Faster response time, r stands for "right now"
- C. Shows routing table
- D. Shows remote networks

Answer: C

Explanation:

The netstat command is used to display the TCP/IP network protocol statistics and information.

SYNTAX:

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

-a	Displays all connections and listening ports.
-e	Displays Ethernet statistics. This may be combined with the -s option.
-n	Displays addresses and port numbers in numerical form.
-p	proto Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option to display per-protocol statistics, proto may be TCP, UDP, or IP.
-r	Displays the routing table.
-s	Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default.

interval	Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.
----------	---

EXAMPLES

netstat- displays all local network information. Below is an example of what may be displayed

Proto	Local Address	Foreign Address	State
TCP	hope:4409	www.computerhope.com:telnet	ESTABLISHED
TCP	hope:3708	multicity.com:80	CLOSE_WAIT
TCP	hope:4750	www.google.com:80	CLOSE_WAIT

Reference: <http://www.computerhope.com/netstat.htm#04>

QUESTION 140

You've just entered the following command on one of the Certkiller hosts:

ipconfig/all

What can you expect to see on your display from this?

- A. All Layer 3 information
- B. IP address and subnet mask only
- C. IP information for all interfaces, including IP address, subnet mask, DNS server, DHCP, and some NetBIOS information
- D. VLAN, MAC address, and ARP cache information.
- E. None of the above
- F. All of the above

Answer: C

Explanation:

It displays ip add. Subnet mask, dns and dhcp and net bios name from a end user system.

Below is an example of the output you should expect to see when running ipconfig /all:

```
Host Name . . . . . : Certkiller 1
DNS Servers . . . . . : 10.45.67.8
111.111.111.1
111.111.111.1
Node Type . . . . . : Broadcast
NetBIOS Scope ID. . . . . :
IP Routing Enabled. . . . . : No
```

WINS Proxy Enabled. : No
NetBIOS Resolution Uses DNS : No
0 Ethernet adapter :
Description : PPP Adapter.
Physical Address. : 44-44-44-54-00-00
DHCP Enabled. : Yes
IP Address. : 10.45.67.80
Subnet Mask : 255.255.0.0
Default Gateway : 10.45.67.1
DHCP Server : 255.255.255.255
Primary WINS Server :
Secondary WINS Server :
Lease Obtained. : 01 01 80 12:00:00 AM
Lease Expires : 01 01 80 12:00:00 AM

QUESTION 141

While pinging a Cisco 7513's loopback interface, you notice intermittent drops. What commands should you use to troubleshoot? (Choose two)

- A. show diag
- B. show buffers
- C. show version
- D. show interface

Answer: A, B

Explanation:

A loopback interface is an internal interface that is always up. The only explanation for the pings only working intermittently would be a problem with the router's hardware or will buffer overflow or leak problems.

A: The output of the show diag command displays hardware information for the router. The information can be used to troubleshoot the router.

B: You can identify a buffer leak using the show buffers command. A buffer leak could explain the behavior of the router.

Incorrect Answers:

C: The version of IOS is not an issue here.

D: No important information on the loopback interface would be gain by the show interface command. A loopback interface is always up and should reply to pings from the router itself at all times.

QUESTION 142

If you wanted to determine the current buffer statistics of router CK1 on the Certkiller network, which of the following commands should you NOT use? (Choose three)

- A. show stat buffers

- B. show buffer stat
- C. show buffers
- D. show buf enable

Answer: A, B, D

Explanation:

This command has been worded to confuse you. It basically asks you which command could you enter to see the statistics of the buffers. Since A,B, and D don't exist as IOS commands, you know that C is the correct answer.

The "show buffers" command will give you statistics on buffer elements, public buffer pools and interface buffer pools.

QUESTION 143

You enter this command on router CK1 during routine maintenance:

```
debugip packet
```

What kinds of information would you expect to see from this command? (Choose three)

- A. CDP packets
- B. Received packets
- C. Forwarded packets
- D. Generated packets
- E. Fast-switched packets

Answer: B, C, D

Explanation:

The debug ip packet command is used to display general IP debugging information and IP security option (IPSO) security transactions. IP debugging information includes packets received, generated, and forwarded.

Sample output:

```
Router CertK # debug ip packetIP: s=172.16.13.44 (Fddi0), d=10.125.254.1 (Serial2),  
g=172.16.16.2, forwardIP: s=172.16.1.57 (Ethernet4), d=10.36.125.2 (Serial2),  
g=172.16.16.2, forwardIP: s=172.16.1.6 (Ethernet4), d=255.255.255.255, rcvd 2IP:  
s=172.16.1.55 (Ethernet4), d=172.16.2.42 (Fddi0), g=172.16.13.6, forwardNote: This  
debug command is normally very CPU intensive, and should only be used with caution.
```

QUESTION 144

Your junior administrator is configuring the Certkiller ATM network. You glance into his monitor and you notice she just entered this command:

```
setport port-number loop internal
```

What will this command accomplish? (Choose all that apply)

- A. to check for network congestion
- B. to stop the loop

- C. to check the port at each end of the trunk
- D. to run remote loop
- E. to run an internal loop
- F. to start loopback test
- G. to perform bit rate check
- H. to perform port check

Answer: E, F

Explanation:

Run an internal loop on the port by entering the following at the cli> prompt:

```
cli> set port <port#> loop internal
```

where <port#> is the port you want to loop. The port number is in card.port format (card = 2 - 10; port = 0 - 7).

The CLI automatically sets the administrative status of the selected port to testing and starts the loopback test. If the internal loop fails and the line does not come up, you have isolated the problem to the line or access card.

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps1893/products_maintenance_guide_chapter09186a008007

QUESTION 145

Which command would you enter if you wanted to view some detailed statistics on a routers CPU usage? (Type in answer below)

Answer: show processes cpu

Explanation:

According to the technical documentation at CCO:

The show processes command displays information about the active processes. Use the show processes cpu command to display detailed cpu utilization statistics on these processes and the show processes memory command to show the amount of memory used.

QUESTION 146

You enter the command "show process cpu" command on router CK1 and this is what you see:

CPU utilization for five seconds: 51%/50%; one minute: 47%; five minutes; 46%

What is the significance of the 50% phrase in the (51%/50%)?

- A. The percentage of the CPU used by CLI routines is 50%.
- B. The percentage of the CPU used by interrupt routines is 50%.
- C. The percentage of the CPU used by process routines is 50%.
- D. The percentage of the CPU used by memory routines is 50%.

Answer: B

Explanation:

This is an example of the header of the show processes cpu command:

CPU utilization for five seconds: X%/Y%; one minute: Z%;

five minutes: W%

PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process

This table describes the fields in the header:

Field	Description
X	Average total utilization during last five seconds (interrupts + processes)
Y	Average utilization due to interrupts, during last five seconds ¹
Z	Average total utilization during last minute ²
W	Average total utilization during last five minutes ²
PID	Process ID
Runtime	CPU time the process has used (in milliseconds)
Invoked	Number of times a process has been called
uSecs	Microseconds of CPU time for each invocation
5Sec	CPU utilization by task in the last five seconds
1Min	CPU utilization by task in the last minute ²
5Min	CPU utilization by task in the last five minutes ²
TTY	Terminal that controls the process
Process	Name of process

¹CPU utilization on process level = X - Y

²Values do not represent an arithmetical average, but an exponentially decayed average.

Thus, more recent values have more influence on the calculated average.

Reference:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a00800a70f2.shtml#show_pr
o

QUESTION 147

When you implement the debug listcommand, you can specify some optional interface type arguments. Which of the following arguments are NOT valid for this command?

- A. parallel
- B. serial
- C. tokenring
- D. fddi
- E. tunnel
- F. Ethernet
- G. null
- H. channel

Answer: A

Explanation:

To filter debugging information on a per-interface or per-access list basis, use the debug list privileged EXEC command. The optional Interface type argument allows the following values:

channel-IBM Channel interface

ethernet-IEEE 802.3

fddi-ANSI X3T9.5

null-Null interface

serial-Serial

tokenring-IEEE 802.5

tunnel-Tunnel interface

There are no options for parallel in the debug, which makes sense since Cisco routers do not support parallel interface.

QUESTION 148

CORRECT TEXT

The following output was displayed on router CK1 :

Minimum process stacks:

Free/Size Name

652/1000 Router Init

726/1000 Init

744/1000 BGP Open

686/1200 Virtual Exec

What command was entered to produce the above output? (Type in answer below):

Answer: show stacks

Explanation:

The show stacks command monitors the stack utilization of processes and interrupt routines. Its display includes the reason for the last system reboot. If the system was

reloaded because of a system failure, a saved system stack trace is displayed. This information can be useful for analyzing crashes in the field.

QUESTION 149

Which of the following commands could you enter to view a routers routing table?

- A. show ip rt-table
- B. show route
- C. show ip stat
- D. show ip route
- E. All of the above

Answer: D

Explanation:

The full command syntax is shown here:

```
showip route [address {mask}] | [protocol {process - id}]
```

This command displays the current state of the routing table. It displays all routes all known networks, from all routing protocol sources, including the directly connected interfaces.

Reference:

CCNP Support Exam Certification Guide, page 164, Amir S. Ranjibar, Cisco Press 2001
ISBN 0-7357-09955-5

Incorrect Answers:

A, B, C: These are invalid Cisco IOS commands.

QUESTION 150

CORRECT TEXT

Which command could you enter to show the names and sources of the configuration files, the system hardware, and the software version of your router?
(Type in answer below):

Answer: show version

Explanation:

According to the technical documentation at CCO:

To display the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images, use the show version EXEC command. It also displays much more additional information, such as the interfaces contained within the device, as well as the system uptime.

QUESTION 151

Why would a network troubleshooter use the command "show running-config"?

- A. To verify that the interface is up
- B. To verify that the line protocol is up

- C. To verify that the ring is well connected
- D. To verify that the ring is connected
- E. To view the router configuration

Answer: E

Explanation:

The show running config command shows the configuration file that the router is currently running. This show running-config command won't tell you the status of the interface or line, and if it's used on a router connected to a token ring or FDDI it won't say anything about the ring status. This command is used to display the current router configuration, not the saved startup configuration.

QUESTION 152

You believe that there may be an issue with the Spanning Tree Protocol (STP) in the Certkiller network. What command could you use to see whether or not a switch's spanning-tree hello frames are being properly exchanged?

- A. debug span-tree
- B. debug stp
- C. debug spanningtree
- D. debug spanning-tree
- E. None of the above

Answer: D

Explanation:

To debug spanning tree activities, use the debug spanning-tree command.

The full command syntax is displayed below:

```
debug spanning-tree {all | bpdu | bpdu-opt | etherchannel | config | events | exceptions |  
general| pvst+ | root | snmp}
```

Syntax Description

all	Displays all spanning tree debugging messages.
bpdu	Debugs spanning tree BPDU.
bpdu-opt	Debugs optimized BPDU handling.
etherchannel	Debugs spanning tree EtherChannel support.
config	Debugs spanning tree configuration changes.
events	Enables TCAM event debugging.
exceptions	Debugs spanning tree exceptions.
general	Debugs general spanning tree activity.

pvst+	Debugs PVST+ events.
root	Debugs spanning tree root events.
snmp	Debugs spanning tree SNMP events.

Incorrect Answers:

A, B, C: These are all invalid Cisco IOS commands.

QUESTION 153

You enter the following command onto your Cisco Catalyst 5000 switch:

showspan

What are you going to see as a result of it?

- A. The ISL trunks attached to the switch.
- B. The designated root bridge and priority.
- C. The spanning-tree settings on the switch.
- D. The switch port being used by a packet analyzer.

Answer: D

Explanation:

The show span command is used to display information about the current SPAN (Switched Port Analyzer) configuration. The information includes SPAN source port and SPAN destination port.

Example output:

```
Certkiller > (enable) show spanStatus : enabledAdmin Source : Port 2/1Oper Source : Port 2/1Destination : Port 2/12Direction : transmit/receiveIncoming Packets:
```

disabled Certkiller > (enable)Incorrect Answers:

- A: Attached ISL trunks are not shown.
 - B: The designated root bridge is not displayed.
 - C: The spanning tree settings are not shown. This is confusing the "show span" command with the "show spanning-tree" command.
-

QUESTION 154

What command could you use to display the amount of memory being used by router processes? (Type in answer below)

Answer: show processes memory

Explanation:

The show processes command displays information about the active processes. Use the "show processes cpu" command to display detailed CPU utilization statistics on these processes and the "show processes memory" command to show the amount of memory used.

QUESTION 155

Which command could you use to display a ports STP state?

- A. show STP
- B. show port states
- C. show STP port
- D. show port spantree
- E. None of the above

Answer: D

Explanation:

Use the show port spantree command to view port spanning tree information.

Examples:

This example shows how to display spanning tree information on a specific module:

Console> (enable) show port spantree 5

Port(s) Vlan Port-State Cost Prio Portfast Channel_id

```
-----  
5/1 1 not-connected 2684354 32 disabled 0  
5/2 1 not-connected 2684354 32 disabled 0
```

QUESTION 156

Router CK1 is using RIP as the routing protocol. What debug command could you use to check the way RIP is working on CK1 ?

- A. Debug ip
- B. Debug rip
- C. Debug ip rip
- D. Debug rip ip
- E. All of the above

Answer: C

Explanation:

Use the debug ip rip EXEC command to display information on RIP routing transactions.

The following is sample output from the "debug ip rip" command:

```
router# debug ip rip  
Updates received from this source address  
----- RIP: received update from 160.89.80.28 on Ethernet0  
160.89.95.0 in 1 hops  
160.89.81.0 in 1 hops  
160.89.66.0 in 2 hops  
131.108.0.0 in 16 hops (inaccessible)  
0.0.0.0 in 7 hop  
Updates sent to these two destination addresses  
----- RIP: sending update to 255.255.255.255 via Ethernet0 (160.89.64.31)  
subnet 160.89.94.0, metric 1  
131.108.0.0 in 16 hops (inaccessible)  
----- RIP: sending update to 255.255.255.255 via Serial1 (160.89.94.31)  
subnet 160.89.64.0, metric 1  
subnet 160.89.66.0, metric 3  
131.108.0.0 in 16 hops (inaccessible)  
default 0.0.0.0, metric 8
```

The output shows that the router being debugged has received updates from one router at source address 160.89.80.28. That router sent information about five destinations in the

routing table update. Notice that the fourth destination address in the update-131.108.0.0-is inaccessible because it is more than 15 hops away from the router sending the update. The router being debugged also sent updates, in both cases to broadcast address 255.255.255.255 as the destination.

QUESTION 157

You have a Cisco Catalyst 5000 switch and you want to capture some packets for troubleshooting. What command could you use to view mirroring one port to an alternative destination port?

- A. Show span
- B. Show slan
- C. View span
- D. Show plan
- E. Show spanning

Answer: A

Explanation:

To get a summary of the current SPAN configuration, just use the show span command:

Example:

```
Certkiller 1 (enable) show span
```

```
Destination : Port 6/2
```

```
Admin Source : Port 6/1
```

```
Oper Source : Port 6/1
```

```
Direction : transmit/receive
```

```
Incoming Packets: disabled
```

```
Learning : enabled
```

```
Multicast : enabled
```

```
Filter : -
```

```
Status : active
```

```
Total local span sessions: 1
```

QUESTION 158

Which command could you use to see the operations of a trunk port on a switch?

- A. Show trunkport
- B. Show trunk
- C. Show t port
- D. Show trunk-port

Answer: B

Explanation:

To verify the VLAN trunk configuration, enter the show trunk command.

The show trunk command is used to verify the trunking status and configuration.

Example:

```
cat4000> (enable) show trunk
```

```
* - indicates vtp domain mismatch
```

```
# - indicates dot1q-all-tagged enabled on the port
```

```
Port Mode Encapsulation Status Native vlan
```

```
-----  
5/1 desirable dot1q trunking 1
```

```
Port Vlans allowed on trunk
```

```
-----  
5/1 1-1005,1025-4094
```

```
Port Vlans allowed and active in management domain
```

```
-----  
5/1 1-2
```

```
Port Vlans in spanning tree forwarding state and not pruned
```

```
-----  
5/1 1-2
```

```
cat4000> (enable)
```

QUESTION 159

CORRECT TEXT

What command would you use if you do NOT want router error messages logged to a syslog server host? (Type in answer below)

Answer: no logging on

Explanation:

The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, terminal lines, or a syslog server. System logging messages are also known as system error messages. You can turn logging on and off for these destinations individually using the logging buffered, logging monitor, and logging global configuration commands. However, if the logging on command is disabled, no messages will be sent to these destinations. Only the console will receive messages. Additionally, the logging process logs messages to the console and the various destinations after the processes that generated them have completed. When the logging process is disabled, messages are displayed on the console as soon as they are produced, often appearing in the middle of command output.

QUESTION 160

In a Catalyst switch, which of the following commands is equivalent to "show running-config"?

- A. run config
- B. sh run conf
- C. running conf
- D. show config

Answer: D

Explanation:

To display the running configuration, use the show running-config command. A compatible command, normally used in switches running Catalyst OS, is the "show config" command which will also display the non-default configuration that is currently running on the device.

Incorrect Answers:

A: This is an invalid Cisco IOS command

B: This is invalid, due to the space between the "run" and the "conf". If this command was used, the IOS would say that the command is invalid after the first letter in the word "Conf."

C: This is an invalid command.

QUESTION 161

You want to see when router CK1 was last booted. What command would you use to display your routers current uptime?

- A. Show status
- B. Show current
- C. Show conf
- D. Show version

Answer: D

Explanation:

The show version command displays the image type, version number, and function sets that identify the exact software that is running on your router. Also displayed is the current configuration register setting as well as the system hardware components.

QUESTION 162

Which command could you use (other than show buffers pool) to view the source of IOS buffer leaks? (Type in answer below)

Answer: show buffers old

Explanation:

Use the following commands to pinpoint the source of the buffer leak:

```
showbuffers old
```

```
showbuffers pool [pool name] [header]
```

Because buffer leaks are Cisco IOS Software bugs, try upgrading to the latest version in your release train to fix known buffer leak bugs (for example, if you are running Cisco IOS Software release 11.2(14), upgrade to the latest 11.2(x) image).

To display statistics for the buffer pools on the network server, use the show buffers command in EXEC mode.

```
show buffers [{address hex-address | failures | pool pool-name | {all | assigned | free | old
```

| input-interface interface-type interface-number } [pool pool-name]} [dump | header | packet]]

Syntax Description

address hex-address	(Optional) Displays buffers at a specified address. Specify address in hexadecimal notation.
failures	(Optional) Displays buffer allocation failures.
pool pool-name	(Optional) Displays buffers in a specified buffer pool.
all	(Optional) Displays all buffers.
assigned	(Optional) Displays the buffers in use.
free	(Optional) Displays the buffers available for use.
old	(Optional) Displays buffers older than one minute.
input-interface interface-type interface-number	(Optional) Displays interface pool information. If an interface type is specified and this interface has its own buffer pool, information for that pool is displayed.
dump	(Optional) Displays the buffer header and all data.
header	(Optional) Displays the buffer header only.
packet	(Optional) Displays the buffer header and packet data.

QUESTION 163

While logged into router CK1 , you enter the following command:

```
telnet 10.10.10.1 2003
```

This accomplishes which of the following?

- A. Initiates a reverse telnet connection to vty 3.
- B. Initiates a reverse telnet connection to line 2.
- C. Initiates a reverse telnet connection to line 3.
- D. Initiates a reverse telnet session to TTY 2003.
- E. Initiates a telnet to the host using TCP port 2003

Answer: C

Explanation:

For a reverse telnet session, following the IP address enter the number 2000 + the line number you want to connect to.

To establish a reverse Telnet session, determine the IP address of your LAN (Ethernet) interface, then enter a Telnet command to port 2000 + n on the access server, where n is the line number to which the modem is connected. For example, to connect to the modem attached to line 1, enter the following command from an EXEC session on the access server:

```
router# telnet 172.16.1.10 2001
Trying 172.16.1.10, 2001 ... Open
```

QUESTION 164

You've just finished modifying your routers configuration and want to make the changes permanent. What command would you use to write your new configuration to NVRAM?

- A. Write nvram
- B. Write memory
- C. Save config
- D. Save memory

Answer: B

Explanation:

You need to write the settings to NVRAM, or you will lose them when you reset the router. To save the currently running router configuration to the startup-configuration, use the "write memory" command.

Note: The "write memory" command is now obsolete and has been replaced by the "copy running-config startup-config" command. The "write memory" command, however, is still supported for backward compatibility.

QUESTION 165

The CEO of your company has installed a new computer game that needs Jumbo Frame Feature support, so he's asked you to stay in a few hours longer to configure the network device. Which command could you use to look at the MTU size of a link?

- A. show ip arp
- B. show ip route
- C. show ip traffic
- D. show ip protocol
- E. show ip interface

Answer: E

Explanation:

The show ip interface command shows a great deal of information, including the

following:

1. Interface Status
2. IP address & subnet mask
3. Broadcast address
4. MTU (maximum transmission unit)
5. IP helper address setting
6. Outgoing/incoming access list settings
7. IP Proxy ARP setting
8. ICMP status
9. Status of IP fast switching
10. Router Discovery Setting

QUESTION 166

Which of the following TCP/IP utilities gives you hop by hop information?

- A. Traceroute
- B. Ping
- C. Netstat
- D. Nstat

Answer: A

Explanation:

Ping is for testing network reachability, and will not give you hop by hop details. Traceroute will display the IP address or name of each hop, as well as the latency between the hops. The following displays is an example:

```
CK1 #trace10.165.202.130
```

```
Type escape sequence to abort.
```

```
Tracing the route to 10.165.202.130
```

```
 1 172.18.124.40 0 msec 0 msec 4 msec
```

```
 2 192.168.200.241 12 msec 8 msec 96 msec
```

```
 3 10.165.202.130 104 msec 8 msec *
```

QUESTION 167

While performing a traceroute to a host on the Internet, you see a series of "P" replies. In a trace output, what does the letter P signify?

- A. The port is unreachable.
- B. The PSTN is unreachable.
- C. The packet is unreachable.
- D. The protocol is unreachable.
- E. None of the above

Answer: D

Explanation:

In Cisco routers, the codes for a traceroute command reply are the following:

- ! -- success
- * -- time out
- N -- network unreachable
- H -- host unreachable
- P -- protocol unreachable
- A -- admin denied
- Q -- source quench received (congestion)
- ? -- unknown (any other ICMP message)

Reference:

<http://www.cisco.com/en/US/products>

QUESTION 168

While performing a traceroute to a host on the Internet from the Certkiller network, you see a series of "Q" replies. In a trace output, what does the letter Q signify?

- A. Source quench
- B. Network unreachable
- C. Port unreachable
- D. For each node, the round-trip time in milliseconds for the specified number of probes.
- E. Unknown packet type
- F. The probe timed out
- G. Protocol unreachable
- H. Host unreachable

Answer: A

Explanation:

When using the traceroute command, a "Q" indicates a source quench packet is received, meaning that the end host is experiencing congestion at the moment. In Cisco routers, the codes for a traceroute command reply are the following:

IP Trace Text Characters

Char	Description
nn msec	For each node, the round-trip time in milliseconds for the specified number of probes.
*	The probe timed out.
?	Unknown packet type.
Q	Source quench.
P	Protocol unreachable.
N	Network unreachable.

U	Port unreachable.
H	Host unreachable.

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps1893/products_command_reference_chapter09186a00800

QUESTION 169

In a trace output, what do the letters U & H signify?

- A. Protocol unreachable
- B. Host unreachable
- C. Port unreachable
- D. Source quench
- E. Unknown packet type
- F. The probe timed out
- G. For each node, the round-trip time in milliseconds for the specified number of probes.
- H. Network unreachable

Answer: B, C

Explanation:

In Cisco routers, the codes for a traceroute command reply are the following:

IP Trace Text Characters

Char	Description
nn msec	For each node, the round-trip time in milliseconds for the specified number of probes.
*	The probe timed out.
?	Unknown packet type.
Q	Source quench.
P	Protocol unreachable.
N	Network unreachable.
U	Port unreachable.
H	Host unreachable.

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps1893/products_command_reference_chapter09186a00800

QUESTION 170

In a trace output, what does the symbol, "*" signify?

- A. Unknown packet type
- B. Protocol unreachable
- C. Source quench
- D. The probe timed out

- E. For each node, the round-trip time in milliseconds for the specified number of probes.
- F. Host unreachable
- G. Network unreachable
- H. Port unreachable

Answer: D

Explanation:

In Cisco routers, the codes for a traceroute command reply are the following:
IP Trace Text Characters

Char	Description
nn msec	For each node, the round-trip time in milliseconds for the specified number of probes.
*	The probe timed out.
?	Unknown packet type.
Q	Source quench.
P	Protocol unreachable.
N	Network unreachable.
U	Port unreachable.
H	Host unreachable.

QUESTION 171

In a trace output, what does the letter N signify?

- A. Protocol unreachable
- B. Host unreachable
- C. The probe timed out
- D. Source quench
- E. Unknown packet type
- F. Network unreachable
- G. Port unreachable
- H. For each node, the round-trip time in milliseconds for the specified number of probes.

Answer: F

Explanation:

In Cisco routers, the codes for a traceroute command reply are the following:
IP Trace Text Characters

Char	Description
nn msec	For each node, the round-trip time in milliseconds for the specified number of probes.

*	The probe timed out.
?	Unknown packet type.
Q	Source quench.
P	Protocol unreachable.
N	Network unreachable.
U	Port unreachable.
H	Host unreachable.

QUESTION 172

From a Cisco device, you want to trace the route to the Certkiller .com server. When executing the 'trace' command, what are the two optional parameters? (Choose two)

- A. Trace
- B. None
- C. Protocol
- D. Destination

Answer: C, D

Explanation:

Use the traceroute EXEC command to discover the IP routes the switch's packets actually take when traveling to their destination.

The full command is:

traceroute [protocol] [destination]

Syntax Description

protocol	(Optional) Protocol that can be used is ip.
destination	(Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed, and the tracing action begins.

Default

The protocol argument is based on the switch's examination of the format of the destination argument. For example, if the switch finds a destination in IP format, the protocol defaults to ip.

QUESTION 173

The trace command has two parameters:

trace[protocol] [destination]

What is true about the destination parameter? (Choose all that apply)

- A. This is required
- B. Can be an address only
- C. This is Optional
- D. Can be an address or a host name

Answer: C, D

Explanation:

Use the traceroute EXEC command to discover the IP routes the switch's packets actually take when traveling to their destination.

The full command is:

traceroute [protocol] [destination]

Syntax Description

protocol	(Optional) Protocol that can be used is ip.
destination	(Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed, and the tracing action begins.

Default

The protocol argument is based on the switch's examination of the format of the destination argument. For example, if the switch finds a destination in IP format, the protocol defaults to IP.

QUESTION 174

From one of the Certkiller routers, you've entered the ping command as shown below:

Router_ Certkiller #pingProtocol [ip]:Target IP address: 192.168.40.1Repeat count [5]:Datagram size [100]:Timeout in seconds [2]:Extended commands [n]: y

When prompted for the extended commands you enter 'Y', option will appear next to continue?

- A. Yes
- B. Verbose
- C. Sweep range
- D. Source address
- E. Destination address

Answer: D

Explanation: You enter the source address (or interface)

Sample output:

```
Router_ Certkiller # ping Protocol [ip]: Target IP address: 192.168.40.1 Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y Source address or interface: 172.16.23.2 Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]: Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 162.108.21.8, timeout is 2 seconds:!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 36/97/132 ms Router_ Certkiller #
```

Reference: Using the Extended ping and Extended traceroute Commands
http://www.cisco.com/warp/public/105/ext_ping_trace.html

QUESTION 175

You are experiencing difficulty reaching network devices from specific hosts, or subnets. How can you specify the source address to assist troubleshooting?

- A. Router# ping
- B. Router> ping
- C. Router> ping 1.1.1.1 2.2.2.2
- D. Router# ping 1.1.1.1 2.2.2.2

Answer: A

Explanation:

In privileged exec mode you have the option of using the extended ping. From the privileged mode, if you just enter the ping command, you will be prompted for the protocol (default is IP). After selecting IP, you are prompted for the target IP address, repeat count, datagram size, and timeout in seconds; finally, you are asked if you are interested in extended commands.

Example:

```
Router_ Certkiller # ping Protocol [ip]: Target IP address: 192.168.40.1 Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y Source address or interface: 172.16.23.2 Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]: Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 162.108.21.8, timeout is 2 seconds:!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 36/97/132 ms
```

QUESTION 176

From a Certkiller router, you issue an extended ping to a remote host. Which of the following are options that can be specified when using the extended ping command? (Choose all that apply)

- A. Ping with long bits
- B. The number of successive pings
- C. An option that looks for increasing input errors
- D. An option that indicates hardware problems

Answer: B

Explanation:

The Extended ping Command

When a normal **ping** command is sent from a router, the source address of the **ping** is the IP address of the interface that the packet uses to exit the router. If an extended **ping** command is used, the source IP address can be changed to any IP address on the router. The extended **ping** is used to perform a more advanced check of host reachability and network connectivity. The extended **ping** command works only at the privileged EXEC command line. The normal ping works both in the user EXEC mode and the privileged EXEC mode. To use this feature, enter ping at the command line and press "Return". You are prompted for the following fields as given in the next section.

Field	Description
Protocol [ip]:	Default is IP.
Target IP address:	Prompts for the IP address or host name of the destination node you plan to ping.
Repeat count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Datagram size [100]:	Size of the ping packet (in bytes). Default: 100 bytes.
Timeout in seconds [2]:	Timeout interval. Default: 2 (seconds).
Extended commands [n]:	Specifies whether a series of additional commands appears. Many of the following displays and tables show and describe these commands. Default: no.
Source address:	IP address that appears in the ping packet as the source address.
Type of service [0]:	Internet service quality selection. See RFC 791 for more information. Default: 0.
Set DF bit in IP header?	Don't Fragment. Specifies that if the packet encounters a node in its path that is configured for a smaller MTU than the packet's MTU, that the packet is to be dropped and an error message is to be sent to the router at the packet's source address. If performance problems are encountered on the network, a node configured for a small MTU could be a contributing factor. This feature can be used to determine the smallest MTU in the path. Default: no.
Data pattern [0xABCD]:	Sets 16-bit hexadecimal data pattern. Default: 0xABCD. Varying the data pattern in this field (to all ones or all zeros for example) can be useful when debugging data sensitivity

	problems on CSU/DSUs, or detecting cable-related problems such as cross talk.
Loose, Strict, Record, Timestamp, Verbose [none]:	Supported Internet header options. The Cisco IOS software examines the header options to every packet that passes through it. If it finds a packet i h i lid i h f

Reference: Using the Extended ping and Extended traceroute Commands
http://www.cisco.com/warp/public/105/ext_ping_trace.html

QUESTION 177

What kind of ICMP packet types do pings use? (Choose two)

- A. Echo Requests
- B. Echo Replies
- C. TTL-Exceeded
- D. Unreachable

Answer: A, B

Explanation:

The two types of packets used by ICMP are echo and echo replies.

Informational Messages:

ICMP Information Message	Type Field value	Code Field value	Description
Echo Request Message	128	0	Used to check and troubleshoot connectivity using the ping command.
Echo Reply Message	129	0	This message is generated in response to an echo request message.

QUESTION 178

When troubleshooting an MTU problem, what options in the extended ping utility should you use? (Choose two)

- A. Data pattern
- B. Type of Service
- C. Sweep range of sizes
- D. MTU size of interface
- E. Set DF bit in IP header

Answer: C, E

Explanation:

C: The Sweep range of sizes option allows you to vary the size of the packets. This can be useful when troubleshooting a MTU problem.

E: The Set DF bit in IP header option specifies whether or not the Don't Fragment (DF) bit is set on the ping packet. This is useful for checking the MTU along the path to a destination.

The Extended ping Command

When a normal ping command is sent from a router, the source address of the ping is the IP address of the interface that the packet uses to exit the router. If an extended ping command is used, the source IP address can be changed to any IP address on the router. The extended ping is used to perform a more advanced check of host reachability and network connectivity. The extended ping command works only at the privileged EXEC command line. The normal ping works both in the user EXEC mode and the privileged EXEC mode. To use this feature, enter ping at the command line and press "Return". You are prompted for the following fields as given in the next section.

Field	Description
Protocol [ip]:	Default is IP.
Target IP address:	Prompts for the IP address or host name of the destination node you plan to ping.
Repeat count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Datagram size [100]:	Size of the ping packet (in bytes). Default: 100 bytes.
Timeout in seconds [2]:	Timeout interval. Default: 2 (seconds).
Extended commands [n]:	Specifies whether a series of additional commands appears. Many of the following displays and tables show and describe these commands. Default: no.

642-831

Source address:	IP address that appears in the ping packet as the source address.
Type of service [0]:	Internet service quality selection. See RFC 791 for more information. Default: 0.
Set DF bit in IP header?	Don't Fragment. Specifies that if the packet encounters a node in its path that is configured for a smaller MTU than the packet's MTU, that the packet is to be dropped and an error message is to be sent to the router at the packet's source address. If performance problems are encountered on the network, a node configured for a small MTU could be a contributing factor. This feature can be used to determine the smallest MTU in the path. Default: no.
Data pattern [0xABCD]:	Sets 16-bit hexadecimal data pattern. Default: 0xABCD. Varying the data pattern in this field (to all ones or all zeros for example) can be useful when debugging data sensitivity problems on CSU/DSUs, or detecting cable-related problems such as cross talk.
Loose, Strict, Record, Timestamp, Verbose [none]:	Supported Internet header options. The Cisco IOS software examines the header options to every packet that passes through it. If it finds a packet i h i lid i h f

Reference: Using the Extended ping and Extended traceroute Commands

http://www.cisco.com/warp/public/105/ext_ping_trace.html

Incorrect Answers:

A: Different data patterns are used to troubleshoot framing errors and clocking problems on serial lines.

B: TOS is not useful here.

D: There is no such option.

QUESTION 179

You have a series of pings running to a host from router CK1 but you want to stop this session prematurely. What keyboard escape sequence would you enter on a Cisco router if you wanted to abort a ping session?

A. Ctrl + Alt + 6

B. Ctrl + Alt + Del

- C. Ctrl + Shift + 6
- D. Ctrl + Shift + Del
- E. Ctrl + Break
- F. All of the above are acceptable

Answer: C

Explanation:

To abort a ping session, type the escape sequence. By default, this is Ctrl-^ X. You enter this by simultaneously pressing the Ctrl, Shift, and 6 keys, letting go, and then pressing the X key.

QUESTION 180

You are able to successfully ping the IP address of a web server but not the corresponding hostname. What is the likely cause of such a problem? (Choose all that apply.)

- A. Misspelled hostname
- B. Corrupted ARP
- C. Misspelled IP address
- D. DNS server problem
- E. None of the above

Answer: A, D

Explanation:

When you can ping an IP but not the name, the problem has to be a name resolution problem.

QUESTION 181

You want to verify IPSec connectivity through a tunnel with a ping command, so you enter:

```
Router#ping 172.16.1.100
```

And you notice the initial echo replies are unsuccessful:

Type escape sequence to abort.

```
Sending 5. 100-bute ICMP Echos to 172.16.1.100, timeout is 2 seconds:
```

```
..!!!
```

```
Success rate is 60 percent (3/5), round-trip min/avg/max = 72/72/72 ms
```

Which is a possible cause for this?

- A. Slow WAN link
- B. Mismatched transform sets
- C. Time delay in establishing security associations
- D. Incorrectly configured access control list on remote peer

Answer: C

Explanation:

The first two pings were unsuccessful, but the last three were all successful. Extra security means extra overhead to process, so the first two unsuccessful pings represent the time delay in establishing the proper security associations. After the initial IPsec tunnel was established, traffic was able to traverse over the secure link. The next series of ping requests should be successful immediately after the tunnel is established.

Incorrect Answers:

A: If the link was slow, the pings would still be successful, but the latency time would be increased. Even the slowest link will be able to have ICMP traffic traverse it within the ping timeout value of 2 seconds.

B: If this were the case, the security associations would never be established, and no traffic would cross the link.

D: If this were the case, then all of the ICMP traffic would be filtered, not just the first two packets.

QUESTION 182

Reverse telnet is not functioning on router CK1, which is a Cisco access server. What command will enable this feature?

- A. transport input telnet
- B. transport output all
- C. modem dialin
- D. modem inout
- E. Reverse telnet is enable by default

Answer: A

Explanation:

Cisco routers do not accept incoming network connections to asynchronous ports (TTY lines) by default. You have to specify an incoming transport protocol, or specify transport input all before the line will accept incoming connections. For example, if you are using your router as a terminal server to make console-port connections to routers or other devices, you will not be able to use Telnet to connect to these devices. You will receive the message "Connection Refused."

transportinput - Used to define which protocols to use to connect to a specific line of the router.

* transportinput {all | lat | mop | nasi | none | pad | rlogin | telnet | v120}

o all- Selects all protocols.

o none- Prevents any protocol selection on the line. This makes the port unusable by incoming connections.

o none- Prevents any protocol selection on the line. This makes the port unusable by incoming connections.

Note: In our configuration example, the async lines use the minimum configuration of

transport input telnet so you can Telnet to the devices on the async line.
telnet - This EXEC command is used to login to a host that supports Telnet.

QUESTION 183

You work as a network technician at Certkiller .com. An ISDN connection is currently not functioning. You have already verified that communications between the router and the Central Office switch is performing correctly and that the router is attempting to dial, although the call seems to be disconnecting. Which command can you use to provide information on the ISDN call status and display the reason for the call disconnect?

- A. show isdn status
- B. debug isdn q921
- C. debug isdn q931
- D. show isdn service

Answer: C

Since it was already reported that the router is able to communicate with the ISDN provider's CO, we know that layers 1 and 2 are working properly. Since this is the case, we need to only determine the reason for calls becoming disconnected. The best way to do this is with the "debug isdn q931" command.

The debug isdn q931 command output shown below indicates the disconnect cause code from a failed ISDN call.

Calling#ping 10.10.10.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:

20:52:14: ISDN BR0: TX -> SETUP pd = 8 callref = 0x2E

20:52:14: Bearer Capability i = 0x8890

20:52:14: Channel ID i = 0x83 20:52:14: Keypad Facility i = '5551111'

20:52:15: ISDN BR0: RX <- CALL_PROC pd = 8 callref = 0xAE

20:52:15: Channel ID i = 0x89

20:52:16: ISDN BR0: RX <- PROGRESS pd = 8 callref = 0xAE

20:52:16: Progress Ind i = 0x8A81 - Call not end-to-end ISDN,
may have in-band info

20:52:16: Signal i = 0x01 - Ring back tone on

20:52:34: ISDN BR0: RX <- DISCONNECT pd = 8 callref = 0xAE

20:52:34: Cause i =0x829F08 - Normal,unspecified or Special intercept,
call blocked group restriction

20:52:34: ISDN BR0: TX -> RELEASE pd = 8 callref = 0x2E

20:52:34: ISDN BR0: RX <- RELEASE_COMP pd = 8 callref = 0xAE

The 0x in the disconnect code indicates the bytes that follow are in hexadecimal format and is not part of the actual code. After stripping the 0x from the debug output, see the table below for a breakdown of the code in the example above.

Cause i =			0x829F08
Parsed Hex Bytes	82	9F	08

Description	Cause Code Origination Point	Disconnect Cause Code	Optional Diagnostic field
-------------	------------------------------------	--------------------------	------------------------------

Reference:

http://www.cisco.com/en/US/tech/CK801/CK379/technologies_tech_note09186a008012e95f.shtml

QUESTION 184

On the Certkiller network, you suspect that two devices are configured with the same IP address. Which command can display system messages that indicate the presence of duplicate IP addresses on network devices?

- A. show logging
- B. show interfaces
- C. show IP routing
- D. show IP protocols

Answer: A

Explanation:

Of the following choices, only the "show logging" command will inform us of any known duplicate IP addresses.

Note: Alternatively, the "show arp" or "show ip arp" commands could be used to determine the presence of a duplicate IP address.

Example logging output detecting a duplicate IP address:

```
*Mar 1 00:04:44.039: %IP-4-DUPADDR: Duplicate address 172.27.32.114 on Ethernet 0, sourced by 00e0.1e3e.2d41
```

QUESTION 185

Exhibit

```
CertKiller41(config)# interface vlan 11
CertKiller41(config-if)# no shut
*Mar 1 00:16:41.295: %SYS-5-CONFIG_I: Configured from console by console
*Mar 1 00:16:43.095: %LINK-3-UPDOWN: Interface Vlan11, changed state to up
*Mar 1 00:16:43.099: SB: V111 Interface up
*Mar 1 00:16:43.099: SB11: V111 Init: a/HSRP enabled
*Mar 1 00:16:43.099: SB11: V111 Init: →Listen
*Mar 1 00:16:41.295: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:16:41.295: SB11: V111 Listen: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar 1 00:16:41.295: SB11: V111 Listen → Speak
*Mar 1 00:16:44.187: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 1 00:16:44.187: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:16:43.363: SB11: V111 Speak: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar 1 00:16:44.363: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 1 00:16:44.363: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:16:44.495: SB11: V111 Speak: d/Standby timer expired (unknown)
*Mar 1 00:16:44.623: SB11: V111 Standby router is local
*Mar 1 00:16:44.623: SB11: V111 Speak → Standby
```

You work as a network administrator at Certkiller .com. You are attempting to

enable Certkiller 41 as the active router in an HSRP configuration. However, upon enabling Certkiller 41, you notice that Certkiller 42 still maintains the active role. Give the debug output shown in the exhibit, why does this happen?

- A. Certkiller 42 has a higher priority
- B. Certkiller 42 has a higher IP address
- C. Certkiller 41 is not configured with pre-empt.
- D. Certkiller 41 is not configured under the same standby group.
- E. Certkiller 41 does not have the IP address of the virtual router.

Answer: C

QUESTION 186

You work as a network administrator at Certkiller .com. An ISDN connection is not working correctly. You want to use bottom up Layer 2 troubleshooting to verify that the router is building an ISDN connection is able to communicate with the ISDN switch.

Which command will show real time events at Layer 2?

- A. show isdn neighbor
- B. debug isdn q921
- C. debug isdn q931
- D. show isdn events

Answer: B

QUESTION 187

Exhibit

```
Certkiller13#show frame-relay map
Serial0/0 (up): ip 10.10.10.2 dlci 102(0x66,0x1860), dynamic,
                Broadcast,, status defined, active

Certkiller13# show interface s0/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 10.10.10.10/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  LMI enq sent 404, LMI stat recvd 400, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
  LMI DLCI 1023 LMI type is CISCO frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 3/0, interface broadcasts 0
  Last input 00:00:03, output 00:00:03, output hang never
  Last clearing of "show interface" counters 01:10:06
  Input queue: 0/75/1/0 (size/max/drops/flushes); Total output drops: 0
```

<Output Omitted>

Study the exhibit carefully. Certkiller 13 is unable to ping Certkiller 14.
What is the most likely cause of this problem?

- A. the shut down of the Certkiller 14 Frame Relay interface
- B. incorrect IP address
- C. incorrect Frame Relay encapsulation configured
- D. incorrect DLCI configured
- E. incorrect keepalive setting configured
- F. incorrect LMI set

Answer: B

QUESTION 188

Router Certkiller 1 is attempting to form an ISDN connection. All attempts have failed.

Which debug command will verify the phone number being called by Router Certkiller 1?

- A. debug isdn q921
- B. debug q921
- C. debug isdn q931
- D. debug isdn tgrm

Answer: C

QUESTION 189

Exhibit

Certkiller31# debug ppp negotiation

PPP protocol negotiation debugging is on

Certkiller31#

```
*Mar 1 00:06:36.645: %LINK-3-UPDOWN: Interface BR10:1, changed state to up
*Mar 1 00:06:36.661: BR0:1 PPP: Treating connection as a callin
*Mar 1 00:06:36.661: BR0:1 PPP: Phase is ESTABLISHING, Passive Open [0 sess, 0 load]
*Mar 1 00:06:37.098: BR0:1 LCP: I state is Listen
*Mar 1 00:06:37.102: BR0:1 LCP: CONFREQ [Listen] id 7 len 17
*Mar 1 00:06:37.038: BR0:1 LCP: AuthProto FAP (0x0304C023)
*Mar 1 00:06:37.042: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
*Mar 1 00:06:37.046: BR0:1 LCP: Callback 0 (0x0D0300)
*Mar 1 00:06:37.054: BR0:1 LCP: O CONFREQ [Listen] id 4 len 15
*Mar 1 00:06:37.058: BR0:1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.062: BR0:1 LCP: MagicNumber 0x1081E7E1 (0x05061081E7E1)
*Mar 1 00:06:37.066: BR0:1 LCP: O CONFREQ [Listen] id 7 len 7
*Mar 1 00:06:37.070: BR0:1 LCP: Callback 0 (0x0D0300)
*Mar 1 00:06:37.098: BR0:1 LCP: I CONFACK [REQsent] id 4 len 15
*Mar 1 00:06:37.102: BR0:1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.106: BR0:1 LCP: MagicNumber 0x1081E7E1 (0x05061081E7E1)
*Mar 1 00:06:37.114: BR0:1 LCP: I CONFREQ [ACKrcvd] id 8 len 14
*Mar 1 00:06:37.117: BR0:1 LCP: AuthProto FAP (0x0304C023)
*Mar 1 00:06:37.121: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
*Mar 1 00:06:37.125: BR0:1 LCP: O CONFNAK [ACKrcvd] id 8 len 9
*Mar 1 00:06:37.129: BR0:1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.165: BR0:1 LCP: I CONFREQ [ACKrcvd] id 9 len 15
*Mar 1 00:06:37.169: BR0:1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.173: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
*Mar 1 00:06:37.177: BR0:1 LCP: O CONFACK [ACKrcvd] id 9 len 15
*Mar 1 00:06:37.181: BR0:1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.185: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
*Mar 1 00:06:37.189: BR0:1 LCP: State is Open
*Mar 1 00:06:37.193: BR0:1 PPP: Phase is AUTHENTICATING, by both [0 sess, 0 load]
You work as a network administrator at Certkiller .com. Study the exhibit carefully.
You are troubleshooting a PPP connection between a local and remote router. You
enter the following command at the local router: debug ppp negation
Given the output, which statement is true?
```

- A. The local router is configured to authenticate with PAP or CHAP.
- B. The remote router is configured to authenticate with PAP or CHAP.
- C. The local router is configured to authenticate with PAP only.
- D. The remote router is configured to authenticate with CHAP only.
- E. The two devices were not able to agree on an authentication protocol.

Answer: B

QUESTION 190

Which show command can be used to determine if a DTE or DCE cable has been attached to a serial interface?

- A. show interface serial
- B. show interface brief
- C. show controller serial
- D. show ip interface

Answer: C

QUESTION 191

Exhibit

```
Certkiller28# debug crypto isakmp
Crypto ISAKMP debugging is on
Certkiller28#
00:59:19: ISAKMP (0): received packet from 192.168.192.2 (N) NEW SA
00:59:19: ISAKMP: local port 500, remote port 500
00:59:19: ISAKMP (0:1): processing SA payload. message ID = 0
00:59:19: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 100 policy
00:59:19: ISAKMP: encryption DES-SR
00:59:19: ISAKMP: hash Sh
00:59:19: ISAKMP: default group 1
00:59:19: ISAKMP: auth pre-share
00:59:19: ISAKMP (0:1): atts are acceptable. Next payload is 0
00:59:19: ISAKMP (0:1): SA is doing pre-shared key authentication
00:59:19: ISAKMP (1): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
00:59:19: ISAKMP (1): sending packet to 192.168.192.2 (R) MM_SA_SETUP
00:59:19: ISAKMP (1): received packet from 192.168.192.2 (R) MM_SA_SETUP
00:59:19: ISAKMP (0:1): processing KE payload. message ID = 0
00:59:19: ISAKMP (0:1): processing NONCE payload. message ID = 0
00:59:19: ISAKMP (0:1): SKEYID state generated
00:59:19: ISAKMP (0:1): processing vendor id payload
00:59:19: ISAKMP (0:1): speaking to another IOS box!
00:59:19: ISAKMP (1): sending packet to 192.168.192.2 (R) MM_KEY_EXCH
00:59:20: ISAKMP (1): received packet from 192.168.192.2 (R) MM_KEY_EXCH
00:59:20: ISAKMP: reserved not zero on payload ID!
00:59:20: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 192.168.192.2 failed its sanity check
00:59:20: ISAKMP (0:1): incrementing error counter on sa: PAYLOAD_MALFORMED
00:59:20: ISAKMP (1): sending packet to 192.168.192.2 (R) MM_KEY_EXCH
00:59:20: ISAKMP (0:1): incrementing error counter on sa: reset_retransmission
00:59:21: ISAKMP (0:1): retransmitting phase 1 MM_KEY_EXCH...
00:59:21: ISAKMP (0:1): incrementing error counter on sa: retransmit phase 1

<Output Omitted>
```

You work as a network administrator at Certkiller .com. Study the exhibit carefully. An IPsec connection has failed between Certkiller 28 and Certkiller 29. What is the most likely cause of the problem?

- A. The hash methods do not match.
- B. The Diffie-Hellman group settings do not match.
- C. Pre-shared keys do not match.
- D. There is an invalid peer address.

Answer: C

QUESTION 192

Exhibit:

```
BR0:1 CHAP: I CHALLENGE id 17 len 33 from " Certkiller12562 "
BR0:1 CHAP: Username Certkiller12562 not found
BR0:1 CHAP: Unable to authenticate for peer
BR0:1 PPP: Phase is TERMINATING
```

You work as a network administrator at Certkiller .com. While troubleshooting a PPP connection between a local and a remote router, you enter the following command on the local router:

debugppp authenticate

Give the output displayed in the exhibit, which statement is true?

- A. The global command username Certkiller 12562 password password must be configured on the local router.
- B. The global command username Certkiller 12562 password password must be configured on the remote router.
- C. The interface command ppp chap hostname Certkiller 12562 must be configured on the local router.
- D. The local router is not configured for CHAP authentication.
- E. The remote router is not configured for CHAP authentication.

Answer: A

QUESTION 193

Exhibit, Network Topology



Exhibit, show interfaces

```
Certkiller1# show interfaces s0/1
Serial0/1 is up, line protocol is up
Hardware is PowerQUICC Serial
Internet address is 172.17.1.1/30
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open
Listen: CDPCP
Open: IPCP, loopback not set
Keepalive set (10 sec)
Last input 00:00:01, output 00:00:02, output hang never
Last clearing of "show interface" counters 00:45:43
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
  Conversations 0/2/32 (active/max active/max total)
  Reserved Conversations 0/0 (allocated/max allocated)
  Available Bandwidth 96 kilobits/sec
5 minute input rate 0 bits/ sec 0 packets/sec
5 minute output rate 0 bits/ sec 0 packets/sec
708 packets input, 54670 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
710 packets output, 55689 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
4 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

Certkiller1#

You work as a network administrator at Certkiller .com. Study the exhibit carefully. Certkiller 1 can ping the serial interface of Certkiller 2, but Certkiller 2 does not appear in the CDP neighbor table of Certkiller 1.

Why is this the case?

- A. incomplete NCP negotiation between Certkiller 1 and Certkiller 2.
- B. link encapsulation mismatch between Certkiller 1 and Certkiller 2
- C. incomplete PPP authentication between Certkiller 1 and Certkiller 2
- D. subnet mask mismatch between Certkiller 1 and Certkiller 2
- E. incomplete LCP negotiation between Certkiller 1 and Certkiller 2

Answer: A

QUESTION 194

Which Cisco IOS feature allows a network administrator to manipulate the BGP AS Path attribute?

- A. a prefix list
- B. an access list
- C. a distribute list
- D. a route map

Answer: D

QUESTION 195

Exhibit

```
Certkiller42#debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
Certkiller42#show interfaces s0/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 10.10.101/29
  MTU 1500 bytes: BW 128 kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive not set
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 5/0, interface broadcasts 0
  Last input 00:01:23, output 00:00:13, output hang never
  Last clearing of "show interface" counters 00:55:19
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
  5 minute, input rate 0 bits/sec, 0 packets/sec
  5 minute, input rate 0 bits/sec, 0 packets/sec
    116 packets input, 1850 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
    142 packets output, 2780 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    212 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up
Certkiller42#
```

You work as a network administrator at Certkiller .com. Study the exhibit carefully. Certkiller 42 is unable to establish a Frame Relay connection with Certkiller 43. The

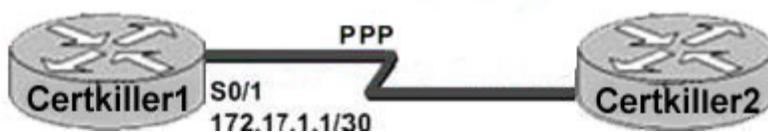
debug frame-relay lmi output reveals no activity.
What is the cause of this problem?

- A. an interface is shut down
- B. an incorrect IP address
- C. an incorrect Frame Relay encapsulation configured
- D. an incorrect DLCI configured
- E. an incorrect keepalive setting configured
- F. an LMI that is disabled.

Answer: E

QUESTION 196

Exhibit, Network Topology



Exhibit, debug ppp negotiation

```
*Mar 1 01:30:05.675: Se0/1 PPP: Using default call direction
*Mar 1 01:30:05.675: Se0/1 PPP: Treating connection as a dedicated line
*Mar 1 01:30:05.675: Se0/1 PPP: Phase is ESTABLISHING, Active Open
*Mar 1 01:30:05.675: Se0/1 LCP: O CONFREQ [Closed] id 5 len 10
*Mar 1 01:30:05.675: Se0/1 LCP: MagicNumber 0x03BDE87E (0x050603BDE87E)
*Mar 1 01:30:05.679: Se0/1 LCP: I CONFREQ [REQsent] id 3 len 10
*Mar 1 01:30:05.679: Se0/1 LCP: MagicNumber 0x03BE21C2 (0x050603BE21C2)
*Mar 1 01:30:05.679: Se0/1 LCP: O CONFACK [REQsent] id 3 len 10
*Mar 1 01:30:05.679: Se0/1 LCP: MagicNumber 0x03BE21C2 (0x050603BE21C2)
*Mar 1 01:30:05.683: Se0/1 LCP: I CONFACK [ACKsent] id 5 len 10
*Mar 1 01:30:05.683: Se0/1 LCP: MagicNumber 0x03BDE87E (0x050603BDE87E)
*Mar 1 01:30:05.679: Se0/1 LCP: State is Open
*Mar 1 01:30:05.679: Se0/1 LCP: Phase is FORWARDING, Attempting Forward
*Mar 1 01:30:05.683: Se0/1 LCP: Phase is ESTABLISHING, Finish LCP
*Mar 1 01:30:05.683: Se0/1 PPP: Phase is UP
*Mar 1 01:30:05.687: Se0/1 IPCP: O CONFREQ [Closed] id 1 len 10
*Mar 1 01:30:05.687: Se0/1 IPCP: Address 172.17.1.1 (0x0306AC110101)
*Mar 1 01:30:05.687: Se0/1 PPP: Process pending ncp packets
*Mar 1 01:30:05.691: Se0/1 IPCP: I CONFREQ [REQsent] id 1 len 10
*Mar 1 01:30:05.691: Se0/1 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 1 01:30:05.691: Se0/1 IPCP: Cannot satisfy pool request
*Mar 1 01:30:05.691: Se0/1 IPCP: Neither side knows remote address
*Mar 1 01:30:05.691: Se0/1 IPCP: O CONFREQ [REQsent] id 1 len 10
```

You work as a network administrator at Certkiller .com. Study the exhibit carefully. Certkiller 1 and Certkiller 2 are directly via a serial link using PPP encapsulation. The IPCP state between the routers is "Open," but they do not have IP connectivity. The Certkiller 1 output from the following command is displayed in the exhibit. Command: debug ppp negotiation. Based on the debug output, which configuration would restore IP connectivity between Certkiller 1 and Certkiller 2? Select two.

- A. On Certkiller 1, the ip unnumbered interface command
- B. On Certkiller 1, the peer default ip address interface command

- C. On Certkiller 1, the ppp authentication chap interface command
- D. On Certkiller 2, the ip address interface command
- E. On Certkiller 2, the peer default ip address pool interface command
- F. On Certkiller 2, the peer neighbor-route interface command.

Answer: B, D

QUESTION 197

Exhibit

```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0
1d00h: ISAKMP (0:1): no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with peer at 172.17.1.2.
```

You work as a network administrator at Certkiller .com. You have configured an IPsec tunnel between two IOSD router, Certkiller 1 and Certkiller 2. When testing the configuration, you see the debug output displayed in the exhibit on Certkiller 1. What could be the cause of this error?

- A. There is a mismatch of IKE Diffie-Hellman groups configured on Certkiller 1 and Certkiller 2.
- B. There is a mismatch of IPsec transform sets configured on Certkiller 1 and Certkiller 2.
- C. ISAKMP is not enabled on Certkiller 1.
- D. Perfect Forwarding Secrecy is enabled on Certkiller 1 but not on Certkiller 2.
- E. The crypto ACL on Certkiller 1 does not mirror the ACL on Certkiller 2.
- F. There is a mismatch of the IPsec SA Lifetime configuration on Certkiller 1 and Certkiller 2.

Answer: A

QUESTION 198

Exhibit

```
Certkiller1(config)# interface vlan 11
Certkiller1(config-if)# no shut

*Mar 1 00:16:41.295: %SYS-5-CONFIG_1: Configured from console by console
*Mar 1 00:16:43.095: %LINK-3-UPDOWN: Interface Vlan11, changed state to up
*Mar 1 00:16:43.099: SB: V111 Interface up
*Mar 1 00:16:43.099: SB11: V111 Init: a/HSRP enabled
*Mar 1 00:16:44.363: SB11: V111 Hello → Listen
*Mar 1 00:16:44.363: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:16:43.295: SB11: V111 Listen: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar 1 00:16:43.295: SB11: V111 Listen → Speak
*Mar 1 00:16:44.187: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 1 00:16:44.187: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:16:43.363: SB11: V111 Speak: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar 1 00:16:44.363: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 1 00:16:44.363: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:16:44.495: SB11: V111 Speak: d/Standby timer expired (unknown)
*Mar 1 00:16:44.623: SB11: V111 Standby router is local
*Mar 1 00:16:44.623: SB11: V111 Speak → Standby
```

You work as a network administrator at Certkiller .com. You are attempting to

enable Certkiller 1 as the active router in an HSRP configuration. However, upon enabling Certkiller 1, you notice that Certkiller 2 still maintains the active role. Give the output of the debug command in the exhibit, what is the reason for this behavior?

- A. Certkiller 2 has a higher priority.
- B. Certkiller 2 has a higher IP address.
- C. Certkiller 1 is not configured with preempt.
- D. Certkiller 1 is not configured under the same standby group.
- E. Certkiller 1 does not have the IP address of the virtual server.

Answer: C

QUESTION 199

Exhibit

```
00:26:51: SSHO: starting SSH control process
00:26:51: SSHO: sent protocol version id SSH-1.5-Cisco-1.25
00:26:52: SSHO: protocol version id is - SSH-1.5-1.2.26
00:26:52: SSHO: SSH_MSG_PUBLIC_KEY msg
00:26:52: SSHO: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSHO: sending encryption confirmation
00:26:52: SSHO: keys exchanged and encryption on
00:26:52: SSHO: SSH_MSG_USER message received
00:26:52: SSHO: authentication request for userid cisco
00:26:52: SSHO: SSH_MSG_FAILURE message sent
00:26:54: SSHO: SSH_CMSG_AUTH_PASSWORD message received
00:26:54: SSHO: password authentication failed for cisco
00:26:54: SSHO: SSH_MSG_FAILURE message sent
00:26:54: SSHO: authentication failed for cisco (code=7)
00:26:54: SSHO: Session disconnected - error 0x07
```

You work as a network administrator at Certkiller .com. You issue the following command on a router: debug ip ssh. The output is displayed in the exhibit. What would have caused the session to become disconnected?

- A. The username is incorrect.
- B. The source IP sent is not listed.
- C. The SSH version is incorrect.
- D. The password is not correct.

Answer: D

QUESTION 200

Exhibit

```
Certkiller102#show crypto map
Crypto Map "MYMAP" 110 ipsec-isakmp
  Peer = 192.168.192.2
  Extended IP access list 120
    access-list 120 permit ip 192.168.0.0 0.0.0.255 192.168.191.0 0.0.0.255
  Current peer: 192.168.192.2
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N) : N
  Transform sets={ MYSET, }
  Interfaces using crypto map MYMAP:
    Serial0/0
```

Certkiller102#

```
Certkiller98#show crypto map
Crypto Map "mymap" 100 ipsec-isakmp
  Peer = 192.168.191.2
  Extended IP access list 110
    access-list 110 permit ip 192.168.200.0 0.0.0.255 192.168.192.0 0.0.0.255
  Current peer: 192.168.191.2
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N) : N
  Transform sets={ myset, }
  Interfaces using crypto map mymap:
    Serial0/1
```

Certkiller98#

You work as a network administrator at Certkiller .com. You study the exhibit carefully. The LANS on Certkiller 98 and Certkiller 102 are to be encrypted across an IPSec tunnel. However, Certkiller 98 and Certkiller 102 cannot establish an IPSec connection.

What is the reason for this problem?

- A. The crypto map names of Certkiller 98 and Certkiller 102 do not match.
- B. The crypto map sequence numbers of Certkiller 98 and Certkiller 102 do not match.
- C. Invalid access lists are configured.
- D. Invalid peer addresses are configured.
- E. The transform set names of Certkiller 98 and Certkiller 102 do not match.

Answer: C

QUESTION 201

You're a network administrator and your users are complaining about a slow response time in accessing their Intranet web server. You begin troubleshooting by establishing a Telnet to the server, which is successful but the response time appears to be very slow. Attempts to use ping and traceroute to reach the server's IP address are not successful.

At this point in time, you're still trying to isolate the problem. What assumptions can you make about the problem?

(Choose three.)

- A. TCP may be blocked by an access list somewhere on the path between the users and the Intranet web server.
- B. Physical layer issues have been eliminated as a possible cause of the slow response.

- C. Application layer issues can be most likely eliminated as a possible cause of the slow response.
- D. The IP address configuration has been eliminated as a possible cause of the slow response.
- E. Divide and conquer troubleshooting approach should be taken.
- F. ICMP may be blocked by an access list somewhere on the path between the users and the Intranet web server.

Answer: C, D, F

Explanation:

C: You can safely assume that the web application works, since you are also seeing problems using another application, telnet.

D: Since you can successfully connect to the server, you know that a valid IP data path exists to the web server.

F: Sometimes when traffic goes through a generic routing encapsulation (GRE) tunnel, you can successfully use the ping command and Telnet, but you cannot download Internet web pages or transfer files using File Transfer Protocol (FTP). Therefore, if a GRE tunnel exists and ICMP is being blocked, problems can occur when trying to view web pages. For more information on this particular problem, see the Cisco document "Why Can't I Browse the Internet when Using a GRE Tunnel" here:

http://www.cisco.com/en/US/tech/CK8_27/CK3_69/technologies_tech_note09186a0080093f1f.shtml

Incorrect Answers:

A: Since Telnet uses TCP port 23, this can not be true because then you would also be unable to telnet to the web server.

B: This is not necessarily true, since physical errors on a link such as CRC errors could cause this slow response times.

E: For complex problems such as the one described here, a bottom-up approach is best.

QUESTION 202

Three of the following conditions indicate a problem at the network layer. Which ones are they? (Choose three)

- A. Users are unable to access applications on a different network segment.
- B. The network is functioning at less than established baseline parameters.
- C. A device cannot obtain a DHCP address.
- D. Two devices on different subnets cannot communicate with each other.
- E. Two devices on the same subnet cannot communicate with each other.

Answer: A, C, D

Explanation:

If a user is unable to access a host on a different network segment, then there is potentially a problem with the network layer, since the network layer deals with IP routing.

If the DHCP server resides on a different network, then a network layer problem would

prevent users from obtaining a DHCP connection. In addition, DHCP servers are used to assign IP addresses, as well as provide for IP default gateway and DNS server information. All of these aspects are associated with the network layer.

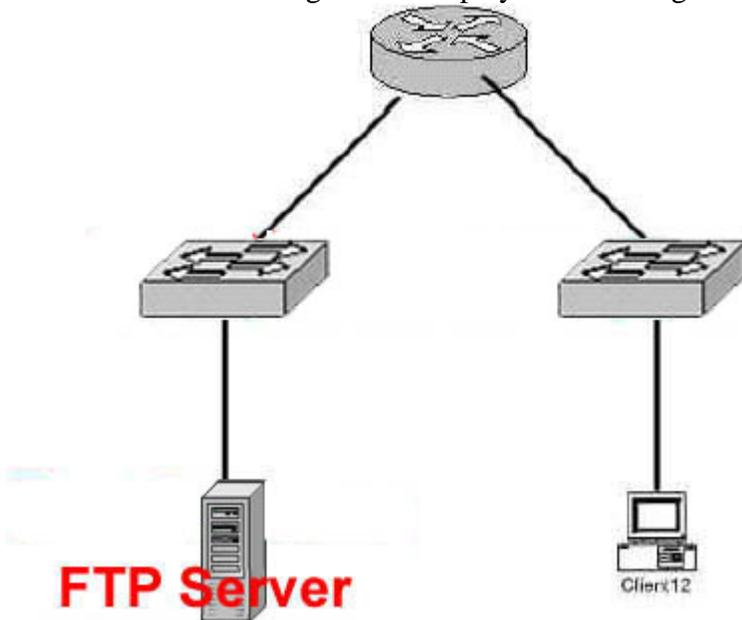
Incorrect Answers:

B: A network functioning at a less than established baseline, could be a result of a problem on any layer, not necessarily the network layer.

E: Since a device that connects to another device on the same subnet do so directly, via a switch, this type of connection resides at the data link layer, and not the network layer. Traffic between devices on the same subnet does not need to be routed, so the network layer is not used in this case.

QUESTION 203

A Certkiller network segment is displayed in the diagram below:



One of the users of the Certkiller network is having trouble downloading a file from the FTP server. You suspect that the problem is most likely in the network or application layer. What's the fastest action you could take to confirm that the problem is within these two layers?

- A. Direct the user to check the cable to the wall jack
- B. Log on to the FTP server to check if the FTP server application is running correctly.
- C. Perform a show ip route command on the router to check if there is a path between the end user and the FTP server.
- D. Issue instructions to the user to ping the FTP server.

Answer: D

Explanation:

To illustrate how the provided guidelines can assist in a real network layer problem isolation scenario, assume that a group of users on an Ethernet LAN has reported that its connection to the Internet has gone down. Examining the topology diagram for the

network, you determine which networking devices are the possible problematic ones. You use Cisco diagnostic commands to narrow the problem to a particular path involving multiple routers. You enter the ping command from the source router that the users have been attempting to connect through to the destination router. As expected, this test fails. You then enter the ping command from the destination router to the source router. The ping works. You test the connectivity between the source and destination routers at the physical and data link layers and determine that both layers are functioning correctly. The results indicate that you have a problem at the network layer. You execute appropriate show and debug commands on the path and discover that an erroneous static route in the routing table of one of the routers in the path is the cause of the problem. The following is a set of general end system commands to isolate network layer problems:

6. ping
7. arp -a
8. netstat -rn
9. netstat -a
10. traceroute /d [destination]

Following are the recommended guidelines for isolating network layer problems:

1. Identify a single pair of problematic source and destination devices.
2. Ping a device across the connection.
3. Test connectivity at each hop of a connection.
4. Troubleshoot in both directions along an IP path.
5. Use a network diagram.

QUESTION 204

You're a help desk technician at a large corporation. You get a call from a user complaining about slow response time when surfing the internet or sending and receiving email. You tell the user to enter a ping the email server, and it resulted in intermittent success and failure messages. For the sake of isolating the problem, what two problems could you eliminate as potential sources of the problem? (Choose two)

- A. Poor quality cabling between the user PC and the access layer switch.
- B. Auto-sense speed and duplex error between the PC and the access layer switch.
- C. Incorrect IP address and subnet mask configuration on the PC.
- D. Email server configuration errors in the PC email client.
- E. High utilization on a router connecting the access layer switch and the server network.
- F. Failing network interface card in the PC.

Answer: C, D

Explanation:

Note the wording of the question: "what can be eliminated as a possible cause?" All other options (A, B, E, and F) are possible causes of the intermittent problem.

C: If you have a wrong subnet mask and a second or third octet wrong on your IP address you will be able to send a request but you probably will not be able to receive an ack. In

this scenario however, you do receive some acks.

D: When you do a ping command from a pc whether by IP address or host name it ends an echo request and waits for a reply. This has nothing to do with the e-mail client configuration.

QUESTION 205

Which command is an effective tool an administrator can use to isolate a UDP problem?

- A. show ip access-list
- B. debug ip traffic
- C. show ip protocols
- D. debug tftp
- E. All of the above

Answer: A

Explanation:

Of the possible choices provided, only the "show ip access-lists" could help in isolating a UDP problem. If an extended access list is configured improperly, UDP packets can be dropped when they are not intended to be.

Example output from the "show ip access-list" command:

The following is sample output from the show ip access-list command when all access lists are requested:

```
Router# show ip access-list
Extended IP access list 101
deny udp any any eq ntp
permit tcp any any
permit udp any any eq tftp
permit icmp any any
permit udp any any eq domain
```

Incorrect Answers:

B: This command will only provide for the source and destination IP traffic information, along with the gateway used. It will not provide for any layer 4 information, unless the "detail" keyword is used.

C: This will only display information pertaining to the routing protocols, and will not provide any UDP information.

D: Although TFTP uses UDP packets, it is only one UDP application and doesn't represent all UDP packets.

QUESTION 206

Which command could you use to view TCP & UDP statistics and isolate transport layer problems at the same time?

- A. show ip traffic
- B. show ip protocols

- C. show ip route
- D. show ip interface brief

Answer: A

Explanation:

The command show ip traffic will show IP traffic statistics such as: packets sent, packets received, error counts, broadcasts, & multicasts, as well as statistics for the various protocols, (including but not limited to) IP, ICMP, UDP, TCP, Probe, ARP, IGRP, OSPF, BGRP, RIP, etc.

Reference:

CCNP Support Exam Certification Guide, page 165-166, Amir S. Ranjibar, ISBN 0-7357-09955-5

QUESTION 207

When troubleshooting a network problem, which of the following sources of information should you avoid using? (Choose all that apply)

- A. Users
- B. Router diagnostic commands
- C. Network management systems
- D. Managers
- E. Protocol analyzer traces
- F. None of the above

Answer: F

Explanation:

Since the question asked for what sources of information you should avoid using, the answer is none of the above since all of these are good sources when gathering facts. You should gather the facts that you need to help isolate possible causes. Ask questions of affected users, network administrators, managers, and other key people. Collect information from sources such as network management systems, protocol analyzer traces, output from router diagnostic commands, or software release notes.

QUESTION 208

During troubleshooting, what can you isolate with the various IOS show commands? (Choose all that apply)

- A. Problematic nodes
- B. Problematic users
- C. Problematic interfaces
- D. Problematic applications
- E. Problematic media

Answer: A, C, D, E

Explanation:

According to the technical documentation at CCO:

The show commands are powerful monitoring and troubleshooting tools. You can use the show commands to perform a variety of functions such as:

Monitor router behavior during initial installation

Monitor normal network operation Isolate problem interfaces, nodes, media, or applications

Determine when a network is congested

Determine the status of servers, clients, or other neighbors

Incorrect Answers:

B: Although the different "show" commands can be used to gather all kinds of information, you can not, however, determine which end users are problematic.

QUESTION 209

You are experiencing some problems on one of the Certkiller frame relay links.

Which of the following commands could you use to look at potential connectivity problems in detail, between DTE equipment and an ISP's Frame Relay switch?

- A. debug frame-relay serial
- B. show frame-relay switch
- C. debug frame-relay lmi
- D. show frame-relay pvc

Answer: C

Explanation:

The result of the debug frame-relay lmi command helps you isolate the issue. If the Frame Relay service were working correctly, you would see an LMI reply from the switch for every LMI request the router sends to the switch. In addition, you should periodically see a full LMI status message from the switch that includes a description of the permanent virtual circuits (PVCs). This full LMI status message is sent in response to a status inquiry message that the router transmits after every six LMI keepalives. With the default keepalive of 10 seconds, you should see the full LMI status every minute.

You should also see an incrementing counter in the yourseen field. In addition, the data terminal equipment (DTE) status should be up. Because everything used to work and no one changed anything on Orlando, you can pinpoint the issue to the Frame Relay carrier and the LMI encapsulation type. You have a defined LMI type in your interface configuration. If your service provider changed the LMI type that was offered to you, the line protocol would fail due to mismatched LMI types.

The following example displays the information pertaining to the LMI sent between the Certkiller frame relay router and the carrier's frame switch:

```
Certkiller 1#debugframe-relay lmiFrame Relay LMI debugging is onDisplaying all
Frame Relay LMI data Certkiller 1#Aug 03 21:43:13.655: Serial1/0(out): StEnq,
myseq 174, yourseen 19, DTE downAug 03 21:43:13.655: datagramstart =
0x3B5BC14, datagramsize = 14Aug 03 21:43:13.655: FR encap =
```

```
0x00010308Aug 03 21:43:13.655: 00 75 95 01 01 00 03 02 AE 13Aug 03
21:43:13.655:Aug 03 21:43:23.656: Serial1/0(out): StEnq, myseq 175, yourseen
19, DTE downAug 03 21:43:23.656: datagramstart = 0x3999F54, datagramsize =
14Aug 03 21:43:23.656: FR encap = 0x00010308Aug 03 21:43:23.656: 00 75 95
01 01 00 03 02 AF 13Aug 03 21:43:23.656:Aug 03 21:43:33.656: Serial1/0(out):
StEnq, myseq 176, yourseen 19, DTE downAug 03 21:43:33.656: datagramstart
= 0x3B5BE94, datagramsize = 14Aug 03 21:43:33.656: FR encap =
0x00010308Aug 03 21:43:33.656: 00 75 95 01 01 00 03 02 B0 13
```

QUESTION 210

If you're dealing with a network problem that's limited to the transport layer, which network devices should you focus your troubleshooting energies on to isolate the culprit of the problem? (Choose two)

- A. Router
- B. Cables
- C. Switch
- D. Hub
- E. End-system

Answer: A, E

Explanation

Cables and hubs belong to the physical layer, and regular switches belong to the data link layer. These two layers are lower than the transport layer, so if you have a problem that's limited to the transport layer, you don't have to waste your time and focus with the lower levels. Of the choices given, only a router or an end system, such as a server, would deal with the transport layer (layer 4).

QUESTION 211

When you use the command "show interfaces" for troubleshooting, which OSI layer do you focus on?

- A. Physical
- B. Transport
- C. Network
- D. Application
- E. Session
- F. None of the above

Answer: A

Explanation:

An interface is a physical component, and using this command will display the physical state of the interface.

Note: This command will also normally provide the line protocol information for some

interfaces as well, such as serial interfaces. This displays the data link state of the interface.

QUESTION 212

You've just connected a new workstation to a switch, and its performance is slow compared to the other workstations on the same switch. So you enter the following command:

```
showinterface
```

and this is what you see:

```
Router CertK #show interface fas0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0005.7428.0e01 (via
9995.7428.0e01)
MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s
input flow-control is off, output flow-c control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:33, output 00:00:03, outgoing hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
Queuing strategy: fifo
Output queue:0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
371 494 packets input, 29182104 bytes, 0 no buffer
Received 371379 broadcasts, 63459 runts, 0 giants, 0 throttles
119899 input errors, 56440 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 371374 multicast, 0 pause input
0 input packets with dribble condition detected
929 671 packets output, 69998797 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets
0 babbles, 0 late collisions, 0 deferred
0 lost carried, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out
What's likely to be causing the problem?
```

- A. Duplex mismatch issue
- B. Portfast issue
- C. Flow-control issue
- D. Udid issue
- E. Speed mismatch issue
- F. Jitter control issue

Answer: A

Explanation:

The main interface configuration commands that may be necessary on the Fast Ethernet interface are media-type and full-duplex. If an interface on the opposite side was set to half-duplex by an administrator on the other end the above duplex mismatch issue would result. In this case, since the duplex and speed settings are hard-coded to full and 100 instead of auto, you should ensure that the end station attached is also configured similarly.

References:

CCNP Support Exam Certification Guide, page 269, Amir S. Ranjibar, ISBN 0-7357-09955-5

<http://www.cisco.com/warp/public/473/46.html>

QUESTION 213

You are the network technician at Certkiller Inc. and you are working on an international troubleshooting project. The remote site at Cape Town, served by a Frame Relay WAN connection, does not have connectivity to the central site in Abu Dhabi. You perform some tests from the Abu Dhabi site and you notice that the Frame Relay interface is UP and the line protocol is also UP, but no IP traffic is being sent or received through the interface. You issue the show interfaces command on the Cape Town router and you see that Frame Relay interface is UP, but the line protocol is DOWN. What can you determine?

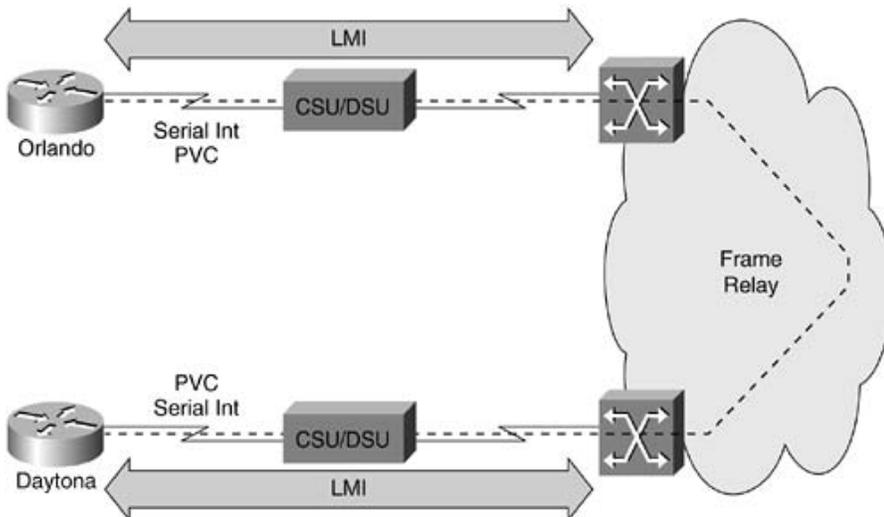
- A. There is a physical layer problem at the Cape Town site router.
- B. There is a network layer problem between the Cape Town site router and the Abu Dhabi site router.
- C. There is a data-link layer problem between the Cape Town site router and the Frame Relay switch.
- D. There is a network layer problem between the Cape Town site router and the Frame Relay switch.
- E. There is a data-link layer problem between the Cape Town site router and the Abu Dhabi site router.
- F. There is a physical layer problem at the Abu Dhabi site router.

Answer: C

Explanation:

The line protocol status of a serial interface will display the layer 2 data link state of the interface. Here's an example of a similar problem between two remote Frame Relay connections in Florida.

Figure 7-2. Frame Relay Connection Between the Remote Branches at Daytona and Orlando



Now imagine that Network Operations calls to inform you that the link to Daytona is down. You ask if anyone had made changes to the configuration of Orlando. Network Operations says that it made no changes. Example 7-5 shows a console message that Network Operations says that it saw on Orlando during a check of the logs. The line protocol down message is an indication that there is a problem with the interface at the data link layer that prevents it from functioning properly. (Note that when the line protocol goes down, Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies time out.)

Example 7-5. Console Message Showing a Symptom of a Data Link Layer

```
ProblemOrlando#Aug 03 21:14:24: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial1/0, changed state to downAug 03 21:14:24: %DUAL-5-NBRCHANGE:
IP-EIGRP 101: Neighbor 172.21.177.1 (Serial1/0) is down: interface downOrlando#To
start problem isolation, you connect into the console port on Orlando and use the show ip
interface brief command to look for interface status. The output of this command shows
that interface Serial 1/0 on Orlando is up, but the line protocol is down. (See the top
portion of Example 7-6.)
```

Example 7-6. Gathering Information to Isolate a Data Link Layer Problem on a Cisco Router

```
Orlando#show ip interface briefInterface IP-Address OK? Method Status
ProtocolFastEthernet0/0 172.21.178.129 YES NVRAM up upSerial1/0 172.21.177.2
YES NVRAM up downOrlando#
```

When an interface is experiencing data link layer problems, entering the show interfaces command might indicate that the interface is up but the line protocol is down.

Data Link Layer Status as Reported by the Output of the show interface

```
Commandrouter1>show interfacesEthernet0/0 is up, line protocol is down(rest of output
is deleted/not shown)router2>show interfacesSerial0/0 is up, line protocol is down(rest of
output is deleted/not shown)
```

QUESTION 214

Certkiller operates a small bank in the Cayman islands which is connected by a WAN to their offshore accounting department on the other side of the island. The accounting department has been experiencing a connectivity problem with the bank system, and has flown you in to troubleshoot. During the symptom gathering

process you find out that the bank website was completely functional twelve hours ago, and that the accounting problem can still access other sites. Which steps should you include in your effort to further isolate the problem? (Choose three)

- A. Verify the local IP address and default gateway configuration on the accounting department PCs.
- B. Use a ping command to verify that the PCs can reach their configured default gateway.
- C. Use a ping command to discover if the DNS name of the bank website will resolve to a reachable IP address.
- D. Attempt to access the bank website from a computer on a different subnet or vlan.
- E. Use a tracert command to determine how the traffic to the bank website is being routed.
- F. Use a ping command from the Internet gateway router to the accounting PCs to verify that the routing is correct.

Answer: C, D, E

Explanation:

The following table shows some useful commands for troubleshooting end system problems:

Command	Type	Description
ping {host ip-address }	General End System	Sends an echo request packet to an address and then waits for a reply. The {host ip-IP address } variable is the IP alias or address of the target system.
arp -a	General End System	Displays the current mappings of the IP address to the MAC address in the ARP table.
Netstat [-rn]	General End System	The net stat command displays active TCP/IP connections. The -rn option is for displaying the routing table in numerical format (without querying Domain Name System [DNS] server).

ipconfig /all	Windows Command for	Displays IP information for hosts that are running Windows NT/Windows2000/Windows XP.
Tracert [destination]	Windows Command	Verifies connectivity (and displays a path) to a destination device for Windows hosts. The destination variable is the IP alias or IP address of the target system.
Winipcfg	Windows Command	Displays IP information for hosts that are running Windows 9x and Windows Me.
ifconfig -a	UNIX and Mac OS	Displays IP information X for UNIX and Mac OS X hosts.
traceroute [destination]	UNIX and Mac OS X	Identifies the path that a packet takes through the work. The destination variable is the host name IP address of the target

QUESTION 215

EIGRP debugging was enabled on router Certkiller A as shown below:
Certkiller A# debug eigrp packets

```
....  
01:39:13: EIGRP received QUERY on Serial0/0 nbr 10.1.2.2  
01:39:13: AS 100, Flags 0x0, Seq 22/36 idbQ 0/0 idbQ 0/0 peerQ un/rely 0/0  
01:39:13: EIGRP: Enqueueing ACK on Serial0/0 nbr 10.1.2.2  
01:39:13: Ack seq 22 iidbQ un/rely 0/0 peerQ un/rely 1/0  
01:39:13: EIGRP: Sending ACK on Serial0/0 nbr 10.1.2.2  
01:39:13: AS 100, Flags 0x0, Seq 0/22 idbQ 0/0 idbQ 0/0 peerQ un/rely 0/0  
01:39:13: EIGRP: Sending REPLY on Serial0/0 nbr 10.1.2.2  
01:39:13: AS 100, Flags 0x0, Seq 37/22 idbQ 0/0 idbQ 0/0 peerQ un/rely 0/1 serno 74-74  
01:39:13: EIGRP: Received ACK on Serial0/0 nbr 10.1.2.2  
01:39:13: AS 100, Flags 0x0, Seq 0/7 idbQ 0/0 idbQ 0/0 peerQ un/rely 0/0 unrelyserno  
0/1
```

A network administrator is troubleshooting an EIGRP connection between Certkiller A with IP address 10.1.2.1 and Certkiller B with IP address 10.1.2.2. Given the debug output on Certkiller A, which statement is true?

- A. Certkiller A is sending a hello packet to Certkiller B for neighbor discovery.
- B. Certkiller A has lost a network connection and does not have a feasible successor.
- C. Certkiller A is requesting an update packet that contains all the routes in the routing table of Certkiller B.
- D. Certkiller B is sending a hello packet to Certkiller A for neighbor discovery.
- E. Certkiller B has lost a network connection and does not have a feasible successor.
- F. Certkiller B is requesting an update packet that contains all of the routes in the routing table of Certkiller A.

Answer: E

Explanation:

Route States:

A topology table entry for a destination can have one of two states. A route is considered in the Passive state when a router is not performing a route recomputation. The route is in Active state when a router is undergoing a route recomputation. If there are always feasible successors, a route never has to go into Active state and avoids a route recomputation.

When there are no feasible successors, a route goes into Active state and a route recomputation occurs. A route recomputation commences with a router sending a query packet to all neighbors. Neighboring routers can either reply if they have feasible successors for the destination or optionally return a query indicating that they are performing a route recomputation. While in Active state, a router cannot change the next-hop neighbor it is using to forward packets. Once all replies are received for a given query, the destination can transition to Passive state and a new successor can be selected. When a link to a neighbor that is the only feasible successor goes down, all routes through that neighbor commence a route recomputation and enter the Active state.

Packet Formats:

EIGRP uses five packet types:

1. Hello/Acks
2. Updates
3. Queries
4. Replies
5. Requests

Hellos do not require acknowledgment. A hello with no data is also used as an acknowledgment (ack). Acks are always sent using a unicast address and contain a non-zero acknowledgment number.

Updates are used to convey reachability of destinations. When a new neighbor is discovered, update packets are sent so the neighbor can build up its topology table. In this case, update packets are unicast. In other cases, such as a link cost change, updates are multicast. Updates are always transmitted reliably.

Queries and replies are sent when destinations go into Active state. Queries are always multicast unless they are sent in response to a received query. In this case, it is unicast back to the successor that originated the query. Replies are always sent in response to queries to indicate to the originator that it does not need to go into Active state because it has feasible successors. Replies are unicast to the originator of the query. Both queries

and replies are transmitted reliably.

In this example, Certkiller B has a route that has gone active, so it is sending a query about the route to Certkiller A.

QUESTION 216

The system administrator has discovered that two routers in the Certkiller network have connectivity but are not exchanging routing information. Which two statements are true as indicated by the layered model troubleshooting technique? (Choose two).

- A. Connectivity indicates Layer 2 is operating OK.
- B. Connectivity indicates Layer 3 is operating OK.
- C. Connectivity indicates Layer 4 is operating OK.
- D. The bottom-up approach should be used.
- E. The divide and conquer approach should be used.
- F. The top-down approach should be used.

Answer: A, E

Explanation:

If two neighboring routers have established connectivity with each other, then we can safely assume that layers 1 (physical) and 2 (data link) are functioning properly. Since routing occurs at layer 3, we can also determine that the problem is likely with the network layer. Since we are already sure the problem is with the network layer, the divide and conquer approach to troubleshooting is recommended.

QUESTION 217

Some internal BGP neighbors are not coming up within the Certkiller network. What are the two most likely problems? (Choose two).

- A. There are duplicate IP addresses.
- B. The routes to the neighbors are missing.
- C. An access list blocking external addresses.
- D. The update source interface command missing in BGP configurations.
- E. There are mismatched subnet masks.
- F. The ebgp-multihop command is missing from the BGP configurations.

Answer: B, D

Explanation:

BGP supports two basic types of sessions between neighbours, internal (sometimes referred to as IBGP) and external. Internal sessions are run between routers in the same autonomous system, while external sessions run between routers in different autonomous systems.

IBGP routers establish a peering relationship through the use of TCP connections (BGP uses TCP port 179). It is typical for IBGP routers to peer to each other's loopback

address, since this is the most reliable interface. IBGP routers are not required to peer with the neighbors directly connected interfaces. In fact, IBGP peers are often numerous router hops away from each other. When this is done, the routers must use the "update-source" command to specify the source IP address of the BGP peer. Therefore, the most typical problems with IBGP peers come from this, or the fact that there is no route to the peer IP address that is being specified.

QUESTION 218

While testing the HSRP configuration on one of the Certkiller routers, you notice that the standby router didn't take over as active. To troubleshoot the issue, you issue the show standby command as shown below:

```
Vlan8 - Group 8
Local state is Active, priority 110, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:01.168
Hot standby IP address is 10.1.2.2 configured
Active router is local
Standby router is unknown expired
Standby virtual mag address is 0000.0c07.ac08
      state state is Active, priority
```

What is the most likely cause of the problem?

- A. Link change is causing the hellos to drop before reaching the router.
- B. This router is set to pre-empt and will not allow another router to be active.
- C. The hello timers do not match and therefore will not peer.
- D. HSRP priority level is higher than the standby.
- E. None of the above.

Answer: A

Explanation:

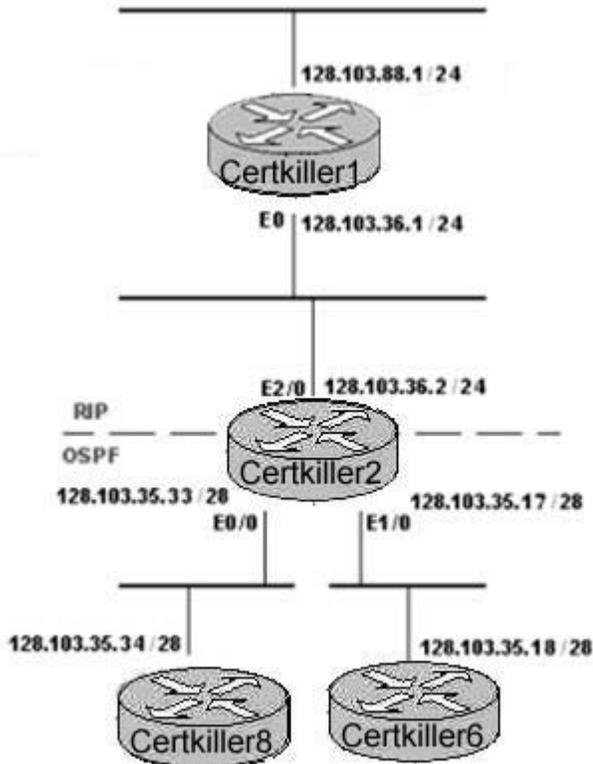
The output that states "standby router is unknown expired" displays the root of the problem, which is that the router is no longer receiving HSRP hellos. Devices running HSRP send and receive multicast UDP-based hello packets to detect router failure and to designate active and standby routers. These messages are not being received by the standby router in this example.

Incorrect Answers:

- B: Preempt means that the router is configured to take over as the primary if the priority is greater. It will not prohibit the standby router from becoming the active at any time.
- C: The timers do not necessarily need to match at each end, as the values have only local significance. The default is 3 seconds, but if a router is configured differently, the other router will still send hello packets every 3 seconds and these will be acknowledged by the other HSRP router. In this example it can be seen that the default value was kept.
- D: This may or may not be true, but until the other HSRP router replies to the hello packets it will be unknown if this is an issue.

QUESTION 219

The Certkiller network is displayed in the following diagram:



An administrator is redistributing OSPF into RIP version 1. RIP is routing the 128.103.36.0/24 network. OSPF is routing the 128.103.35.X/28 networks. Users in the RIP domain cannot reach devices in the OSPF domain. Which two tasks must be done to enable RIP to advertise the routes learned from OSPF into the RIP domain? (Choose two)

- A. Add a static route that points to the RIP domain address space with a /24 network mask and a next hop of 128.103.36.2
- B. Add a static route that points to the OSPF domain address space with a /24 network mask and a next hop of null0.
- C. Tune the OSPF default metrics to allow seamless redistribution into RIP.
- D. Redistribute configured static routes into RIP.
- E. Use a route map statement inserted into a distribute list to control routing updates.

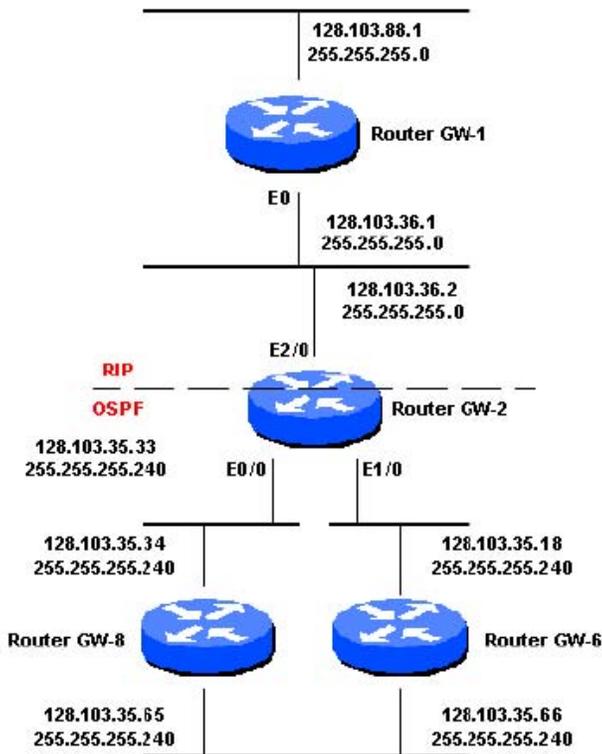
Answer: B, D

Explanation:

When redistributing routes from a classful routing protocol into a classless routing protocol, problems can arise due to the fact that RIP version 1 does not support VLSM information. The following example describes the Cisco recommended solution:

OSPF Has a Longer Mask than RIP:

In the network diagram for this problem, Router GW-2 is redistributing between RIP and OSPF. The OSPF domain has a different mask (longer in this case) than the RIP domain, and they are on the same major network. Therefore, RIP will not advertise routes learned from OSPF and redistributed into RIP.



Solution

The subnet mask of the OSPF domain is difficult to change, so instead, add a static route in Router GW-2 that points to the OSPF domain with a mask of 255.255.255.0, but with a next hop of null0. Then, redistribute static routes into RIP. Here is the configuration to accomplish this task:

```
ip route 128.103.35.0 255.255.255.0 null0
router rip
redistribute static
default metric 1
```

This allows 128.103.35.0 to be advertised through RIP out the E2/0 interface of Router GW-2. However, Router GW-2 still has more specific routes learned from OSPF in its routing table, so the best routing decisions are made.

Reference:

http://www.cisco.com/en/US/tech/CK365/technologies_tech_note09186a0080093fd9.shtml

QUESTION 220

The Certkiller network is being configured for IS-IS as the routing protocol and you wish to verify the configuration. Which show command will display IS-IS neighbors, neighbor level, and type, as well as SNPA's?

- A. Show ip route
- B. Show clns route
- C. Show clns neighbors
- D. Show cdp neighbors

Answer: C

Explanation:

The following is sample output from the show clns neighbors command:

```
Router# show clns neighbors
```

```
System Id InterfaceSNP A State Holdtime Type Protocol
0000.0000.0007Et3/3aa00.0400.6408UP26L1IS-IS
0000.0C00.0C35Et3/20000.0c00.0c36Up91L1IS-IS
0800.2B16.24EAEt3/3aa00.0400.2d05Up27L1M-ISIS
0800.2B14.060EEt3/2aa00.0400.9205Up8L1IS-IS
```

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_chapter09186a00801d

QUESTION 221

In the Certkiller OSPF network, you want to change the router ID of one of the routers. What must you do to configure the router ID for an active OSPF router?

- A. Use the command "router-id" and then issue a "clear counter" command.
- B. Use the command "router-id" and perform a "clear ip ospf process xxx" command.
- C. Use the command "router-id" and then next hello packet will start to propagate the new RID
- D. Use the command "router-id" and then reset the OSPF interfaces.

Answer: B

Explanation:

The router ID is the highest IP address or the highest IP address among loopback addresses (if one is configured) on the Cisco router or can be configured manually by "router-id x.x.x.x".

Once the router ID is chosen, it will not be changed unless the ospf process is reset (from the "clear ip ospf process xx" command) or the router is reloaded.

Reference:

http://www.cisco.com/en/US/tech/CK365/technologies_tech_note09186a0080094a85.shtml

QUESTION 222

A portion of the configuration for router CK1 is displayed below:

```
Class-map match-any GOLD
match ip precedence ef
class-map match-any SILVER
Match ip dscp af31
Policy-map Branch
Class GOLD
Priority percent 20
Class SILVER
```

```
bandwidth percent 15
random-detect dscp-based
interface Serial0/1
description PPP link to BRANCH
bandwidth 1536
ip address 10.200.40.1 255.255.255.252
encapsulation ppp
```

This configuration has been used to prioritize voice traffic on the Certkiller network. After issuing several show commands, the administrator realizes the configuration is not working. What could be the problem?

- A. Voice traffic should be mapped to a different DSCP value.
- B. WRED is not configured for the voice traffic.
- C. The policy map needs to be mapped to an interface.
- D. The given LLQ configuration is not designed for voice traffic.
- E. Custom queuing should be used on converged voice and data networks.
- F. None of the above

Answer: C

Explanation:

Similar to access lists, policy maps must be mapped to an interface. Although the policy map portion of the configuration for prioritizing traffic is complete, the router needs to be informed which interface this policy needs to be applied to. To do this, Use the service-policy interface configuration command to attach a traffic policy to an interface and to specify the direction in which the policy should be applied (either on packets coming into the interface or packets leaving the interface). In this example, this would be done with the "service-policy input Branch" or "service-policy output Branch" command.

QUESTION 223

Routers CK1 and CK2 are connected via a PPP link. In this connection, what field in the PPP negotiation process is used to detect a loopback link?

- A. MTU
- B. MRU
- C. Magic number
- D. Sequence number
- E. None of the above

Answer: C

Explanation:

The Link Control Protocol (LCP) is used to negotiate various PPP options. There are a large number of PPP options that LCP can negotiate, including the following:

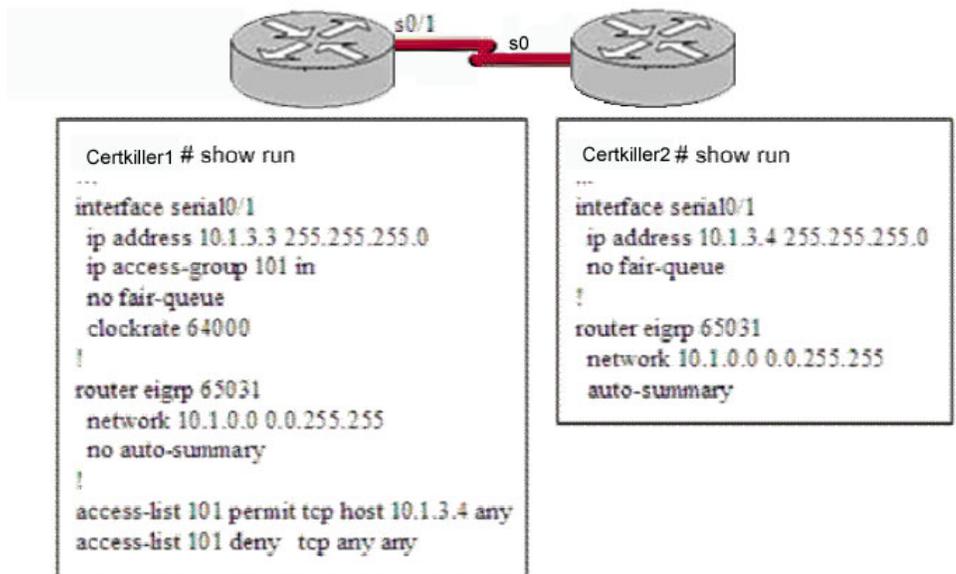
1. MRU size-Maximum receive unit size (always accepted).
2. Magic number-Randomly generated number used to identify one end of a point-to-point

connection. Each side negotiates its magic number, taking note of each other's magic number. If both sides discover that the magic numbers they are negotiating are the same, each side attempts to change its magic number. If they are not successful, and the magic numbers remain the same, the session terminates because of the loopback that is detected. Magic numbers are always accepted. By default, the router always attempts to negotiate a local magic number. The peer can also determine whether to negotiate its magic number-the peer magic number. The router always accepts a peer attempt to negotiate its magic number.

3. Authentication-Requested if configured.
4. Protocol-Field-Compression (PFC) and Address-and-Control-Field-Compression (ACFC)-Accepted, but never requested.
5. Multilink PPP-Additional options can be negotiated when Multilink PPP is configured.

QUESTION 224

Exhibit



You work as a network engineer at Certkiller .com. Certkiller 1 and Certkiller 2 are unable to establish a neighbor relationship through the serial interface. Both interfaces are up and you have permitted Certkiller 2 in the access list. Given the configuration in the exhibit, what is the problem?

- A. An invalid autonomous number
- B. Mismatch hold time between Certkiller 1 and Certkiller 2
- C. EIGRP not permitted in the access list
- D. Need to configure the no auto-summary command on Certkiller 2

Answer: C

Explanation:

EIGRP uses IP protocol number 88. To allow EIGRP via an access list, the following statement should have been configured in the access list:

Access-list 101 permit eigrp host 10.1.3.4 any.

Incorrect Answers:

A: The valid EIGRP autonomous system range is 1-65535, so this is not the problem since both routers are configured in this range and both are configured to be in the same AS.

B: In this case, the hold time is not explicitly configured on these links, so the default values will be used. With default values, the timers would match.

D: EIGRP performs an auto-summarization each time it crosses a border between two different major networks. Since the same major network number is used (10.0.0.0) this is not the problem, even though it is disabled on one of the routers.

QUESTION 225

The following information was displayed on router Certkiller 3:

```
Certkiller3# show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0 interface
dsl 0, interface ISDN Switchtype = basic-ni
Layer4 Status:
Active
Layer 2 Status:
Layer 2 NOT Activated
Spid Status:
TEI Not Assigned, ces = 1, state = 3 (await establishment)
spid1 configured, spid1 NOT sent, spid1 NOT valid
TEI Not Assigned, ces = 1, state = 3 (terminal down)
spid2 configured, spid2 NOT sent, spid2 NOT valid
Layer 3 Status:
TWAIT time Active
0 Active Layer 2 Call(s)
activated dsl 0 CCRs = 0
```

You work as a network technician at Certkiller .com. An ISDN connection is currently not functioning. You have issued the show isdn status command and receive the output in the exhibit.

What is the appropriate action that should be taken next to determine the issue?

- A. Check for the incorrect authentication parameters.
- B. Ensure that the interface is activated (not shutdown).
- C. Issue the debug dialer command to ensure that the router is dialing the far end.
- D. Turn on debugging for q921 and then clear the BRI interface.

Answer: D

Explanation:

From the information provided, the problem appears to be with layer 2, since it is not active and the SPID status is not active for each one. Since Q.921 operates at layer 2 at the ISDN level, debug this to troubleshoot a layer 2 ISDN problem.

Use the debug isdn q921 privileged EXEC command to display data link layer (layer 2) access procedures that are taking place at the router on the D channel (LAPD) of its

Integrated Services Digital Network (ISDN) interface.

Incorrect Answers:

A: An authentication problem would have no effect on the ISDN layer 2 functionality.

B: Since layer 1 of the ISDN status displayed is active, the interface must be administratively enabled.

C: Until the layer 2 issues are resolved with this interface, no dialing can occur.

QUESTION 226

At one of the Certkiller remote locations, Catalyst 2950 series switch has been attached to a Cisco 2600 series router that will perform inter-vlan routing for devices connected to the switch. Reports indicate that the routing between VLANs is not taking place. What may be a possible cause for this?

A. Interface Ethernet 0 on the Cisco 2600 does not have the speed and duplex manually set.

B. Trunking using ISL has not been enabled on the Catalyst 2950.

C. Trunking using IEEE 802.1q has not been enabled on the Cisco 2600.

D. Sub-interfaces have not been configured on the Catalyst 2950.

Answer: C

Explanation:

In case of 2940/2950 series switches, none of the trunk configuration commands are used. Cisco 2940/2950 series switches only support 802.1q encapsulation which is configured automatically, when trunking is enabled on the interface by using switchport mode trunk command.

Since the encapsulation methods must match on each end of the trunk, the Cisco 2600 must also be configured using 802.1Q trunking.

Incorrect Answers:

A: Manually setting the speed and duplex settings are not a requirement for inter-VLAN routing.

B: ISL trunking is not supported on the Cisco 2940 and 2950 series switches.

D: Sub-interfaces need to be created on the router side of the trunk, not on the switch.

QUESTION 227

A new ISDN circuit is being installed at a remote Certkiller office. Which two troubleshooting steps should be taking when isolating a connectivity problem with a new ISDN BRI installation? (Select two)

A. Verify that the DLCI and LMI types are correctly set

B. Verify that the correct ISDN switch type is configured

C. Determine whether or not a SPID is needed

D. Check the connection between the S/T and the NT-1

Answer: B, C

Explanation:

Some service providers use service profile identifiers (SPIDs) to define the services subscribed to by the Integrated Services Digital Network (ISDN) device that is accessing the ISDN service provider. The service provider assigns the ISDN device one or more SPIDs when you first subscribe to the service. If you are using a service provider that requires SPIDs, your ISDN device cannot place or receive calls until it sends a valid assigned SPID to the service provider when accessing the switch to initialize the connection.

Currently, only the DMS-100 and NI-1 switch types require SPIDs. The AT&T 5ESS switch type may support a SPID, but you should contact your provider for information on what the SPID must be configured as. Remember that SPIDs are only required in North America and are configured only if required by your telco/provider.

Once the ISDN line is provisioned, you must specify the appropriate switch type on the router. The ISDN switch type can be verified using the command `show isdn status`. The Telco should explicitly indicate the switchtype that needs to be configured. Occasionally (especially in North America) the Telco may indicate the switchtype is "custom" or "national".

Incorrect Answers:

A: DLCI and LMI are terms used in frame relay circuits, not in ISDN.

D: This step should be taken only if the circuit continues to have problems after the initial configuration setup has been completed.

QUESTION 228

On one of the Certkiller routers, you perform a "no shutdown" command on the ISDN interface to start TEI. What is the first AI value you should see in the "debug isdn q921" output?

- A. 0
- B. 64
- C. 127
- D. 128

Answer: C

Explanation:

A terminal endpoint can be any ISDN-capable device attached to an ISDN network. The TEI is a number between 0 and 127, where 0-63 are used for static TEI assignment, 64-126 are used for dynamic assignment, and 127 is used for group assignments. (0 is used only for PRI and is discussed later.) The TEI provides the physical identifier, and the service access point identifier (SAPI) carries the logical identifier.

The following is sample output from the `debug isdn q921` command for a startup message on a DMS-100 switch:

```
Router# debug isdn q921
```

```
Jan 3 14:47:28.455: ISDN BR0: RX <- IDCKRQ ri = 0 ai = 127 0
```

```
Jan 3 14:47:30.171: ISDN BR0: TX -> IDREQ ri = 31815 ai = 127
```

```
Jan 3 14:47:30.219: ISDN BR0: RX <- IDASSN ri = 31815 ai = 64
```

642-831

```
Jan 3 14:47:30.223: ISDN BR0: TX -> SABMEp sapi = 0 tei = 64
Jan 3 14:47:30.227: ISDN BR0: RX <- IDCKRQ ri = 0 ai = 127
Jan 3 14:47:30.235: ISDN BR0: TX -> IDCKRP ri = 16568 ai = 64
Jan 3 14:47:30.239: ISDN BR0: RX <- UAF sapi = 0 tei = 64
Jan 3 14:47:30.247: ISDN BR0: TX -> INFOc sapi = 0 tei = 64 ns = 0 nr = 0
Jan 3 14:47:34.267: ISDN BR0: RX <- RRR sapi = 0 tei = 64 nr = 2
Jan 3 14:47:43.815: ISDN BR0: RX <- RRP sapi = 0 tei = 64 nr = 2
Jan 3 14:47:43.819: ISDN BR0: TX -> RRF sapi = 0 tei = 64 nr = 0
Jan 3 14:47:53.819: ISDN BR0: TX -> RRP sapi = 0 tei = 64 nr = 0
```

The first seven lines of this example indicate an L2 link establishment.

The following lines indicate the message exchanges between the data link layer entity on the local router (user side) and the assignment source point (ASP) on the network side during the TEI assignment procedure. This assumes that the link is down and no TEI currently exists.

```
Jan 3 14:47:30.171: ISDN BR0: TX -> IDREQ ri = 31815 ai = 127
```

```
Jan 3 14:47:30.219: ISDN BR0: RX <- IDASSN ri = 31815 ai = 64
```

At 14:47:30.171, the local router data link layer entity sent an Identity Request message to the network data link layer entity to request a TEI value that can be used in subsequent communication between the peer data link layer entities. The request includes a randomly generated reference number (31815) to differentiate among user devices that request automatic TEI assignment and an action indicator of 127 to indicate that the ASP can assign any TEI value available. The ISDN user interface on the router uses automatic TEI assignment.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_command_reference_chapter09186a00800e

QUESTION 229

The following output was seen on router Certkiller 1:

```
Certkiller1# debug ppp negotiation
PPP protocol negotiation debugging is on
Certkiller1#
*Mar 1 00:06:36.643: %LINK-3-UPDOWN: Interface br10:1 ..., changed state to up
*Mar 1 00:06:36.661: BR0:1 PPP: Treating connection as a callin
*Mar 1 00:06:36.665: BR0:1 PPP: Phase is ESTABLISHING, Passive Open [0 sess, 0 load]
*Mar 1 00:06:36.669: BR0:1 LCP: State is Listen
*Mar 1 00:06:37.034: BR0:1 LCP: I CONFREQ [Listen] id 7 len 17
*Mar 1 00:06:37.038: BR0:1 LCP: AuthProto PAP (0x0304C023)
*Mar 1 00:06:37.042: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
*Mar 1 00:06:37.046: BR0:1 LCP: Callback 0 (0x0D0300)
*Mar 1 00:06:37.054: BR0:1 LCP: O CONFREQ [Listen] id 4 len 15
*Mar 1 00:06:37.058: BR0:1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.062: BR0:1 LCP: MagicNumber 0x1081E7E1 (0x05061081E7E1)
*Mar 1 00:06:37.066: BR0:1 LCP: O CONFREQ [Listen] id 7 len 7
*Mar 1 00:06:37.070: BR0:1 LCP: Callback 0 (0x0D0300)
*Mar 1 00:06:37.098: BR0:1 LCP: I CONFACK [REQsent] id 4 len 15
*Mar 1 00:06:37.102: BR0:1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.106: BR0:1 LCP: MagicNumber 0x1081E7E1 (0x05061081E7E1)
*Mar 1 00:06:37.114: BR0:1 LCP: I CONFREQ [ACKrcvd] id 8 len 14
*Mar 1 00:06:37.117: BR0:1 LCP: AuthProto PAP (0x0304C023)
*Mar 1 00:06:37.121: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
```

642-831

You work as network engineer for Certkiller .com. You are troubleshooting a PPP connection between a local and remote and remote router by entering the command debug ppp negotiation on the local router. Given the output, which statement is true? (Choose all that apply)

- A. The remote router is configured as a callback server.
- B. The local router is configured as a callback server.
- C. The remote router is configured as a callback client.
- D. The local router accepted a callback request from the remote router.
- E. The remote router accepted a callback request from the local router.

Answer: B, C

Explanation:

This is an annotated description of debug ppp negotiation command output example:

```
CK1 #debug ppp negotiation
```

```
PPP protocol negotiation debugging is on
```

```
CK1 #
```

```
*Mar 1 00:06:36.645: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up
```

```
!--- The Physical Layer (BRI Interface) is up. Only now can PPP negotiation begin.
```

```
*Mar 1 00:06:36.661: BR0:1 PPP: Treating connection as a callin
```

```
*Mar 1 00:06:36.665: BR0:1 PPP: Phase is ESTABLISHING, Passive Open [0 sess, 0 load]
```

```
!--- The PPP Phase is ESTABLISHING. LCP negotiation now occurs.
```

```
*Mar 1 00:06:36.669: BR0:1 LCP: State is Listen
```

```
*Mar 1 00:06:37.034: BR0:1 LCP: I CONFREQ [Listen] id 7 len 17
```

```
!--- This is the incoming CONFREQ. The ID field is 7.
```

```
*Mar 1 00:06:37.038: BR0:1 LCP: AuthProto PAP (0x0304C023)
```

```
*Mar 1 00:06:37.042: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
```

```
*Mar 1 00:06:37.046: BR0:1 LCP: Callback 0 (0x0D0300)
```

```
!--- The peer has requested:
```

```
!--- Option: Authentication Protocol, Value: PAP
```

```
!--- Option: MagicNumber (This is used to detect loopbacks and is always sent.)
```

```
!--- Option: Callback, Value: 0 (This is for PPP Callback; MS Callback uses 6.)
```

In this example, the router is receiving a callback request from the remote peer, making the local router the PPP Callback Server, and the remote router the PPP Callback Client.

Reference:

http://www.cisco.com/en/US/tech/CK7_13/CK5_07/technologies_tech_note09186a00800ae945.shtml

QUESTION 230

When OSPF neighbor adjacency problems are being troubleshot, which two OSPF network types require analysis of the DR/BDR election? Select two.

- A. point-to-point
- B. point-to-multipoint
- C. broadcast
- D. non-broadcast multi-access
- E. point-to-multipoint non-broadcast

Answer: C, D

QUESTION 231

Which three conditions can cause BGP neighbor establishment to fail? Select three.

- A. There is an access list blocking all TCP traffic between the two BGP neighbors.
- B. The EBGP neighbor ebgp-multihop option is set to the default value.
- C. The IBGP neighbor is not directly connected.
- D. BGP synchronization is enabled in a transit autonomous system with fully-meshed IBGP neighbors.
- E. The BGP update interval is different between the two BGP neighbors.
- F. The BGP neighbor is referencing an incorrect autonomous system number in its neighbor statement.

Answer: A, B, F

QUESTION 232

DRAG DROP

Drag the task to the appropriate tool.

Tools	Tasks, place here
Cable tester	Place here
BERT	Place here
Network Monitor	Place here
Modeling Software	Place here
TDR	Place here
Protocol Analyzer	Place here

Tasks, Select from these

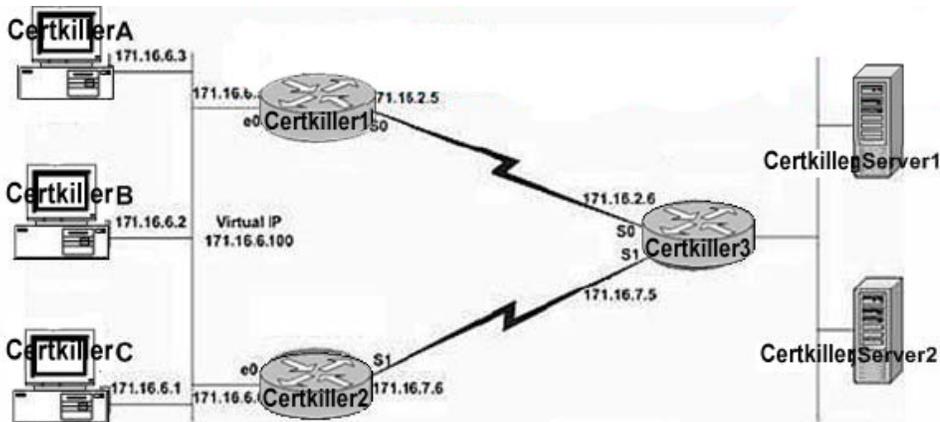
- Analyze network design.
- Examine DTE-to-DCE communications
- Capture and decode packets.
- Locate crosstalk
- Locate cable fault.
- Profile LAN traffic.

Answer:

Tools	Tasks, place here
Cable tester	Locate crosstalk
BERT	Examine DTE-to-DCE communications
Network Monitor	Profile LAN traffic.
Modeling Software	Analyze network design.
TDR	Locate cable fault.
Protocol Analyzer	Capture and decode packets.

Tasks, Select from these

QUESTION 233
Exhibit



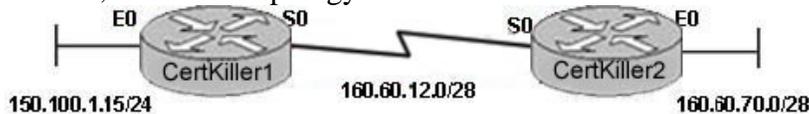
You work as a network administrator at Certkiller .com. Study the exhibit carefully.
 You issue the following command on Router Certkiller 2: show standby
 You learn that the router does not have a standby IP address.
 What are two possible causes of the problem? Select two.

- A. A routing protocol is not configured on Certkiller 2.
- B. The Ethernet network connecting Certkiller 1 and Certkiller 2 is overloaded.
- C. HSRP is incorrectly configured on Certkiller 2.
- D. IP redirection is disabled.
- E. The Ethernet network between Certkiller 1 and Certkiller 2 is down.
- F. A serial interface on Certkiller 1 or Certkiller 2 is down.

Answer: B, E

QUESTION 234

Exhibit, Network Topology



Exhibit, show ip protocols

```
Certkiller1# show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 0 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 1, receive any version
  Interface        Send Recv Triggered RIP Key-chain
  Ethernet0        1 2 1 2
  Serial0          1 1 2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for networks:
    150.100.0.0
    160.60.0.0
  Routing Information Sources:
    Gateway         Distance  Last Update
    150.100.1.15    120      00:00:10
    160.60.12.2     120      00:00:11
  Distance: (default is 120)
```

```
Certkiller2# show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 5 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
  Interface        Send Recv Triggered RIP Key-chain
  Ethernet0        2 2
  Serial0          2 2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    160.60.0.0
  Routing Information Sources:
    Gateway         Distance  Last Update
    160.60.12.1     120      00:03:17
    160.60.70.3     120      00:03:18
  Distance: (default is 120)
```

You work as a network administrator at Certkiller .com. Study the exhibit carefully.

The serial interfaces are up/up and they can ping each other. However, Certkiller 1 and Certkiller 2 fail to see all the RIP routes in their routing table. What is causing this issue?

- A. Different versions of RIP are configured on Certkiller 1 and Certkiller 2.
- B. RIP is being redistributed into itself.
- C. Certkiller 2 needs a network statement for 150.100.0.0.
- D. Automatic summarization is enabled on Certkiller 1 and Certkiller 2.
- E. The hold-down timers are set too high.

Answer: A

QUESTION 235

You work as a network administrator at Certkiller .com. You need to verify that the web server is accessible to all employees within the Certkiller .com intranet and also verify connectivity at all OSI layers.

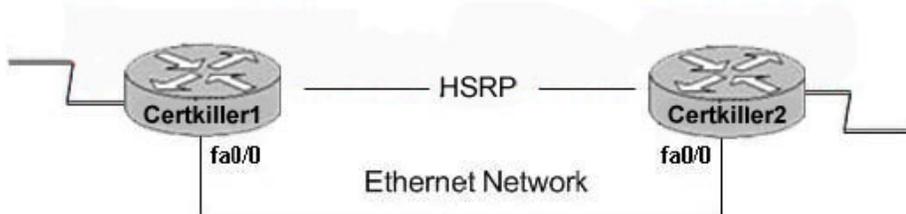
How can you test to ensure all layers of the OSI model are working correctly?

- A. Ping the web server.
- B. Telnet to port 80 of the web server.
- C. Issue the debug ip http server command.
- D. Issue the show ip http server command.
- E. Issue the netstat -r command.
- F. Ping the web server by name.

Answer: B

QUESTION 236

Exhibit, Network Topology



Exhibit, Console Messages

```
Jan 9 08:00:42.623: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Standby -> Active
Jan 9 08:00:56.011: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Active -> Speak
Jan 9 08:01:03.011: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Speak -> Standby
Jan 9 08:01:29.427: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Standby -> Active
Jan 9 08:01:36.808: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Active -> Speak
Jan 9 08:01:43.808: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Speak -> Standby
```

You work as a network administrator at Certkiller .com. Study the exhibit carefully.

The two routers Certkiller 1 and Certkiller 2 are configured with HSRP and are displaying similar console messages.

What are two possible causes of these console messages? Select two.

- A. overloaded Ethernet network
- B. incorrect routing protocol configuration
- C. Ethernet interface down
- D. intermittent physical layer problem
- E. ICMP redirection disabled.

Answer: A, D

QUESTION 237

On an Ethernet segment, users are experiencing sporadic connectivity. You issue the following command: show interface ethernet

The command reveals that the interface is up.

What are two other issues to address? Select two.

- A. Verify that the number of collisions in respect to the number of output packets is less than .01%.
- B. Verify that the number of collisions in respect to the number of output packets is less than .1%.
- C. Use a TDR to check for a jabbering transceiver.
- D. Make sure that the timers are set correctly on the Ethernet interface that connects the segments.

Answer: B, C

QUESTION 238

Exhibit

```
Certkiller1# debug crypto isakmp
Certkiller1#
01:02:54: ISAKMP (0): received packet from 192.168.192.2 (N) NEW SA
01:02:54: ISAKMP: local port 500, remote port 500
01:02:54: ISAKMP (0:1): processing SA payload. message ID = 0
01:02:54: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 100 policy
01:02:54: ISAKMP: encryption DES-CBC
01:02:54: ISAKMP: hash MD5
01:02:54: ISAKMP: default group 1
01:02:54: ISAKMP: auth pre-share
01:02:54: ISAKMP (0:1): atts are not acceptable. Next payload is 0
01:02:54: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 65535 policy
01:02:54: ISAKMP: encryption DES-CBC
01:02:54: ISAKMP: hash MD5
01:02:54: ISAKMP: default group 1
01:02:54: ISAKMP: auth pre-share
01:02:54: ISAKMP (0:1): atts are not acceptable. Next payload is 0
01:02:54: ISAKMP (0:1): no offers accepted!
01:02:54: ISAKMP (0:1): SA not acceptable!
01:02:54: ISAKMP (0:1): incrementing error counter on sa: PROPOSAL NOT CHOSEN
01:02:54: %CRYPTO-6-ISKMP_MODE_FAILURE: Processing of Main mode failed with peer at 192.168.192.2
01:02:54: ISAKMP (1): sending packet to 192.168.192.2 (R) MM_NO_STATE
01:06:19: ISAKMP (0:1): peer does not do paranoid keepalives.

01:06:19: ISAKMP (0:1): deleting SA reason "QM_TIMER expired" state (R) MM_NO_STATE (peer 192.168.192.2)
01:07:19: ISAKMP (0:1): purging SA.
```

You work as a network administrator at Certkiller .com. Study the exhibit carefully. An IPSec connection has failed between Certkiller 2 and Certkiller 3. Which two items are the most likely source of the problem? Select two.

- A. The hash methods do not match.
- B. The Diffie-Hellman group settings do not match.
- C. Pre-shared keys do not match.
- D. There is an invalid peer address.
- E. Paranoid keepalives need to be configured.

Answer: A, B

QUESTION 239

You work as a network administrator at Certkiller .com. You are troubleshooting a network connection and have issued the ping command. Which layer(s) of connectivity are you testing?

- A. Layer 1
- B. Layer 2
- C. Layer 3
- D. Layers 1-2
- E. Layers 1-3
- F. Layers 1-4

Answer: E

QUESTION 240

Certkiller works as a network administrator at Certkiller .com. When issuing a show interface serial command, Jack notices that the number of output drops is continuously increasing. She asks you what might be the cause of this. What should you tell her?

- A. The system is attempting to hand off packet to a transit buffer but no buffers are available.
- B. This is a normal and desirable effect.
- C. Too many packets from that interface are still being processed in the system.
- D. The cable is bad.

Answer: A

QUESTION 241

Over the past year the amount of traffic between certain access-layer network segments and the Certkiller 's intranet website has increased dramatically. The CPU utilization levels of network devices and intranet server are will within acceptable limits. Congestion has been observed at the connection between the access-layer switches and the distribution layer multilayer switches.

What should be done to help eliminate congestion?

- A. Upgrade access-layer switches to better performing models.
- B. Implement QoS features on the access-layer switches.
- C. Upgrade the end user Gigabit Ethernet links.
- D. Increase the bandwidth on the upstream links from the access-layer switches.
- E. Upgrade the distribution layer, multilayer switches to better performing models.
- F. Implement QoS features on the distribution layer, multilayer switches.
- G. None of the above

Answer: D

Explanation:

Since the congestion in this example appears to have been isolated to only the connection between the access switches and the distribution layer switches, to alleviate the congestion on these links the easiest and best way to do this would be to increase the bandwidth between these two devices.

Incorrect Answers:

- A: This will not help the problem. In fact, it may make matters worse since higher powered access switches may actually send more traffic to the distribution switches, causing even more congestion on the links.
- B, F: Although QoS mechanisms can be used to ensure that mission critical traffic gets priority over other traffic types, implementing this alone will do nothing to alleviate the overall congestion problems on the links.
- C: This would enable the end stations to send and receive even more data, causing even more congestion on the links between the access and distribution layers.
- E: This solution would be better if the distribution layer switches were experiencing high utilization and high memory and CPU usage, but it would not help in reducing the overall congestion on the ethernet links to the access layer switches.

QUESTION 242

What are three possible causes of slow performance on a VLAN in a switched network? (Choose three.)

- A. No default route configured on the router used for inter-VLAN routing
- B. Incorrect VTP domain defined on a switch
- C. Malfunctioning network adapter in a device
- D. Duplex mismatch with devices on switch ports
- E. Incorrect cable between a device and the switch port
- F. None of the above

Answer: C, D, E

Explanation:

An incorrect or faulty network cable, malfunctioning network adapter, or duplex mismatch could decrease performance. For traffic destined to a network not within the

same IP subnet problems can arise when there is no default route configured on the router.

Incorrect Answers:

A: For traffic destined to a network not within the same IP subnet problems can arise when there is no default route configured on the router. However, this would stop all inter-vlan traffic from being processed, which would effectively stop the traffic, not slow the performance.

B: An incorrectly configured VTP domain would stop the traffic, not reduce it.

QUESTION 243

After updating your company's network security policy, a handful of users have been complaining that they can reach hosts through the router, but not all hosts on the other side of the network. Other users are not experiencing any problems at all. If the local host is properly configured, what could be the cause of the problem?

- A. The local router is down.
- B. The remote host is down.
- C. There is a misconfigured access list.
- D. There is no default gateway on the local host.

Answer: C

Explanation:

A misconfigured access list could prevent the client from accessing certain networks.

Incorrect Answers:

A: The local router cannot be down since we are able to access hosts on some remote networks.

B: The problem is not reachability of a single host. Some networks are not reachable.

D: We know that the router can be reached since we can reach some remote networks. The default gateway is correctly configured on the local host.

Reference: "Configuring IP Access Lists"

<http://www.cisco.com/warp/public/707/confaccesslists.html>

QUESTION 244

For the sake of maintaining a secure network, you've just set up an access list on router CK1 to prevent a route from being distributed via EIGRP, and now want to verify the access list to make sure that it's working correctly. What command could you issue (from the neighboring router) to verify this?

- A. show access-lists
- B. show route eigrp
- C. show ip eigrp route
- D. show ip route
- E. All of the above

Answer: D

Explanation:

showaccess-list: Show's the details of configured access lists for all protocols. therefore choice A is wrong.

showip route eigrp:is used to see the eigrp learned routes...Choice C is wrong because of the format of the command. Choice B is also wrong because there is no such command.

showip route

To display all static IP routes, or those installed using the AAA (authentication, authorization, and accounting) route download function, use the show ip route command in EXEC mode.

showip route [address [network-mask] [longer-prefixes]] | [protocol [process-id]] | [static [download]]

show ip route command is used to verify the IP routes that are valid.

QUESTION 245

It has just come to your attention that an access list your junior administrator has implemented (access list 80) is preventing web traffic from coming in through your router. What command could you do to undo this mishap?

- A. no ip access-group 80 in
- B. ip access-group 80 out
- C. ip access-group 80 in
- D. no ip access-group 80 out

Answer: A

Explanation:

The only questions with the correct syntax are A & D as the the 'no' parameter has to be specified to remove an access list. The access list mentioned in this access list is an inbound access list, because it is blocking traffic from coming in and going through; so the command no ip access-group 80 in is correct.

QUESTION 246

You need to ensure that NTP traffic can pass through access list 101, which is configured on router CK1 . Which of the following choices will allow NTP traffic?

- A. access-list 101 permit ICMP 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
- B. access-list 101 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
- C. access-list 101 permit udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
- D. access-list 101 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255

Answer: C

Explanation:

Network Time Protocol (NTP) is used to synchronize time on multiple devices. The

Network Time Protocol (NTP) is a protocol used to provide for timestamp information to network devices. NTP runs over UDP, which in turn runs over IP. Only the access list in choice C permits the necessary UDP traffic.

QUESTION 247

SIMULATION

Case Study:

You're the senior network administrator at Certkiller . A few weeks ago you completed a migration to a value orientated ISP, and you outsourced a technician to configure the GATE router with the new address space, and new access lists. Since then productivity is down, because lower tiered employees have no access to the internet. Customers have also been complaining that they can't reach any of the services they subscribed to on the web server. However, employees local to the site have had no problems at all.

Certkiller 's new company security policies revolve around a strict implementation of NAT and ACLs on the Gate router; which dictates that traffic to the inside hosts **MUST** be explicitly defined in the ACL. Also, command authorizations have been put in place to prevent the usage of any debug commands. Your task is to find and correct the access issues.

Make use of the following information:

Use the topology provided and the following information to find and current the current issues.

LAN

Fa0/0: 10.10.11.2/24

Fa0/1: 10.20.0.1/16

GATE

FA0/0: 10.10.11.1/24

FA0/1: 10.10.10.1/24

INTERNET

S0/1: 172.16.0.1/30

Web Server

Internal: 10.10.10.10/24 (Inside local Address)

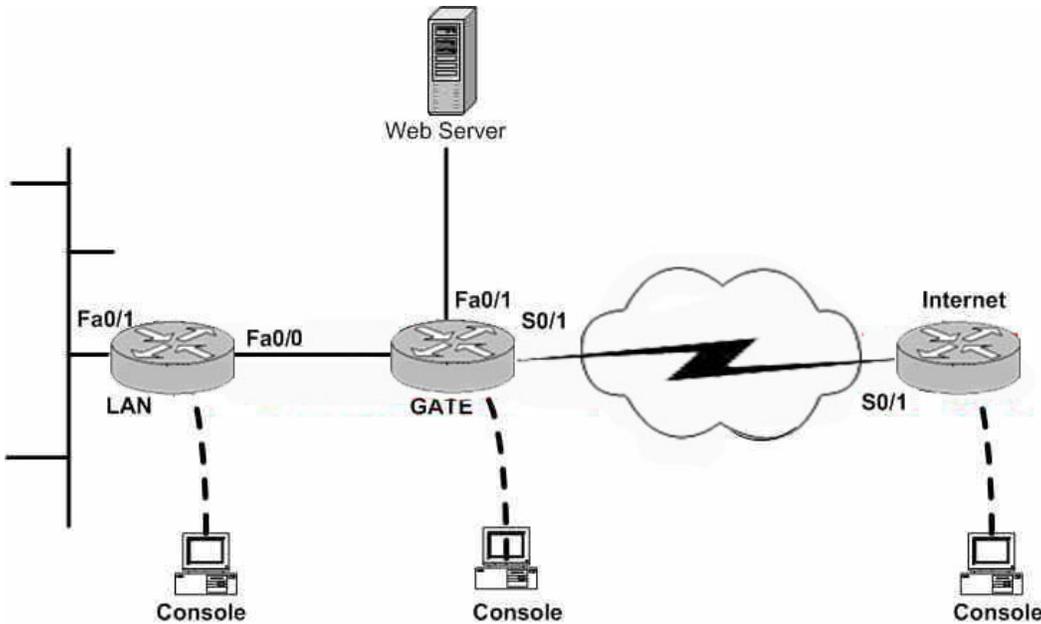
External: 198.133.219.10/24 (Inside Global Address)

LAN

Inside Global Address: 198.133.219.1/24

All passwords: Certkiller

To configure the router click on the host icon that is connected to a router by a serial cable.



Answer:

Disable access list 101 from Serial 0/1 on GATE router.

No ip access-group 101 in

Create a new ACL 130 (example)

Access-list 130 permit tcp any host 198.133.219.10 eq 80

(allows Any access from internet by port 80 to the Web server which has NAT to 10.10.10.10)

Access-list 130 permit ip any host 198.133.219.1 (loopback interface IP Address)

The GATE router is configured so that any outgoing access from Internal LAN addresses gets translated to the Loopback Interface IP address. The question does not specify which ports and therefore allowing IP is the best option.

Note: If you're using HOST in the ACL then you do not need to define 255.255.255.255.

This would be wrong.

Apply access list 130 to the Serial0/1

Ip access-group 130 in

To Test:

1. Ping from internal router to the Internet Router. (Out going access to Internet Checked)
2. Telnet from the Internet router to the web server external IP by port 80. (Incoming access to Web server from customers checked)

QUESTION 248

What criteria does a standard access-list use to block traffic? (Choose all that apply)

- A. User account
- B. Wildcard mask
- C. Source IP address
- D. Domain name
- E. Full MAC address only

Answer: B, C

Explanation:

Standard access lists (access lists numbered 1-99) only filter traffic based on the source IP address or source IP subnet. Only extended access lists are able to filter based on additional criteria, such as destination IP subnet and transport layer port information.

QUESTION 249

You enter "show crypto map" command on Two separate Certkiller routers, RouterA and RouterB as shown below:

```
RouterA#show crypto map
Crypto Map "test" 10 ipsec-isakmp
Peer = 172.26.167.2
Extended IP access list 140
access-list 140 permit ip 172.26.160.0 0.0.3.255 172.20.0.0 0.3.255.255
access-list 140 permit ip 172.26.164.0 0.0.1.255 172.20.0.0 0.3.255.255
access-list 140 permit ip 172.26.160.0 0.0.3.255 172.24.0.0 0.1.255.255
access-list 140 permit ip 172.26.164.0 0.0.1.255 172.24.0.0 0.1.255.255
Current peer: 172.26.167.2
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={
auth2,
}
Interfaces using crypto map test
Serial1/0
RouterA#
```

```
RouterB#show crypto map
Crypto Map "test" 10 ipsec-isakmp
Peer = 172.26.167.1
Extended IP access list 133
access-list 133 permit ip 172.26.160.0 0.0.3.255 172.20.0.0 0.3.255.255
access-list 133 permit ip 172.26.164.0 0.0.1.255 172.20.0.0 0.3.255.255
access-list 133 permit ip 172.26.160.0 0.0.3.255 172.24.0.0 0.1.255.255
access-list 133 permit ip 172.26.164.0 0.0.1.255 172.24.0.0 0.1.255.255
Current peer: 172.26.167.1
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={
auth2,
}
Interfaces using crypto map test:
Serial1/0
RouterB#
```

From your analysis of the above command output; what will happen if an IPSec connection is attempted between RouterA and RouterB?

- A. Because there are no transform sets configured, no security association will be established.
- B. Because there are misconfigured access control lists, no security association will be established.
- C. Because of the mirror image of peer IP addresses, no security association will be

established.

D. Security association will be established normally as expected.

Answer: B

Explanation:

The access lists on each peer should mirror each other (all entries should be reversible). This example illustrates this point.

Incompatible or Incorrect Access Lists

If the access lists on the two routers do not match or at least overlap, INVALID PROXY IDS or PROXY IDS NOT SUPPORTED results. It is recommended that access lists on the two routers be 'reflections' of each other. It is also recommended that you do not use the key word "any" in match address access lists.

```
3d00h: IPsec(validate_proposal_request): proposal part #1,  
(key eng. msg.) dest= 172.16.171.5,
```

```
src=http://www.cisco.com/univercd/cc/td/doc/product/vpn/solution/aswan15/om
```

```
172.16.171.27, dest_proxy= 172.16.171.5/255.255.255.255/0/0 (type=1),
```

```
src_proxy= 172.16.171.27/255.255.255.255/0/0 (type=1),
```

```
protocol= ESP, transform= esp-des esp-sha-hmac , lifedur=
```

```
0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
```

```
3d00h: validate proposal request 03d00h:
```

```
IPsec(validate_transform_proposal): proxy identities not
```

```
supported3d00h: ISAKMP (0:3): IPsec policy invalidated
```

```
proposal3d00h: ISAKMP (0:3): phase 2 SA not acceptable!
```

```
Access List:accesslist 110 permit ip host 172.16.171.5 host
```

```
172.16.171.30Reference:
```

```
http://www.cisco.com/en/US/netsol/ns341/ns396/ns172/ns334/networking_solutions_design_guide_chapter0918
```

QUESTION 250

While you were out on vacation, your junior administrator has made a handful of configuration changes. As soon as you arrive to the job site, a swarm of users are complaining about their Internet connection. They can all browse the web, but they can't access their email. What is the most likely cause of the problem?

- A. IP RIP filters
- B. IP access list is misconfigured
- C. IPX encapsulation conflicts with IP
- D. Buffer size are configured too small.
- E. EIGRP is not configured on the WAN interface.

Answer: B

Explanation:

Web browsing traffic, but not email traffic, is passing the router. It seems that the router is blocking SMTP (and/or POP) traffic. IP Access lists can be used to block or allow

traffic based on the IP protocol. We must make sure the IP Access lists does not block SMTP traffic.

Reference: "Configuring IP Access Lists"

<http://www.cisco.com/warp/public/707/confaccesslists.html>

QUESTION 251

Exhibit:

Mar 2 12:26:51.091: CRYPTO-SDU: Connection failed due to incompatible policy

What does the above command output imply?

- A. The wrong peer is set on the crypto map.
- B. The crypto algorithms do not match.
- C. The DSS key is missing or invalid.
- D. The IP address for the remote peer is incorrect.

Answer: B

Explanation:

You must enable all Data Encryption Standard (DES) algorithms that are used to communicate with any other peer encrypting router. If you do not enable a DES algorithm, you will not be able to use that algorithm, even if you try to assign the algorithm to a crypto map at a later time.

If your router attempts to set up an encrypted communication session with a peer router, and the two routers do not have the same DES algorithm enabled at both ends, the encrypted session fails. If at least one common DES algorithm is enabled at both ends, the encrypted session can proceed.

If the crypto algorithms do not match, you receive this error message.

Mar 2 12:26:51.091: CRYPTO-SDU: Connection failed due to incompatible policy

Reference:

http://www.cisco.com/en/US/tech/CK5_83/CK3_72/technologies_tech_note09186a0080094628.shtml

QUESTION 252

You've just enabled the OSPF process on your router with the command `router ospf 1` but the process fails to start, what is probably causing the problem?

- A. The OSPF process id does not match the neighbor's process ID.
- B. The router is already running another OSPF process (e.g. `router ospf 2`).
- C. All the IP interfaces on the router are down.
- D. The OSPF process will start only after the network statements have been given.
- E. The OSPF process will start only after the OSPF neighbor is detected.

Answer: C

Explanation:

All OSPF routers need to have a local router ID. For an OSPF router, the IP address assigned to the first interface that comes up is the router ID. If a loopback address is configured, then the IP address assigned to this interface will become the router ID. If no IP networks are up, the OSPF router will be unable to obtain a router ID, so the entire OSPF process will fail.

QUESTION 253

Part of the configuration file for router CK1 is displayed below:

```
router ospf 1
redistribute eigrp 100 metric 20 metric-type 1
network 172.16.0.0 0.0.255.255
```

A network administrator is troubleshooting a route redistribution configuration between EIGRP 100 and OSPF 1. Currently, some of the networks, such as network 10.1.1.0/24 and network 10.2.2.0/24 within the EIGRP domain are not being redistributed into OSPF 1.

Given the above configuration, what is the problem?

- A. The redistribute command should specify metric-type 2.
- B. The redistribute command is missing the subnets option.
- C. The redistribute command should be configured under eigrp 100.
- D. The redistribute command should use an EIGRP compatible metric value such as 64 1000 100 1 1500.

Answer: B

Explanation:

When routes are redistributed into OSPF, only routes that are not subnetted are redistributed if the subnets keyword is not specified. Since EIGRP and OSPF both support the use of Variable Length Subnet Masking (VLSM), using the keyword "subnets" is needed to ensure that all IP subnets are redistributed into OSPF.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_chapter09186a008017

QUESTION 254

You're a network administrator at Certkiller and to keep up with growth you've upgraded the networks to use BGP as the external routing protocol. While verifying operations you notice that one of your routes (192.27.125.0/24) isn't being propagated to all the devices in the network. After checking the access lists and the routing configurations, there does not appear to be any reason why this route is not being propagated. What should be the next step in resolving this issue?

- A. Clear the BGP session.
- B. Use the release BGP routing command.
- C. Use the service-policy command to adjust the QOS policy to allow the route to propagate.

D. Change both the inbound and outbound policy related to this route.

Answer: A

Explanation:

The clear "ip bgp" command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions. After configuring BGP initially, it may be necessary to reset the BGP process by using the "clear ip bpg *" in order to ensure that all routes get propagated throughout the network.

QUESTION 255

While troubleshooting an EIGRP connection between Router CK1 (10.1.2.1) and Router CK2 (10.1.2.2) you enter the following command on CK1 :

```
Router CK1 # debug eigrp packets
```

```
01:39:13: EIGRP: Received HELLO on Serial0/0 nbr 10.1.2.2
```

```
01:39:13: AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 un/rely 0/0
```

```
peerQ un/rely 0/0
```

```
01:39:13: K-value mismatch
```

Based on the output above, what is true about Router CK1 ?

- A. Router CK1 received a hello packet with mismatched autonomous system numbers.
- B. Router CK1 received a hello packet with mismatched hello timers.
- C. Router CK1 received a hello packet with mismatched authentication parameters.
- D. Router CK1 received a hello packet with mismatched metric-calculation mechanisms.
- E. Router CK1 will form an adjacency with Router CK2 .
- F. Router CK1 will not form an adjacency with Router CK2 .

Answer: D, F

Explanation:

The command debug eigrp packet shows the packets sent and received by the router. Although Router CK1 received a hello packet, all of the values except for the AS came up to zero, so its safe to assume that there's a mismatched metric-calculation mechanism. Router CK1 will NOT form an adjacency with Router CK2 because the K values are mismatched. Mismatched K values (EIGRP metrics) can prevent neighbor relationships from being established and can negatively impact network convergence. The following error message is displayed in the console of ROUTER-B because the K values are mismatched:

```
*Apr 26 13:48:41.811: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
```

```
10.1.1.1 (Ethernet0/0) is
```

```
down: K-value mismatch
```

Reference: Configuring IP Enhanced EIGRP

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfeigrp.htm

QUESTION 256

In order for an OSPF neighbor relationship to form between two Certkiller routers, which three hello packet parameters have to match? (Choose three)

- A. Hello/dead timer
- B. Router priority
- C. Stub area flag
- D. Area ID
- E. DR IP address
- F. BDR IP address

Answer: A, C, D

When troubleshooting OSPF neighbor relationships, verify that the following HELLO parameters match on the neighboring interfaces:

1. OSPF area number (Issue the show ip ospf interface interface-name command to check.)
2. OSPF area type, such as stub or NSSA (Issue the show ip ospf command to check.)
3. Subnet and subnet mask (Issue the show interface command to check.)
4. OSPF HELLO and Dead timer values (Issue the show ip ospf interface interface-name command to check.)

Reason for Neighbor Adjacency Problem	Commands for Diagnosing the Problem
OSPF is not configured on one of the routers.	show ip ospf
OSPF is not enabled on an interface where it is needed.	show ip ospf interface
OSPF HELLO or Dead timer interval values are mismatched.	show ip ospf interface
ipospf network-type mismatch on the adjoining interfaces.	show ip ospf interface
OSPF area-type is stub on one neighbor, but the adjoining neighbor in the same area is not configured for stub.	show running-config show ip ospf interface
OSPF neighbors have duplicate Router	show ip ospf

IDs.	show ip ospf interface
OSPF is configured on the secondary network of the neighbor, but not on the primary network; this is an illegal configuration which prevents OSPF from being enabled on the interface.	show ip ospf interface show running-config
OSPF HELLOs are not processed due to a lack of resources, such as high CPU utilization or not enough memory.	show memory summary show memory processor
An underlying Layer problem is preventing OSPF HELLOs from being received.	show interface

QUESTION 257

When troubleshooting an EIGRP configuration across the Certkiller discontinuous network; what should you do to ensure that the routers receive the correct routing information?

- A. Nothing, EIGRP supports discontinuous networks by default.
- B. The administrator must disable automatic summarization with the command no auto-summary.
- C. The administrator must enable manual summarization with the command ip summary-addresss.
- D. The administrator must enable classless routing with the command ip classless.
- E. The administrator must specify a default network with the command ip default-network.

Answer: B

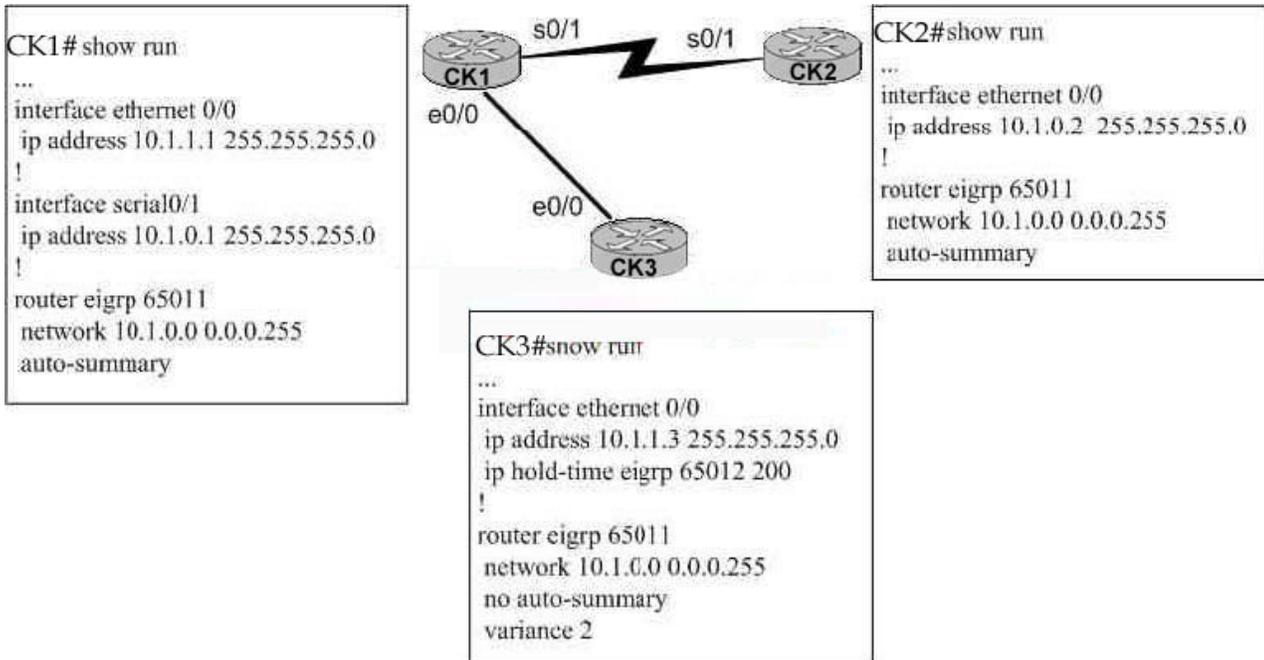
Explanation:

By default, EIGRP routers will automatically summarize the IP networks at the class boundary. Therefore, in order to ensure that all networks get propagated across a discontinuous network, EIGRP should have the automatic summarization function disabled.

QUESTION 258

The Certkiller network is displayed below:

642-831



CK1 has an EIGRP neighbor relationship with CK2 , but is unable to establish a neighbor relationship with CK3 . CK1 and CK3 can successfully ping each other. Based on the configuration files of the 3 routers shown above, what problems exist? (Select two)

- A. The no auto-summary command needed on CK3 .
- B. Incorrect mask on the EIGRP network statement of CK1 .
- C. Mismatch autonomous system number between CK1 and CK3 .
- D. Mismatch variance multiplier between CK1 and CK3 .
- E. Mismatch hold-time between CK1 and CK3 .

Answer: B, C

Explanation:

B: The mask on CK1 's network statement is 10.1.0.0 0.0.0.255, which means that the EIGRP process will only be running on interface S0/1. The correct network statement should be 10.1.0.0 0.0.255.255.

C: The CK3 ´s autonomous system number is 65012, while the CK1 ´s autonomous system number is 65011. There is a mismatch.

Incorrect Answers:

A: Since all networks belong to the same 10/8 major network boundary, the automatic summarization will not become a factor.

D: The variance parameter on router CK3 is not a factor. Variance is used for load balancing traffic over unequal-cost paths. In this case, router CK3 only has one single link so no load balancing will take place.

E: The configured hold time values on CK3 apply to EIGRP process 65012, and not 65011 so this is not a factor.

QUESTION 259

You are reviewing a BGP configuration on router CK1 due to reported routing issues.

What result would the following BGP commands have when applied to the CK1 ?

```
routerbgp 100
```

```
redistributeospf 1 match external
```

- A. Only OSPF type 1 external routes will be distributed into BGP.
- B. All types of OSPF routes will be distributed into BGP, including external routes.
- C. Only type 1 and type 2 external OSPF routes will be distributed into BGP.
- D. The external OSPF route types must be specified. This is an incomplete configuration.

Answer: C

Explanation:

If you configure the redistribution of OSPF into BGP without keywords, only OSPF intra-area and inter-area routes are redistributed into BGP, by default. You can use the internal keyword along with the redistribute command under router bgp to redistribute OSPF intra- and inter-area routes.

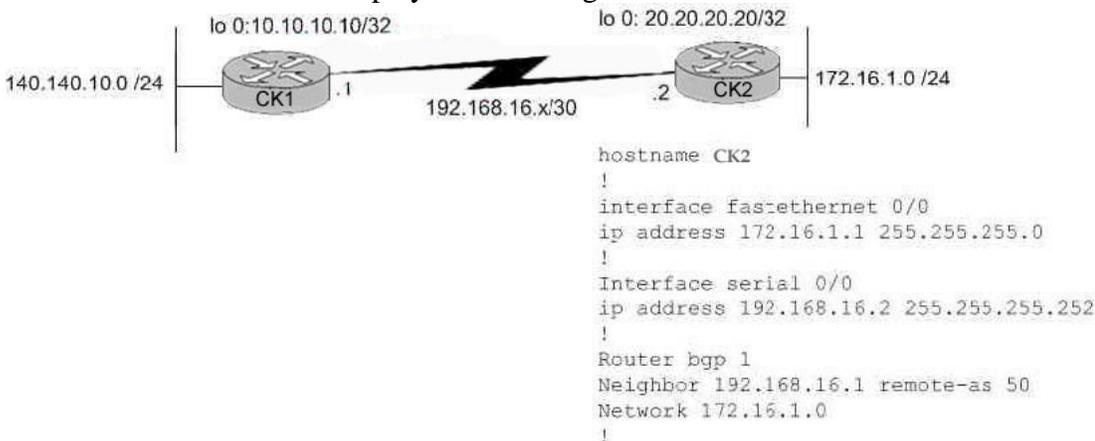
Use the external keyword along with the redistribute command under router bgp to redistribute OSPF external routes into BGP. With the external keyword, you have three choices:

1. redistribute both external type-1 and type-2 (Default)
2. redistribute type-1
3. redistribute type-2

Therefore, in this example, both Type 1 and Type 2 external routes will be redistributed.

QUESTION 260

The Certkiller network is displayed in the diagram below:



The following are occurring on this network:

1. Hosts on network 140.140.10.0 are unable to reach hosts on network 172.16.1.0.
2. Router CK1 does NOT have a route in its routing table pointing to 172.16.1.0
3. A valid EBGP session is established between CK1 and CK2 , as confirmed with "show ip bgp neighbor"

What is causing this problem?

- A. The network statement is missing the mask.
- B. The auto-summary is feature disabled.
- C. An aggregate address is needed on CK2 .
- D. 172.16.1.0/24 does not appear in the route table of CK2 .

Answer: A

Explanation:

Routes Announced Using a Basic Network Statement:

When announcing routes using a basic network statement, the behavior of the network command varies depending on whether auto-summary is enabled or disabled. When auto-summary is enabled, it summarizes the locally originated BGP networks (network x.x.x.x) to their classful boundaries (auto-summary is enabled by default in BGP). If a subnet exists in the routing table and the following three conditions are satisfied, any subnet (component route) of that classful network in the local routing table prompts BGP to install the classful network into the BGP table:

1. Auto-summary enabled
2. Classful network statement for a network in the routing table
3. Classful mask on that network statement

When auto-summary is disabled, the routes introduced locally into the BGP table are not summarized to their classful boundaries.

Reference:

http://www.cisco.com/en/US/tech/ CK3 65/technologies_tech_note09186a00800945ff.shtml#topic1

QUESTION 261

While troubleshooting a BGP router on the Certkiller network, it comes to your attention that the IP routing table isn't being updated with the iBGP-learned route. What do you suspect is causing this problem?

- A. The administrative distance for the route is too high.
- B. iBGP routes are not synchronized.
- C. The update-source interface command is missing from the BGP configuration.
- D. There is a misconfigured route reflector.
- E. The AS has been partitioned into confederations.

Answer: B

Explanation:

If BGP synchronization is enabled, which it is by default in Cisco IOS(r) Software, there must be a match for the prefix in the IP routing table in order for an internal (iBGP) path to be considered a valid path. If the matching route is learned from an OSPF neighbor, its OSPF router ID must match the BGP router ID of the iBGP neighbor. Most users prefer to disable synchronization using the no synchronization BGP subcommand.

Note: Synchronization is disabled by default in Cisco IOS Software version 12.2(8)T and later.

QUESTION 262

Your apprentice network technician has just enabled route redistribution between EIGRP and RIP on RTA as shown below:

```
RTA(config)# router eigrp 24
RTA(config-router)# network 172.24.0.0
RTA(config-router)# redistribute rip
RTA(config-router)# redistribute connected
RTA(config-router)# default-metric 2
```

Based on this information, which of the following is true?

- A. The redistribute rip command is missing the subnets option.
- B. The redistribute connected command is missing the metric-type option.
- C. Both redistribute commands are missing the metric option.
- D. The default-metric value specified is incorrect.
- E. All of the above

Answer: D

Explanation:

EIGRP uses 5 different values for the metric called K-values. These 5 values represent the bandwidth, delay, reliability, load, and MTU. Therefore, 5 different values must be used, not just one as shown in this example.

The following example takes redistributed Routing Information Protocol (RIP) metrics and translates them into EIGRP metrics with values as follows: bandwidth = 1000, delay = 100, reliability = 250, loading = 100, and MTU = 1500.

```
router eigrp 109
network 172.16.0.0
redistribute rip
default-metric 1000 100 250 100 1500
```

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a008009

QUESTION 263

The Certkiller network is using IS-IS for the interior routing protocol. Which show command could you use to list all the system IDs of the known IS-IS routers?

- A. show clns neighbors
- B. show isis database
- C. show isis topology
- D. show clns neighbors detail
- E. show is-is neighbors detail

Answer: C

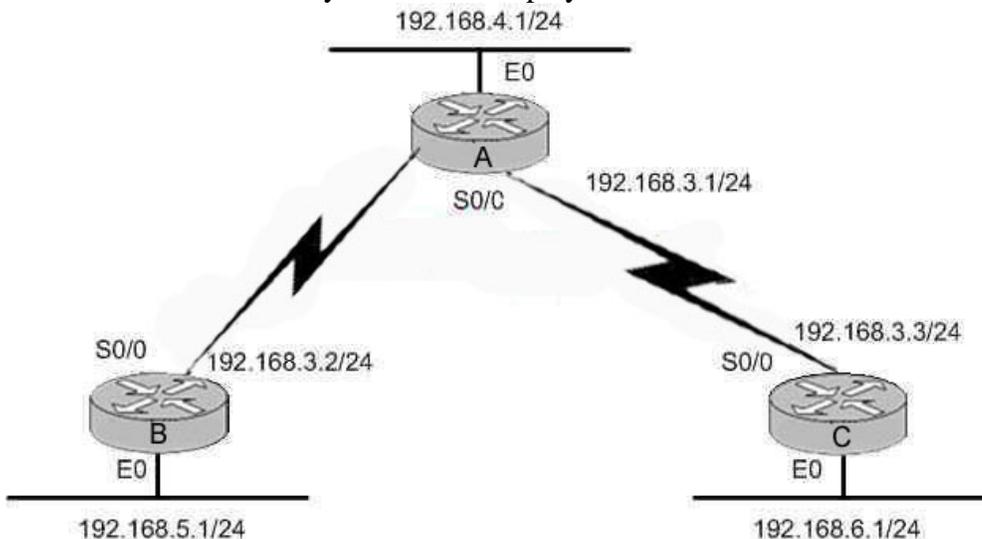
Explanation:

The command show isis topology is used to identify the presence and the connectivity of all IS-IS routers in all areas, including the following information fields:

Field	Description
Tag	Identifies the routing process.
System Id	Six-byte value that identifies a system in an area.
Metric	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system [ES], or a CLNS prefix).
Next-Hop	The address of the next hop router.
Interface	Interface from which the system was learned.
SNPA	Subnetwork point of attachment. This is the data-link address.

QUESTION 264

The Certkiller frame relay network is displayed below:



In this Certkiller frame relay network, the routing protocol used is EIGRP, and the entire network resides in autonomous system 1. RTB and RTC aren't receiving

routes from each other. What could you do to solve this problem?

- A. Configure the auto summary command under router eigrp.
- B. Issue the no ip split horizon command.
- C. Configure subinterfaces on the spoke routers and assign different IP address subnets for each subinterface.
- D. Check and change the access lists on RTA.
- E. Issue the no ip split horizon EIGRP 1 command.
- F. Configure a distribute list that allows the router to advertise all routes.

Answer: E

Explanation:

The split horizon rule prohibits a router from advertising a route through an interface that the router itself is using to reach the destination. To disable the split horizon behavior, use the no ip split-horizon eigrp as-number interface command. Some important points to remember about EIGRP split horizon are:

1. Split horizon behavior is turned on by default.
2. Changing the EIGRP split horizon setting on an interface resets all adjacencies with EIGRP neighbors reachable over that interface.
3. Split horizon should only be disabled on a hub site in a hub-and-spoke network.
4. Disabling split horizon on the spokes radically increases EIGRP memory consumption on the hub router, as well as the amount of traffic generated on the spoke routers.
5. EIGRP's split horizon behavior is not controlled or influenced by the ip split-horizon command.

IP split horizon checking is disabled by default for Frame Relay encapsulation to allow routing updates to go in and out of the same interface. An exception is the Enhanced Interior Gateway Routing Protocol (EIGRP) for which split horizon must be explicitly disabled.

Certain protocols such as AppleTalk, transparent bridging, and Internetwork Packet Exchange (IPX) cannot be supported on partially meshed networks because they require split horizon to be enabled (a packet received on an interface cannot be transmitted over the same interface, even if the packet is received and transmitted on different virtual circuits).

Configuring Frame Relay subinterfaces ensures that a single physical interface is treated as multiple virtual interfaces. This capability allows you to overcome split horizon rules so packets received on one virtual interface can be forwarded to another virtual interface, even if they are configured on the same physical interface.

Note: The use of sub-interfaces could also be used on router A to enable the remote locations to connect to each other.

QUESTION 265

Two routes are being learned on a Certkiller router from two different IP routing protocols. However, the protocol selected on the router is running on a slower interface. Which command should you use so that the protocol being run on the faster interface is more preferred?

- A. ip cost
- B. distance
- C. ip distance
- D. default-metric
- E. distribute-list
- F. All of the above

Answer: B

Explanation:

Routers will prefer routes with the lower administrative distance.

Default Distance Value Table

The table below lists the administrative distance default values of the protocols that Cisco supports.

Route Source	Default Distance Values
Connected interface	0
Static route*	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown**	255

* Static route pointing is always 1 regardless if it points to a next hop IP address or to an outgoing interface.

** If the administrative distance is 255, the router does not believe the source of that route and does not install the route in its routing table.

When using route redistribution, occasionally there may be a need to modify the administrative distance of a protocol so that it takes precedence. For example, if you want the router to select RIP-learned routes (default value 120) rather than IGRP-learned

routes (default value 100) to the same destination, you must increase the administrative distance for IGRP to 120+, or decrease the administrative distance of RIP to a value less than 100.

You can modify the administrative distance of a protocol using the distance command in the routing process subconfiguration mode, which specifies that the administrative distance is assigned to the routes learned from a particular routing protocol. This procedure is generally used when the network is being migrated from one routing protocol to another, the latter having a higher administrative distance. Keep in mind, however, that changing the administrative distance may lead to routing loops and black holes. So use caution if you change it.

In our example, we want to adjust the default AD of a particular route, which is done via the distance command.

QUESTION 266

You're in the midst of troubleshooting an OSPF neighbor establishment over a Frame Relay interface on router CK1 . Assuming that you've used the default OSPF network type on this interface, what additional change should you make to the frame network's configuration?

- A. Add the neighbor statements under router ospf.
- B. Add the ip ospf network point-to-multipoint statement under the Frame Relay interface.
- C. Add the ip ospf priority 0 statement under the Frame Relay interface on the DR.
- D. Add the ip ospf priority 0 statement under the Frame Relay interface on the BDR.
- E. Add the ip ospf priority 255 statement under the Frame Relay interface on the DROTHER.

Answer: A

Explanation:

On non-broadcast media such as Frame Relay, X.25, ATM, and Switched Multimegabit Data Service (SMDS), OSPF can run in two modes:

1. NBMA: simulates a broadcast model by electing a designated router (DR) and a backup designated router (BDR). There are two ways to simulate a broadcast model on an NBMA network: define the network type as broadcast with the ip ospf network broadcast interface sub-command or configure the neighbor statements using the router ospf command.

2. Point-to-multipoint: treats non-broadcast network as a collection of point-to-point links by configuring the ip ospf network point-to-multipoint command.

Incorrect Answers:

B: The network type should be specified as broadcast, not point to multipoint.

C, D: Although the hub site frame relay interface should be configured to ensure that it becomes the DR, when the priority is set to 0, the interface will be ineligible to become the DR or the BDR.

E: The hub site should be configured as the DR, not the DROTHER (neither a DR nor a BDR).

QUESTION 267

What command could an administrator use to see if the OSPF process is running on an interface?

- A. show interfaces
- B. show ip interface
- C. show ip protocols
- D. show ip ospf interface

Answer: D

Explanation:

The OSPF process ID on an interface is one of the pieces of information that the "show ip ospf interface" command provides all of the following:

1. interface state
2. IP address and Area
3. Process ID
4. Router ID
5. Network Type
6. Cost
7. Transmit Delay
8. State
9. Priority
- Designated Router
10. Interface Address
11. Designated Router
12. Interface Address
13. BDR
14. Timer Intervals
15. Neighbor Counts
16. Adjacent Neighbor Counts
17. Suppress Hello
18. Flood Queue Length

QUESTION 268

A portion of the routing table for the Certkiller router RTA is displayed below:

```
RTA#show ip router
<output omitted>
C   10.1.1.0 is directly connected, Serial0
D   172.16.1.0 [90/2681856] via 10.1.1.1, Serial0
D EX 192.168.1.0 [170/2681856] via 10.1.1.1,
00:00:04, Serial0
```

Based on this information, which of the following is true?

- A. 192.168.1.0 is known via a static route.

- B. 192.168.1.0 is known via a summarized route.
- C. 192.168.1.0 is known via a redistributed route into EIGRP.
- D. 192.168.1.0 is equal path load balancing with 172.16.1.0.

Answer: C

Explanation:

An external EIGRP route is displayed as EX when viewed in the routing table. Whenever any route is redistributed into another protocol, the route is considered to be external.

QUESTION 269

Two companies run different routing protocols after they are merged. Users experience intermittent IP communications problems. All desktop protocols work correctly.

What is the most likely cause of this problem?

- A. There is a virus being inherited
- B. NAT was not property configured
- C. There is a spanning tree loop in the network.
- D. The access list is not property implemented to stop feedback routes.

Answer: B

Explanation:

NAT (network address translation) is a system that translates addresses within a system. Typically, when two different networks merge, both network use the same private (RFC 1918) address space. To provide connectivity when this happens, NAT is used to translate the address space of one network into something else. In this example, it appears that NAT was not implemented properly, which is why there appear to be problems.

Incorrect Answers:

- A: Dangerous virus attacks don't cause intermittent communication problems, if they compromise communication they tend to compromise complete end system usability too. This is not the most probably cause for the problems.
 - C: Spanning tree is designed to prevent bridging loops, not to cause them. It will also not become a factor in reaching other IP subnets, since routing is used, not bridging.
 - D: If an access list was improperly configured, it would block traffic right from the beginning. The block wouldn't cause intermittent problems.
-

QUESTION 270

The Certkiller network is using EIGRP as the internal routing protocol. What is true about EIGRP? (Choose all that apply)

- A. EIGRP routers maintain an EIGRP Neighbor Table and an EIGRP Topology table.
- B. EIGRP triggered updates are flooded to every EIGRP router within the EIGRP AS.
- C. An EIGRP route will be in the active state if it lost the successor and no feasible successor is available.

- D. On Ethernet (Broadcast) networks, EIGRP routers only establish adjacencies with the DR and BDR.
- E. None of the above.

Answer: A, C

Explanation:

EIGRP routers always maintain two separate tables to provide connectivity to the network: the EIGRP neighbor table provides neighbor state information while the EIGRP topology table is used to maintain the overall state of the network.

When an EIGRP route is lost, the feasible successor is used to route around the failure. If no successors exist, the route will become stuck in active (SIA).

Incorrect Answers:

B: Although EIGRP does indeed utilize triggered updates, these are only sent to neighboring routers, not all routers.

D: Adjacencies are established with all routers on the segment. This statement is true for OSPF, not EIGRP.

QUESTION 271

OSPF is configured throughout the Certkiller network. What is true about OSPF?
(Select all that apply)

- A. OSPF uses a MAC address on the router as its router ID
- B. OSPF uses an IP address on the router as its router ID
- C. OSPF uses an IP address on the router as its OSPF community ID
- D. To configure the OSPF protocol on a router, you need at least one active interface configured with an IP address

Answer: B, D

Explanation:

OSPF routers use the highest configured IP address as the router ID. If a loopback address is configured, the IP address assigned to it will always be used as the router ID. In order for OSPF process to start, at least one IP interface on the router must be up and operational.

QUESTION 272

While attempting to configure OSPF on router CK1 you receive the following message:

OSPF: Could not allocate router id

What is the reason for the above response?

- A. too many interfaces with an IP address
- B. no OSPF ID
- C. no active interface with an IP address
- D. no active ARP entry with an IP address

Answer: C

Explanation:

All OSPF routers need to have a local router ID. For an OSPF router, the IP address assigned to the first interface that comes up is the router ID. If a loopback address is configured, then the IP address assigned to this interface will become the router ID. If no IP networks are up, the OSPF router will be unable to obtain a router ID, so the entire OSPF process will fail. Every OSPF router needs a router ID in order to operate, and therefore at least one interface with an IP address must be operational.

QUESTION 273

The Certkiller network is migrating from RIP version 1 to RIP version 2. Which of the following features are compatible with RIP version 2? (Choose two)

- A. Authentication
- B. Subnet mask information
- C. Unlimited hops
- D. Bandwidth, Delay, and Load used as metrics

Answer: A, B

Explanation:

RIP version 2 overcomes some of the limitations of RIP version 1. Namely, RIPv2 supports neighbor authentication and the use of Variable Length Subnet Masking (VLSM) through the use of advertising subnet mask information across the network.

Incorrect Answers:

- C: Like RIP version 1, the maximum number of hops for a RIPv2 network is 16 hops.
- D: RIPv2 only uses the number of hops as the routing metric, like version 1.

QUESTION 274

While troubleshooting a router, it comes to your realization that routing was never enabled. What is the first step needed to enable a dynamic routing protocol?

- A. Use the route-enable global configuration command.
- B. Use the router-config global configuration command.
- C. Use the route global configuration command.
- D. Use the router global configuration command.
- E. Use the router interface configuration command.

Answer: D

Explanation:

To enable a dynamic routing protocol, use the "router" global configuration command, followed by the network statements you want to advertise via the routing protocol.

Example: To enable RIP:

```
CK1 #config t
CK1 (config)# router RIP
```

QUESTION 275

You want to increase the security of the OSPF process used in the Certkiller network. Which authentication types can you configure on an OSPF interface? (Choose all that apply)

- A. PAP
- B. Message digest key
- C. Plain text authentication
- D. CHAP
- E. IPSec

Answer: B, C

Explanation:

OSPF supports both plain text password and MD5 neighbor authentication: RFC 2329(OSPF Standardization Report)

1. You must configure the MD5 key ID and password with the address message-digest-key md5 command.

1. Use to enable OSPF MD5 authentication and configure the MD5 key.

2. The MD5 key is a character string up to 16 characters long. You must also specify a key identifier and whether the key is entered in unencrypted or encrypted format. If you do not specify which, the string is assumed to be unencrypted.

3. Configures an interface already created, or creates a new OSPF interface and configures the MD5 key. The interface can have an IP address, or it can be unnumbered.

4. Example

5. host1(config-router)#address 10.1.1.1 message-digest-key 1 md5 0

6. 9mwk6gdr76

<http://www.jnx.com/techpubs/software/erx/junose52/swconfig-routing-vol1/html/ospf-config10.html>

QUESTION 276

You want to configure router CK1 to forward traffic whenever possible to the best route. What command could you use to forward packets to the best route, when no default route exists?

- A. IP split horizon
- B. IP redirects
- C. IP proxy-arp
- D. IP classless

Answer: D

Explanation: Where the ip classless configuration command falls within the routing and forwarding processes is often confusing. In reality, IP classless only affects the operation of the forwarding processes in IOS; it doesn't affect the way

the routing table is built. If IP classless isn't configured (using the no ip classless command), the router won't forward packets to supernets. As an example, let's again place three routes in the routing table and route packets through the router. Note: If the supernet or default route is learned via IS-IS or OSPF, the no ip classless configuration command is ignored. In this case, packet switching behavior works as though ip classless were configured.

```
router# show ip route
```

```
....
```

```
172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
```

```
D 172.30.32.0/20 [90/4879540] via 10.1.1.2
```

```
D 172.30.32.0/24 [90/25789217] via 10.1.1.1
```

```
S* 0.0.0.0/0 [1/0] via 10.1.1.3
```

Remembering that the 172.30.32.0/24 network includes the addresses 172.30.32.0 through 172.30.32.255, and the 172.30.32.0/20 network includes the addresses 172.30.32.0 through 172.30.47.255, we can then try switching three packets through this routing table and see what the results are.

1. A packet destined to 172.30.32.1 is forwarded to 10.1.1.1, since this is the longest prefix match.
2. A packet destined to 172.30.33.1 is forwarded to 10.1.1.2, since this is the longest prefix match.
3. A packet destined to 192.168.10.1 is forwarded to 10.1.1.3; since this network doesn't exist in the routing table, this packet is forwarded to the default route.
4. A packet destined to 172.30.254.1 is dropped.

The surprising answer out of these four is the last packet, which is dropped. It's dropped because its destination, 172.30.254.1, is within a known major network, 172.30.0.0/16, but the router doesn't know about this particular subnet within that major network.

This is the essence of classful routing: If one part of a major network is known, but the subnet toward which the packet is destined within that major network is unknown, the packet is dropped.

The most confusing aspect of this rule is that the router only uses the default route if the destination major network doesn't exist in the routing table at all.

Reference:

http://www.cisco.com/en/US/tech/CK3_65/technologies_tech_note09186a0080094823.shtml#forwarding

QUESTION 277

You are considering the proper routing protocol to use within the Certkiller network. For larger networks, why is it preferable to use OSPF over RIP? (Choose all that apply)

- A. Diffusing Update Algorithm
- B. Faster convergence
- C. Higher routing update overhead
- D. Lower routing update overhead
- E. No hop count limitation
- F. None of the above

Answer: B, D, E

Explanation:

The biggest advantage of OSPF is that it is efficient; OSPF requires very little network overhead even in very large internetworks. The biggest disadvantage of OSPF is its complexity; OSPF requires proper planning and is more difficult to configure and administer.

OSPF uses a Shortest Path First (SPF) algorithm to compute routes in the routing table. The SPF algorithm computes the shortest (least cost) path between the router and all the networks of the internetwork. SPF-calculated routes are always loop-free.

Instead of exchanging routing table entries like RIP routers, OSPF routers maintain a map of the internetwork that is updated after any change to the network topology. This map, called the link state database, is synchronized between all the OSPF routers and is used to compute the routes in the routing table. Neighboring OSPF routers form an adjacency, which is a logical relationship between routers to synchronize the link state database.

Changes to internetwork topology are efficiently flooded across the entire internetwork to ensure that the link state database on each router is synchronized and accurate at all times. Upon receiving changes to the link state database, the routing table is recalculated. OSPF using link cost information in determining routes instead of hop counts, overcoming the 16 hop limitation of RIP.

QUESTION 278

One of the Certkiller routers contains a CxBus. What is the speed of this Cisco Extended Bus in Mbps?

- A. 384
- B. 533
- C. 1000
- D. 256
- E. None of the above.

Answer: B

Explanation:

According to the technical documentation at CCO:

CxBus shorts for Cisco Extended Bus. It is the 533-megabit-per-second (Mbps) data bus in the Cisco 7000 series routers used for interface processors. It is the high speed backplane used by Cisco 7000 routers.

Reference:

http://www.cisco.com/en/US/products/hw/routers/ps332/products_user_guide_chapter09186a00800ed64d.html

QUESTION 279

While verifying the IPSec configuration on router Certkiller 333, debugging was enabled as shown below:

Certkiller333 # debug crypto ipsec

```
IPSEC(validate_proposal): invalid local address 12.2.6.2  
ISAKMP (0:3): atts not acceptable. Next payload is 0  
ISAKMP (0:3): SA not acceptable.
```

What is the possible cause of this error message?

- A. The crypto map is applied to the incorrect interface
- B. The Phase 1 policy map does not match.
- C. The remote peer IP address is incorrectly specified
- D. The IPsec transform proposals do not match

Answer: A

Explanation:

Invalid Local Address:

This output is an example of the error message.

```
IPSEC(validate_proposal): invalid local address 12.2.6.2
```

```
ISAKMP (0:3): atts not acceptable. Next payload is 0
```

```
ISAKMP (0:3): SA not acceptable!
```

This error message is attributed to one of these two common problems.

1. The crypto map map-name local-address interface-id command causes the router to use an incorrect address as the identity because it forces the router to use a specified address.
2. Crypto map is applied to the wrong interface or is not applied at all. Check the configuration in order to ensure that crypto map is applied to the correct interface.

Reference:

http://www.cisco.com/en/US/tech/CK5_83/CK3

[72/technologies_tech_note09186a00800949c5.shtml#inv_local](http://www.cisco.com/en/US/tech/CK5_83/CK3_72/technologies_tech_note09186a00800949c5.shtml#inv_local)

QUESTION 280

Two Certkiller EIGRP routers are connected as shown below:



<pre>Certkiller1# show run ... router eigrp 65031 network 10.1.0.0 0.0.255.255 metric weights 0 0 1 1 0 0 auto-summary no eigrp log-neighbor-changes ... Certkiller1 # show ip int brief Interface IP-Address OK? Method Status Prot serial0/1 10.1.0.1 YES NVRAM up up</pre>	<pre>Certkiller2# show run ... router eigrp 65031 network 10.1.0.0 0.0.255.255 metric weights 0 0 1 1 1 0 no auto-summary no eigrp log-neighbor-changes ... Certkiller2# show ip int brief Interface IP-Address OK? Method Status Prot serial0/1 10.1.0.2 YES NVRAM up up</pre>
---	---

Certkiller 1 and Certkiller 2 cannot establish an EIGRP neighbor relationship. Both Certkiller 1 and Certkiller 2 serial interfaces are showing status protocol up and can

successfully ping each other. Give the show outputs in the exhibit, what is the problem?

- A. auto-summary mismatch
- B. no eigrp log-neighbor changes
- C. metric weights mismatch
- D. needs a more specific network statement
- E. both routers missing the neighbor ip-address command

Answer: C

Explanation:

Mismatched K values (EIGRP metrics) can prevent neighbor relationships from being established and can negatively impact network convergence. The following example explains this behavior between 2 EIGRP peers (ROUTER-A and ROUTER-B).

The following error message is displayed in the console of ROUTER-B because the K values are mismatched:

```
*Apr 26 13:48:41.811: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
10.1.1.1 (Ethernet0/0) is down: K-value mismatch
```

There are two scenarios where this error message can be displayed:

The two routers are connected on the same link and configured to establish a neighbor relationship. However, each router is configured with different K values.

The following configuration is applied to ROUTER-

A. The K values are changed with

the metric weights command. A value of 2 is entered for the k1 argument to adjust the bandwidth calculation. The value of 1 is entered for the k3 argument to adjust the delay calculation.

```
hostnameROUTER-A
```

```
interfaceserial 0
```

```
ip address 10.1.1.1 255.255.255.0
```

```
exit
```

```
routerigrp 100
```

```
network 10.1.1.0 0.0.0.255
```

```
metric weights 0 2 0 1 0 0
```

The following configuration is applied to ROUTER-B. However, the metric weights command is not applied and the default K values are used. The default K values are 1, 0, 1, 0, and 0.

```
hostnameROUTER-B
```

```
interfaceserial 0
```

```
ip address 10.1.1.2 255.255.255.0!
```

```
exit
```

```
routerigrp 100
```

```
network 10.1.1.0 0.0.0.255
```

The bandwidth calculation is set to 2 on ROUTER-A and set to 1 (by default) on ROUTER-B. This configuration prevents these peers from forming a neighbor relationship.

The K-value mismatch error message can also be displayed if one of the two peers has transmitted a "goodbye" message, and the receiving router does not support this message. In this case, the receiving router will interpret this message as a K-value mismatch.

Reference:

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008045296f.html

QUESTION 281

You work as an administrator at Certkiller and you need to troubleshoot an ISDN connection. The output from the show isdn status command indicates that the communication between the router and the telco switch is performing correctly. However, the debug dialer command reveals no dialer activity.

What might be a possible reason for this problem?

- A. No dialer map is present or the IP address is incorrect
- B. Incorrect authentication parameters exist.
- C. The remote ISDN service line is busy.
- D. An incorrect ISDN switch type is defined.
- E. An interface has been shut down.

Answer: A

Explanation:

The dialer map statements translate next-hop protocol addresses to telephone numbers. Without statically configured dialer maps, DDR call initiation cannot occur. When the routing table points at a dialer interface, and the next-hop address is not found in a dialer map, the packet is dropped.

QUESTION 282

You work as a network administrator at Certkiller .com. During initial testing, a new Frame Relay link shows no connectivity between a local router and a remote router. The show interface command issued on the local router shows that the serial line is up and the line protocol is down.

Which condition could be causing this problem?

- A. bad cabling
- B. incorrect DLCIs
- C. excessive BECNs from the Frame Relay switch
- D. LMI type mismatch

Answer: D

QUESTION 283

A new Certkiller remote office has just been cabled and you are performing tests on the LAN. What should you pay particular attention to when troubleshooting copper cabling?

- A. Category 5 cable is used for all Ethernet connections.
- B. Straight-through cables are used for inter-switch links.
- C. Category 5 cables should not exceed 100 meters in length.
- D. Cross-over cables are used between switches and routers

Answer: A, C

Explanation:

When a network contractor try's to use a cheaper grade of cable, or try's to stretch a cable beyond a hundred meters without using a repeater, the segment will likely experience trouble. The distance and quality limits don't necessarily mean that data won't flow if a cable is over 100 meters, but past a certain point the integrity of the data can't be guaranteed. The IEEE recommended distance limitation for ethernet links is 100 meters. In some cases the problems won't appear until after a few months, or the problems will be intermittent if the line degrades, or the quality of the signal going through that line degrades.

Incorrect Answers:

B, D: Straight through cables are used for connecting hubs, routers, hosts, and other switches to a switch. Cross-over cables are used when connecting two routers together directly, or a host that is directly connected to a router's LAN port.

QUESTION 284

Which of the following symptoms are indicative of a network problem on the physical layer?

- A. Output of a show ip interface brief command shows DOWN/DOWN.
- B. Pings succeed only a percentage of the time.
- C. Output of show ip interface brief command shows UP/DOWN.
- D. The interface LED is amber on the affected device.

Answer: A

Explanation:

An interface is a physical layer device, and if the interface and the line is down, then you can reason that there is a problem with the physical layer.

Incorrect Answers:

B: Any successful ping verifies that the physical layer is operational. Intermittent ping successes indicate a layer 3 problem.

C: The status of the line protocol indicates the state of the data link layer.

D: This would indicate an operational physical connection, but a problem with the data link layer exists.

QUESTION 285

You need to troubleshoot some problems with the physical cabling at one of the Certkiller remote office branches. Which of the following tools are effective for checking the physical connection of a category 5 UTP network cable? (Choose two)

- A. TDR
- B. OTDR
- C. RMON
- D. Network monitor
- E. Digital multimeter

Answer: A, E

Explanation:

A: At the top end of cable testing equipment are those devices that provide time domain reflectometer (TDR), wire-map, and traffic monitoring functionality. The more expensive equipment of this kind surpasses the physical layer and reports on Media Access Control (MAC) layer information such as frame, error, and utilization statistics.

E: A digital multimeter can be used to troubleshoot a physical-layer problem in UTP cabling.

Incorrect Answers:

B: A TDR made for fiber-optic cable testing is called an optical TDR (OTDR). OTDR cannot be used on Category 5 UTP network cabling.

C: RMON is a network monitor. It is used to monitor network traffic, not to test physical-layer problems.

D: Network monitors are used to monitor network traffic, not to test physical-layer problems.

QUESTION 286

You need to troubleshoot some problems with the physical cabling at one of the Certkiller remote office branches. Which of the following network tools could you use to locate a damaged cable segment that's broken but with no opens or shorts?

- A. TDR
- B. network monitor
- C. digital multimeter
- D. protocol analyzer
- E. CiscoWorks 2000

Answer: A

Explanation:

TDRs are the most sophisticated cable testers. These devices can quickly locate open and short circuits, crimps, sharp bends, impedance mismatches, and other defects in metallic cables.

Reference: System Troubleshooting Guidelines

<http://www.cisco.com/univercd/cc/td/doc/product/voice/ics7750/tblshoot/trouble.htm>

QUESTION 287

You need to troubleshoot some problems with the physical cabling at one of the

Certkiller remote office branches. Which of the following tools are low cost and capable of determining cable continuity? (Choose two.)

- A. TDR
- B. OTDR
- C. volt-ohm meter
- D. digital-multi meter
- E. protocol analyzer

Answer: C, D

Explanation:

Volt-ohm meters and digital multimeters are at the lower end of the spectrum of cable-testing tools. These devices measure parameters such as AC and DC voltage, current, resistance, capacitance, and cable continuity. They are used to check physical connectivity.

Reference: Troubleshooting Tools

http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1902.htm

QUESTION 288

What actions should a network administrator execute, if they believe that there is faulty cabling connecting their LAN switches? (Choose all that apply)

- A. Check whether the Connected LED on the LAN switch port is on.
- B. Make sure the cable is correctly wired.
- C. If the LED is not on, check to make sure you are using the correct cable and that it is properly and securely attached.
- D. If the LED is on, check to make sure you are using the correct cable and that it is properly and securely attached.
- E. None of the above

Answer: A, B, C

Explanation:

The correct answers are common sense. If the LED is on, then it means the cable is secured properly, and if it is not broke it doesn't have to be fixed.

QUESTION 289

What could a trouble shooter do to eliminate the uncertainty of an incorrect punchdown connection?

- A. Replace the network adapter in the device.
- B. Replace the patch cable connected to the device.
- C. Check the impedance of the cable run with a cable scanner.
- D. Connect the device to the switch using a known-good external cable.

Answer: C

Explanation:

Do a cable test to check for incorrect punchdown or wiring maps using a cable tester. The other solutions provided in this question could be used to eliminate a bad port, cable, or NIC but it would not aid in the troubleshooting of the punchdown connection itself. Since we are not asked to provide for more than one answer, the best answer choice is C.

Reference:

General Troubleshooting Tools, Low-End Cable Test Equipment (CIT, Cisco Press)

QUESTION 290

Issuing the show controllers or show interface commands can help isolate problems on the _____ layer of the OSI model.

- A. Physical
- B. Application
- C. Transport
- D. Network
- E. Intermediate

Answer: A

Explanation:

Controllers and interfaces are physical components.

QUESTION 291

Line coding errors on a previously operational link are indicative of a problem at the _____ layer of the OSI model?

- A. Physical layer
- B. Data link layer
- C. Network layer
- D. Transport layer
- E. Application layer

Answer: A

Explanation:

Line coding errors are indicative of a physical layer problem with the circuit. Contact your Service Provider for framing and line coding settings. It is common to use binary 8-zero substitution (B8ZS) line coding with Extended Superframe (ESF), and alternate mark inversion (AMI) line coding with Super Frame (SF). For T1 interfaces, look for Clock Source is Line Primary in the show controller t1 output to verify that the clock source is derived from the network.

QUESTION 292

Hypothetically speaking; if a routers serial interface was NOT receiving clocking, what would the interface status and protocol state indicate?

- A. Status up
Protocol up
- B. Status administratively-down
Protocol up
- C. Status up
Protocol Down
- D. Status Down
Protocol Down

Answer: D

Explanation:

An interface receives clocking with the data it receives. If an interface wasn't receiving clocking it would mean that it wouldn't be receiving any data at all, so the status and the protocol would both be down.

Reference:

<http://www.cisco.com/univercd/cc/td/doc/product/voice/ics7750/tblshoot/tsserial.htm#1058610>

QUESTION 293

If you want to set the clock rate on Serial 0 of CK1 to 128000, what would be the configuration sequence?

- A. log in to CK1 , enable, config t, interface e0, clock rate 128000
- B. log in to CK1 , enable, config t, clock rate 128000
- C. log in to CK1 , enable, interface serial 0, clock rate 128000
- D. log in to CK1 , enable, config t, interface serial 0, clock rate 128000

Answer: D

QUESTION 294

If the show interfaces serial command output for CRC, framing errors, and aborts exceed _____% of the traffic, clocking problem is likely happening.

- A. 50%
- B. 30%
- C. 2.0%
- D. 20%

Answer: C

Explanation:

If you enter the exec command: show interfaces serial on both routers, and you see CRC,

framing errors, or aborts in EXCEEDING 0.5%-2.0% of all the traffic on the interface then you can be sure that there are clocking problems somewhere on the WAN

Reference:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1915.htm#xtocid12

QUESTION 295

On one of the Certkiller routers, you notice a large number of clocking problems on the serial interface. Which of the following conditions are capable of causing clocking problems? (Choose all that apply)

- A. Poor patch panel connections
- B. Cables out of specification
- C. Incorrect DSU/CSU configuration
- D. Several cables connected too far away (in a row)
- E. None of the above

Answer: A, B, C, D

Explanation:

In general, clocking problems in serial WAN interconnections can be attributed to one of the following causes:

1. Incorrect DSU configuration
2. Incorrect CSU configuration
3. Cables out of specification (longer than 50 feet [15.24 meters] or unshielded)
4. Noisy or poor patch panel connections
5. Several cables connected in a row

Reference:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1915.htm#xtocid12

QUESTION 296

Router Certkiller A is being used for a DSL connection and the following show command was issued:

```
Certkiller A# show dsl interface atm 0
ATU-R (DS ATU-C (US)
Modem Status: Showtime (DSTDSL_SHOWTIME)
DSL Mode: ITU G. 992.1 (G.DMT)
ITU STD NUM: 0x01 0x1
Vendor ID: 'ALCB' 'GSPN'
Vendor specific: 0x0000 0x0002
Vendor Country: 0x00 0x00
Capacity Used: 97% 100%
Noise Margin: 5.0 dB 6.0 dB
Output Power: 9.5 dBm 12.0 dBm
What can be determined with the given router output?
```

- A. The correct virtual path identifier/virtual identifier (VPI/VCI) values are configured

on the router.

- B. PPP is negotiating properly.
- C. The carrier detect light on the interface is off.
- D. The interface has successfully trained to the DSLAM.
- E. Layers 1, 2 and 3 are operating properly.

Answer: D

Explanation:

After you make sure that you have the right cable pinout and that your ISP has turned on the DSL service, you can further troubleshoot the DSL connection by watching the modem state of the ADSL interface as the line retrains.

To troubleshoot the modem state, follow these steps:

1. On the router, issue terminal monitor and debug atm event commands.

```
Router#terminal monitor
```

```
Router#debug atm event
```

```
ATM events debugging is on
```

2. Watch the debug messages on the screen.

If the modem state stays at "0x8" and says "Could not establish connection," it means that the Cisco SOHO77 has not heard from the central office (CO) . It does not see an incoming signal.

```
Router#
```

```
1d01h: DSL: 1: Modem state = 0x8
```

```
1d01h: DSL: 2: Modem state = 0x8
```

```
1d01h: DSL: 3: Modem state = 0x8
```

```
1d01h: DSL: 4: Modem state = 0x8
```

```
1d01h: DSL: 5: Modem state = 0x8
```

```
1d01h: DSL: Could not establish connection
```

```
<... snipped ...>
```

If the modem state changes from "0x8" to "SHOWTIME," it means that the Cisco SOHO77 has successfully trained with the DSLAM.

```
Router#
```

```
00:24:18: DSL: 2: Modem state = 0x8
```

```
00:24:21: DSL: 3: Modem state = 0x8
```

```
00:24:23: DSL: 4: Modem state = 0x8
```

```
00:24:26: DSL: 5: Modem state = 0x8
```

```
00:24:28: DSL: 6: Modem state = 0x10
```

```
00:24:31: DSL: 7: Modem state = 0x10
```

```
00:24:33: DSL: 8: Modem state = 0x10
```

```
00:24:36: DSL: 9: Modem state = 0x10
```

```
00:24:37: DSL: Received response: 0x24
```

```
00:24:37: DSL: Showtime!
```

Reference:

http://www.cisco.com/en/US/tech/ CK1 75/ CK1 5/technologies_tech_note09186a0080093e62.shtml

QUESTION 297

You work as a network engineer at Certkiller .com, an ISP. You have noticed that the PRI line connected to your access is not receiving dial-in users. After the PRI line connectivity to the access server was verified, you contact the line service provider. The service provider performs the necessary testing procedures and finds no problems with the line.

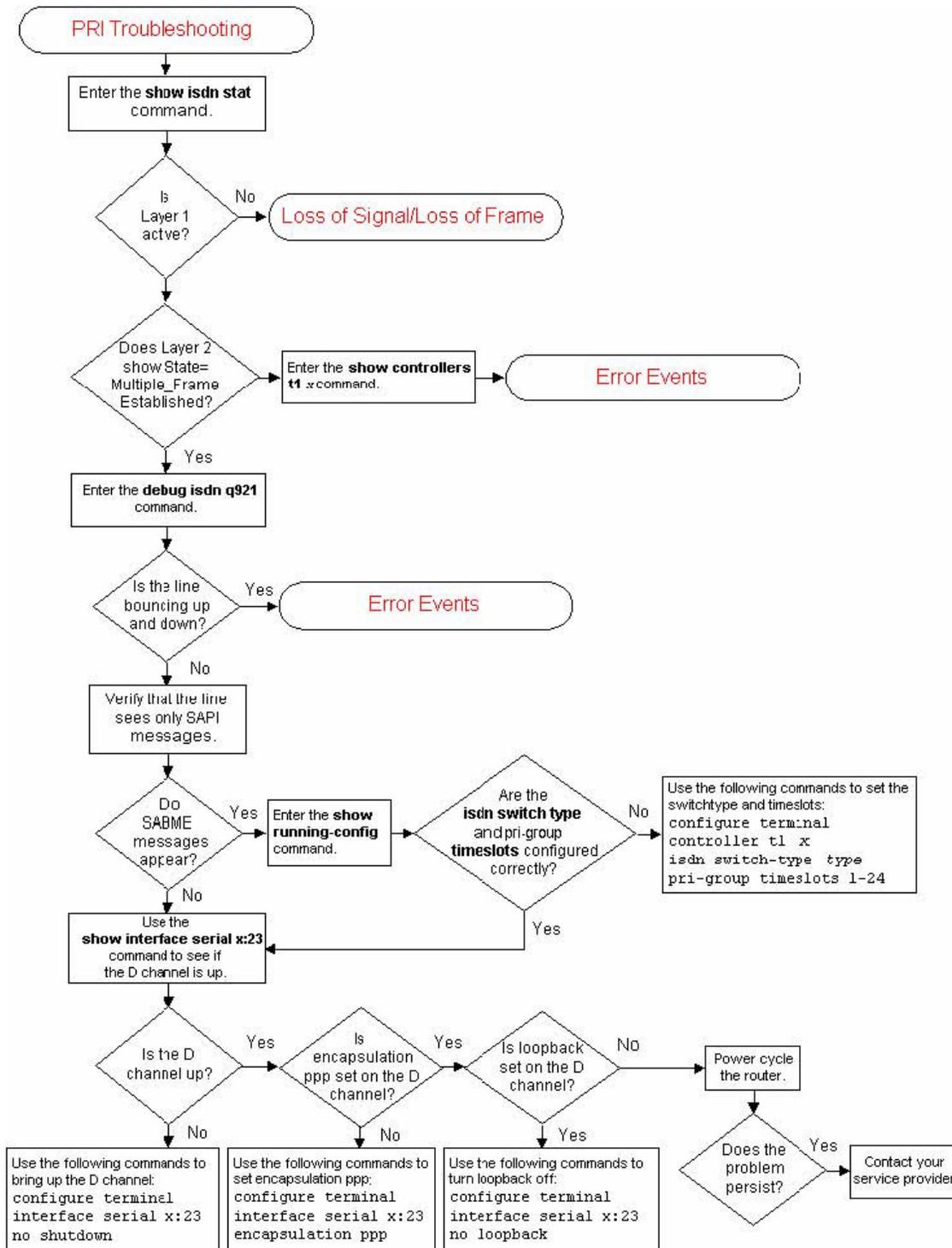
Which action should you perform next to further isolate the problem?

- A. Trace the PRI cable to verify physical layer connectivity
- B. Perform a hard loopback test on PRI line at access server
- C. Replace the access server interface module
- D. Change the PRI cable connected to access server

Answer: B

Explanation:

Since the ISDN service provider was able to successfully test the line with no problems found, the next logical step would be to check the connectivity on the PRI line at the access server. The general steps in troubleshooting a PRI line is outlined in the following flowchart:



Incorrect Answers:

A: This step was already taken.

C: This should be done only after some additional troubleshooting was done and the interface module is determined to in fact be the problem.

D: Before replacing the cable, a loopback test should be performed to see if the cable is working properly.

Reference: http://www.cisco.com/warp/public/116/t1_flchrt_pri.html

QUESTION 298

What type of interface will be created when the command `ppp multilink` is added to an ISDN BRI interface?

- A. serial 0/0
- B. BRI 0/0
- C. BRI 0:1 and BRI 0:2
- D. BRI 0/0:23
- E. virtual-access 1
- F. virtual-template 1

Answer: E

Explanation:

MPPP is a method for splitting, recombining, and sequencing datagrams across multiple logical data links. It was originally motivated by the desire to exploit multiple bearer channels in ISDN, but it is equally applicable to any situation in which multiple PPP links connect two systems, including async links.

Traffic routed across an MPPP link via its controlling interface (a Virtual Access interface) will be fragmented, with the fragments being sent across the different physical links. At the remote end of the link, the fragments are reassembled and forwarded to the next hop toward their ultimate destination.

After MPPP has been successfully negotiated during the LCP phase of PPP negotiation and Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) have completed successfully, a Virtual Access interface will be created by the Cisco IOS Software to represent the MPPP bundle.

Reference:

http://www.cisco.com/en/US/tech/CK7_13/CK5_07/technologies_tech_note09186a0080112d3b.shtml

QUESTION 299

You work as a network administrator at Certkiller .com. You are using an external ISDN NT1. Your router's ISDN Layer 1 is NOT active.

What is the correct wiring for the external NT1?

- A. 4-wire goes to both the terminal equipment and the switch.
- B. 2-wire goes to both the terminal equipment and the switch.
- C. 4-wire goes to the terminal equipment and 2-wire goes to the switch.
- D. 2-wire goes to the terminal equipment and 42-wire goes to the switch.

Answer: C

QUESTION 300

In the systematic troubleshooting approach it's beneficial to keep a model of the network baseline. Why? (Choose two)

- A. To supply information to a TAC engineer
- B. To minimize downtime when a network failure occurs
- C. To identify a normal network behavior and an abnormal behavior
- D. To keep all network equipment inventory up-to-date for next year's budget

Answer: A, C

Explanation:

When you call TAC they're going to be asking you for very specific questions about your networks capability, your networks statistics, and the type of performance it usually provides. Since terms like the term 'slow' and 'reduced performance' are subjective, and the TAC engineer has never been on your network, he or she is going to ask for numbers. By having numbers you're going to objectively know for sure beyond a doubt when your network is having a performance problem, and to what exact degree, so you won't have to rely on feeling.

When understanding the network baseline, it becomes easy to identify when the network begins to behave abnormally. This can aid in taking a more proactive approach to network management.

QUESTION 301

What could you do to determine whether or not your network performance is within normal expectations?

- A. Confirm that the Syslog server is receiving messages.
- B. Compare the network performance to baseline statistics.
- C. Ask users if the network seems to be performing slower than usual.
- D. Evaluate the results of traceroute to the most geographically site on your network.

Answer: B

Explanation:

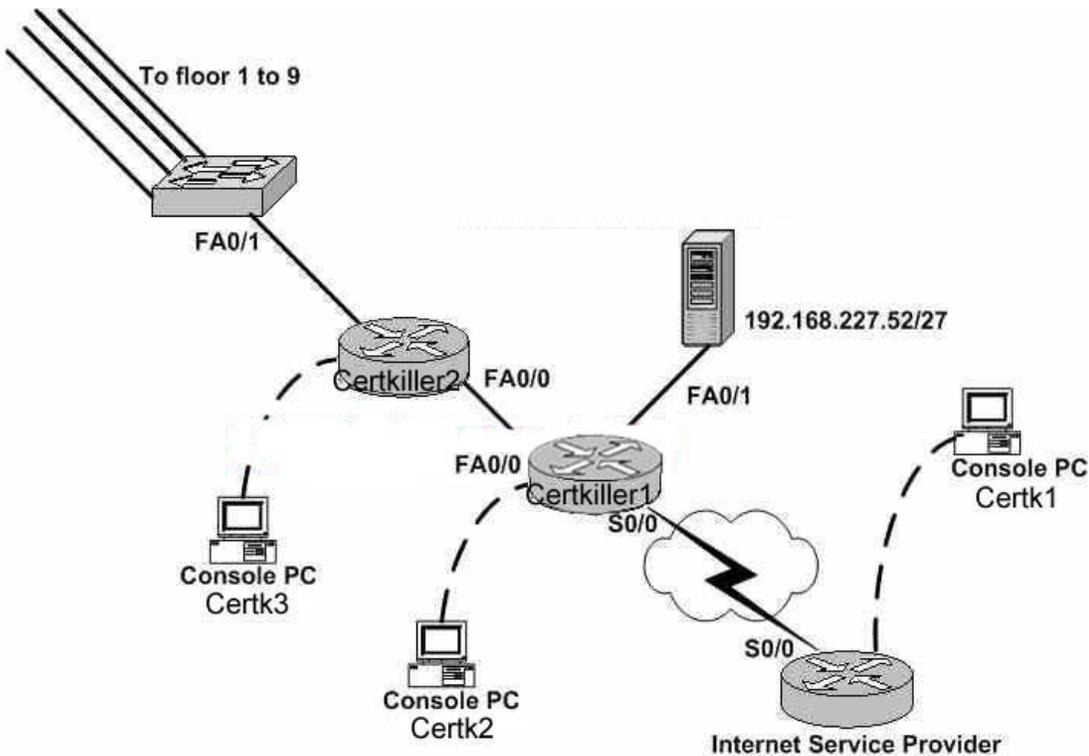
The network performance should be compared to baseline statistics. The baseline is a record of the network under normal, optimal conditions. When you suspect that the network is behaving abnormally, the first thing you should do is compare the current state with the network baseline.

Note: Establishing network baseline is to make a recording of regular network activity over a period of time.

QUESTION 302

SIMULATION

The Certkiller network is displayed in the following diagram:



You are the CTO of Certkiller .Inc and you've encountered a major network problem. On Friday afternoon the gateway router that connects your networks to the ISP failed. The network administrator came in on Saturday morning. He replaced the router, reconfigured the network, and restored internet connectivity. However, on Monday morning NONE of the workstations could access the internet via the local web-server. You lost your temper and terminated his employment, and now you're left to fix the problem yourself. Your goal is to restore connectivity from the distribution router to the gateway router; and you will do this by reconfiguring the gateway router.

(The name of the gateway router is Certkiller 1 and the name of the distribution router is Certkiller 2)

Answer:

Click on the Console CertK 1

```
Gateway> enable
```

```
Password: Certkiller
```

```
Gateway#configure terminal
```

```
Gateway(config)# interface fa 0/0
```

```
Gateway(config-if)# ip address 192.168.113.51 255.255.255.224
```

```
Gateway(config-if)# speed 100
```

```
Gateway(config-if)# duplex full
```

```
Gateway(config-if)# ^Z
```

```
Gateway# copy running-config startup-config
```

Explanation:

The IP Address already configured on fa0/0 is wrong. It has network bits of /28. So, first

of all you have to change it to /27. After that line protocol on Fast Ethernet port is down. Reason is that the Fast Ethernet port is configured as a 10Mbps Half Duplex port. So, you have to put the Fast Ethernet 0/0 port in full duplex mode and configure its speed as either auto or full. The line protocol will automatically turn to the up state. Verify it by giving the "show interface" command and also see the routing tables of both routers.

QUESTION 303

You're in the midst of troubleshooting a remote network connection to your ISP from router CK1 . What could you eliminate as a problem source before you even contact the ISP? (Select two)

- A. Frame Relay network.
- B. Segment between the local router and the CSU.
- C. Segment between the remote router and the remote CSU.
- D. Segment between the local CSU and the service provider's switch.
- E. Segment between the remote CSU and the service provider's switch.

Answer: B, D

Explanation:

Before contacting the ISP for fault isolation, first we should successfully complete the loopback testing on your local and remote segments. The service provider can not help fixing the local segments between your routers and the local CSU. In this case, we really only have visibility on the local side. We can test connectivity between the local router and CSU using a loopback test. If that succeeds, we can then try to test the connection between the local CSU and the ISP. If that fails, then we can contact the service provider.

QUESTION 304

When a problem with a Cisco device overwhelms your capabilities you can always turn to Cisco TAC for help. Before calling TAC, what three pieces of information should you know? (Choose three)

- A. Packet traces
- B. Switch error logs
- C. Client patch levels
- D. Trace Server event logs
- E. Recent configuration changes

Answer: A, B, E

Explanation:

When you contact the Cisco TAC, it is necessary to have the Packet traces, Switch error logs and recent configuration changes at hand as it would expedite a good, effective response from TAC.

Incorrect Answers:

C, D: Since this deals with LAN devices that are not related to Cisco networking equipment, the TAC will not need to receive any information pertaining to these.

QUESTION 305

Is the following statement true or false?

When troubleshooting a network problem that's beyond your capability, you should contact the Cisco TAC right away if you can't resolve the problem immediately.

- A. True if you are a Cisco silver partner
- B. True if you are a Cisco gold partner
- C. True
- D. False
- E. True if you are a Cisco reseller

Answer: D

Explanation:

If the problem has not been resolved, you must create an action plan based on the next most likely problem in your list. Change one variable at a time, and repeat the process until the problem is solved. If you exhaust all the common causes and actions-either those outlined in this [Cisco] book or ones that you have identified for your environment, you should contact your Cisco technical support representative. You may consider opening a case with TAC and commit certain resources into looking after the problems. However, this should normally only be done as a last resort.

QUESTION 306

You suspect that there may be an IOS bug in the version you are using on the Certkiller network. Where can you find the Cisco bug watcher, and any interim patches?

- A. Cisco Navigator
- B. Open Q&A Forum
- C. Cisco Support CD
- D. Software Bug Toolkit
- E. Online Tech Support
- F. None of the above

Answer: D

Explanation:

The Software Bug Toolkit focuses on errors and bugs found in IOS and other software utilities.

For the latest information on known problems, follow these steps to create a bug Watcher Bin in the Software Bug Toolkit from Cisco Connection Online (CCO):

Step1 Connect to CCO as directed in Cisco Connection Online.

Step2 On the CCO home page, click LOGIN (which appears in green in the menu bar at the top

of the page) and log in to CCO. If you are not a registered CCO user, follow the instructions to register so that you can log in. Login is complete when the word LOGIN no longer appears in green text in the menu bar.

Step3 After you log in, click Software & Support on the CCO home page.

Step4 Under the Technical Support menu, click Software Bug Toolkit II. (Software Bug Toolkit II is not visible on the Software & Support page unless you are logged into CCO as directed in Step 2.)

Step5 Click Search for Bug by ID Number from the main menu or click Search by ID under Bug Toolkit in the left column of the screen.

Step6 Enter a bug ID, such as CSCdj80580, in the Search for Bug by ID Number window and click SEARCH. The bug information is displayed.

Step7 To watch activity on the selected bug, click the WATCH this bug button at the top of the screen. The Pick a Watcher Bin entry screen is displayed.

Step8 Create a Watcher Bin for the bug selected by entering a New Bin Watcher name, such as V.90 Bugs. A new Watcher Bin is created. The new Watcher Bin creates a link to the Bug Watcher screen.

Step9 Click Watcher to access the Bug Watcher screen. The new Watcher Bin link is displayed in the left column of the screen.

QUESTION 307

You need to download a newer version of IOS from the Cisco website. What does a guest need in order to apply for user access on the Cisco Connection Online?

- A. Member ID
- B. Staff Resource ID
- C. Guest Resource ID
- D. Service contract number
- E. All of the above

Answer: D

Explanation:

If you bought equipments from Cisco you can gain user access if maintenance was also purchased. When the maintenance contract is purchased, a service contract number will be provided from Cisco. If the equipment was purchased directly from Cisco, you can also download IOS software from them. More information on obtaining Cisco software is shown below:

Obtaining Fixed Software

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's Worldwide Web site at

<http://www.cisco.com/pcgi-bin/tablebuild.pl/cs-ac-s-win>.

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for assistance with the upgrade or patch, which should be free of charge.

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC).

QUESTION 308

Where can you go on the Cisco website to look for past questions posted by other Cisco users, and post some answers?

- A. Cisco Support CD
- B. Cisco Navigator
- C. Open Q&A Discussion Forum
- D. Online Tech Support
- E. There is currently no way of doing this

Answer: C

Explanation:

In the Open Q&A forum you can Share questions, suggestions, and information about networking solutions, products, and technologies in discussion forums, Tech Talks and Ask the Expert forums. The discussion forum can be found at the Netpro section of cisco.com found here:

<http://www.cisco.com/go/netpro/>

QUESTION 309

What level of CCO (Cisco Connection Online) access is offered to non-Cisco employees? (Select all that apply)

- A. Guest
- B. Power user
- C. Admin
- D. User
- E. Privileged
- F. None of the above

Answer: A, D

Explanation:

CCO offers two different access levels for non-employees. Guest access allows anyone to access a limited amount of resources, while user access is available to registered users. User access allows for additional access, including technical information, Cisco tools, the software center for downloading Cisco IOS software, and the TAC.

QUESTION 310

Where can you find and access the IOS upgrade planner?

- A. Software Center
- B. Cisco Support CD
- C. Cisco Navigator
- D. Bug toolkit

Answer: A

Explanation:

The Cisco IOS Planner allows you more flexibility to browse for your preferred software. You can view all major releases, all platforms, and all software features from a single interface. Choosing a platform, a maintenance release, or software feature will automatically limit the other menu choices based on your selection, until you arrive at your preferred software. The link to launch the IOS upgrade planner tool is (requires login):

<http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi?>

QUESTION 311

When an administrator is overwhelmed by a troubleshooting issue and calls the Cisco TAC, what information is taken into consideration before routing the case to the Customer Engineering Response Team? (Choose all that apply)

- A. Name of the customer
- B. Monthly service plan
- C. Type of problem
- D. Priority level

Answer: C, D

Explanation:

The focal point of all Cisco software and hardware maintenance and support services is the Cisco TAC. The TAC is staffed by Customer Support Engineers (CSEs) who have experience with the Cisco product line and all aspects of data communications networking technology. When you call the TAC or open a case online, you are asked for the type of problem, as well as the priority level of the issue/outage.

QUESTION 312

You are seeing problems with the ISDN line at one of your locations, and call the ISDN provider to troubleshoot. When an ISP troubleshoots a problem on their ISDN local loop, they are checking network connectivity from the ISDN switch to the _____?

- A. TA
- B. TE1
- C. TE2
- D. NT1

Answer: D

Explanation:

ISDN local loop is terminated using a Network Termination Type 1 (NT1)

The NT1's responsibilities include line performance monitoring, timing, physical signaling protocol conversion, power transfer, and multiplexing of B and D channels.

Reference:

Standard ISDN BRI Roles and Interface Reference Points (CIT,Cisco Press)

QUESTION 313

During your lunch break your junior administrator made a mistake on the network and is on the phone with a TAC engineer trying to work it out. You overhear the phone conversation and notice that the engineer assigned to his ticket asks for the "show interface" and "show protocol" output. Which two situations is the engineer probably investigating? (Choose two)

- A. A crash or hung system
- B. Memory allocation problem
- C. Partial loss of system function
- D. Lost data or performance problems

Answer: C, D

Explanation:

If you have a problem with performance degradation then TAC will probably ask for the results of:

1. show interfaces
2. show buffers
3. show memory
4. show processes [cpu]

If there's a loss of functionality (perhaps; a faulty protocol or connection) you'll be asked for:

1. show ip protocol
2. show ip route
3. show ip traffic
4. show ip interfaces
5. show ip access-lists

Reference:

CCNP Support Exam Certification Guide, page 127 Amir S. Ranjibar, ISBN 0-7357-09955-5

QUESTION 314

DRAG DROP

Cisco Technical Assistance Center (TAC) has priority levels. Move the corresponding priority level on the left to the appropriate network impact on the right. (Hint: You may use the same priority more than once, so all priorities may not necessarily be

used.)

Select from these	Troubleshooting function	
Priority 1	Request for installation assistance	Place here
Priority 2	Network performance degraded	Place here
Priority 3	Information needed on Cisco product capabilities	Place here
Priority 4	Production network severely degraded	Place here

Answer:

Select from these	Troubleshooting function	
Priority 1	Request for installation assistance	Priority 4
Priority 2	Network performance degraded	Priority 3
Priority 3	Information needed on Cisco product capabilities	Priority 4
Priority 4	Production network severely degraded	Priority 2

Explanation:

Priority 1: Production network is down, causing critical impact to business operations if service is not restored quickly.

Priority 2: Production network is severely degraded, impacting significant aspects of your business operations.

Priority 3: Network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.

Priority 4-Customer requires information or assistance on Cisco product capabilities, installation, or configuration.

QUESTION 315

You are seeing some problems between an Adtran router and a Cisco router in the Certkiller network. What online tool could you use to find a solution to a complex problem that's related to compatibility concerns between multiple vendor products?

- A. Case Query Tool
- B. Cisco Open Forum
- C. Cisco Stack Decoder
- D. Troubleshooting Assistant

Answer: A

Explanation:

To get assistance on this complex compatibility problem the Case Query Tool should be

used.

Every time you open a technical support case online, the Cisco TAC Case Open tool's "recommendation" feature gives you a customized list of solutions selected by TAC engineers. Simply fill out three drop-down fields describing your situation, and the Case Open tool instantly displays links to documents and tools that may resolve your issue right away.

Incorrect Answers

B: The Open Forum is not the best way to find solution to complex problems.

C: The Stack Decoder is used to analyze and diagnose stack traces from Cisco router platforms.

D: A powerful online tool, the Troubleshooting Assistant helps registered Cisco.com users solve common hardware, configuration, and performance problems. However, it is not well suited for the complex problem of this scenario.

QUESTION 316

Which of the following troubleshooting tools are valid and are included in the Cisco Connection Online (CCO) website?

- A. Cisco Technical Information Center (TIC) web site
- B. Cisco Technical Assistance Center (TAC) web site.
- C. Cisco Center for Aid in Troubleshooting (CAT) web site.
- D. Cisco Internetworking Troubleshooting Center (ITC) web site.
- E. All of the above

Answer: B

Explanation:

The TAC Service Request Tool allows you to:

- * Open severity 3 and 4 service requests, and after you describe your service request online, the tool recommends resources that may provide a solution immediately.
- * Check the current status of open service requests
- * Update open service requests with your own notes
- * Attach files to open service requests
- * View service requests closed within the last 18 months

Reference: <http://tools.cisco.com/ServiceRequestTool/create/launch.do>

QUESTION 317

Your junior systems administrator has just finished downloading an updated IOS software image from the CCO. Knowing your administrators track record, you suspect that the image may have been corrupted during the download process. What could you do to quickly verify the integrity of the image file?

- A. Compare the MD5 checksum value to the image on CCO
- B. Compare the SHA-1 checksum value to the image on CCO
- C. Download the image from CCO again and compare the two images
- D. Enter a show version command on the router and compare the image to that on CCO

Answer: A

Explanation:

The checksum value is a function of the data. If the data integrity is compromised, then the checksum value changes. So if the checksum value changed, then you can reason that the data has changed. If the checksum value stayed the same, then you can be assured that the data has remained the same.

QUESTION 318

You wish to obtain some statistical information on the Certkiller network. Which tool could you use to gather network information such as packet sizes, packet errors, connection utilizations, and traffic load?

- A. Network Monitor
- B. Load Balancer
- C. Network Supervisor
- D. Traffic Director
- E. None of the above

Answer: A

Explanation:

The network monitor is a Cisco WAN Manager tool for monitoring network traffic and packets. Details of network alarm and configuration status can be retrieved by a single click in the network monitor GUI. Alarm filtering can be enabled with a single click to view a specific class of alarms such as node, card, port, Cisco WAN Manager, critical, major, or minor. The network monitor also provides for detailed information such as error counts, packet information, and utilization information.

QUESTION 319

Is the following statement true or false?

You can use Connectivity Tools to produce a simulated network environment.

- A. True only when the CWSI Visual Map component is installed
- B. True only when the CWSI Visual Tracker component is installed
- C. True only when the CWSI Visual Designer component is installed
- D. True
- E. False

Answer: D

Explanation:

According to the technical documentation at CCO:

Using the Connectivity Tools to create a simulation environment, network planners can study the impact of such factors as failed devices and links, and preview the effects of

various configuration changes before implementing them in their networks. This tool can be used as a stand-alone feature, and no additional CWSI components need to be installed.

QUESTION 320

Which of the following tools contains the "scenario what-if" Simulator?

- A. Connectivity Baseline
- B. Router Configuration File Loader
- C. Connectivity Solver
- D. Topology Builder
- E. Diagnostic Report Generator
- F. All of the above

Answer: C

Explanation:

According to the technical documentation at CCO:

The Connectivity Tools currently have two components; the Connectivity Baseline and the Connectivity Solver. The Connectivity Baseline is a pre-requisite of the Connectivity Solver. As such, the additional functionality of the Connectivity Solver is used in conjunction with the Connectivity Baseline. The functionality provided is:

- Connectivity Baseline
 - Router Configuration File Loader
 - Diagnostic Report Generator
 - Topology Builder
 - Connectivity Solver
 - Connectivity Requirements Analyzer
 - Scenario "what-if" Simulator
 - Delta IOS command generation
-

QUESTION 321

You want to test how a new bandwidth intensive application will impact your T1 link. Which tool can you use for network stress testing and analysis?

- A. Network monitor
- B. Simulation/modeling software
- C. Network Management System (NMS) software
- D. Protocol analyzer
- E. All of the above

Answer: B

Explanation:

Simulation and Modeling Tools allow you to put a test network together and see how it

performs. Can be used to design a new network or to see how and existing network will perform if you modify it, expand it, or put traffic stress on it.

QUESTION 322

In order to better manage the Certkiller network, the CiscoWorks 2000 bundle was purchased. Which of the following applications are included in this bundle? (Choose two)

- A. RMON
- B. NetView
- C. VlanDirector
- D. TrafficDirector
- E. Cisco IOS software

Answer: C, D

Explanation:

CiscoWorks for Switched Internetworks (CWSI) is a suite of network management applications. CWSI applications enable you to configure, monitor, and manage a switched internetwork and includes the following features:

1. TrafficDirector
2. VlanDirector
3. AtmDirector
4. CiscoView
5. UserTracking

QUESTION 323

DRAG DROP

Match the troubleshooting tool on the left next to its proper troubleshooting function on the right:

Select from these	Troubleshooting function	
<div style="border: 1px solid black; background-color: #e0ffe0; padding: 5px; text-align: center;">CiscoView</div>	<div style="border: 1px solid black; padding: 5px; text-align: center;">Network modeling</div>	<div style="border: 1px solid black; background-color: #e0ffff; padding: 5px; text-align: center;"><i>Place here</i></div>
<div style="border: 1px solid black; background-color: #e0ffe0; padding: 5px; text-align: center;">NetSys</div>	<div style="border: 1px solid black; padding: 5px; text-align: center;">Inventory and software distribution</div>	<div style="border: 1px solid black; background-color: #e0ffff; padding: 5px; text-align: center;"><i>Place here</i></div>
<div style="border: 1px solid black; background-color: #e0ffe0; padding: 5px; text-align: center;">CRM</div>	<div style="border: 1px solid black; padding: 5px; text-align: center;">Network utilization</div>	<div style="border: 1px solid black; background-color: #e0ffff; padding: 5px; text-align: center;"><i>Place here</i></div>
<div style="border: 1px solid black; background-color: #e0ffe0; padding: 5px; text-align: center;">TrafficDirector</div>	<div style="border: 1px solid black; padding: 5px; text-align: center;">Graphically configure a device</div>	<div style="border: 1px solid black; background-color: #e0ffff; padding: 5px; text-align: center;"><i>Place here</i></div>

Answer:

Select from these

Troubleshooting function

Network modeling	NetSys
Inventory and software distribution	CRM
Network utilization	TrafficDirector
Graphically configure a device	CiscoView

Explanation:

Netsys is an offline tool. It is a complex program that imports Cisco device configuration and then creates a model based on the configurations. The program is used to model changes to a network before they are actually implemented.

Cisco Resource Manager (CRM)

is web-based and among its components there are four essential applications: Inventory Manager, Availability Manager, Syslog Analyzer, and Software Image Manager.

TrafficDirector obtains traffic information from embedded RMON agents. With this information about different segments, TrafficDirector can inform you of collision, error, utilization, and broadcast rates.

CiscoView provides real-time device level monitoring, fault management, and troubleshooting, with a Graphic User Interface.

QUESTION 324

While brosing through the Cisco website, you stumble upon the Software Center section. What can you do within the Cisco Software Center? (Choose all that apply)

- A. Search for software bugs in all available software platforms
- B. Get selected demonstration and beta distributions for Cisco's latest products
- C. Consult Software Upgrade Planners that collect and present product literature, release information, documentation, and release notes
- D. Use Software Checklists to ensure current availability and compatibility of Cisco software products for your internetworking platforms
- E. None of the above

Answer: B, C, D

Explanation:

B: The Cisco Software Center offers selected demo and beta distributions for their latest products.

C: Software Upgrade Planners, available from the Cisco Software Center, collect and present product literature, release information, documentation and release notes, plus known defect information from Cisco's Bug Toolkit in a single comprehensive view.

D: Software Checklists, available from the Cisco Software Center, ensure the current availability and compatibility of Cisco software products for your internetworking

platforms.

Incorrect Answers:

A: The CCO bug Toolkit would provide search functions for software bugs. However, the CCO bug Toolkit is only available for registered customers. It is not available from the Cisco Software Center.

QUESTION 325

You've arrived at the job site and you're greeted by your junior administrator who tells you that she's just diagnosed a flapping link on the Frame Relay network, and asks you what two problems could lead to a flapping link? (Choose two)

- A. Too much line noise.
- B. Improperly configured keepalives.
- C. Mismatched encapsulation types.
- D. Improperly configured IP addresses.

Answer: B, C

Explanation:

Link flapping refers to losing and re-gaining link (status transitioning from up to down)

B: Normally, the keepalives on the serial interfaces need to match on each end to keep the link from flapping. In some cases, the keepalive on the Cisco device needs to be set slightly shorter (about 8 seconds) than the keepalive on the switch. You'll see the need for this if the interface keeps coming up and down.

C: The encapsulation at each end of the link needs to be set identically or there is a potential for perpetual link flapping. Normally, when two Cisco devices are used, Cisco frame relay encapsulation is used. However, when connecting to a non-Cisco frame relay router, the typical encapsulation method is the IETF standard, as specified by the "encapsulation frame-relay ietf" interface command.

Reference: "Comprehensive Guide to Configuring and Troubleshooting Frame Relay"

http://www.cisco.com/en/US/tech/CK7_13/CK2_37/technologies_tech_note09186a008014f8a7.shtml

QUESTION 326

The Certkiller frame relay network is displayed in the following exhibit:



At this time, the link between Router CK2 and the service provider network is down. The following items have also been verified:

1. the connection is properly configured
2. static routes have been configured to facilitate connectivity
3. static maps have also been configured for the same reason

Which of the following commands would be best to use to indicate the problem?

- A. show frame-relay map
- B. show frame-relay pvc
- C. show ip interface brief
- D. show ip route
- E. show frame-relay lmi

Answer: A

Explanation:

The show frame-relay map command will give the information needed for this question.

1. Interface status (down, administratively down, or up)
2. Destination address
3. DLCI number
4. Mapping (static or dynamic, in point-to-point connection these are unmentioned)
5. Broadcast support
6. Encapsulation (Cisco or IETF)
7. PVC status (defined or deleted, a defined status may also be active or inactive)

Reference:

CCNP Support Exam Certification Guide, pages 320, 328 Amir S. Ranjibar, ISBN 0-7357-09955-5

QUESTION 327

After setting up a Frame Relay configuration, your users start to experience problems with dropped packets and you believe it is being caused by PVC congestion. Which command could you use to indicate that the service provider is responsible for dropping frames?

- A. debug frame-relay routing
- B. show frame-relay pvc
- C. show frame-relay lmi
- D. debug frame-relay pvc
- E. debug frame-relay dlci
- F. show frame-relay dlci

Answer: B

Explanation:

The "show frame-relay pvc" command will provide information pertaining to the level of congestion in the frame network on a PVC basis, namely, the FECN, BECN, and DE frames. A large number of FECN, BECN, and DE packets are an indication of congestion.

The forward explicit congestion notification (FECN) bit is set by the Frame Relay network in a frame to tell the DTE receiving the frame that congestion was experienced in the path from source to destination. The backward explicit congestion notification (BECN) bit is set by the Frame Relay network in frames travelling in the opposite direction from frames encountering a congested path. The notion behind both of these

bits is that the FECN or BECN indication can be promoted to a higher-level protocol that can take flow control action as appropriate. (FECN bits are useful to higher-layer protocols that use receiver-controlled flow control, whereas BECN bits are significant to those that depend on emitter-controlled flow control.)

DE (Discard Eligible) frames are the number of frames that are sent that burst above the Committed Information Rate (CIR). Any frame marked as DE will be delivered on a best effort basis only, and can be dropped by the carrier at any time.

QUESTION 328

Which command would you use to define the mapping between an address and a DLCI?

- A. no frame-relay map
- B. frame-relay dlci map
- C. show frame-relay pvc
- D. frame-relay map

Answer: D

Explanation:

To define the mapping between a destination protocol address and the data-link connection identifier (DLCI) used to connect to the destination address, use the frame-relay map interface configuration command. This is typically done to statically map an IP address to a DLCI, although other layer 3 protocols are also supported in addition to IP.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800c

QUESTION 329

The Certkiller network topology is displayed in the diagram below:



You enter the following command on router CK1 :

```
debugip packet
```

and in your command output you notice the line:

```
3d04h: IP: s=192.168.1.1 (local), d=192.168.47.2, len 100, encapsulation failed.
```

What do you suspect is the problem?

- A. The problem is that router Certkiller serial interface is down.
- B. The problem is that Certkiller 1 router has no route to the destination IP address.

C. The problem is that router Certkiller has no Layer 2 mapping for the destination IP address.

D. The problem is that Certkiller 1 and Certkiller 2 routers have been configured with different Frame Relay encapsulations.

Answer: C

Explanation:

The output shows "encapsulation failed".

This is because there is no mapping between the destination IP and the FR DLCI (Layer 2) which leads

to answer C. Answer D is only half true. When there are different encapsulation types configured it leads

to inverse-arp is not working for dynamic mapping between IP addresses and FR DLCIs which can cause

an "encapsulation failed" message but when there is a static mapping between the destination IP and the

corresponding DLCI the router is sending the packet. Furthermore if there are two Cisco Router connected

back-to-back the pings go through because the cisco router understand both types when he receives the packets.

I tested this in a lab environment with static mapping but different encapsulation types:

Here is the output from both sites

Router Berlin

```
interface Serial0/1
ip address 192.168.70.1 255.255.255.0
encapsulation frame-relay IETF
frame-relay map ip 192.168.70.2 100
no frame-relay inverse-arp
frame-relay intf-type dce
```

Router Tokyo

```
interface Serial0
ip address 192.168.70.2 255.255.255.0
encapsulation frame-relay
clockrate 64000
frame-relay map ip 192.168.70.1 100
no frame-relay inverse-arp
```

For my opinon answer C is right.

```
debug ip packet
```

Berlin#ping 192.168.70.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.70.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/40 ms

Berlin#

*Mar 7 18:10:08.243: IP: tableid=0, s=192.168.70.1 (local), d=192.168.70.2 (Serial0/1), routed via FIB

*Mar 7 18:10:08.243: IP: s=192.168.70.1 (local), d=192.168.70.2 (Serial0/1), len 100, sending

*Mar 7 18:10:08.283: IP: tableid=0, s=192.168.70.2 (Serial0/1), d=192.168.70.1 (Serial0/1), routed via RIB

*Mar 7 18:10:08.283: IP: s=192.168.70.2 (Serial0/1), d=192.168.70.1 (Serial0/1), len 100, rcvd 3

*Mar 7 18:10:08.283: IP: tableid=0, s=192.168.70.1 (local), d=192.168.70.2 (Serial0/1), routed via FIB

*Mar 7 18:10:08.287: IP: s=192.168.70.1 (local), d=192.168.70.2 (Serial0/1), len 100, sending

*Mar 7 18:10:08.323: IP: tableid=0, s=192.168.70.2 (Serial0/1), d=192.168.70.1 (Serial0/1), routed via RIB

*Mar 7 18:10:08.323: IP: s=192.168.70.2 (Serial0/1), d=192.168.70.1 (Serial0/1), len 100, rcvd 3

*Mar 7 18:10:08.327: IP: tableid=0, s=192.168.70.1 (local), d=192.168.70.2 (Serial0/1), routed via FIB

*Mar 7 18:10:08.327: IP: s=192.168.70.1 (local), d=192.168.70.2 (Serial0/1), len 100, sending

*Mar 7 18:10:08.363: IP: tableid=0, s=192.168.70.2 (Serial0/1), d=192.168.70.1 (Serial0/1), routed via RIB

*Mar 7 18:10:08.363: IP: s=192.168.70.2 (Serial0/1), d=192.168.70.1 (Serial0/1), len 100, rcvd 3

*Mar 7 18:10:08.367: IP: tableid=0, s=192.168.70.1 (local), d=192.168.70.2 (Serial0/1), routed via FIB

*Mar 7 18:10:08.367: IP: s=192.168.70.1 (local), d=192.168.70.2 (Serial0/1), len 100, sending

*Mar 7 18:10:08.407: IP: tableid=0, s=192.168.70.2 (Serial0/1), d=192.168.70.1 (Serial0/1), routed via RIB

*Mar 7 18:10:08.407: IP: s=192.168.70.2 (Serial0/1), d=192.168.70.1 (Serial0/1), len 100, rcvd 3

*Mar 7 18:10:08.407: IP: tableid=0, s=192.168.70.1 (local), d=192.168.70.2 (Serial0/1), routed via FIB

*Mar 7 18:10:08.407: IP: s=192.168.70.1 (local), d=192.168.70.2 (Serial0/1), len 100, sending

*Mar 7 18:10:08.447: IP: tableid=0, s=192.168.70.2 (Serial0/1), d=192.168.70.1 (Serial0/1), routed via RIB

*Mar 7 18:10:08.447: IP: s=192.168.70.2 (Serial0/1), d=192.168.70.1 (Serial0/1), len 100, rcvd 3

So answer C should be right

QUESTION 330

The Certkiller Frame Relay network is experiencing an LMI problem. At what OSI layer should you begin your troubleshooting investigations?

- A. Layer 3
- B. Layer 2

- C. Layer 1
- D. Layer 4
- E. Layer 5
- F. All of the above

Answer: B

Explanation:

Frame Relay operates on OSI layers 1 & 2. The LMI (local management interface) was developed as an addressing extension to give DLCI's (data-link connection identifier's) global significance. LMI is the Link Management Interface, and it works at the data link layer of the OSI model.

QUESTION 331

In Frame Relay, what DLCI number is associated with the ANSI LMI type?

- A. 0
- B. 1024
- C. 1023
- D. 256
- E. None of the above

Answer: A

Explanation:

The three LMI types and their respective DLCI number's are:

1. Cisco - 1023
2. Ansi - 0
3. Q933a - 0

Monitoring ANSI Frame Relay

Use the show interface EXEC command to determine the LMI type implemented. The following sample display illustrates the resulting display from a show interfaces command executed for a serial interface with the ANSI LMI enabled.

Serial 1 is up, line protocol is up

Hardware is MCI Serial

Internet address is 131.108.121.1, subnet mask is 255.255.255.0

MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255

Encapsulation FRAME-RELAY, loopback not set, keepalive set

LMI DLCI 0, LMI sent 10, LMI stat recvd 10

LMI type is ANSI Annex D

Last input 0:00:00, output 0:00:00, output hang never

Output queue 0/40, 0 drops; input queue 0/75, 0 drops

Five minute input rate 0 bits/sec, 1 packets/sec

Five minute output rate 1000 bits/sec, 1 packets/sec

261 packets input, 13212 bytes, 0 no buffer

Received 33 broadcasts, 0 runts, 0 giants

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
238 packets output, 14751 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets, 0 restarts

Two fields distinguish the use of the ANSI LMI from the default LMI. In the sixth line of this display, the LMI DLCI field indicates a zero value. If the LMI is set to the default (Cisco), the value would be 1023. In addition, the next line is added to the display, stating that the LMI type is ANSI Annex D.

QUESTION 332

Part of the configuration file for one of the Certkiller routers is displayed below:

```
interface Serial1
ip address 2.1.1.2 255.255.255.0
encapsulation frame-relay
ip ospf network broadcast
no keepalive
no cdp enable
frame-relay map llc2 23 broadcast
farme-relay map ip 2.1.1.1 23 broadcast
```

In the following line:

```
frame-relaymap ip 2.1.1.1 23 broadcast
```

What is significant of the word "broadcast"?

- A. It enables the use of the DHCP server 2.1.1.1 for IP addressing
- B. It enables OSPF routing to emulate a NBMA environment for the 2.1.1.0/24 network
- C. It forwards broadcast frame via DLCI 23 to the mapped neighbor 2.1.1.1
- D. It bridges between sites so NETBIOS can be sent across the WAN
- E. None of the above

Answer: C

Explanation:

By default, broadcast frames are not sent across frame relay neighbors that are mapped statically. The use of the "broadcast" keyword enables broadcast and multicast frames to be sent across the map. This is important when you want dynamic routing protocols to function across the frame relay network using frame-relay maps. Without the use of the "broadcast" keyword, all multicast and broadcast traffic will be dropped, including routing protocol traffic.

QUESTION 333

Many of the Certkiller routers are being upgraded to IOS version 11.2. When Cisco released IOS version 11.2, they added a feature called "autosense" which enables a router to automatically detect the _____ on a Frame Relay DTE/DCE.

- A. Destination DLCI
- B. Hardware interface
- C. LMI type

- D. Keepalive increments
- E. Layer 2 encapsulation
- F. PVC CIR

Answer: C

Explanation:

Beginning with Cisco IOS Release 11.2, the software supports Local Management Interface (LMI) autosense, which enables the interface to determine the LMI type supported by the switch. Support for LMI autosense means that you are no longer required to configure the LMI explicitly.

See the following sections for further details on configuring the LMI:

- * Activating LMI Autosense
- * Explicitly Configuring the LMI

For information on using Enhanced Local Management Interface with traffic shaping, see the "Configuring Frame Relay Traffic Shaping" section later in this chapter.

For an example of configuring the LMI, see the "Pure Frame Relay DCE Example" section later in this chapter.

Activating LMI Autosense

LMI autosense is active in the following situations:

- * The router is powered up or the interface changes state to up.
- * The line protocol is down but the line is up.
- * The interface is a Frame Relay DTE.
- * The LMI type is not explicitly configured.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a008008

QUESTION 334

The Certkiller network contains a hub and spoke frame relay network. What could you do to avoid split horizons issue on a hub-and spoke Frame Relay topology?

- A. Configure different keepalives
- B. None of the answers
- C. Configure subinterfaces
- D. Configure different dlci mapping

Answer: C

Explanation:

Point-To-Point Subinterfaces

The concept of subinterfaces was originally created in order to better handle issues caused by split-horizon over Non-Broadcast Multiple Access (NBMA) networks (e.g. frame relay, X.25) and distance-vector based routing protocols (e.g. IPX RIP/SAP, AppleTalk). Split-horizon dictates that a routing update received on an interface cannot be retransmitted out onto the same interface. This rule holds even if the routing update

was received on one frame relay PVC and destined to retransmit out onto another frame relay PVC. Referring to figure 2, this would mean that sites B and C can exchange routing information with site A, but would not be able to exchange routing information with each other. Split-horizon does not allow Site A to send routing updates received from Site B on to Site C and vice versa.

Note: For TCP/IP, Cisco routers can disable split-horizon limitations on all frame relay interfaces and multipoint subinterfaces and do this by default. However, split-horizon cannot be disabled for other protocols like IPX and AppleTalk. These other protocols must use subinterfaces if dynamic routing is desired.

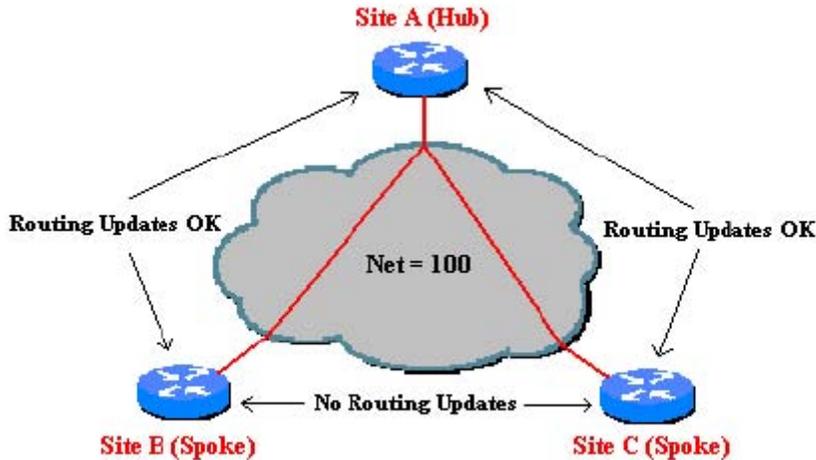


Figure 2: Split-horizon does not allow remote sites to send routing updates to each other.

By dividing the partially-meshed frame relay network into a number of virtual, point-to-point networks using subinterfaces, the split-horizon problem can be overcome. Each new point-to-point subnetwork is assigned its own network number. To the routed protocol, each subnetwork now appears to be located on separate interfaces (Figure 3). Routing updates received from Site B on one logical point-to-point subinterface can be forwarded to site C on a separate logical interface without violating split horizon.

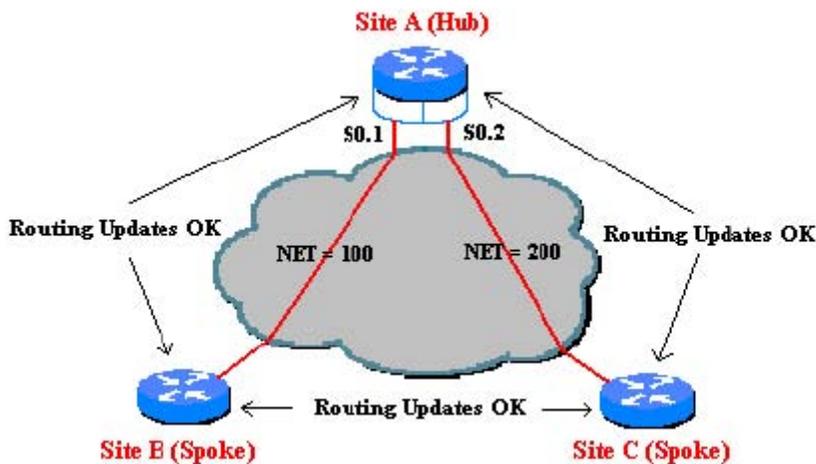


Figure 3: Subinterfaces allow remote sites to exchange routing updates with each other.

Reference:

http://www.alliancedatacom.com/manufacturers/cisco-systems/framerelay_design/subinterfaces.asp

QUESTION 335

When configuring Frame Relay, which of the following commands WILL NOT help you find keepalive settings? (Choose all that apply)

- A. Use show statistics serial
- B. Use show interfaces serial-line
- C. Use show interfaces (show interface serial)
- D. Use show interfaces frame-reply
- E. Use show interfaces serial-enable

Answer: A, B, D, E

Explanation:

Choices A, B, D, and E are all correct as they will not aid in discovering the keepalive settings of the frame relay interfaces. All of these choices are invalid IOS commands.

Incorrect Answers:

C: This question basically asks you which command shows Frame Relay keepalive settings. The command show interfaces serial will show you:

1. The type of Frame Relay encapsulation used on an interface or PVC
 2. The keepalive interval configured
 3. The Frame Relay LMI type used
 4. The status of Frame Relay LMI
 5. Information on whether the interface is configured as a Frame Relay DTE or a DCE device
-

QUESTION 336

Router CK1 is a frame-relay router configured with the following command:

```
encapsulationframe-relay ietf
```

Which two choices below display reasons why this configuration command would be entered as shown above? (Select two)

- A. To configure IETF encryption on the Cisco Frame Relay interface
- B. When connecting Cisco device with non-cisco device
- C. To configure IETF encapsulation on the Cisco Frame Relay interface
- D. When connecting Cisco device with Cisco device

Answer: B, C

Explanation:

By default the frame relay encapsulation is "Cisco." An alternative encapsulation method is the industry standard IETF. When a Cisco router connects to a non-Cisco router, the IETF encapsulation should be used to ensure interoperability between the two devices.

Incorrect Answers:

- A: The IETF option is an encapsulation option, not an encryption method.
- D: When two Cisco frame relay routers are used, the default cisco encapsulation method is typically used.

QUESTION 337

Which commands would you use if you wanted to learn the Frame Relay encapsulation type that is being used on a serial interface of your router?

- A. show frame-relay lmi
- B. show frame-relay pvc
- C. show frame-relay encapsulation
- D. show interfaces
- E. None of the above

Answer: D

Explanation:

The following example illustrates this point:

Example 8-6 *Investigating the State of the Serial 0 (Frame Relay) Interface Using the show interface and show frame-relay lmi Commands*

```
Orlando#show interface serial 0
Serial0 is up, line protocol is down
Hardware is HD64570
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation FRAME-RELAY, loopback not set
Keepalive set (10 sec)
LMI enq sent 196, LMI stat recvd 0, LMI upd recvd 0, DTE LMI down
LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
LMI DLCI 0 LMI type is ANSI Annex D frame relay DTE
... (output text deleted)
```

References: CCNP CIT Exam Certification Guide Page No. 137, 209 Second Edition
ISBN: 1-58720-081-3

QUESTION 338

Which frame-relay command would you use to view the PVC status on your frame links? (Choose all that apply)

- A. show frame-relay pvc
- B. frame-relay map
- C. no frame-relay map
- D. frame-relay dlci map

Answer: A

Explanation:

To show the status of the frame relay PVC (permanent virtual circuit) you enter the command:

```
show frame-relay pvc
```

The following example displays the information that can be gathered from this command:

```
CK1 #show frame-relay pvc 202
```

```
PVC Statistics for interface Serial1 (Frame Relay DTE)
```

```
DLCI = 202, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =  
Serial1.1
```

```
input pkts 2878 output pkts 2879 in bytes 964143
```

```
out bytes 964641 dropped pkts 0 in pkts dropped 0
```

```
out pkts dropped 0 out bytes dropped 0
```

```
in FECN pkts 0 in BECN pkts 0 out FECN pkts 0
```

```
out BECN pkts 0 in DE pkts 0 out DE pkts 0
```

```
out bcast pkts 2699 out bcast bytes 753021
```

```
pvc create time 1d20h, last time pvc status changed 1d20h
```

QUESTION 339

Which show command gives you a Frame Relay interface's LMI DLCI number?

- A. show interface
- B. show frame-relay lmi
- C. show frame-relay pvc
- D. show frame-relay dlci

Answer: A

Explanation:

Only the show interface command will display the DLCI that is used for the LMI. The following is an example:

```
CK1 #show interface serial 0
```

```
Serial0 is up, line protocol is up
```

```
Hardware is M4T
```

```
Internet address is 10.0.0.1/24
```

```
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
```

```
reliability255/255, txload 5/255, rxload 1/255
```

```
Encapsulation FRAME-RELAY, crc 16, loopback not set
```

```
Keepalive set (10 sec)
```

```
Restart-Delay is 0 secs
```

```
LMI enq sent 40, LMI stat recvd 40, LMI upd recvd 0, DTE LMI up
```

```
LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
```

```
LMI DLCI 1023LMI type is CISCO frame relay DTE
```

Incorrect Answers:

B: The show frame-relay lmi command displays LMI statistics. However, the output does not include any LMI DLCI number.

C: The show frame-relay pvc command displays PVC statistics. The output also

includes the LMI DLCI number, but not the DLCI of the LMI.

Sample output:

```
CK1 #show frame-relay pvc
PVC Statistics for interface Serial1 (Frame Relay DTE)
DLCI = 202, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial1.1
input pkts 2878 output pkts 2879 in bytes 964143
out bytes 964641 dropped pkts 0 in pkts dropped 0
out pkts dropped 0 out bytes dropped 0
in FECN pkts 0 in BECN pkts 0 out FECN pkts 0
out BECN pkts 0 in DE pkts 0 out DE pkts 0
out bcast pkts 2699 out bcast bytes 753021
pvc create time 1d20h, last time pvc status changed 1d20h
cir 100000 bc 8000 be 8000 byte limit 2000 interval 80
mincir 50000 byte increment 1000 Adaptive Shaping none
pkts 183 bytes 215082 pkts delayed 100 bytes delayed 142800
shaping inactive
traffic shaping drops 0
Queueing strategy: fifo
Output queue 0/40, 0 drop, 100 dequeued
D: There is no such command.
```

QUESTION 340

Which show command displays the status of BECN and FECN packets on a Frame Relay?

- A. show frame-relay fecn and show frame-relay becn
- B. show frame-relay pvc
- C. show interfaces
- D. show frame-relay lmi

Answer: B

Explanation:

Explanation:

The show frame-relay pvc command is used to display statistics about permanent virtual circuits (PVCs) for Frame Relay interfaces. The output includes status of FECN and BECN packets.

Sample output:

```
Router CertK # show frame-relay pvc
PVC Statistics for interface Serial2/1 (Frame Relay DTE)Active Inactive Deleted Static
Local 115 0 0 0 Switched 0 0 0 0 Unused 0 0 0 0DLCI = 100, DLCI USAGE = LOCAL,
PVC STATUS = ACTIVE, INTERFACE = Serial2/1input pkts 12 output pkts 7 in bytes
4406out bytes 1366 dropped pkts 0 in FECN pkts 0in BECN pkts 0 out FECN pkts 0 out
BECN pkts 0in DE pkts 0 out DE pkts 0outbcast pkts 7 out bcast bytes 1366pvc create
```

time 1d04h, last time pvc status changed 00:30:32 Incorrect Answers:

A: These are invalid IOS commands.

C: The show interface (or show interfaces) command is used to display statistics for all interfaces configured. The output does not include status on FECN and BECN packets however.

Sample output:

```
Certkiller _Switch (enable) show interface
sl0: flags=51<UP,POINTOPOINT,RUNNING>
slip0.0.0.0 dest 0.0.0.0
sc0: flags=63<UP,BROADCAST,RUNNING>
vlan
100 inet 144.251.100.111 netmask 255.255.255.0 broadcast
144.251.100.255
```

D: The show frame-relay lmi command displays statistics about the Local Management Interface (LMI), It does not display status of FECN and BECN packets however.

Sample output:

```
Router CertK # show frame-relay lmi
LMI Statistics for interface Serial3 (Frame Relay NNI) LMI TYPE = CISCO
Invalid Unnumbered info 0 Invalid Prot Disc 0
Invalid dummy Call Ref 0 Invalid Msg Type 0
Invalid Status Message 0 Invalid Lock Shift 0
Invalid Information ID 0 Invalid Report IE Len 0
Invalid Report Request 0 Invalid Keep IE Len 0
Num Status Enq. Rcvd 11 Num Status msgs Sent 11
Num Update Status Rcvd 0 Num St Enq. Timeouts 0
Num Status Enq. Sent 10 Num Status msgs Rcvd 10
Num Update Status Sent 0 Num Status Timeouts 0 Reference:
http://www.cisco.com/en/US/tech/ CK7 13/ CK2
37/technologies_configuration_example09186a0080094a3c.shtml
```

QUESTION 341

On router CK1 , one of the PVC's is configured with an incorrect DLCI entry. What command would you use to delete a false or incorrect DLCI number entry on a frame relay?

- A. frame-relay map
- B. show frame-relay pvc
- C. no frame-relay map
- D. frame-relay dlci map

Answer: C

Explanation:

To define the mapping between a destination protocol address and the data-link connection identifier (DLCI) used to connect to the destination address, use the frame-relay map interface configuration command. To delete the map entry, use the no

form of this command.

Reference:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/wan_r/wrdfrely.htm#wp1020191

QUESTION 342

While verifying a Frame Relay connection on a Certkiller router you enter the command:

```
debug frame-relay lmi
```

From this, you notice this line in your output:

```
type 1 status field reads 0x00.
```

What is the status this LMI connection?

- A. Added/active
- B. Added/inactive
- C. Deleted
- D. Disabled
- E. None of the above

Answer: B

Explanation

The debug frame-relay lmi command should show you the status inquiry and the status message that the router receives every ten seconds from the switch. Every minute it sends a FULL LMI to the router that includes all the PVC DLCI's and the status of each DLCI and its corresponding CIR. The status of each DLCI reported on the LMI type 1 status message can be:

```
0x00 (added/inactive)
```

```
0x02 (added active)
```

```
0x04 (deleted)
```

```
0x08 (new/inactive)
```

```
0x0a (new/active)
```

Reference:CCNP Support Exam Certification Guide, page 324, Amir S. Ranjibar, ISBN 0-7357-09955-5

QUESTION 343

In order to identify the possible cause of a connectivity problem with an end-to-end connection on a Frame Relay network, which debug command should you use?

- A. debug frame-relay packet
- B. debug frame-relay events
- C. debug frame-relay dlci
- D. debug frame-relay map
- E. debug frame-relay pvc

Answer: B

Explanation:

The debug frame-relay events command displays debugging information about Frame Relay ARP activities (on networks that support dynamic addressing).

QUESTION 344

You have a 512 kbps Frame Relay network, and you are experiencing some network latency with some real-time data because of the time it's taking to serialize packets. What could you do to reduce the delay on this network? (Choose two)

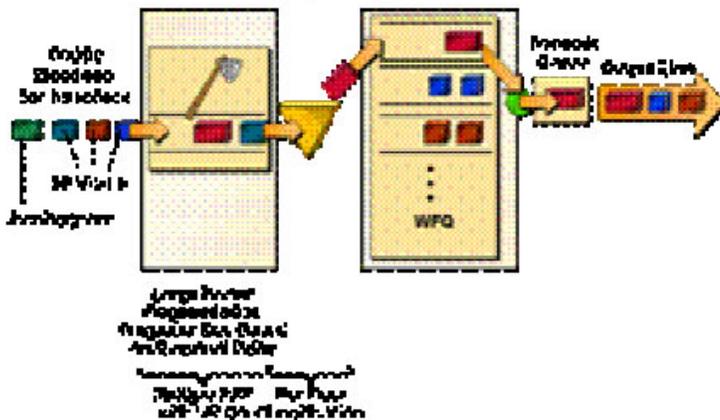
- A. Link fragmentation and interleaving
- B. Frame Relay traffic shaping
- C. Low latency queuing
- D. IP RTP header compression
- E. Traffic classification and policing

Answer: A, C

Explanation:

Interactive traffic (Telnet, voice on IP, and the like) is susceptible to increased latency and jitter when the network processes large packets, (LAN-to-LAN FTP transfers traversing a WAN link, for example), especially as they are queued on slower links. The Cisco IOS Link Fragmentation and Interleaving (LFI) feature reduces delay and jitter on slower-speed links by breaking up large datagrams and interleaving low delay traffic packets with the resulting smaller packets;

Link Fragmentation and Interleaving (LFI)



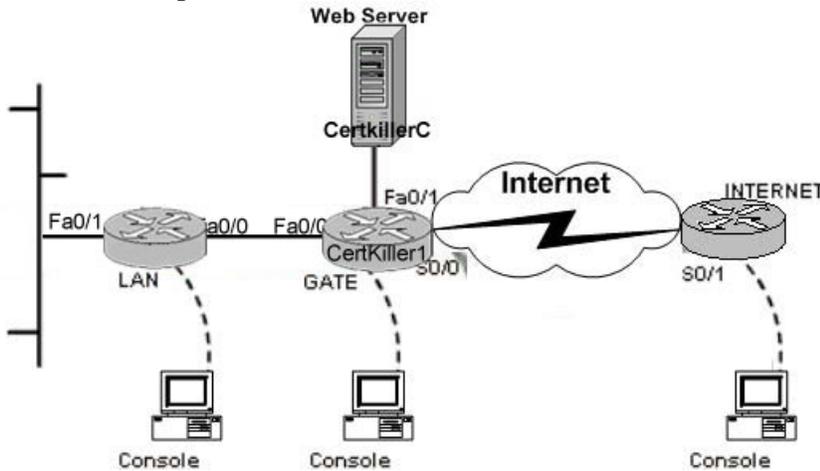
LFI was designed especially for lower-speed links where serialization delay is significant.

The Low Latency Queuing feature brings strict priority queuing to Class-Based Weighted Fair Queuing. This feature is extremely useful for low speed links carrying time sensitive traffic such as voice and video.

QUESTION 345

SIMULATION

Use the network depicted below for this simulation:



Certkiller .com recently completed migrating to a new ISP provider. A technician configured the Certkiller 1 router to compensate for the new address space being issued and implemented a basic ACL for security purposes. Since the move, reports from Certkiller employees indicate that the Internet is inaccessible. Also, customers have reported that the Web server, named Certkiller C, cannot be accessed. However, local employees have been able to access the Web server. Due to the Certkiller .com Company policies, NAT and security ACL have been implemented and placed on the Certkiller 1 router's Internet connecting interface. The security policy indicates that traffic to the inside hosts must be explicitly defined in the ACL. Command authorizations put in place will not allow for the usage of "debug" commands. Using the topology provided and the following information find any current issues and correct them.

Web Server:

Inside Local Address: 10.10.10.10/24

Inside Global Address: 198.133.219.10/24

LAN:

Inside Global Address: 198.133.219.1/24

All passwords: Certkiller

All "debug" commands have been disabled.

LAN

Fa0/0: 10.10.11.2/24

Fa0/1 10.20.0.1/16

Certkiller 1

Fa0/0: 10.10.11.1/24

Fa0/1: 10.10.10.1/24

S0/0: 172.16.0.2/30

Internet

S0/1: 172.16.0.1/30

Certkiller C

Internal: 10.10.10.10

External: 198.133.219.10

Start the simulation by clicking on the console connected to the router you want to configure.


```
Certkiller1# sh run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Certkiller1
!
!
enable secret 5 $1$0/yW$toqA0XRiCtY@gh7pM06fS0
!
ip subnet-zero
!
!
!
!
interface Loopback0
 ip address 198.133.219.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 10.10.11.1 255.255.255.0
 ip nat inside
!
interface FastEthernet0/1
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
!
!
interface Serial0/0
 ip address 172.16.0.2 255.255.255.252
 ip access-group 101 in
 ip nat outside
Clock:

ip nat inside source list 1 interface loopback0 overload
ip nat inside source static 10.10.10.10 198.133.219.10
!
ip route 0.0.0.0 0.0.0.0 Serial0/0
ip route 10.20.0.0 255.255.0.0 FastEthernet0/0
!
access-list 1 permit 10.0.0.0 0.255.255.255
access-list 101 permit ip any host 10.10.10.10
access-list 101 permit ip any 10.20.0.0 0.0.255.255
access-list 101 permit ip any 10.10.11.0 0.0.0.255

line con 0
 transport input none
line aux 0
line vty 0 4
 session-timeout 60
 password cisco
 login
!
end
Certkiller1#
```

Certkiller 1 Configuration Exhibit, part 2

Internet Configuration Exhibit

```
INTERNET#sh ru
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname INTERNET
!
!
enable secret 5 $1$0/yW$toqA0XRiCtY8gh7pM06ES0
!
ip subnet-zero
!
!
!
interface Serial0/0
no ip address
shutdown
!
interface Serial0/1
ip address 172.16.0.1 255.255.255.252
!
!
ip route 198.133.219.0 255.255.255.0 Serial0/1
!
!
line con 0
transport input none
line aux 0
line vty 0 4
session-timeout 60
password
login
!
end
INTERNET#
```

Answer: See below

The following two configuration commands need to be placed on router Certkiller 1:
access-list 101 permit ip any host 198.133.219.10 in global configuration mode.
"ip nat outside" under interface loopback 0.

Explanation:

In order to allow Internet users to reach the Web Server, the access list must be configured to allow access to it. Currently, the access list allows traffic destined to the IP address 10.10.10.10, which is the real IP address of the Web server. However, since the input access list is checked before the address translation takes place, the access list must be configured to permit traffic to the global IP address, since this is the IP address that Internet users will use to access the web server. For the NAT order of operation, see below:

In the table below, when NAT performs the global to local, or local to global, translation is different in each flow.

Inside-to-Outside	Outside-to-Inside
<ol style="list-style-type: none"> 1. If IPSec then check input access list 2. decryption - for CET (Cisco Encryption Technology) or IPSec 3. check input access list 4. check input rate limits 5. input accounting 6. policy routing 7. routing 8. redirect to web cache 9. NAT inside to outside (local to global translation) 10. crypto (check map and mark for encryption) 11. check output access list 12. inspect (Context-based Access Control (CBAC)) 13. TCP intercept 14. encryption 	<ol style="list-style-type: none"> 1. If IPSec then check input access list 2. decryption - for CET or IPSec 3. check input access list 4. check input rate limits 5. input accounting 6. NAT outside to inside (global to local translation) 7. policy routing 8. routing 9. redirect to web cache 10. crypto (check map and mark for encryption) 11. check output access list 12. inspect CBAC 13. TCP intercept 14. encryption

Also, since the Loopback address is being used as the IP address for translating outside hosts when going to the Internet, it must be configured to participate in the NAT process, so the "ip nat outside" command should be used.

QUESTION 346

The Certkiller router had frame relay debugging enabled, and the output from this is shown below:

```
Serial 1 (out): StEnq, clock 20212769, myseq 206, mineseen
205, yourseen 136, DTE up
```

```
Serial 1 (in): Status, clock 20212764, myseq 206
```

```
RT IE 1, length 1, type 1
```

```
KA IE 3, length 2, yourseq 138, myseq 206
```

....

```
Serial 1 (out): StEnq, clock 20252760, myseq 210,mineseen
209, yourseen 144, DTE up
```

```
Serial 1 (in): Status, clock 20252764, myseq 210
```

```
RT IE 1, length 1, type 1
```

```
KA IE 3, length 2, yourseq 146, myseq 210
```

```
PVC IE 0x7, length 0x6, dlci 400, status 0, bw 56000
```

```
PVC IE 0x7, length 0x6, dlci 401, status 0, bw 56000
```

What is true about the phrase:

```
(out): StEnq message
```

shown in the above exhibit?

- A. A PVC status enquiry sent by the router.
- B. An LMI status enquiry sent by the router.
- C. A PVC status enquiry sent by the switch.
- D. An LMI status enquiry sent by the switch.

Answer: B

Explanation:

This could be output of a debug frame-relay lmi command issued at a router. The first line describes the LMI request the router has sent to the switch.

Note 1: The debug frame-relay lmi command is used to display information on the local management interface (LMI) packets exchanged by the router and the Frame Relay service provider.

Note 2: StEnq stands for Status Enquiry.

Serial 1 (out): StEnq, clock 20212769, myseq 206, mineseen 205, yourseen 136, DTE up

Incorrect Answers:

A, C: This is LMI exchange, not a PVC exchange.

D: It is send by the router, not by the switch. The "out" is from the point of view of the router, so it is the one sending the status enquiry out to the frame relay switch.

Reference:

http://www.cisco.com/en/US/tech/CK7_13/CK2_37/technologies_configuration_example09186a0080094a3c.shtml

QUESTION 347

Which commands would you use if you were troubleshooting a Microsoft Windows based end system, and you needed to gather information? (Choose all that apply.)

- A. traceroute
- B. route print
- C. show route
- D. print route
- E. arp -a
- F. show interface

Answer: B, E

Explanation:

See Below From Win2000 Workstation:

+++++

C:\>route print

=====

Interface List

0x1 MS TCP Loopback interface
0x1000003 ...00 d0 09 f4 32 a0 NDIS 5.0 driver

=====

=====

Active Routes:

Network Destination Netmask Gateway Interface Metric

0.0.0.0 0.0.0.0 172.16.26.1 172.16.26.10 1
127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1
172.16.26.0 255.255.255.0 172.16.26.10 172.16.26.10 1
172.16.26.10 255.255.255.255 127.0.0.1 127.0.0.1 1
172.16.255.255 255.255.255.255 172.16.26.10 172.16.26.10 1
224.0.0.0 224.0.0.0 172.16.26.10 172.16.26.10 1
255.255.255.255 255.255.255.255 172.16.26.10 172.16.26.10 1
Default Gateway: 172.16.26.1

=====

Persistent Routes:

None

C:\>arp -a

Interface: 172.16.26.10 on Interface 0x1000003

Internet Address Physical Address Type

172.16.26.1 00-30-ab-04-2c-d5 dynamic

C:\>

QUESTION 348

Your junior administrator is troubleshooting a Windows based end system. You notice that she's just entered the command nslookup. At what OSI layer does she suspect the problem to be at?

- A. Physical
- B. Data Link
- C. Network
- D. Transport
- E. Application

Answer: E

Explanation:

This command displays the DNS name/IP host information, indicating that a problem exists while trying to connect to a web site via HTTP or an email server. Either way, the problem appears with an application not working properly.

On end systems that are running Windows operating systems, `ipconfig` or `wiipcfg`, `tracert`, `nslookup`, and `ping` are among the useful commands that can help you isolate application layer problems. The `wiipcfg` command displays IP information for hosts that are running Windows 9x and Windows Me, whereas its counterpart, `ipconfig`, displays the same information on hosts that are running Windows NT/2000/XP. The `tracert` command works on all Microsoft operating systems; it verifies connectivity to an IP address or host and displays the path to that destination based on current best network path. The `nslookup` command allows you to discover the IP address of an IP host using its name, or to discover the host name for an IP address with the help of a name server. `ping` allows you to test connectivity to another IP host:

```
C:\> winipcfg /all (Windows 9X and Me command)
C:\> ipconfig /all (Windows NT/2000/XP command)
C:\> tracert {ip-address | ip host}
C:\> nslookup
```

Reference:

CCNP CIT Exam Certification Guide Page No. 209 Second Edition ISBN:
1-58720-081-3

QUESTION 349

Which command would you use to trace a packet from a Windows PC to a host on 192.168.2.1 without resolving addresses to hostnames?

- A. Tracert 192.168.2.1
- B. Tracert -r 192.168.2.1
- C. Tracert -d 192.168.2.1
- D. Tracert 192.168.2.1 /all

Answer: C

Explanation:

The Tracert command determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination with incrementally increasing Time to Live (TTL) field values. The path displayed is the list of near-side router interfaces of the routers in the path between a source host and a destination. The near-side interface is the interface of the router that is closest to the sending host in the path. Used without parameters, tracert displays help.

Syntax

```
tracert[-d] [-h MaximumHops] [-j HostList] [-w Timeout][TargetName]
```

Parameters

-d: Prevents tracert from attempting to resolve the IP addresses of intermediate routers to their names. This can speed up the display of tracert results.

-hMaximumHops: Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops.

-jHostList: Specifies that Echo Request messages use the Loose Source Route option in the IP header with the set of intermediate destinations specified in HostList. With loose source routing, successive intermediate destinations can be separated by one or multiple routers. The maximum number of addresses or names in the host list is 9. The HostList is

a series of IP addresses (in dotted decimal notation) separated by spaces.

-wTimeout: Specifies the amount of time in milliseconds to wait for the ICMP Time Exceeded or Echo Reply message corresponding to a given Echo Request message to be received. If not received within the time-out, an asterisk (*) is displayed. The default time-out is 4000 (4 seconds).

TargetName: Specifies the destination, identified either by IP address or host name.

Reference:

<http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/tracert.msp>

QUESTION 350

You're troubleshooting a Microsoft Windows based end system, and you need to verify the validity of a declared layer 3 address to the corresponding layer 2 MAC address. Which command would you use?

- A. ping
- B. tracert
- C. telnet
- D. arp -a
- E. None of the above

Answer: D

Explanation:

arp -a will list all the entries in the ARP table:

```
C:\>arp -a
Interface: 205.153.63.30 on Interface 2
Internet Address Physical Address
Type 205.153.63.1 00-00-a2-c6-28-44 dynamic
205.153.63.239 00-60-97-06-22-22 dynamic
```

Reference: www.tarpat.com/books/network2/tshoot/ch02_03.htm

QUESTION 351

You want to view all of the active data sessions on a PC host in the Certkiller network. Which Microsoft Windows command would you use to display information on an active TCP/IP connection?

- A. ifconfig -a
- B. traceroute
- C. netstat
- D. ping
- E. All of the above

Answer: C

Explanation:

Netstat is a windows command that shows the following:

- * active TCP connections
- * ports on which the computer is listening

- * statistics on the Ethernet
 - * the IP routing table
 - * and IPv4 and IPv6 statistics
-

QUESTION 352

When creating a record of network applications that are available on an end-system it's good practice to put special emphasis on high bandwidth applications which have a high impact on network performance. Which of the following applications consume a great deal of bandwidth? (Choose two)

- A. IPTV multicast applications
- B. Calendar software clients
- C. Email clients
- D. Streaming video players
- E. Internet browsers

Answer: A, D

Explanation:

Consuming high bandwidth is a relative term, and the question asks you which two applications consume more bandwidth than the others. IPTV and streaming video are by far more bandwidth intensive than the other three choices. Any application utilizing Video streams requires a great deal of bandwidth, as well as high QoS and low latency and jitter guarantees.

QUESTION 353

When troubleshooting a Windows end-system, which command gathers data by identifying the path that a packet takes through the network?

- A. route print
- B. tracert
- C. routetrace
- D. traceroute
- E. ping

Answer: B

Explanation:

Tracert for Microsoft and traceroute for Cisco will help the network administrator to carry out troubleshooting by gathering the symptoms and identifying the path a packet takes through the network. This utility will show the router hops that the path takes, as well as the latency between each hop.

Note: Tracert is a valid Microsoft PC command, while Traceroute is supported only a Cisco router.

QUESTION 354

You are a mobile troubleshooter, and you've arrived to a jobsite to troubleshoot an old Windows NT network. The local MCSE technician tells you that users are unable to browse the network neighborhood. What could be causing this problem? (Choose two)

- A. Inaccurate routing entries in the LMHOSTS file.
- B. Inaccurate resolution of non-IP entities into IP addresses.
- C. Incomplete resolution of non-IP entities into IP addresses.
- D. Incomplete configuration of IP entities to the IP routing table.

Answer: B, C

Explanation:

Windows NT, contrary to Windows 2000/XP/.NET, use WINS for name resolution. WINS map NetBios names to IP addresses. Inaccurate or incomplete mappings of NetBIOS name to IP address could cause browsing problems.

Incorrect Answers:

A: LMHOSTS files contain NetBIOS to IP addresses mappings. It does not contain routing entries.

D: Windows NT name resolution does not depend on routing entries.

QUESTION 355

You are troubleshooting a connectivity problem on an NT host and issue the "route print" DOS command. What will be displayed after entering a route print command on a Windows NT system? (Choose four)

- A. Metric
- B. Network mask
- C. Routing protocol
- D. Gateway address
- E. Interface address

Answer: A, B, D, E

Explanation:

The route command with the route parameter prints a route or routes. It will disclose: 1) The network destination 2) The subnet mask 3) The gateway 4) The metric 5) The interface.

Incorrect Answers:

C: Routing Protocols are generally only used by routers and most PC hosts do not participate in a routing protocol, so any information used by a protocol is not listed.

QUESTION 356

Which of the following end-stations use the traceroute command to identify the path through a network that a packet takes? (Choose two)

- A. Unix
- B. DOS
- C. Windows NT/2000/XP
- D. Windows9x/ME
- E. Mac OS X

Answer: A, E

Explanation:

DOS and Windows are proprietary of Microsoft, and their operating systems don't use traceroute. When DOS and Windows were originally developed, they were developed as simple user focused alternatives to UNIX, and had the mandate to lean away from UNIX commands. Secondly Microsoft wanted to make as much profit as it could on its operating systems, so with full intention, made commands that they could call their own intellectual property. The Microsoft version of the traceroute command is "tracert." Only the tracert command is valid in a Windows machine, not traceroute.

QUESTION 357

Which of these Windows 2000 commands could you use to show the information that is used in an end-system configuration table? (Choose four)

- A. route print
- B. ifconfig -a
- C. arp /all
- D. arp -a
- E. ping [ip-address | hostname]
- F. telnet [ip-address | hostname]

Answer: A, D, E, F

Explanation:

The commands: route print, arp -a, ping, and telnet will all give you good information to include in an end-system configuration table. All of these commands provide for different details regarding the TCP/IP configuration of an end host.

Incorrect Answers:

B: The command ifconfig -a is a Linux command.

C: The command arp/all isn't correct, as the/all parameter doesn't exist.

QUESTION 358

The CEO of your company phones you up one morning complaining that he can't browse the email server through his Network Neighborhood on his Windows NT workstation. What is likely to be causing this problem?

- A. The WINS server is down.
- B. The Browse Master has gone down.

- C. The Internet Firewall is blocking access.
- D. The email server was moved to a different IP subnet.
- E. None of the above.

Answer: A

Explanation:

Windows NT uses WINS for name resolution. A WINS server which is down could prevent the NT workstation from browsing resources on the network. This is the most likely problem in this scenario.

Incorrect Answers:

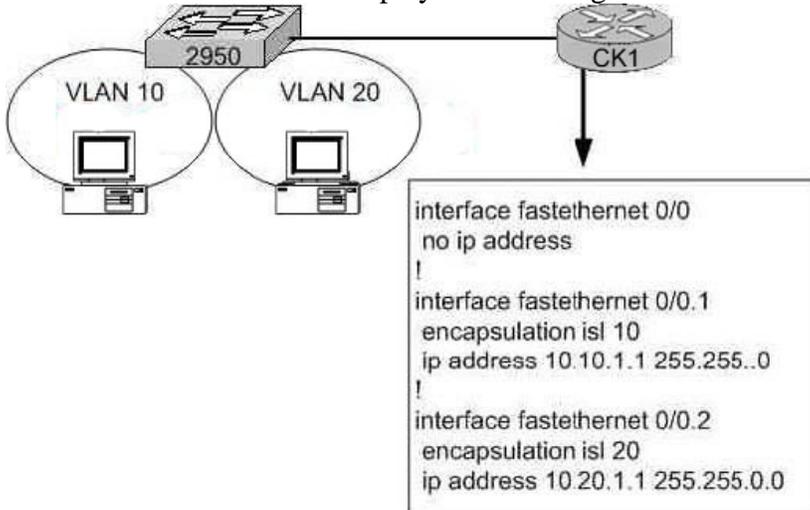
B: A Browse Master that goes down might slow down browsing, but would not prevent name resolution from functioning.

C: The internet firewall is not applied when browsing local resources.

D: Moving a server to a different subnet could make it inaccessible if the IP configuration is not adjusted. So this could cause the problem described in the scenario. However, there are no reports on that the E-mail server is not functioning. The most likely problem is a name resolution problem.

QUESTION 359

The Certkiller Network is displayed in the diagram below:



You are trying to bring up a trunk between a Catalyst 2950 switch and router CK1 . However, the trunk will not become operational. Based on the CK1 router configuration shown above, what is the most likely reason for the problem?

- A. The encapsulation type must be set to dot1q.
- B. The subinterface number must be equal to the ISL VLAN number.
- C. An IP address must be configured on the physical interface.
- D. The encapsulation must be configured on the physical interface.
- E. The IP addresses for VLAN 10 and VLAN20 must be in the same subnet.

Answer: A

Explanation:

The current encapsulation for CK1 is ISL, and the Cisco 2950 series switch does not support ISL. Since both sides of a trunk must have their encapsulations match and the Catalyst 2950 does not support ISL trunking, use 802.1Q trunking instead.

Reference:

http://www.cisco.com/en/US/tech/CK3_89/CK2_13/technologies_configuration_example09186a0080094bc5.shtml

QUESTION 360

Some information on one of the Certkiller switches is displayed below:

```
VTP Version : 2
Configuration Revision : 247
Maximum VLANs supported locally : 1005
Number of existing VLANs : 38
VTP Operating Mode :
VTP Domain Name : Lab
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80
Configuration last modified by 0.0.0.0 at 8-12-99 15:04:49
Switch#
```

On this switch, you try to add VLAN2 to the configuration, but you are unsuccessful. Based on the information provided above, what is the most likely reason for this?

- A. VTP v2 mode must be enabled.
- B. VTP version must be 1.
- C. VTP operating mode must be changed.
- D. VTP pruning must be disabled.

Answer: C

Explanation:

When you look halfway through the configuration you'll notice the line:

```
VTP Operating Mode : Client
```

When a switch is in VTP client mode, it can not create new VLANs. Only switches in VTP server mode are able to create, modify, and delete VLAN information within the VTP domain.

QUESTION 361

A Certkiller layer 3 switch named DSW111 is configured with HSRP on VLAN 11. To verify the configuration, the "debug standby" command was issued. The output from this is shown below:

```
DSW111(config)# interface vlan 11
DSW111(config-if)# no shut

*Mar 1 00:16:41.295: %SYS-5-CONFIG I: Configured from console by console
*Mar 1 00:16:43.095: %LINK-3-UPDOWN: Interface Vlan11, changed state to up
*Mar 1 00:16:43.099: SB: Vlan11 Interface up
*Mar 1 00:16:43.099: SB11: Vlan11 Init: a HSRP enabled
*Mar 1 00:16:43.099: SB11: Vlan11 Init: → Listen
*Mar 1 00:16:43.295: SB11: Vlan11 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:16:43.295: SB11: Vlan11 Active router is 172.16.11.112
*Mar 1 00:16:43.295: SB11: Vlan11 Listen: hHello rcvd from lower pri Active router (50/172.16.11.112)
*Mar 1 00:16:43.295: SB11: Vlan11 Active router is local, was 172.16.11.112
*Mar 1 00:16:43.295: SB11: Vlan11 Coup out 172.16.11.111 Listen pri 100 ip 172.16.11.115
*Mar 1 00:16:43.299: %STANDBY-6-STATECHANGE: Vlan11 Group 11 state Listen → Active
*Mar 1 00:16:43.303: SB11: Vlan11 Hello in 172.16.11.112 Speak pri 50 ip 172.16.11.115
*Mar 1 00:16:44.000: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan11, changed state to up
*Mar 1 00:16:44.187: SB11: Vlan11 Hello in 172.16.11.112 Speak pri 50 ip 172.16.11.115
*Mar 1 00:16:44.187: SB11: Vlan11 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
```

Based on the information above, what is true about the HSRP configuration on DSW11?

- A. DSW111 is configured with preempt.
- B. DSW111 transitioned to the standby router.
- C. DSW111 has a physical IP address of 172.16.11.112.
- D. DSW111 has a priority of 50.

Answer: A

Explanation:

The standby preempt command enables the Hot Standby Router Protocol (HSRP) router with the highest priority to immediately become the active router. Priority is determined first by the configured priority value, and then by the IP address. In each case, a higher value is of greater priority. When a higher priority router preempts a lower priority router, it sends a Coup message. When a lower priority active router receives a Coup message or a Hello message from an active, higher priority router, it changes to the Speak state and sends a resign message. In this case, DSW111 immediately transitioned to the active HSRP router due to having a higher HSRP priority. Because of this, the preempt configuration command must have been issued.

Reference:

How to Use the standby preempt and standby track Commands Document ID: 13780

<http://www.cisco.com/warp/public/619/6.html>

QUESTION 362

While logged into the Router CertK router, you issue the following command:

```
Router CertK # show vlan
```

What kind of specific VLAN information will you see from this command? (Choose three)

- A. VLAN ID
- B. VLAN name
- C. VTP domain
- D. The router subinterface for the VLAN.
- E. Network address for each configured protocol.

Answer: A, B, D

Explanation:

VLAN ID, VLAN name, and the router subinterfaces for the VLAN are included in the output of the show vlan command.

Sample output:

```
RouterCK# show vlan
VLAN Name Status Ports
-----1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4,
Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Gi0/1, Gi0/2
100 Server-Farm active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
VLAN
Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----1 enet 100001 1500 - - - - 1002 1003 100 enet 100100 1500 - - - - 0
01002 fddi 101002 1500 - - - - 1 1003 1003 tr 101003 1500 1005 0 - - srb 1 1002
1004 fdnet 101004 1500
- - 1 ibm - 0 01005 trnet 101005 1500 - - 1 ibm - 0 0
RouterCK #
```

Incorrect Answers:

C: VTP domain is not displayed.

E: Network addresses for configured protocols are not displayed. Only layer 2 information is provided from the "show vlan" command.

QUESTION 363

You are booting up a new Certkiller Catalyst 5000 switch for the first time. Which of the following tests are performed on a Catalyst 5000 switch upon power-up self-test? (Choose all that apply)

- A. LED test
- B. EARL test
- C. ROM Checksum
- D. Trunk Status Test
- E. None of the above

Answer: A, B, C

Explanation:

Sample Output, Catalyst 5000 Power-on Self-Test:

```
ATE0
ATS0=1
Power Up Diagnostics
Init NVRAM Log
LED Test
ROM CHKSUM
```

DUAL PORT RAM r/w
RAM r/w
RAM address test
Byte/Word Enable test
EARL test
EARL test Done
BOOTROM Version 2.1, Dated Jun 4 1996 12:02:33
BOOT date: 06/08/00 BOOT time: 12:43:07
SIMM RAM address test
SIMM Ram r/w 55aa
SIMM Ram r/w aa55
Uncompressing NMP image. This will take a minute...
Cisco Systems Console

QUESTION 364

You have been assigned the task to troubleshoot a non-operational external router connection that's supporting inter-VLAN routing. What two steps should you take first? (Choose two)

- A. Ensure that the correct IP address is configured on the main interface.
- B. Verify that the subinterface for each VLAN has the correct IP address.
- C. Verify the correct media-type statement for each VLAN subinterface.
- D. Ensure that the full duplex setting on the main router interface matches that on the switch port.

Answer: B, D

Explanation:

B: Each subinterface must have a correct IP address. Each subinterface will correspond to one VLAN member of the trunk, and the IP address on this subinterface will act as the default gateway for the LAN hosts.

D: The main interface configuration commands that may be necessary on the Fast Ethernet interface are media-type and full-duplex. If you are troubleshooting a trunk connection between a router and a switch, it is best if you decide on the duplexing mode and do a manual configuration on both devices. Relying on the autosensing feature is usually discouraged. You should always ensure that the speed and duplex settings match on each end.

Incorrect Answers:

A: If a Fast Ethernet interface is used for trunking purposes, it should not have any Layer 3 (OSI network layer) address or any bridging commands configured on the main interface. These types of commands must be appropriately entered on the subinterfaces. Each subinterface will correspond to one VLAN member of the trunk.

C: The media type should be set on the main interface, not on the subinterfaces.

Reference: Troubleshooting InterVLAN Routing on a Catalyst 5000 Switch with RSM
<http://www.cisco.com/warp/public/473/56.html>

QUESTION 365

The Certkiller switched LAN is being redesigned to enhance the performance of the Spanning Tree Protocol (STP) algorithm. Which design considerations make the STP troubleshooting process easier? (Choose two)

- A. Do not set the max age metric too low.
- B. Do not connect a router to a trunk port.
- C. Use gigabit ports for router connections.
- D. Set the network diameter to less than or equal to 7 switches.

Answer: A, D

Explanation:

One important topic of interest in switched internetworks is the convergence time of the spanning tree. Two factors, the diameter of a network measured in terms of the number of hops (bridges/switches), and the values of the spanning tree timers, such as the max_age parameter, affect the time it takes for the bridged/switched internetwork to converge. The diameter of the STP domain is the maximum number of bridges between any two points of attachment of end stations. The IEEE considers a maximum diameter of seven bridges.

max age takes into account that the switch at the periphery of the network should not time out the root information under stable condition (that is, if the root is still alive). This is the value that max age needs to take into account the total BPDU propagation delay and the message age overestimate. As such, the formula for max age is as follows:

$$\begin{aligned} \text{Max_age} &= \text{End-to-end_BPDU_propa_delay} + \text{Message_age_overestimate} \\ &= 14 + 6 \\ &= 20 \text{ sec} \end{aligned}$$

This explains how IEEE reaches the default recommended value for max age. Generally, the default values should only be changed with caution.

Reference:

http://www.cisco.com/en/US/tech/CK389/CK621/technologies_tech_note09186a0080094954.shtml

QUESTION 366

For some troubleshooting applications in highly secured environments, it is necessary to remove certain access lists. Which statement is the most accurate regarding temporarily removing an access list in a highly secured network?

- A. It will correct the network problem.
- B. It makes the configuration of the router cleaner.
- C. It removes the security that the list was meant to provide.
- D. It improves the network performance because using access lists is a CPU-intensive process.

Answer: C

Explanation:

Access lists are used to filter traffic to prevent specific traffic from going through a router. In this highly-secured network they are most likely used for implementing security policies. Removing it will remove the security it implements.

Incorrect Answers:

A, B, D: Although all of these answers are correct in certain circumstances, it is not important to understand why the access list was implemented in the first place. In a network where security is most important, the removal of any access lists for troubleshooting purposes should be done only as a last resort.

QUESTION 367

You delegated the task of implementing a new network security policy to the Certkiller network and to your dismay some of the users are now unable to access their servers. What should you do first to solve the problem?

- A. Call TAC/SE.
- B. Call McAfee/Norton and report a virus attack.
- C. Remove access lists, one at a time, and observe the results.
- D. Repeat the problem-solving process repeatedly until you resolve the problem.

Answer: D

Explanation:

If there's a problem, regardless of what you think the obvious may be, always stick to your problem solving model, because there can always be the chance that the problem could be the result of another factor.

Incorrect Answers:

- A: This should be done as a last resort, and only when you have evidence that the problem is Cisco-related.
- B: This should only be done after you have concluded that the problem does indeed stem from a virus.
- C: This should only be done as a last resort, as doing so will increase the security vulnerability of your network.

QUESTION 368

Your junior administrator has just finished implementing interVLAN routing on an external router of an already existing switched network. After doing so, you receive numerous complaints from disgruntled users that they are now unable to surf the internet and access other resources. What is likely causing the problem?

- A. The user's switch ports have portfast disabled.
- B. Many users are using Category 3 patch cables.
- C. The router has introduced a spanning-tree loop.
- D. The VLAN configuration does not match on both sides of the trunk.

Answer: D

Explanation:

The VLAN configuration on both sides of the trunk must match. If not, users will not be able to access any device that resides in another IP subnet or in another VLAN.

Incorrect Answers:

A: Portfast only helps to decrease the link startup time. Portfast could resolve the problem in this scenario, but it would not be the most likely cause of the problem.

B: Usage of Category 3 patch would not cause this problem.

C: A spanning-tree loop would degrade overall performance, not the performance of a group of users. When a loop exists, the STP would automatically solve the problem by logically disabling one of the redundant links.

Reference: Using Portfast and Other Commands to Fix Workstation Startup Connectivity Delays

<http://www.cisco.com/warp/public/473/12.html>

QUESTION 369

On a Certkiller Catalyst 5000 switch you enter the "show interface" command. From this, which of the following pieces of information would be displayed? (Select two)

- A. Ports that are in trunking mode
- B. All interfaced defined on the RSM.
- C. VLAN information of the SC0 interface.
- D. The management IP address of the switch.
- E. The spanning-three settings of switch ports.

Answer: C, D

Explanation:

The show interface command is used to display operational characteristics and statistics for interfaces configured for the storage router.

C: VLAN information of the sc0 interface is shown (see sample output below)

D: The interface sc0 is an internal management interface that is connected to the switching fabric and participates in all of the functions of a normal switch port. The IP address of sc0 is show in the sample output below.

Sample Output:

```
Console CertK > show interfaceme1:flags=63<UP,BROADCAST,RUNNING> inet 0.0.0.0 netmask 255.0.0.0 broadcast 0.0.0.0sl0:flags=51<UP,POINTOPOINT,RUNNING> slip 0.0.0.0 dest 0.0.0.0 sc0:flags=63<UP,BROADCAST,RUNNING> vlan 1 inet 171.69.199.168 netmask 255.255.255.0 broadcast 171.69.199.255
```

Incorrect Answers:

A: The show interface command displays the status and statistics information about all of your router's interfaces. You cannot display a subset of interfaces based on their type.

B: All interfaces, not only interfaces defined on the RSM are displayed.

Note: A router Switch Module (RSM) is commonly used in Catalyst switches for the purpose of routing between VLANs.

E: The show span command is used for this purpose.

QUESTION 370

Fill in the blanks to correctly complete the following statement:

The lack of _____ and _____ prevents VTP information from propagating between switches. (Choose two)

- A. VLAN 1
- B. A trunk port
- C. VTP priority
- D. A root VTP server
- E. A transparent switch
- F. A VTP client

Answer: B, D

Explanation:

Virtual Local Area Network (VLAN) Trunk Protocol (VTP) reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere. VTP is a Cisco-proprietary protocol that is available on most of the Cisco Catalyst Family products.

B: VTP packets are carried on VLAN 1, but only on trunks (ISL, dot1Q, or LANE).

Therefore, at least one port on the switch must be configured as a trunk.

D: A VTP switch can operate in any one of these three VTP modes:

1. Server-VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over trunk links. VTP server is the default mode.
2. Client-VTP clients function the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client.
3. Transparent-VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements.

Since VLAN information is only propagated from a VTP server, at least one of the switches in the VTP domain must be configured as a server.

QUESTION 371

It is desired to manually control the designation of the Spanning-tree Protocol (STP) root switch in the Certkiller network. What is the best way to specify the switch that should become the STP root?

- A. By enabling uplink-fast on the ports of the desired switch.
- B. By lowering the bridge priority on the desired switch.
- C. By setting a lower MAC address on the designated switch.
- D. By raising the bridge ID on one switch.
- E. By increasing the bridge priority value of the desired switch.

Answer: B

Explanation:

To configure a switch to become the root, use the spanning-tree mst instance-id root global configuration command. This will change the switch priority from the default value of 32768 to a significantly lower value. With the lowest root priority, this switch will become the root switch for the specified spanning-tree instance. When this command is entered, the switch will check the switch priorities of the root switches. The switch will set its own priority for the specified instance to 24576 because of the extended system ID support. If any root switch for the specified instance has a switch priority lower than 24576, the switch will set its own priority to 4096 less than the lowest switch priority. Remember, for STP, a lower value is preferred when the selection of the STP root bridge takes place.

QUESTION 372

VTP is being implemented in the Certkiller network. What purpose does the VLAN Trunking Protocol (VTP) serve?

- A. To provide load sharing on inter-switch links.
- B. To prevent loops on redundant switch trunks.
- C. To ensure that VLANs are only active on trunk ports.
- D. To provide consistent mapping of VLANs across the switched domain
- E. None of the above

Answer: D

Explanation:

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs within a VTP domain. A VTP domain (also called a VLAN management domain) is made up of one or more network devices that share the same VTP domain name and that are interconnected with trunks. VTP minimizes misconfigurations and configuration inconsistencies that can result in a number of problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

With VTP, you can make configuration changes centrally on one or more network devices and have those changes automatically communicated to all the other network devices in the network.

QUESTION 373

The Certkiller network is in the process of configuring VTP throughout the switched LAN. Which is true about VTP domains? (Choose two)

- A. A switch can support up to 1024 VTP domains.
- B. Many switches can be in the same VTP domain.
- C. A VLAN can participate in up to 16 VTP domains.
- D. VLAN configurations remain consistent within a VTP domain.

Answer: B, D

Explanation:

B: A VTP domain is made up of one or more interconnected switches that share the same VTP domain name.

D: When you make a change to the VLAN configuration on a VTP server, the change is propagated to all switches in the VTP domain.

Understanding VTP Domains

A VTP domain (also called a VLAN management domain) is made up of one or more interconnected switches that share the same VTP domain name. A switch can be configured to be in only one VTP domain. You make global VLAN configuration changes for the domain using either the command-line interface (CLI) or Simple Network Management Protocol (SNMP).

Incorrect Answers:

A: The question asked for VTP not for VLAN support. IEEE 802.1Q VLAN trunks support VLANs 1 through 4095. ISL VLAN trunks support VLANs 1 through 1024 (1005 to 1024 are reserved).

C: A single switch can only belong to one VTP domain.

Reference: Configuring VTP

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_6_1/config/vtp.htm

QUESTION 374

Switch CK1 is configured for VTP and is sending out VTP advertisements to other switches in the network. Which of the following properly describe VTP messages? (Choose all that apply)

- A. It is a broadcast messaging protocol
- B. It operates at layer 2
- C. It is a multicast messaging protocol
- D. It operates at layer 3
- E. None of the above

Answer: B, C

Explanation:

B: VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can result in a number of problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

C: Each network device in the VTP domain sends periodic advertisements out each trunking LAN interface to a reserved multicast address. VTP advertisements are received by neighboring network devices, which update their VTP and VLAN configurations as necessary.

The following global configuration information is distributed in VTP advertisements:

1. VLAN IDs (ISL and 802.1Q)
2. Emulated LAN names (for ATM LANE)
3. 802.10 SAID values (FDDI)
4. VTP domain name
5. VTP configuration revision number
6. VLAN configuration, including maximum transmission unit (MTU) size for each VLAN
7. Frame format

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps4324/products_configuration_guide_chapter09186a008019

QUESTION 375

What is the term used to describe the process of a Cisco switch (with ASIC) using layer 3 information to switch traffic to the best path?

- A. Layer 3 Routing
- B. Layer 3 Forwarding
- C. Layer 3 Switching
- D. Layer 3 Cut through

Answer: C

Explanation:

Multi-Layer Switching (MLS) has become a highly desired method of accelerating routing performance through the use of dedicated Application Specific Integrated Circuits (ASICs). Traditional routing is done through a central CPU and software. MLS offloads a significant portion of routing (packet rewrite) to hardware, and thus has also been termed switching. MLS and Layer 3 switching are equivalent terms. Routing works at layer 3. Switches that deploy an Application Specific Integrated Circuit (ASIC) for routing are known as Layer 3 switching devices.

QUESTION 376

SIMULATION

While you were out on vacation, your junior administrator tried to use a telnet session to load a configure file on the router Certkiller 2, but midway through the download he lost the session for no apparent reason. He tested the interface on the Certkiller 1 router and saw that both the line and protocol are up, however he has been unsuccessful in re-establishing another telnet session, and he's been unsuccessful at pinging Certkiller 2. He called up the administrator at router Certkiller 3 and asked him to ping Certkiller 2 but he was also unsuccessful (although the line and protocol are both up on Certkiller 3 as well). It appears that the IP addresses on router CK2 may have changed, but the exact change is unknown. So you cut your vacation short and arrive in the office. Your task is to re-establish IP connectivity between all three routers, and to make sure that routing updates go through.

1. the configuration on Certkiller 1 & Certkiller 3 are locked
2. only the show commands are available
3. it would be beneficial for you to discover the incorrect IP addresses too
4. the passwords for all the routers are the same

Privileged mode password: Certkiller

VTY password: Certkiller

IP Addresses are shown below:

Certkiller 1

S0 10.16.15.10/24

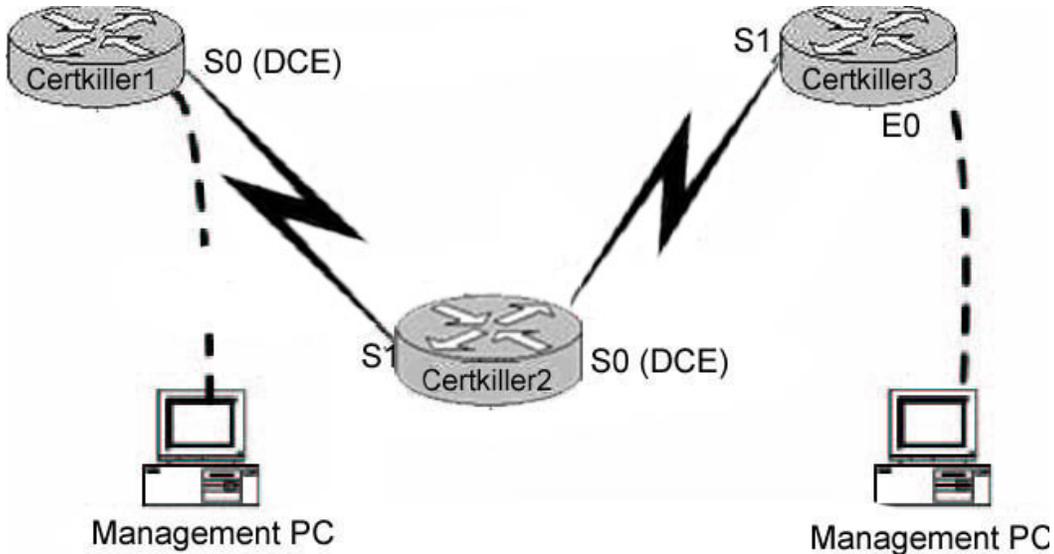
Certkiller 2

S0 172.18.140.2/24

S1 10.16.15.2/24

Certkiller 3

S1 172.18.140.10/24



To configure the router click on the host icon that is connected to a router by a serial cable.

Answer:

1. Login with management PC to router Certkiller 3
2. show cdp neighbor detail (if this works layers 1 and 2 are ok)
3. read output and see neighbor address x.x.x.60
4. telnet to x.x.x.60 (telnet to Certkiller 2)
5. show running config
6. there is no rip running, so do it
7. config t
8. router rip
9. version 2
10. network 10.16.15.0
11. network 172.18.140.0
12. exit
13. interface serial 1 (change ip first of s1 otherwise your connection lost without

changing ip at serial 0)

14. ip address 10.16.15.2 255.255.255.0

15. no shut

17. interface serial 0

18. ip address 172.18.140.2 255.255.255.0

19. no shut

20. exit

21. copy run start

Note:

When you check the Topology exhibit you will lose the telnet connection, and you would have to start all over.

Alternative #1:

Certkiller 1

S0 172.16.72.10/24

Certkiller 2

S0 192.168.226.2/24

S1 172.16.72.2/24

Certkiller 3

S1 192.168.226.10/24

Alternative #2:

Certkiller 1

S0 172.16.109.10/24

Certkiller 2

S0 192.168.236.2/24

S1 172.16.109.2/24

Certkiller 3

S1 192.168.236.10/24

Alternative #3:

Certkiller 1

S0 172.16.79.10/24

Certkiller 2

S0 192.168.177.2/24

S1 172.16.79.2/24

Certkiller 3

S1 192.168.177.10/24

QUESTION 377

The LAN users on a Certkiller office are unable to reach the other Certkiller offices. After some troubleshooting effort, you have determined that the problem is a default gateway problem somewhere in the network. What should you do to correct this? (Choose all that apply)

- A. Check to make sure that the IP addresses are allocated dynamically.
- B. Check to make sure that all servers and other end systems on the LAN have a default gateway specification.
- C. Check whether there is a default gateway configured on the LAN switch.

- D. If any of these devices does not have a default gateway specified, configure a default gateway using the IP address of a router interface on the directly connected LAN
- E. None of the above.

Answer: B, C, D

Explanation:

If you suspect that a device doesn't have a default gateway configured, the obvious thing to do would be to check. Check the device, check the LAN switch, and check all the other devices on the LAN. If you discover that a device doesn't have a default gateway, then it would be wise to configure one.

QUESTION 378

A brand new router has just arrived and you must configure it for the first time. What steps must be taken to bring up an IP interface for the first time? (Choose all that apply)

- A. Configure an interface with the IP address interface configuration command
- B. Use the no shutdown interface configuration command to bring an interface up
- C. Configure an interface with the IP range interface configuration command
- D. Use the shutdown interface configuration command to bring an interface up

Answer: A, B

Explanation:

In order to configure an interface to participate in the network using IP, it must contain an IP address. After this is done, the interface must be enabled through the use of the "no shutdown" command. By default, all interfaces in a router are disabled. Each interface must be manually enabled.

QUESTION 379

The Certkiller network uses non-standard UDP ports for remote IP hosts to reach the DHCP servers. If you had to configure the router to forward these broadcast packets through the use of a helper addresses, which two commands could you use? (Choose two)

- A. ip forward-protocol
- B. ip any helper-address
- C. ip explicit-protocol
- D. ip helper-address

Answer: A, D

Incorrect Answers:

Enabling a helper address or UDP flooding on an interface causes the Cisco IOS software to forward particular broadcast packets. You can use the ip forward-protocol command to specify exactly which types of broadcast packets you would like to have forwarded. A

number of commonly forwarded applications are enabled by default. Enabling forwarding for some ports (for example, Routing Information Protocol (RIP) may be hazardous to your network.

If you use the `ip forward-protocol` command, specifying only UDP without the port enables forwarding and flooding on the default ports.

One common application that requires helper addresses is Dynamic Host Configuration Protocol (DHCP). DHCP is defined in RFC 1531. DHCP protocol information is carried inside of BOOTP packets. To enable BOOTP broadcast forwarding for a set of clients, configure a helper address on the router interface closest to the client. The helper address should specify the address of the DHCP server. If you have multiple servers, you can configure one helper address for each server. Because BOOTP packets are forwarded by default, DHCP information can now be forwarded by the software. The DHCP server now receives broadcasts from the DHCP clients.

If an IP helper address is defined, UDP forwarding is enabled on default ports. If UDP flooding is configured, UDP flooding is enabled on the default ports.

If a helper address is specified and UDP forwarding is enabled, broadcast packets destined to the following port numbers are forwarded by default:

Trivial File Transfer Protocol (TFTP) (port 69)

Domain Naming System (port 53)

Time service (port 37)

NetBIOS Name Server (port 137)

NetBIOS Datagram Server (port 138)

Boot Protocol (BOOTP) client and server datagrams (ports 67 and 68)

TACACS service (port 49)

IEN-116 Name Service (port 42)

In this question, since we need to forward broadcast DHCP packets, the "`ip helper-address`" command is needed. Since the non-standard UDP ports are required, the "`ip forward-protocol`" command is needed.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_chapter09186a008017

QUESTION 380

The Certkiller network is utilizing IP multicast, and you wish to configure the routers to use Multicast Distributed Switching. What would you do to enable IP multicast fast switching or IP multicast distributed switching?

- A. By using the `ip directed-broadcast` command.
- B. By using the `ip mroute-cache` command.
- C. By using the `ip redirects` command.
- D. By using the `ip multicast` command.
- E. None of the above

Answer: B

Explanation:

To configure IP multicast fast switching or multicast distributed switching (MDS), use the `ip mroute-cache` interface configuration command.

Prior to multicast distributed switching (MDS), IP multicast traffic was always switched at the Route Processor (RP) in the Route Switch Processor (RSP)-based platforms. With Cisco IOS Release 11.2 GS, IP multicast traffic can be distributed switched on RSP-based platforms with VIPs. Furthermore, MDS is the only multicast switching method on the Cisco 12000 Gigabit Switched Router (GSR), starting with Cisco IOS Release 11.2(11) GS.

Switching multicast traffic at the RP had disadvantages:

1. The load on the RP increased. This affected important route updates and calculations (for BGP, among others) and could stall the router if the multicast load was significant.
2. The net multicast performance was limited to what a single RP could switch.

MDS solves these problems by performing distributed switching of multicast packets received at the line cards (VIPs in the case of RSP, and line cards in the case of GSR). The line card is the interface card that houses the VIPs (in the case of RSP) and the GSR line card (in the case of GSR). MDS is accomplished using a forwarding data structure called a Multicast Forwarding Information Base (MFIB), which is a subset of the routing table. A copy of MFIB runs on each line card and is always kept up to date with the RP's MFIB table.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1820/products_feature_guide09186a00800f488c.html#367

QUESTION 381

Which of the following commands has the ability of enabling a router to answer ARP requests originally intended for another device?

- A. `ip proxy-arp`
- B. `ip routing`
- C. `ip redirects`
- D. `ip mroute-cache`
- E. `ip address dhcp`
- F. `ip split-horizon`

Answer: A

Explanation:

Proxy ARP is the technique in which one host, usually a router, answers ARP requests intended for another machine. By "faking" its identity, the router accepts responsibility for routing packets to the "real" destination. Proxy ARP can help machines on a subnet reach remote subnets without configuring routing or a default gateway. Proxy ARP is defined in RFC 1027.

To enable this functionality, use the `"ip proxy-arp"` command.

QUESTION 382

What command can you use to allow the forwarding of all UDP broadcasts using

port 200?

- A. ip 200 forward-protocol udp set
- B. ip protocol udp 200
- C. ip forward-protocol udp 200
- D. ip forward 200 udp
- E. ip forward-protocol tcp 200

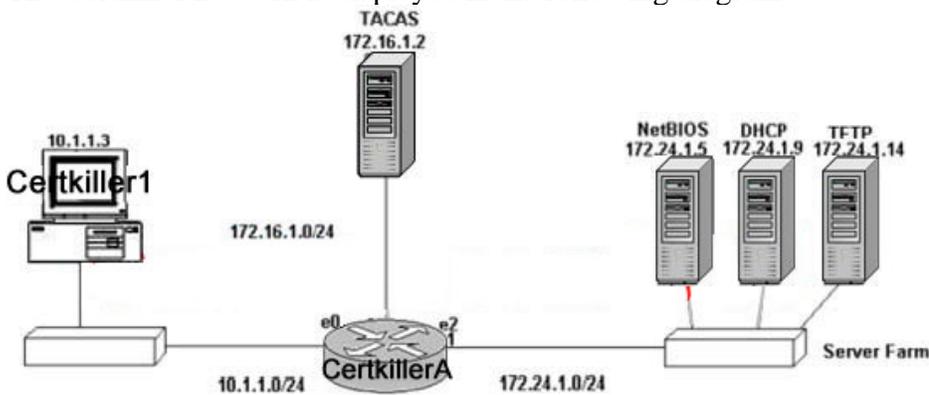
Answer: C

Explanation:

Enabling a helper address or UDP flooding on an interface causes the Cisco IOS software to forward particular broadcast packets. You can use the `ip forward-protocol` command to specify exactly which types of broadcast packets you would like to have forwarded. In this example, to enable the router to forward all UDP port 200 broadcast packets to the IP host specified in the "ip helper-address" configuration command, use the "ip forward-protocol udp 200" command.

QUESTION 383

The Certkiller network is displayed in the following diagram:



In this network, host Certkiller 1 is configured for DHCP and must obtain its IP configuration from the DHCP server at 172.24.1.9. Which configuration of Router Certkiller A will allow Host Certkiller 1 to obtain its IP and DNS configuration while also utilizing the other servers?

- A. Certkiller A(config)#interface e0
Certkiller A(config)# ip helper-address 172.24.1.9
- B. Certkiller A(config)#interface e0
Certkiller A(config)# ip helper-address 172.24.1.255
- C. Certkiller A(config)#interface e0
Certkiller A(config)# ip forward-protocol udp
- D. Certkiller A(config)#interface e2
Certkiller A(config)# ip helper-address 172.24.1.255
- E. Certkiller A(config)#interface e2
Certkiller A(config)# ip helper-address 172.16.255.255
- F. Certkiller A(config)#interface e2

Certkiller A(config)# ip forward-protocol

Answer: A

Explanation:

Combined with the ip forward-protocol global configuration command, the "ip helper-address" command allows you to control which broadcast packets and which protocols are forwarded.

One common application that requires helper addresses is Dynamic Host Configuration Protocol (DHCP), which is defined in RFC 1531. DHCP protocol information is carried inside of BOOTP packets. To enable BOOTP broadcast forwarding for a set of clients, configure a helper address on the router interface closest to the client (interface e0 in this example). The helper address should specify the address of the DHCP server. If you have multiple servers, you can configure one helper address for each server. Because BOOTP packets are forwarded by default, DHCP information can now be forwarded by the router. The DHCP server now receives broadcasts from the DHCP clients.

QUESTION 384

You work as a network administrator at Certkiller .com. A Certkiller employee is complaining of intermittent connectivity to the primary file server. Upon investigation it is determined that other users are having the same problem. Further investigation determines that the users are able to access a backup file server located on the same segment as the primary file server.

Where should you begin the troubleshooting process?

- A. Check the physical layer at the end-user device.
- B. Check that the application is functioning correctly at the device of the end user.
- C. Check that a path to the route exists in the route table.
- D. Check that the application is installed and running correctly at the primary file server.
- E. Check the physical layer at the primary filer server.

Answer: E

QUESTION 385

You work as a network administrator at Certkiller .com. A user complains of being unable to access the Certkiller .com e-mail server but being able to do so in recent past. Other users on the same segment have not reported any problems. A ping from the end-user's device to the server returns a successful response.

At which layer is the problem most likely residing?

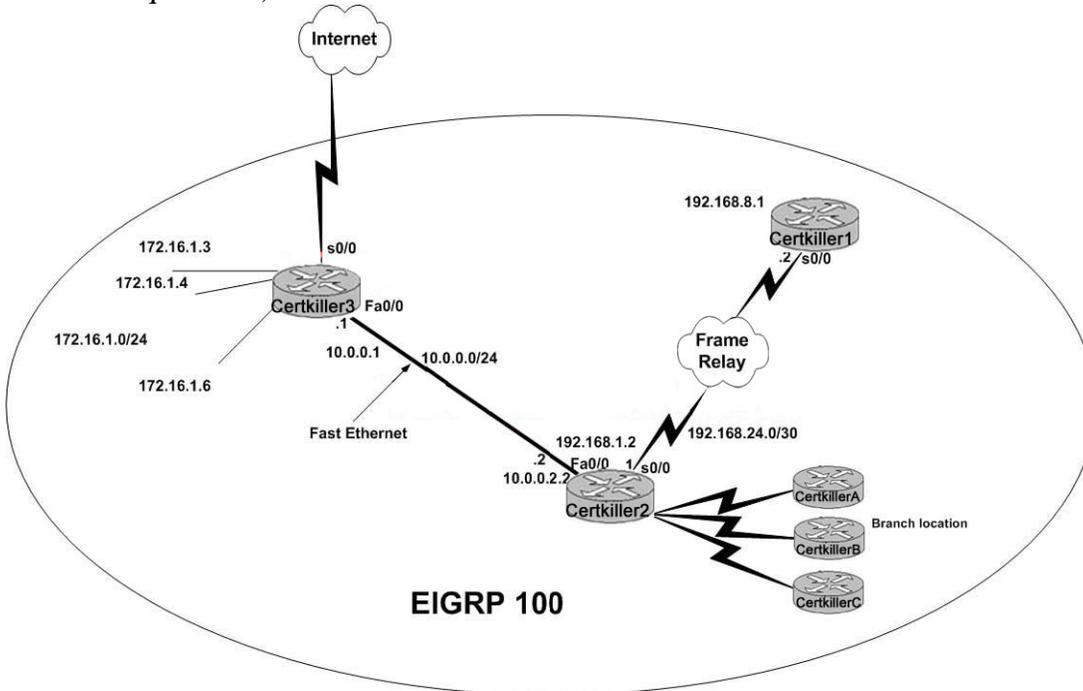
- A. It is a Layer 1 problem.
- B. It is a Layer 3 routing problem.
- C. It is an upper layer problem at the mail server side.
- D. It is an upper layer problem at the user side.

Answer: D

Case Study Certkiller .com, Scenario

Case Study:

The Certkiller network is displayed in the diagram below: (Use as a reference for the next three questions)



Scenario:

Please reference the topology shown above. This network topology and the Scenario described below will be used for the next three exam questions.

The network uses EIGRP as its routing protocol throughout the corporation.

Recently, administrators installed asynchronous modules on Certkiller 3 to allow regionally located mobile workers access for filing reports from the field.

Certkiller .com has encountered a dramatic increase in trouble reports regarding connectivity since adding the mobile access to their network.

Case Study Certkiller .com (4 Questions)

QUESTION 386

An excerpt from Certkiller 2's routing table indicates the following routes exist:

D 172.16.1.3/32 [90/146235264] via 10.0.0.1

D 172.16.1.4/32 [90/146235264] via 10.0.0.1

D 172.16.1.6/32 [90/146235264] via 10.0.0.1

Consider these route entries and the presented syslog messages from the other questions shown below. Which two solutions would stabilize the Certkiller 3 and Certkiller 2 routers and reduce the frequency of SIA routes? (Choose two)

- A. Enable EIGRP auto-summary on the Certkiller 2 router
- B. Summarize the PPP host routes for mobile workers into EIGRP at Certkiller 3

- C. Resolve the degraded Frame Relay WAN link between Certkiller 2 and Certkiller 1
- D. Use EIGRP manual summarization at Certkiller 2 for the networks advertised from the Branch locations
- E. Enable EIGRP auto-summary on the Certkiller 1 router

Answer: A, B

Explanation:

In order to best stabilize the routing tables in this example, the host routes used for remote access should be summarized on router Certkiller 3. This can be done either through the use of EIGRP's auto-summarization feature, or through manual summarization. This will advertise all of the host routes into one route, thereby reducing the total number of route entries in the other two Certkiller routers, as well as stabilizing the routing table. As long as any of the host routes are active, the summarized route will be advertised.

Note: Summarization should be configured as close to the source as possible. In this example, it should be accomplished on router Certkiller 3. However, you would want to summarize PPP host routes for mobile workers on Certkiller 2 and use EIGRP auto summarization on Certkiller 2.

QUESTION 387

Most branch locations are reporting reliable connectivity to the Certkiller 2 router. However, connectivity between the core routers is excessively erratic. The following is a partial view of several similar syslog messages on Certkiller 2:
%DUAL-5-NBRCHANGE:IP-EIGRP 100: Neighbor 10.0.0.1 (FastEthernet0/0) is down: peer restarted
%DUAL-5-NBRCHANGE:IP-EIGRP 100: Neighbor 192.168.24.2 (Serial 0/0) is down: retry limit exceeded

From the Scenario and syslog messages, which two statements describe why routing between the core routers is unstable? (Choose two)

- A. Certkiller 3 is clearing the EIGRP neighbor adjacency with Certkiller 2
- B. Hellos from Certkiller 2 to Certkiller 1 are failing
- C. A query reply to Certkiller 2 has not been received from Certkiller 1
- D. The branch location routers are replying to Certkiller 2 that the active routes are unreachable
- E. The SIA timer on Certkiller 1 has reached approximately 3 minutes

Answer: A, B

Explanation:

Neighbor discovery/recovery is the process that routers use to dynamically learn of other routers on their directly attached networks. Routers must also discover when their neighbors become unreachable or inoperative. Neighbor discovery/recovery is achieved with low overhead by periodically sending small hello packets. As long as hello packets

are received, the Cisco IOS software can determine that a neighbor is alive and functioning. Once this status is determined, the neighboring routers can exchange routing information.

The reliable transport protocol is responsible for guaranteed, ordered delivery of Enhanced IGRP packets to all neighbors. It supports intermixed transmission of multicast and unicast packets. Some Enhanced IGRP packets must be transmitted reliably and others need not be. For efficiency, reliability is provided only when necessary. For example, on a multiaccess network that has multicast capabilities (such as Ethernet) it is not necessary to send hellos reliably to all neighbors individually. Therefore, Enhanced IGRP sends a single multicast hello with an indication in the packet informing the receivers that the packet need not be acknowledged. Other types of packets (such as updates) require acknowledgment, and this is indicated in the packet. The reliable transport has a provision to send multicast packets quickly when there are unacknowledged packets pending. Doing so helps ensure that convergence time remains low in the presence of varying speed links.

Based on the information shown here, the neighbor adjacency state is failing, which could be caused by lost Hello packets to neighbor Certkiller 1 over the frame relay connection, or from router Certkiller 3 clearing the adjacency.

QUESTION 388

All sites are reporting inconsistent connectivity to resources and the Internet. A partial view of the syslog messages from the Certkiller 3 router displays the following.

```
%DUAL-5-NBRCHANGE:IP-EIGRP 100: Neighbor 10.0.0.2 (FastEthernet0/0) is down: stuck in active
```

```
%DUAL-3-SIA: Route 172.16.1.2/32 stuck-in-active state in IP-EIGRP 100. Cleaning up
```

```
%DUAL-5-NBRCHANGE:IP-EIGRP 100: Neighbor 10.0.0.2 (FastEthernet0/0) is down: stuck in active
```

```
%DUAL-3-SIA: Route 172.16.1.2/32 stuck-in-active state in IP-EIGRP 100. Cleaning up
```

Which two courses of action should be taken to identify the cause of the SIA errors?

(Choose two)

- A. Identify why the Certkiller 2 router is sending query requests to the Certkiller 3 router
- B. Determine what has caused the Certkiller 2 peer to enter the passive state
- C. Identify why the Certkiller 3 router did not receive a query reply from its peer
- D. Determine what has caused the Certkiller 3 router hold-timer for its peer to be exceeded
- E. Identify why the routes 172.16.1.x/32 went into an active state

Answer: C, D

Explanation:

When the SIA error message occurs, it indicates that the EIGRP routing protocol failed to converge for the specified route. Usually, this failure is caused by a flapping interface, a configuration change, or dialup clients (the route loss is normal). The routing to other

destinations is not affected while the EIGRP process is in active state for the specified route. When the SIA timer for the neighbor that did not reply expires, the neighbor is cleared (EIGRP does not trust the state of a neighbor that exceeds the timer). As a consequence, routes in the topology table beyond that neighbor are cleared and must then re-converge. This means that the forwarding table can be affected by an SIA, and that packets can be dropped while the network is converging.

Note: Since the EIGRP hold down timer is approximately 3 minutes, determining the source of the problem can be difficult.

Incorrect Answers:

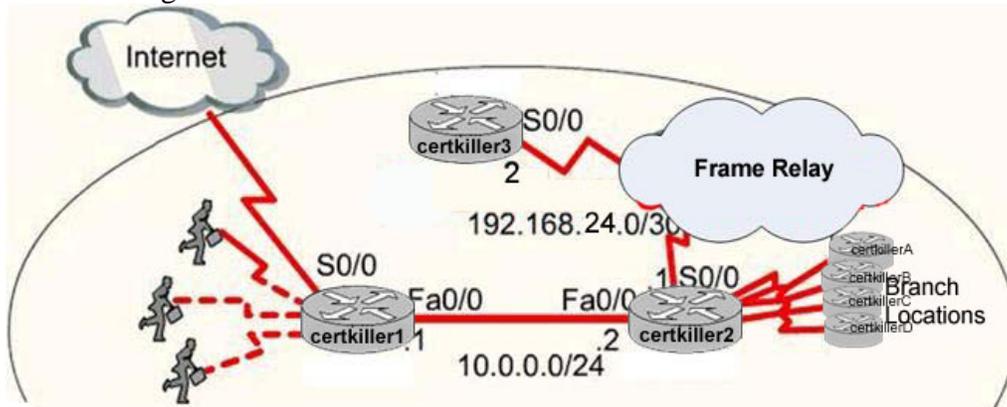
A: Sending queries to the neighbor is normal.

B: Routers go into passive and active states for individual routes, not for neighbor relationships. Routes can go into the passive state, but not neighbors. Besides, the passive state is the normal state of operation.

E: Since this route was used for dial-in access, this is normal. The end user most likely simply ended the dial-up session.

QUESTION 389

Connectivity with the Router Certkiller 3 has been experiencing problems for several weeks. A trouble ticket is still being worked through with the Frame Relay provider. However, the syslog files of Certkiller 3 have several more recent entries similar to the following:



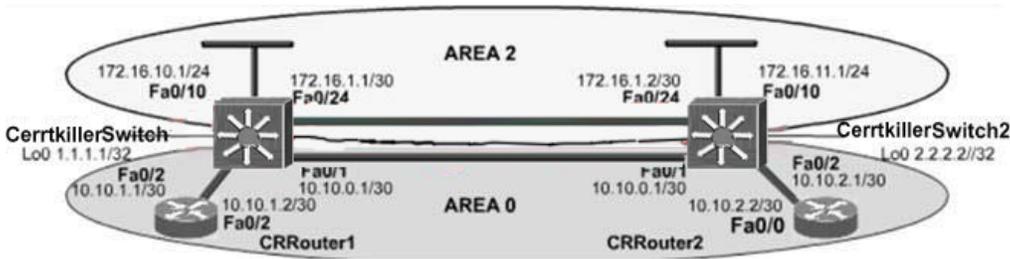
- A. The SIA timer on Certkiller 3 has reached approximately 3 minutes.
- B. Certkiller 2 is clearing the neighbor adjacency with Certkiller 3.
- C. A query reply has not been received by Certkiller 3 from Certkiller 2.
- D. Certkiller 3 has replied to the query from Certkiller 2 that the SIA networks are unreachable.
- E. Hellos from Certkiller 3 to Certkiller 2 are failing.

Answer: B

Case Study Certkiller , Scenario

Scenario

Exhibit, Network Topology



Certkiller is an Internet game provider. They provide their services at www.Certkiller.com. The game service network uses OSPF as its routing protocol. Recently, system administrators have experienced discrepancies in synchronizing their database servers at separate locations within OSPF area 0. Link failures have been observed in the network as several additions, moves, and changes have been applied during Certkiller's rapid growth. However, it is the intent that OSPF be able to converge around these failures.

Case Study Certkiller (4 Questions)

QUESTION 390

The syslog of Certkiller Switch1 reports the following:

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down

%OSPF-5-ADJCHG: Process 1; Nbr 2.2.2.2 on FastEthernet0/1 from FULL to DOWN,

Neighbor Down: Interface down or detached

This event was anticipated due to maintenance; however, it resulted in excessive lost routes. Which route should be the only one network removed from the multiple routers' routing table?

- A. 1.1.1.1/32
- B. 2.2.2.2/32
- C. 10.10.0.0/30
- D. 10.10.1.0/30
- E. 10.10.2.0/30

Answer: C

QUESTION 391

Certkiller Router1 has lost connectivity to Certkiller Router2. The current route table of Certkiller Router1 is as follows:

172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks

O IA 172.16.10.0/24 [110/11] via 10.10.1.1, 00:00:03, FastEthernet0/0

O IA 172.16.11.0/24 [110/11] via 10.10.1.1, 00:00:03, FastEthernet0/0

O IA 172.16.1.0/30 [110/11] via 10.10.1.1, 00:00:03, FastEthernet0/0

Which expected route is missing from CRRouter1's route table based on the topology during the maintenance period?

- A. O 10.10.0.0 [110/2] via 10.10.1.1, 00:00:09, FastEthernet0/0
- B. O IA 10.10.0.0 [110/2] via 10.10.1.1, 00:00:09, FastEthernet0/0
- C. O 10.10.2.0 [110/3] via 10.10.1.1, 00:00:09, FastEthernet0/0
- D. O IA 10.10.2.0 [110/3] via 10.10.1.1, 00:00:09, FastEthernet0/0
- E. O 1.1.1.1 [110/2] via 10.10.1.1, 00:00:09, FastEthernet0/0
- F. O 2.2.2.2 [110/3] via 10.10.1.1, 00:00:09, FastEthernet0/0

Answer: C

QUESTION 392

Examine this excerpt from the show ip ospf command on Certkiller Switch1

```
....  
Area BACKBONE(0)  
Number of interfaces in this area is 2  
Area has no authentication  
SPF algorithm last executed 00:00:31.280 ago  
SPF algorithm executed 5 times  
Area ranges are  
Number of LSA 13. Checksum Sum 0x16F0FD  
Number of opaque link LSA 0. Checksum Sum 0x000000  
Number of DCbitless LSA 0  
Number of indication LSA 0  
Number of DoNotAge LSA 0  
Flood list length 0  
Area 69  
Number of interfaces in this area is 2  
Area has message digest authentication  
SPF algorithm last executed 00:00:34.928 ago  
SPF algorithm executed 7 times
```

- A. Area 2 has been configured as a stub network
- B. Area 2 has been configured as a total stub network
- C. Area 0 and Area 2 have been configured with mismatched LSA numbers.
- D. Area 2 has been configured to use the same interfaces as Area 0.
- E. Area 0 is discontinuous.
- F. Area 2 is configured with authentication.

Answer: E

QUESTION 393

Which configuration command on Certkiller Switch1 (with a similar command on Certkiller Switch2) will provide an immediate solution to the missing route problem?

- A. no area 2 stub
- B. no area 2 stub no-summare

- C. no area 2 authentication message-digest
- D. area 2 virtual-link 2.2.2.2
- E. area 2 virtual-link 172.16.1.2
- F. network 172.16.0.0 0.0.255.255 area 2

Answer: D

Mixed Questions (65 Questions)

QUESTION 394

A network administrator notices that the CPU utilization on the router is at 58 percent. What should be the first step in troubleshooting this issue?

- A. Create an access list to allow only traffic that meets the business policy.
- B. Check the network baseline test for the router.
- C. Check the syslog server for any abnormal behavior.
- D. Check interface counter error statistics.
- E. Check the vendor website for any new virus definitions that may cause vulnerabilities to the router.

Answer: B

QUESTION 395

Which command is an effective tool an administrator can use to isolate a UDP problem?

- A. show ip access-lists
- B. debug ip traffic
- C. show protocols
- D. debug tftp

Answer: A

Explanation:

Access control lists (ACLs) are lists of instructions you apply to a router's interface. These lists tell the router what kinds of packets to accept and what kinds of packets to deny. Acceptance and denial can be based on certain specifications, such as

- source address
- destination address
- port number
- Type of protocol etc

So ACL can accept or deny the UDP protocol based services. There is a way of troubleshooting with UDP problem is by verifying the Access-List.

QUESTION 396

```
hostname CERTKILLER1
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
interface Serial11
 ip address 10.10.10.1 255.255.255.0
!
router bgp 400
 neighbor 1.1.1.1 remote-as 400
!
ip route 1.1.1.1 255.255.255.255 10.10.10.2

hostname CERTKILLER2
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface Serial10
 ip address 10.10.10.2 255.255.255.0
!
router bgp 400
 neighbor 2.2.2.2 remote-as 400
!
ip route 2.2.2.2 255.255.255.255 10.10.10.1
```

Refer to the exhibit. Certkiller 1 and Certkiller 2 have not been able to establish a successful BGP neighbor relationship. Which configuration set will create an established condition for this connection?

- A. Certkiller 1(config-router)# neighbor 1.1.1.1 update-source loopback 0
Certkiller 2(config-routers)# neighbor 2.2.2.2 update-source loopback 0
- B. Certkiller 1(config-router)# neighbor 1.1.1.1 ebgp-multihop
Certkiller 2(config-routers)# neighbor 2.2.2.2 ebgp-multihop
- C. Certkiller 1(config-router)# network 2.0.0.0
Certkiller 2(config-routers)# network 1.0.0.0
- D. Certkiller 1(config-router)# ip route 10.0.0.0 255.0.0.0 s1
Certkiller 2(config-routers)# ip route 10.0.0.0 255.0.0.0 s0

Answer: A

Explanation:

When two routers establish a TCP enabled BGP connection, they are called neighbors or peers. Each router running BGP is called a BGP speaker. Peer routers exchange multiple messages to open and confirm the connection parameters, such as the version of BGP to be used. If there are any disagreements between the peers, notification errors are sent and the connection fails.

When BGP neighbors first establish a connection, they exchange all candidate BGP routes. After this initial exchange, incremental updates are sent as network information changes. As discussed in earlier modules, incremental updates are more efficient than complete table updates. This is especially true with BGP routers, which may contain the complete Internet routing table.

For a BGP router to establish a neighbor relationship with another BGP router, issue the following configuration command:

Router(config-router)#neighbor ip-address remote-as AS-number

This command serves to identify a peer router with which the local router will establish a session. The ip-address argument is the IP address of the neighbor interface. The AS-number argument determines whether the neighbor router is an EBGP or an IBGP neighbor

In this example, the option specified is update-source loopback 0. If multiple pathways to the neighbor exist, then the router can use any IP interface to speak BGP with that neighbor. The update-source loopback 0 command is used to instruct

the router to use interface loopback zero (0) for TCP connections. This command is typically used in all IBGP configurations. Without this command, BGP routers can use only the closest IP interface to the peer. The capability to use any operational interface provides BGP with robustness in case the link to the closet interface fails. Because EBGP sessions are typically point-to-point, there is no need to use this command with EBGP.

QUESTION 397

What three types of actions can be configured for CAR when traffic exceeds the rate limit? (Choose three.)

- A. drop
- B. continue
- C. exceed
- D. set precedence and continue
- E. conform

Answer: A, B, D

QUESTION 398

A network is performing below the established baseline. A protocol analyzer reveals that the network is experiencing an excessive number of broadcasts as well as CRC and FCS errors. Which two statements are correct? (Choose two.)

- A. The problem is most likely at the physical layer.
- B. The problem is most likely at the data link layer.
- C. The problem is most likely at the network layer.
- D. The problem is most likely at the transport layer.
- E. A bottom-up troubleshooting approach should be applied.
- F. A top-down troubleshooting approach should be applied.

Answer: B, E

Explanation:

1. Frame errors
2. CRC errors
3. Interface and/or line protocol down

These symptoms show that error occurred in data link layer. So if you would like to troubleshoot, you need to start from the lower layer called bottom-up approach.

When applying a bottom-up approach towards troubleshooting a networking problem, the examination starts with the physical components of the network and then is worked up through the layers of the OSI model until the cause of the problem is identified. It is a good approach for a troubleshooter to use when the problem is suspected to be physical. Most networking problems reside at the lower levels, so implementing the bottom-up approach will often result in effective results. The downside to selecting this approach is that it requires checking of every device

and interface on the network until the possible cause of the problem is found. It is a requirement to document each conclusion and possibility. The challenge is to determine which devices to start with.

In many cases, problems within the first four layers can be determined by entering a ping or traceroute command. If the connection is successful, then the cause is likely at the application level. Otherwise, a closer look at the lower levels will be needed to locate the problem.

Verify that Internet control message protocol (ICMP) echo request and echo reply are enabled on the network in order for commands such as ping and traceroute to work. This action should include authorization from the network administrator and documentation of that authorization. If ping has been disabled on the network, it is a result of the implementation of policy. Document in a station log or your personal work log that ping, or any command that was initially disabled, was enabled for network testing and subsequently disabled. This is important should there be an unauthorized intrusion into the network while you are troubleshooting the network. If disabled, the failure of a ping or traceroute command can easily be mistaken for a loss of connectivity.

QUESTION 399

```
CertkillerC# show mls rp
multilayer switching is globally enabled
mls id is 00e0.fefc.6000
mls ip address 10.20.26.64
mls flow mask is ip-flow
vlan domain name: WBU
    current flow mask: ip-flow
    current sequence number: 80709115
    current/maximum retry count: 0/10
    current domain state: no-change
    current/next global purge: false/false
    current/next purge count: 0/0
    domain uptime: 13:03:19
    keepalive timer expires in 9 seconds
    retry timer not running
    change timer not running
    fcp subblock count = 7
    1 management interface(s) currently defined:
        vlan 1 on Vlan1
    7 mac-vlan(s) configured for multi-layer switching:
        mac 00e0.fcfc.6000
            vlan id(s)
            1    10  91  92  93  95  100
    router currently aware of following 1 switch(es):
        switch id 0010.1192.b5ff
```

CertkillerC#

Observe the exhibit. Which two statements are true concerning the show mls rp

output? (Choose two.)

- A. The default flow mask is being used.
- B. Because the current flow mask is ip-flow, an extended ACL was applied to the
- C. The router ID for the MLS switch is 10.20.26.64
- D. The command mls rp ip was used

Answer: B, D

Explanation:

Catalyst switches are the basis for Layer 3 switching in the Cisco environment.

Multilayer

Switching (MLS) performs IP data (also IPX and IP multicast) packet flows at a much higher

level of performance than traditional routing. This preserves the CPU of an upstream router

without compromising functionality.

Router(config)#mls rp ip

QUESTION 400

What are two possible reasons that CRC errors occur? (Choose two.)

- A. An authentication error occurred.
- B. A serial line is noisy.
- C. A serial cable is too long.
- D. The clockrate has not been set on the DTE.

Answer: B, C

Explanation:

The data-link layer uses standardized frame formats and physical addressing to establish communications within a broadcast domain. If devices disagree on the frame format communications will fail.

Problems with the frame format usually translate to encapsulation incompatibilities between nodes. Actual framing errors occur when a frame does not end on an 8-bit byte boundary for one of the following reasons:

1. Noisy serial line.
2. Improperly designed cable. This could be caused by serial cable that is too long, or the cable from the CSU or DSU to the router is not shielded.
3. The CSU line clock is incorrectly configured. For example, the clock on one of the CSUs may be configured for local clocking.
4. One's density problem on T1 link. This is caused by incorrect framing or a coding specification.

All of these problems result in a receiver having difficulty establishing where one frame ends and another frame starts. When the interface is capable of recognizing this condition, the show interfaces command will reveal an incrementing frame

error count.

These problems are critical as they will cause the communications protocol itself to fail or frames will be incorrectly addressed and fail to reach their destination.

At times the framing problems may be minor and the interface may not recognize that a framing error has occurred. However, a misread bit will result in the Layer 2 frame having an invalid Cyclic Redundancy Check or CRC. This error will also be seen as an incrementing error count with the show interfaces command. In this case the CRC error count will be incrementing.

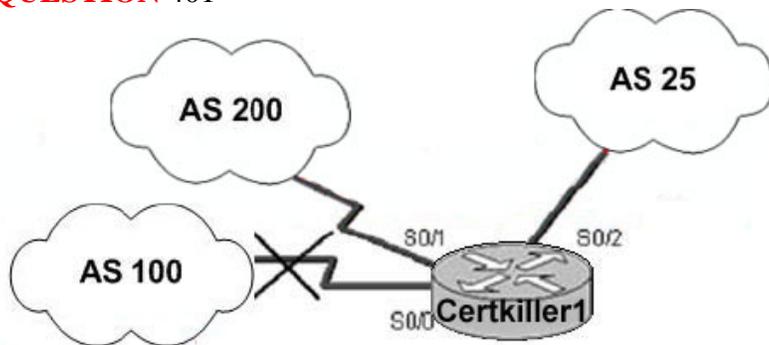
Depending on the severity of the framing problem, the interface may be able to interpret some of the frames. Too many invalid frames may prevent valid keepalives from being exchanged, causing the show interfaces command to report:

Interface is up, line protocol is down

In summary, the following are all symptoms of a framing or related clocking problem:

1. Frame errors
2. CRC errors
3. Interface and/or line protocol down

QUESTION 401



Users are experiencing loss of connectivity to a remote site. The administrator thinks the problem might be a TCP problem. Which Cisco IOS command will display the status of the TCP connection of a BGP peer?

- A. show interface s0/0
- B. show ip route bgp
- C. show ip bgp
- D. show ip bgp summary

Answer: D

Explanation:

If the router has not installed the BGP routes expected, use the show ip bgp command to verify that BGP has learned these routes.

Notice that the output of this command includes the BGP table version number, which increments each time the local router receives changed route information.

The AS_Path, among other key attributes, is also included in this table. Routes that are considered the best are denoted by the > character and are installed in the

router IP routing table.

An expected BGP route may not appear in the BGP table. If this happens, use the `show ip bgp neighbors` command to verify that the router has established a BGP connection with its neighbors. The most important information output of this command is the BGP state that exists between the neighbors. Anything other than "Established" indicates that the peers are not fully communicating.

Command	Description
<code>show ip bgp</code>	Displays entries in the BGP routing table. A network can be specified to get more detailed information about a particular prefix. Use the <code>subnets</code> keyword to get information about a particular prefix and all its subnets.
<code>show ip bgp summary</code>	Displays a summary of all BGP connections.
<code>show ip bgp neighbors</code>	Displays detailed information for each BGP connection.
<code>show ip bgp paths</code>	Displays all the BGP paths in the database.

QUESTION 402

Which Cisco IOS command displays the usability status of interfaces configured for IP?

- A. `show ip interface`
- B. `show ip protocols`
- C. `show ip traffic`
- D. `show interfaces`

Answer: A

Explanation:

`show ip interface` command displays the status of configured all IP Addresses.

QUESTION 403

CertkillerA# debug ppp negotiation

PPP protocol negotiation debugging is on

CertkillerA

```
*Mar 1 00:06:36.645: %LINK-3-UPDOWN: Interface BR10:1, changed state to up
*Mar 1 00:06:36.661: BR0:1 PPP: Treating corection as a callin
*Mar 1 00:06:36.665: BR0:1 PPP: Phase is ESTABLISHING, Passive Open [0 sess, 0 load]
*Mar 1 00:06:36.669: BR0:1 LCP: State is Listen
*Mar 1 00:06:37.034: BR0:1 LCP: I CONFREQ [Listen] id 7 len 17
*Mar 1 00:06:37.038: BR0:1 LCP: AuthProto PAP (0x0304C023)
*Mar 1 00:06:37.042: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
*Mar 1 00:06:37.046: BR0:1 LCP: Callback 0 (0x0D0300)
*Mar 1 00:06:37.054: BR0:1 LCP: O CONFREQ [Listen] id 4 len 15
*Mar 1 00:06:37.058: BR0:1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.062: BR0:1 LCP: MagicNumber 0x1081E7E1 (0x05061081E7E1)
*Mar 1 00:06:37.054: BR0:1 LCP: O CONFREQ [Listen] id 7 len 7
*Mar 1 00:06:37.058: BR0:1 LCP: Callback 0 (0x0D0300)
*Mar 1 00:06:37.062: BR0:1 LCP: I CONFACK [REQsent] id 4 len 15
*Mar 1 00:06:37.102: BR0:1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.106: BR0:1 LCP: MagicNumber 0x1081E7E1 (0x05061
*Mar 1 00:06:37.114: BR0:1 LCP: I CONFREQ [ACKrcvd] id 8 len 14
*Mar 1 00:06:37.117: BR0:1 LCP: AuthProto PAP (0x0304C023)
*Mar 1 00:06:37.121: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
```

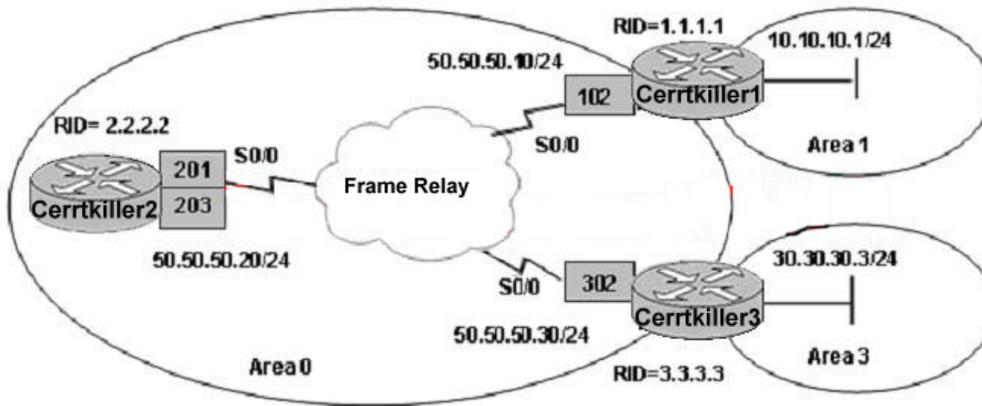
An administrator is troubleshooting a PPP connection between a local and remote router by entering the command debug ppp negotiation on the local router. Given the output, which statement is true?

- A. The remote router is configured as a callback server.
- B. The local router is configured as a callback server.
- C. The remote router is configured as a callback client.
- D. The local router accepted callback requests from the remote router.
- E. The remote router accepted a callback request from the local router.

Answer: C

Explanation: the line treating corection as a callin and callback 0 line of outout represents that the remote router is configured as a callback client.

QUESTION 404



```
Cerrtkiller2#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	1	FULL/DROTHER	00:00:36	50.50.50.30	Serial0/0
1.1.1.1	1	FULL/DR	00:00:32	50.50.50.10	Serial0/0

OSPF is configured over Frame Relay network as shown in the exhibit. All PVCs are active. However, Certkiller 1 and Certkiller 3 fail to see all OSPF routes in their routing tables. The show ip ospf neighbor command executed on Certkiller 2 shows the state of the neighbors. What should be done to fix the problem?

- A. The ip ospf network non-broadcast command should be configured on each Frame Relay interface.
- B. The ip ospf network broadcast command should be configured on each Frame Relay interface.
- C. The neighbor command should be configured under the OSPF routing.....
- D. The ip ospf priority value on the hub router should be set to 0.
- E. The ip ospf priority value on the spoke router should be set to 0.

Answer: E

Explanation: OSPF state can be :

OSPF States

The key to effectively designing and troubleshooting OSPF networks is to understand the relationships, or states, that develop between OSPF routers. OSPF interfaces can be in one of seven states. OSPF neighbor relationships progress through these states, one at a time.

1. Down State

In the Down state, the OSPF process has not exchanged information with any neighbor. OSPF is waiting to enter the next state, which is the Init state.

2. InitState

OSPF routers send Type 1 packets, or Hello packets, at regular intervals to establish a relationship with neighbor routers. These intervals are usually ten seconds. When an interface receives its first Hello packet, the router enters the Init state. This means the router knows a neighbor is out there and is waiting to take the relationship to the next step.

The two kinds of relationships are the two-way state and adjacency. A router must receive a Hello from a neighbor before it can establish any relationship.

3. Two-Way State

Using Hello packets, every OSPF router tries to establish a two-way state, or bidirectional communication, with every neighbor router on the same IP network. Among other things, Hello packets include a list of the sender's known OSPF neighbors. The two-way state is the most basic relationship that OSPF neighbors can have, but routing information is not shared between routers in this relationship. To learn about the link states of other routers and eventually build a routing table, every OSPF router must form at least one adjacency. An adjacency is an advanced relationship between OSPF routers that involves a series of progressive states that rely not just on Hellos, but also on the other four types of OSPF packets. Routers attempting to become adjacent to one another exchange routing information even before the adjacency is fully established. The first step toward full adjacency is the ExStart state, which is described next.

4. ExStartState

Technically, when a router and its neighbor enter the ExStart state, their conversation is characterized as an adjacency, but they have not become fully adjacent. ExStart is established using Type 2 database description (DBD) packets, also known as DDPs. The two neighbor routers use Hello packets to negotiate who is the "master" and who is the "slave" in their relationship and use DBD packets to exchange databases.

The router with the highest OSPF router ID "wins" and becomes the master. The OSPF router ID is discussed later in this module. When the neighbors establish their roles as master and slave, they enter the Exchange state and begin sending routing information.

5. ExchangeState

In the Exchange state, neighbor routers use Type 2 DBD packets to send each other their link-state information. In other words, the routers describe their link-state databases to each other. The routers compare what they learn with their existing link-state databases. If either of the routers receives information about a link that is not already in its database, the router requests a complete update from its neighbor. Complete routing information is exchanged in the Loading state.

6. LoadingState

After the databases have been described to each router, they may request information that is more complete by using Type 3 packets, link-state requests (LSRs). When a router receives an LSR, it responds with an update by using a Type 4 link-state update (LSU) packet. These Type 4 LSU packets contain the actual link-state advertisements (LSAs), which are the heart of link-state routing protocols. Type 4 LSUs are acknowledged using Type 5 packets, called link-state acknowledgments (LSAcks).

7. Full Adjacency

With the Loading state complete, the routers are fully adjacent. Each router keeps a list of adjacent neighbors, called the adjacency database. Do not confuse the adjacency database with the link-state database or the forwarding database. Setting the OSPF priority is 0 means never can be either DR/BDR.

QUESTION 405

Which troubleshooting stage identifies the characteristics of problems at each logical layer of the network in order to select the most likely cause?

- A. correct the problem
- B. gather symptoms
- C. define the problem
- D. isolate the problem

Answer: D

Explanation:

The stages of the general troubleshooting process are:

Step 1	Gather symptoms
Step 2	Isolate the problem
Step 3	Correct the problem

The stages are not mutually exclusive. At any point in the process, it may be necessary to retrace to previous steps. For instance, it may be required to gather more symptoms while isolating a problem. Additionally, when attempting to correct a problem, another unidentified problem could be created. As a result, it would be necessary to gather the symptoms, isolate, and correct the new problem.

A troubleshooting policy should be established for each stage. A policy will give a consistent manner in which to perform each stage. Part of the policy should include documenting every important piece of information.

Gathering Symptoms- To perform the "Gathering Symptoms" stage of the general troubleshooting process, the troubleshooter gathers and documents symptoms from the network, end systems, or users. In addition, the troubleshooter determines what network components have been affected and how the functionality of the network has changed compared to the baseline. Symptoms may appear in many different forms. These forms include alerts from the network management system, console messages, and user complaints.

While gathering symptoms, questions should be used as a method of localizing the problem to a smaller range of possibilities. However, the problem is not truly isolated until a single problem, or a set of related problems, is identified.

Isolation of Problem- To perform the "Isolate the Problem" stage of the general troubleshooting process, the troubleshooter identifies the characteristics of problems at the logical layers of the network so that the most likely cause can be selected. At this stage, the troubleshooter may gather and document more symptoms depending on the problem characteristics that are identified.

Correct the Problem- To perform the "Correct the Problem" stage, the troubleshooter corrects an identified problem by implementing, testing, and documenting a solution. If the troubleshooter determines that the corrective action has created another problem, the attempted solution is documented, the changes are removed, and the troubleshooter returns to gathering symptoms and isolating the problem.

QUESTION 406

Which commands are used in Windows 2000 to display information that is used in an end-system configuration table? (Choose four.)

- A. route print
- B. ifconfig -a
- C. arp /all
- D. arp -a
- E. ping [ip-address | hostname]
- F. telnet [ip-address | hostname]

Answer: A, D, E, F

Explanation: Answer A, D, E and F are correct

routeprint : command prints the routing table configured in windows.

Arp -a : prints the all ARP (Address Resolution Protocol) table

Ping:Test the Network Connectivity

telnet :Used to login in remote maching

QUESTION 407

```

Certkiller3# show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
       M - MSDP created entry, X - Proxy Join Timer Running
       A - Advertised via   DP
Timers: Uptime/Expire
Interface state: Interface, Next-Hop or VCD, State, Mode

(*, 224.0.1.40), 00:00:01/00:00:00, RP 0.0.0.0, flags: DJCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet0/1, Forward/Sparse-Dense, 00:00:01/00:00:00

(*, 224.1.1.1), 00:00:02/00:02:57, RP 0.0.0.0, flags: D
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet0/1, Forward/Sparse-Dense, 00:00:02/00:00:00
  
```

Observe the exhibit. Host 3.1.1.2 is not receiving the multicast traffic from server 1.1.1.1. On the basis of the exhibited show ip mroute command output, what could be the reason for this problem?

- A. There is no source listed for 224.1.1.1.
- B. There is an RPF issue

- C. The source interface is incorrect for 224.0.1.40.
- D. The PIM mode does not match between connected routers.

Answer: A

Explanation:

The concept of IP multicast is defined as sending IP packets to a group of hosts on the network.

One of the obvious benefits of this technology is the preservation of bandwidth by sending a single data stream to a group of clients instead of sending to all clients or having multiple streams at once. IP multicast is first described in RFC 1112, Host Extensions for IP Multicasting. A more current RFC, RFC 2236, describes IGMP, Version 2.

IP multicasting has the following characteristics:

Facilitates transmission of an IP datagram to a multicast group comprised of zero or more

hosts identified by a single IP destination address

Delivers a multicast datagram to all members of the multicast group with the same "best effort"

Reliability as regular unicast IP datagrams

Supports dynamic membership of a multicast group

Supports all multicast groups regardless of the location or number of members

Supports the membership of a single host in one or more multicast groups

Upholds multiple data streams at the application level for a single group address

Supports a single group address for multiple applications on a host

Another benefit of multicasting is that it is limited in network delay. This limitation is due to the one-to-many nature of multicasting, which limits the path. In contrast, unicasting transmits multiple copies of the same stream to potentially large

numbers of hosts. Multicasting carries with it the benefit of being anonymous. This anonymity is accomplished because any given server transmits to a single multicast group address, representing an entire group of recipients. The server never knows

the unicast network address of any given recipient. Multicast traffic is handled at the transport layer using the User Datagram Protocol (UDP). Unlike the

Transmission Control Protocol (TCP), UDP has no reliability functionality, which means no error correction or flow control. Because of the simplicity of UDP, data packet headers contain fewer bytes and consume less network overhead than TCP.

Well-Known Class D Address Purpose

224.0.0.1 All hosts on a subnet

224.0.0.2 All routers on a subnet

224.0.0.4 All Distance Vector Multicast Routing Protocol (DVMRP) routers

224.0.0.5 All Open Shortest Path First (OSPF) routers

224.0.0.6 All OSPF designated routers

224.0.0.9 All Routing Information Protocol, version 2 (RIP) routers
Leading the way in IT testing and certification tools, [www.Certkiller.com](http://www.certkiller.com)

2) routers

224.0.0.13 All Protocol Independent Multicast (PIM) routers

QUESTION 408

Which command displays the Frame Relay encapsulation type?

- A. show interfaces
- B. show frame-relay lmi
- C. show frame-relay pvc
- D. show frame-relay encapsulation

Answer: A

Explanation:

Frame Relay encapsulation must be specified when an interface is configured for Frame Relay. The two possible Frame Relay encapsulations are ietf and cisco. Cisco is the default encapsulation. The cisco method is proprietary and should not be used if the router is connected to another vendor's equipment across a Frame Relay network.

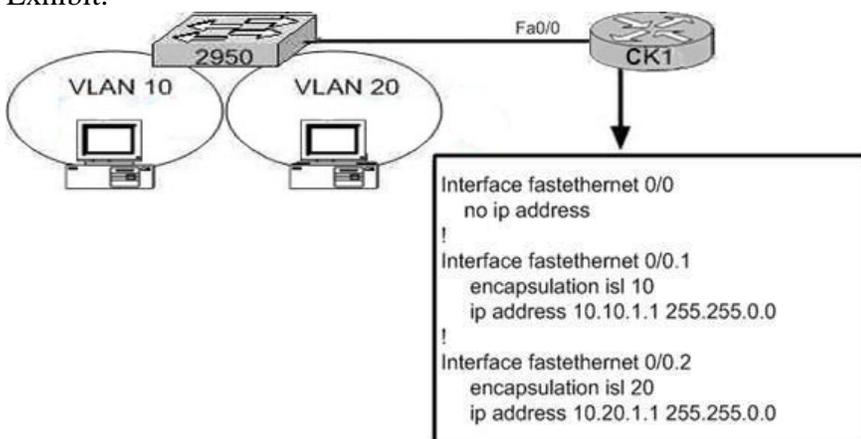
To configure basic Frame Relay using Inverse ARP and LMI autosensing, all that is needed is to configure the Layer 3 IP address on the interface and set the encapsulation to Frame Relay.

Router(config-if)#encapsulation frame-relay {cisco | ietf}

The show interfaces command displays information regarding the encapsulation and the status of Layer 1 and Layer 2. It also displays information about the multicast DLCI, the DLCIs used on the Frame Relay-configured serial interface, and the DLCI used for the LMI signaling.

QUESTION 409

Exhibit:



A network administrator is troubleshooting an interVLAN routing configuration between a 2950 Cisco switch and a Cisco router. Assuming that the switch is configured correctly and given the above graphic and configuration, what is the problem?

- A. The encapsulation type must be set to dot1q.
- B. The subinterface number must be equal to the ISL VLAN number.
- C. An IP address must be configured on the physical interface.
- D. The encapsulation must be configured on the physical interface

Answer: A

Explanation

When a router's interface is configured as a trunk link, frames received on that interface from the native VLAN on the switch enter the interface untagged. Frames from the other non-native VLANs enter the interface tagged as ISL or 802.1Q. Configuring the router's interface as a trunk link requires the use of subinterfaces. Each VLAN is configured on a separate subinterface. Each subinterface is configured to match the proper trunking protocol on the switch, ISL or 802.1Q. This is done with the router interface command:
encapsulation[dot1q | isl] vlan.
This problem occurred due to the mismatched of encapsulation type. So ISL is configured still problem is going on so need to configure the dot1q.

QUESTION 410

The system administrator has identified a problem, gathered the appropriate information, and isolated the problem. After implementing and testing the correction, it is noted that the problem is still occurring. What steps should the system administrator now perform to correct the problem?

- A. Remove the correction and gather more information.
- B. Document the attempt and remove the correction.
- C. Gather more information and correct the correction and document it.
- D. Document the attempt, remove the correction, resume gathering information.

Answer: D

Explanation

The stages of the general troubleshooting process are:

Step 1	Gather symptoms
Step 2	Isolate the problem
Step 3	Correct the problem

The stages are not mutually exclusive. At any point in the process, it may be necessary to retrace to previous steps. For instance, it may be required to gather more symptoms while isolating a problem. Additionally, when attempting to correct a problem, another unidentified problem could be created. As a result, it would be necessary to gather the symptoms, isolate, and correct the new problem.

A troubleshooting policy should be established for each stage. A policy will give a consistent manner in which to perform each stage. Part of the policy should include documenting every important piece of information.

Gathering Symptoms- To perform the "Gathering Symptoms" stage of the general troubleshooting process, the troubleshooter gathers and documents symptoms from

the network, end systems, or users. In addition, the troubleshooter determines what network components have been affected and how the functionality of the network has changed compared to the baseline. Symptoms may appear in many different forms. These forms include alerts from the network management system, console messages, and user complaints.

While gathering symptoms, questions should be used as a method of localizing the problem to a smaller range of possibilities. However, the problem is not truly isolated until a single problem, or a set of related problems, is identified.

Isolation of Problem- To perform the "Isolate the Problem" stage of the general troubleshooting process, the troubleshooter identifies the characteristics of problems at the logical layers of the network so that the most likely cause can be selected. At this stage, the troubleshooter may gather and document more symptoms depending on the problem characteristics that are identified.

Correct the Problem- To perform the "Correct the Problem" stage, the troubleshooter corrects an identified problem by implementing, testing, and documenting a solution. If the troubleshooter determines that the corrective action has created another problem, the attempted solution is documented, the changes are removed, and the troubleshooter returns to gathering symptoms and isolating the problem.

QUESTION 411

A network administrator has identified two IP routers that have connectivity but are not exchanging routing information. The administrator issues the show cdp neighbors command and is able to see the directly connected router in question. Which troubleshooting approach would be the most efficient to use?

- A. bottom-up
- B. divide and conquer
- C. top-down
- D. determine the scope
- E. gather the symptoms

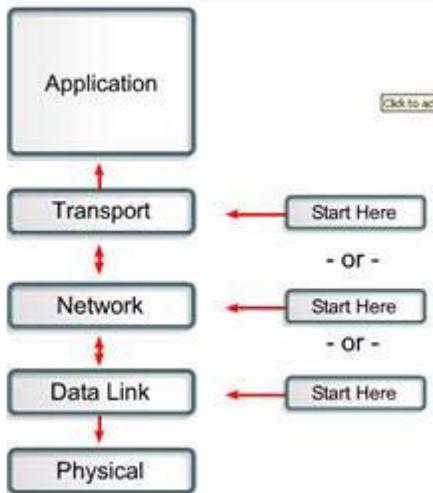
Answer: B

Explanation:

When the divide and conquer approach is applied towards troubleshooting a networking problem, a layer is selected and tested in both directions from the starting layer. The divide and conquer approach is initiated at a particular layer. The layer is based on troubleshooter experience level and the symptoms gathered about the problem. Once the direction of the problem is identified, troubleshooting follows that direction until the cause of the problem is identified.

If it can be verified that a layer is functioning, it is typically a safe assumption that the layers below it are functioning as well. If a layer is not functioning properly, gather symptoms of the problem at that layer and work downward to lower layers.

Divide and Conquer Troubleshooting Approach



QUESTION 412

The Cisco IOS software logging options enable message logging to various destinations. What is default setting?

- A. logging to the buffer
- B. logging to the console
- C. logging monitor to terminal monitor
- D. logging IP address to a syslog server
- E. logging off except for normal but significant condition messages

Answer: B

Explanation: Log message can redirect to different location ie. Log server, console etc but the default settings is console.

QUESTION 413

During a redistribution of routes from OSPF into EIGRP, an administrator notices that none of the OSPF routes are showing in EIGRP. What are two possible causes? (Choose two.)

- A. incorrect distribute lists have been configured
- B. CEF not enabled
- C. No default metric configured for EIGRP
- D. Missing ip classless command

Answer: A, C

Explanation

Use the distribute-list command to pick and choose which routing updates a router will send or receive. By referencing an access list, the distribute-list creates a route filter. This is a set of rules that precisely controls what routes a router will send or

receive in a routing update. This command is available for all IP routing protocols and can be applied to either inbound or outbound routing updates. When applied to inbound updates, the syntax for configuring a route filter is as follows:

```
Router(config-router)#distribute-list access-list-number in [interface-name]
```

To support multiple routing protocols within the same internetwork efficiently, routing information must be shared among the different routing protocols. For example, routes learned from a RIP process may need to be imported into an IGRP process. This process of exchanging routing information between routing protocols is called route redistribution. Such redistribution can be one-way or two-way.

One-way routes are where one protocol receives the routes from another. Two-way routes are where both protocols receive routes from each other. Routers that perform redistribution are called boundary routers because they border two or more autonomous systems or routing domains. This section examines route redistribution in detail, including the use of administrative distance, guidelines for redistribution implementation, and issues with redistribution configuration.

Syntax of Redistribute

```
Router(config-router)#redistribute protocol [process-id] {level-1 | level-1-2 | level-2} [metric metric-value][metric-type type-value] [match {internal | external 1 | external 2}][tag tag-value] [route-map map-tag][weight weight] [subnets]
```

The redistribute rip command enables route redistribution. RIP routes learned by RTB will be imported into the EIGRP process. The metric argument sets up the values used by EIGRP to translate the metric from the hop count on RIP to the composite metric on EIGRP. When used with IGRP/EIGRP, the metric keyword sets the bandwidth value, the delay, the reliability, the load, and the maximum transmission unit (MTU). The bandwidth value is in Kbps, the delay is in tenths of microseconds, while the reliability and the load are out of 255.

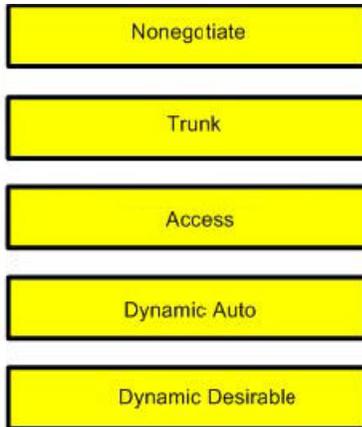
QUESTION 414

DRAG DROP

Place the DTP mode with its correct description

Select here	Place here
<div style="border: 1px solid black; background-color: yellow; padding: 5px; text-align: center;">Trunk</div>	<div style="border: 1px solid black; background-color: cyan; padding: 5px;">specifies that DTP packets are not sent out this interface</div>
<div style="border: 1px solid black; background-color: yellow; padding: 5px; text-align: center;">Nonegotiate</div>	<div style="border: 1px solid black; background-color: cyan; padding: 5px;">Sets the switch port to trunk mode and negotiates to become a trunk</div>
<div style="border: 1px solid black; background-color: yellow; padding: 5px; text-align: center;">Access</div>	<div style="border: 1px solid black; background-color: cyan; padding: 5px;">Sets a switch to permanent nontrunking mode</div>
<div style="border: 1px solid black; background-color: yellow; padding: 5px; text-align: center;">Dynamic Auto</div>	<div style="border: 1px solid black; background-color: cyan; padding: 5px;">Sets the switch port to respond, but not actively send DTP frames</div>
<div style="border: 1px solid black; background-color: yellow; padding: 5px; text-align: center;">Dynamic Desirable</div>	<div style="border: 1px solid black; background-color: cyan; padding: 5px;">Makes the interface actively attempt to convert the link into a trunk link</div>

Answer:



Explanation:

Explanation:

- when you set nonegotiate it specifies that DTP packets are not sent out this interface
- When you set the trunk mode of an interface, interface can carry the information of more than one VLAN.
- When you set the access mode of an interface, it can carry the information of only one VLAN. In Cisco Switch it is the default.
- Dynamic Auto : When you set the Dynamic Auto on an interface, it will responds to neighbour but not actively sends DTP frames
- Dynamic Desirable : When you set the Dynamic Desirable it actively attempts to convert the link into a trunk.

QUESTION 415

What are three common causes for the Spanning Tree Protocol (STP) to fail?
(Choose three.)

- A. a trunk port configured with PortFast
- B. a change in the hello timer to two seconds and the maxage timer to 20 seconds
- C. unidirectional links
- D. a change in the diameter of the STP domain to seven
- E. a duplex mismatch
- F. a speed mismatch

Answer: A, C, E

Explanation:

Spanning-Tree Protocol (STP) is a Layer 2 protocol that utilizes a special-purpose algorithm to discover physical loops in a network and effect a logical loop-free topology. STP creates a loop-free tree structure consisting of leaves and branches that span the entire Layer 2 network. The actual mechanics of how bridges communicate and how the STP algorithm works will be discussed at length in the following topics. Note that the terms bridge and switch are used interchangeably when discussing STP. In addition, unless otherwise indicated, connections between switches are assumed to be trunks.

Spanning tree PortFast is a Catalyst feature that causes a switch or trunk port to enter the spanning tree Forwarding state immediately, bypassing the Listening and Learning states. IOS-based switches only use PortFast on access ports connected to end stations.

So correct Answers are A, C , E

QUESTION 416

Users are complaining of poor network performance. Which three symptoms would typically be associated with a physical layer problem? (Choose three.)

- A. Excessive CRC errors are reported.
- B. Framing, line coding, or synchronization errors are reported.
- C. Address resolution errors occur.
- D. Collisions are excessive.
- E. Port LEDs are off, red, or displaying an alarm state.

Answer: B, D, E

Explanation:

Although these are very different problems that can be caused by Layer 2 or Layer 1 faults or design issues, they share some similar symptom:

1. Network delays.
2. Lack of throughput.
3. Poor network application performance.

It is important to remember that the loss of some frames can be tolerated by many applications, since TCP will retransmit the lost segment. For delay sensitive traffic such as voice, video, or SNA of IBM, suboptimal levels of performance can actually bring the application to a halt.

An example of a problem which would cause frames to take an illogical path through the network would be a poorly designed Layer 2 spanning-tree topology. In this case, the network might experience high bandwidth utilization on links that should not have that level of traffic. Problems that cause frames to actually be dropped can be identified through error counter statistics and console error messages that appear on the switch or router. In an Ethernet environment, an extended or continuous ping will also reveal if any frames are being dropped. There are Layer 2 protocols, such as X.25, that have their own retransmission mechanisms which will ensure that dropped frames are retransmitted. In this case, it can be difficult to determine if frames are being dropped. Variations in round trip times for ping replies can indicate a problem, but to be certain that frames are being lost or corrupted, an examination of the error counters on the interface would be required.

QUESTION 417

On a Cisco 3600 series router, a network administrator attempts to connect to the router via the console port and receives no response. To avoid a similar issue in the future, the network administrator configures the router with the command

scheduler interval 750. What does this command accomplish?

- A. limits all processes to 750 milliseconds of processor time in any given inception of the process.
- B. Allows low priority processes to be scheduled every 750 milliseconds so the console exec process can operate even is CPU usage is 100%
- C. Gives high priority processes 75% of the processor time and low priority processes 25% of the processor time.
- D. Causes the console exec process to interrupt the CPU every 750 milliseconds to allow input

Answer: B

Explanation: shcdules interval 750 specify that to allow low priority processes to be scheduled every 750 milliseconds so the console exec process can operate even is CPU usages is 100%.

QUESTION 418

All nodes on a particular network segment are periodically exhibiting poor performance. Host network applications are working, but slowly at times. What should an administrator do when troubleshooting the source of the problem?

- A. Check any access lists on the router that may be blocking traffic.
- B. Check the number of broadcasts on the network segment.
- C. Check the routing tables for proper entries.
- D. Check the network cable from the host to the switch.

Answer: C

Explanation: According to question, it symptoms is due to the incorrect routing table so you need to check the routing table.

QUESTION 419

A ping command fails on a new Frame Relay connection from a local router to a remote router. What are two possible causes for this scenario? (Choose two.)

- A. An encapsulation mismatch has occurred
- B. No broadcast keyword is found in frame-relay map statements.
- C. There is no neighbor command specified.
- D. No DR is configured for OSPF.

Answer: A, B

Explanation:

Frame Relay encapsulation must be specified when an interface is configured for Frame Relay. The two possible Frame Relay encapsulations are ietf and cisco. Cisco

is the default encapsulation. The cisco method is proprietary and should not be used if the router is connected to another vendor's equipment across a Frame Relay network.

```
Router(config-if)#encapsulation frame-relay {cisco | ietf}
```

When using dynamic address mapping, Inverse ARP requests a next-hop protocol address for each active PVC. Once the requesting router receives an Inverse ARP response, it updates its DLCI-to-Layer 3 address mapping table. Dynamic address mapping is enabled by default for all protocols enabled on a physical interface. If the Frame Relay environment supports LMI autosensing and Inverse ARP, dynamic address mapping takes place automatically. Therefore, no static address mapping is required.

If the environment does not support LMI autosensing and Inverse ARP, a Frame Relay map must be manually configured. Use the frame-relay map command to configure static address mapping. Once a static map for a given DLCI is configured, Inverse ARP is disabled on that DLCI.

To configure a frame-relay static map use the following syntax.

```
Router(config-if)#frame-relay map protocol protocol-address dlci [broadcast] [ietf | cisco]
```

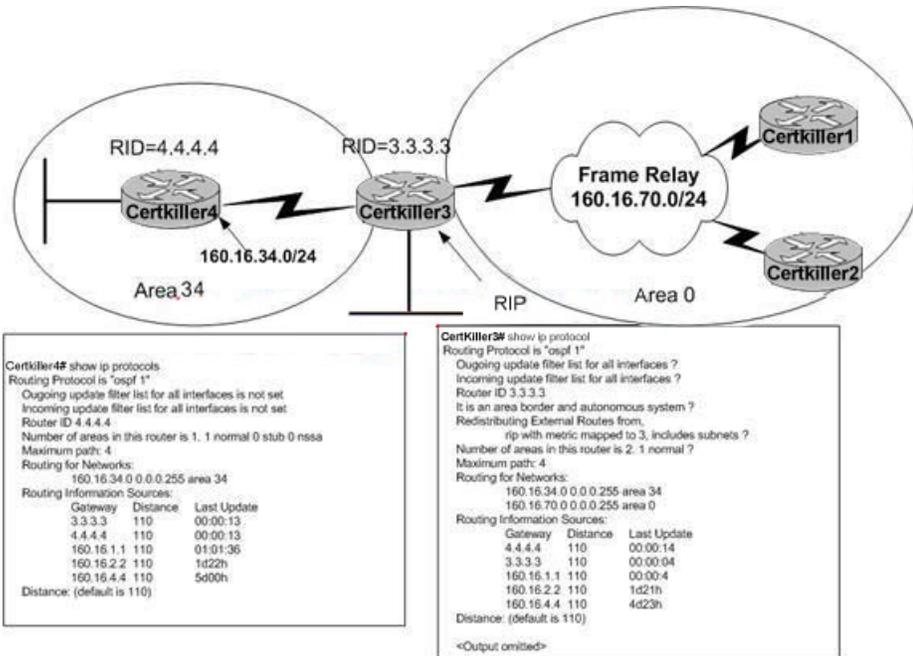
The Central site router is configured with a static map to the branch router. The broadcast keyword is commonly used with the frame-relay map command. The broadcast keyword provides two functions. First, it forwards broadcasts when multicasting is not enabled and secondly, it simplifies the configuration of OSPF for nonbroadcast networks that use Frame Relay.

The broadcast keyword might also be required for routing protocols such as AppleTalk that depend on regular routing table updates. This is especially true when the router at the remote end is waiting for a routing update packet to arrive before adding the route.

Using the broadcast keyword in frame relay configuration can assist OSPF in locating neighbors. OSPF can be configured to treat a nonbroadcast, multi-access network such as Frame Relay in much the same way as it treats a broadcast network. This is done by requiring a designated router. In previous releases, selection of a designated router required manual assignment in the OSPF configuration using the neighbor interface router command. When the frame-relay map command used with the broadcast keyword and the ip ospf network command used with the broadcast keyword are configured, there is no need to configure any neighbors manually. OSPF now automatically uses the Frame Relay network as a broadcast network.

QUESTION 420

Exhibit:



OSPF is configured on all routers. All routers can ping their directly connected neighbors but none of the routers in Area 0 can see the routes coming from Area 34. What could the problem be?

- A. Both Certkiller 3 and Certkiller 4 must be an ABR in order to become neighbors.
- B. Both Certkiller 3 and Certkiller 4 must be an ASBR in order to become neighbors.
- C. Because the area parameters do not match, Certkiller 3 and Certkiller 4 cannot become neighbors.
- D. Because of the redistribution configured on Certkiller 3, Certkiller 3 and Certkiller 4 cannot become neighbors.

Answer: D

Explanation:

Although the redistribution command is available for all IP routing protocols, it behaves differently depending on the actual IP routing protocols involved. However, the underlying principles are the same. Therefore, the examples in this section can be used as a starting point for any redistribution scheme.

Syntax of Redistribute is

```
Router(config-router)#redistribute protocol [process-id] {level-1 | level-1-2 | level-2}
[metric metric-value][metric-type type-value] [match {internal | external 1 | external
2}][tag tag-value] [route-map map-tag][weight weight] [subnets]
```

The redistribute rip command enables route redistribution. RIP routes learned by RTB will be imported into the EIGRP process. The metric argument sets up the values used by EIGRP to translate the metric from the hop count on RIP to the composite metric on EIGRP. When used with IGRP/EIGRP, the metric keyword sets the bandwidth value, the delay, the reliability, the load, and the maximum transmission unit (MTU). The bandwidth value is in Kbps, the delay is in tenths of

microseconds, while the reliability and the load are out of 255.
The configuration is incorrect so unable to establish the neighbor relationship

QUESTION 421

Exhibit:

```
Router#show run
!
no ip routing
mls rp ip
!
interface Vlan1
 ip address 172.20.26.56 255.255.255.0
 mls rp vtp-domain Engineering
 mls rp ip

interface Vlan 2
 ip address 128.6.2.73 255.255.255.0
 mls rp vtp-domain Marketing
!
interface Vlan3
 ip address 128.6.3.73 255.255.255.0
 mls rp vtp-domain Engineering
```

Refer to the exhibit. PCs in VLAN2 are not able to communicate with PCs in VLAN3. What could be the cause?

- A. IP routing is not enabled.
- B. VTP is not configured correctly on the interfaces.
- C. The command `mls rp management-interface` is missing.
- D. The command `mls rp ip` must be disabled to enable the routing.

Answer: A

Explanation: IP routing enable the IP routing, To perform the Inter-VLAN communication between VLAN using the Layer 3 switch you need to enable the IP routing.

QUESTION 422

Users are complaining of poor network performance. Which two symptoms would typically be associated with a network layer problem? (Choose two.)

- A. Packets are delivered to incorrect destinations.
- B. Broadcasts are excessive.
- C. CRC errors are excessive.
- D. Pings succeed only part of the time.
- E. Framing, line coding, or synchronization errors are reported.
- F. Address resolution errors occur.

Answer: A, D

Explanation:

If routes are not installed in the routing table, the router will not forward the packets to the destinations that are missing. It is possible that the packets could be incorrectly forwarded using a supernet or default route. This scenario was previously discussed in the section, Using Discard Routes.

Missing routes in the routing table create reachability problems. Users start complaining that they cannot reach a server or a printer. When this problem is investigated, one of the first things to look for is if the appropriate routers have a route for this destination in their routing tables.

Three possibilities exist for routes not being installed in the routing table:

1. Receiver problem - The router is receiving the updates, but it is not installing the routes.
2. Intermediate media problem, Layer 2 - The sender has sent the updates, but they were lost along the way and the receiver did not receive them.
3. Sender problem - The sender is not advertising the routes, so the receiving side is not seeing the routes in the routing table.

Some of the common causes for routes not being installed in the routing table are:

1. Missing or incorrect network or neighbor statement
2. Layer 1/2 down
3. Distribute-list in/out blocking (sender/receiver)
4. Access list blocking
5. Advertised Network Interface is down
6. Passive interface

QUESTION 423

Which elements would normally be illustrated in the topological diagram of a network? (Choose three.)

- A. interface names
- B. operating system versions of network devices
- C. device addresses
- D. network manager contact information
- E. standardized graphical symbols for each network device
- F. network management software type

Answer: A, C, E

Explanation:

When designing the topological diagram, it includes the interface name, device name and graphical symbol of network device are included.

QUESTION 424

Which three procedures should be used to effectively select a troubleshooting approach? (Choose three.)

- A. Determine ownership.

- B. Analyze the symptoms.
- C. Apply past experience.
- D. Determine the scope of the problem.
- E. List all applications being utilized.
- F. Determine the length of time the problem has persisted.

Answer: B, C, D

Explanation:

The stages of the general troubleshooting process are:

Step 1	Gather symptoms
Step 2	Isolate the problem
Step 3	Correct the problem

The stages are not mutually exclusive. At any point in the process, it may be necessary to retrace to previous steps. For instance, it may be required to gather more symptoms while isolating a problem. Additionally, when attempting to correct a problem, another unidentified problem could be created. As a result, it would be necessary to gather the symptoms, isolate, and correct the new problem.

A troubleshooting policy should be established for each stage. A policy will give a consistent manner in which to perform each stage. Part of the policy should include documenting every important piece of information.

Gathering Symptoms

- To perform the "Gathering Symptoms" stage of the general troubleshooting process, the troubleshooter gathers and documents symptoms from the network, end systems, or users. In addition, the troubleshooter determines what network components have been affected and how the functionality of the network has changed compared to the baseline. Symptoms may appear in many different forms. These forms include alerts from the network management system, console messages, and user complaints.

While gathering symptoms, questions should be used as a method of localizing the problem to a smaller range of possibilities. However, the problem is not truly isolated until a single problem, or a set of related problems, is identified.

Isolation of Problem - To perform the "Isolate the Problem" stage of the general troubleshooting process, the troubleshooter identifies the characteristics of problems at the logical layers of the network so that the most likely cause can be selected. At this stage, the troubleshooter may gather and document more symptoms depending on the problem characteristics that are identified.

Correct the Problem - To perform the "Correct the Problem" stage, the troubleshooter corrects an identified problem by implementing, testing, and documenting a solution. If the troubleshooter determines that the corrective action has created another problem, the attempted solution is documented, the changes are removed, and the troubleshooter returns to gathering symptoms and isolating the problem.

QUESTION 425

What is true of the stages in the general troubleshooting process?

- A. Each stage should be done in linear order.
- B. Efficient troubleshooting could begin with any of the stages.
- C. At any point in the process, the next step may be a previous stage.
- D. If the problem is not corrected using the general troubleshooting process, a different troubleshooting process must be used.

Answer: C

Explanation:

The stages of the general troubleshooting process are:

Step 1	Gather symptoms
Step 2	Isolate the problem
Step 3	Correct the problem

The stages are not mutually exclusive. At any point in the process, it may be necessary to retrace to previous steps. For instance, it may be required to gather more symptoms while isolating a problem. Additionally, when attempting to correct a problem, another unidentified problem could be created. As a result, it would be necessary to gather the symptoms, isolate, and correct the new problem.

A troubleshooting policy should be established for each stage. A policy will give a consistent manner in which to perform each stage. Part of the policy should include documenting every important piece of information.

Gathering Symptoms- To perform the "Gathering Symptoms" stage of the general troubleshooting process, the troubleshooter gathers and documents symptoms from the network, end systems, or users. In addition, the troubleshooter determines what network components have been affected and how the functionality of the network has changed compared to the baseline. Symptoms may appear in many different forms. These forms include alerts from the network management system, console messages, and user complaints.

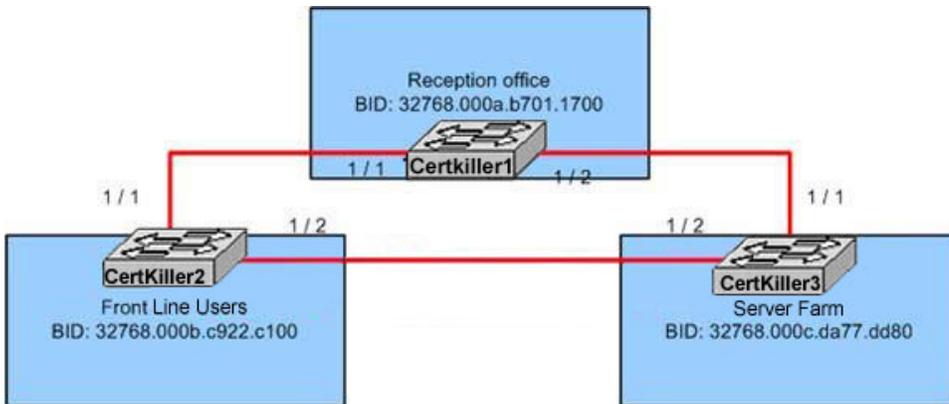
While gathering symptoms, questions should be used as a method of localizing the problem to a smaller range of possibilities. However, the problem is not truly isolated until a single problem, or a set of related problems, is identified.

Isolation of Problem- To perform the "Isolate the Problem" stage of the general troubleshooting process, the troubleshooter identifies the characteristics of problems at the logical layers of the network so that the most likely cause can be selected. At this stage, the troubleshooter may gather and document more symptoms depending on the problem characteristics that are identified.

Correct the Problem- To perform the "Correct the Problem" stage, the troubleshooter corrects an identified problem by implementing, testing, and documenting a solution. If the troubleshooter determines that the corrective action has created another problem, the attempted solution is documented, the changes are removed, and the troubleshooter returns to gathering symptoms and isolating the problem.

QUESTION 426

Exhibit:



Refer to the exhibit. All network links are FastEthernet. Although there is complete connectivity throughout the network, Front Line users have been complaining that they experience slower network performance when accessing the server farm than the Reception office experiences. Based on the exhibit, which two statements are true? (Choose two.)

- A. Changing the bridge priority of Certkiller 1 to 4096 would improve the network performance.
- B. Changing the bridge priority of Certkiller 1 to 36864 would improve the network performance.
- C. Changing the bridge priority of Certkiller 2 to 36864 would improve the network performance.
- D. Changing the bridge priority of Certkiller 3 to 4096 would improve the network performance.
- E. Disabling the Spanning Tree Protocol would improve network performance.
- F. Upgrading the link between Certkiller 2 and Certkiller 3 to Gigabit Ethernet would improve performance.

Answer: D, F

D, F seems to be the correct answers

D : with a lower id , Certkiller 3 will be the root STP

Normally all switches have a default priority value of 32768. The root STP will be the switch having the lower MAC address. In your case , office is the root STP because the lowest MAC.

To change the root STP, a switch muss have a lower that the default value. The lowest value is 4096.

F : supposing the devices have Giga port, so a bigger BW will automatically increase also the performance

The STP looks first the BPDU containing the MAC and the port ID. At the boot all switches have by default the same port id (32768), To change the elected root switch, we can modify the value of this port id.

Election of the Root Switch

All switches in the Layer2 network participating in spanning tree gather information about other switches in the network through an exchange of data messages called Bridge Protocol Data Units (BPDUs). This exchange of messages results in the following actions:

1. The election of a unique root switch for each instance of spanning tree
2. The election of a designated switch for every switched LAN segment
3. The removal of loops in the switched network by blocking switch ports connected to redundant links

The switch with the highest bridge priority (the lowest numerical priority value) is elected as the root switch. If all switches are configured with the default priority (32768), the switch with the lowest MAC address in the Layer2 network becomes the root switch. The spanning-tree root switch is the logical center of the spanning-tree topology in a switched network. All paths that are not needed to reach the root switch from anywhere in the switched network are placed in STP blocking mode.

BPDU contains information about the transmitting switch and its ports, including switch and port MAC addresses, switch priority, port priority, and port cost. The STP uses this information to elect the root switch and root port for the switched network, as well as the root port and designated port for each switched segment.

Bridge Protocol Data Units

The stable active spanning-tree topology of a switched network is determined by the following:

1. The unique bridge ID (MAC address) associated with each switch
2. The path cost to the root associated with each switch port
3. The port identifier (MAC address) associated with each switch port

The switch sends configuration BPDUs to communicate and compute the spanning-tree topology. Each configuration BPDU contains the following minimal information:

1. The unique bridge ID of the switch that the transmitting switch believes to be the root switch
2. The cost of the path to the root from the transmitting port
3. The identifier of the transmitting port

When a switch transmits a BPDU frame, all switches connected to the LAN on which the frame is transmitted receive the BPDU. When a switch receives a BPDU, it does not forward the frame but instead uses the information in the frame to calculate a BPDU, and, if the topology changes, initiate a BPDU transmission.

A BPDU exchange results in the following:

1. One switch is elected as the root switch.
2. The shortest distance to the root switch is calculated for each switch.
3. A designated switch is selected. This is the switch closest to the root switch through which frames will be forwarded to the root.
4. A root port for each switch is selected. This is the port providing the best path from the switch to the root switch.
5. Ports included in the spanning tree are selected.

QUESTION 427

A group of routers running EIGRP are missing routes. Which three troubleshooting questions should you be asking? (Choose three.)

- A. Is autosummarization disabled if you are using discontinuous networks?
- B. Is the local router forming EIGRP neighbors with the router or routers that should be advertising routes?

- C. Are neighboring routers attached via the same secondary network?
 D. If the hold timers or hello interval for EIGRP is manually changed, are both the hello interval value and the hold timer the same for the neighboring routers?
 E. Do any of the routers have duplicate MTU settings?
 F. Are the routes in the EIGRP topology table?

Answer: A, B, F

Explanation: Answer A, B and F are correct:

If there is problem with EIGRP routing protocol first check whether auto-summarization is disabled or not. If auto-summarization is not disabled, it will create the problem in discontinuous network. Disable the eigrp auto summarization using no auto-summary in router mode. Check whether local router forming the neighbour relationship with other router or not. Similarly routes in EIGRP topology table or not.

QUESTION 428

```

SW2# show vlan
VLAN Name                Status    Ports
-----
 1  default                 active    Fa0/17, Fa0/18, Fa0/19, Fa0/20,
                                Fa0/21, Fa0/22, Fa0/23
10  VLAN0010                suspended Fa0/1, Fa0/2, Fa0/3, Fa0/4,
                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
20  VOICE                   active    Fa0/9, Fa0/10, Fa0/11, Fa0/12,
                                Fa0/13, Fa0/14, Fa0/15, Fa0/16

1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active
  
```

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	1002	1003
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	1	1003
1003	tr	101003	1500	1005	0	-	-	srb	1	1002
1004	fdnet	101004	1500	-	-	1	-	ibm	0	0
1005	trnet	101005	1500	-	-	1	-	ibm	0	0

Refer to the exhibit. The status light over the switchport FastEthernet 0/1 is amber and the port does not forward any frames. Given the information in the exhibit, what would correct the problem?

- A. SW2# vlan database
 SW2(vlan)# vlan 1 are 1
 B. SW2# vlan database
 SW2(vlan)# vlan 1 state active
 C. SW2# vlan database
 SW2(vlan)# vlan 1 stp type auto
 D. SW2# vlan database
 SW2(vlan)# vlan 10 are 1
 E. SW2# vlan database

```
SW2(vlan)# vlan 10 state active
F. SW2# vlan database
SW2(vlan)# vlan 10 stp type auto
```

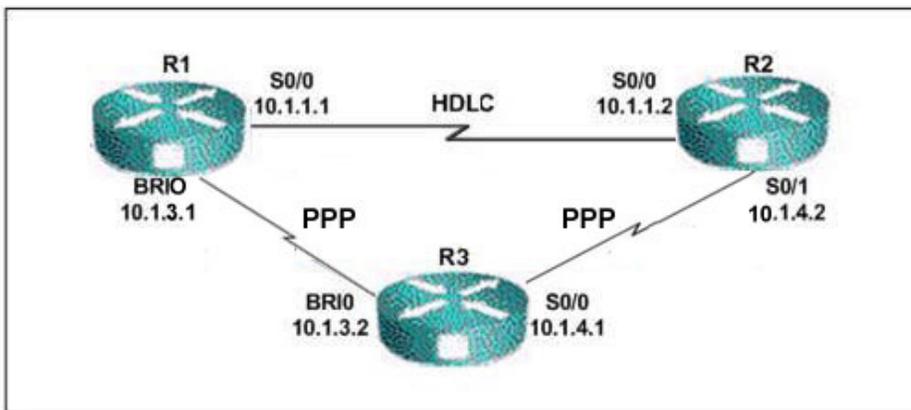
Answer: E

Explanation: Port is amber due the suspended status because fa0/1 is belongs to VLAN 10 and in suspended mode, to troubleshoot you need to bring the interface into the active status.

#vlan database :Enter into vlan database

vlan 10 state active : Brings the interfaces belongs to vlan 10 into active status.

QUESTION 429



Refer to the exhibit. The R1 to R3 ISDN link has been configured for dial backup in the event that the primary link to R2 fails. The backup command has been configured properly. However, during testing, the backup link does not attempt a call. What could be the cause of the problem?

- A. HDLC does not support dial backup.
- B. Interesting traffic has not been defined on R1.
- C. The backup load command has not been configured on the S0/0 interface.
- D. The routing protocol has not yet converged.
- E. DDR is not setup correctly on R3

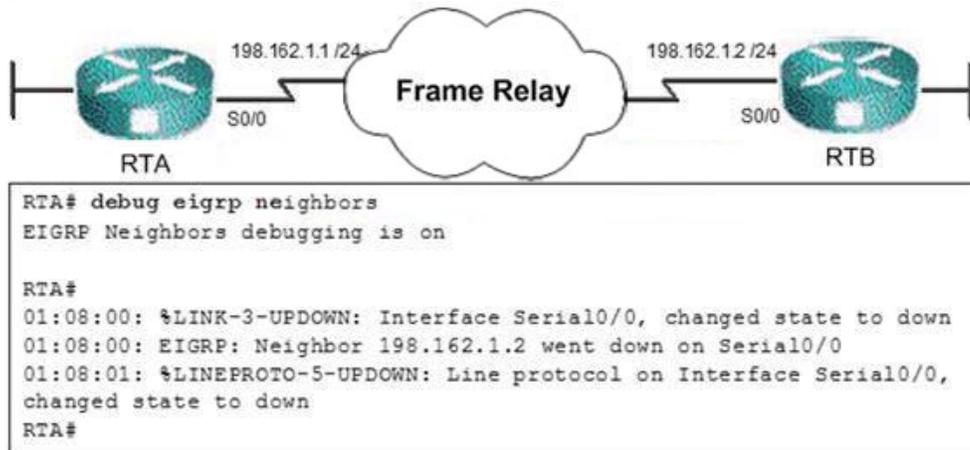
Answer: B

Explanation:

The entire configuration of DDR depends on how the traffic types that cause a call setup to occur are triggered. This traffic is known as interesting traffic.

This problem may be occurred due the Interesting traffic has not been defined on R1.

QUESTION 430



Refer to the exhibit. Hosts on the LAN of router RTA are no longer able to connect to the hosts on the LAN of router RTB. Based on the console message and the debug message generated on RTA, what kind of a problem is likely?

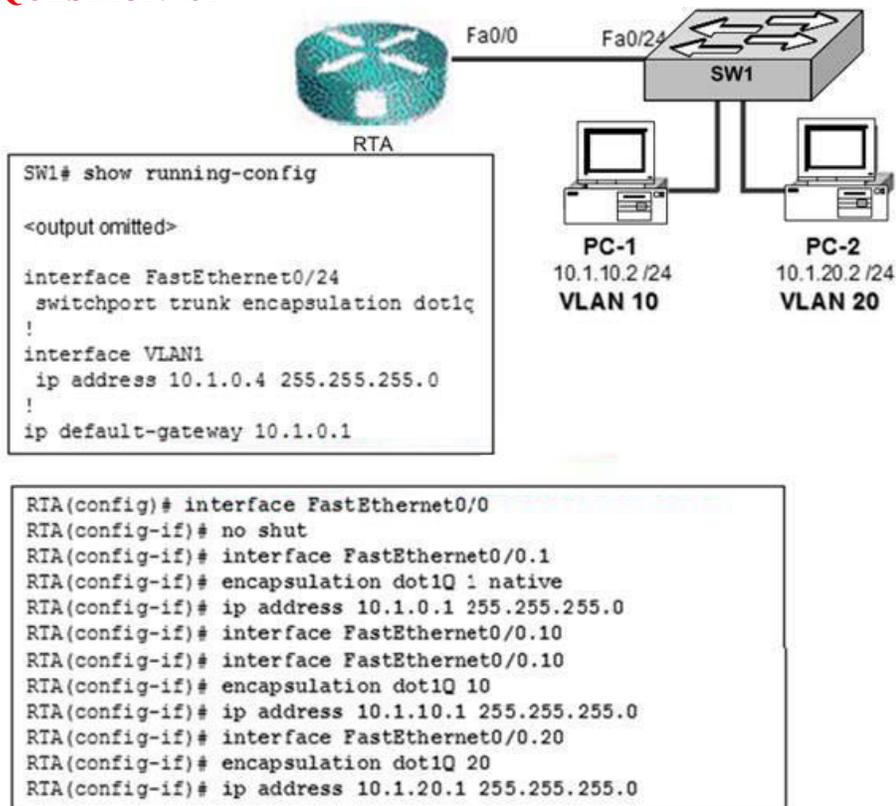
- A. Layer 1
- B. Layer 2
- C. EIGRP route transitions to an "active" state
- D. EIGRP neighbor IP address changed

Answer: B

Explanation:

In the output Line protocol is down this is generally problem on layer 2. So above log is generated due to problem on Layer 2.

QUESTION 431



Refer to the exhibit. PC-1 on VLAN 10 must be able to connect with PC-2 on VLAN 20. The switch SW1 has been configured to support a trunk link to router RTA. A trunk link was configured on router RTA as displayed in the exhibit. However, the trunk link fails to route between VLANs. What command sequence is required to correct this problem?

- A. SW1(config)# interface vlan 1
SW1(config-if)# no shut
- B. SW1(config)# interface FastEthernet 0/24
SW1(config-if)# switchport trunk encapsulation dot1q
- C. RTA(config)# interface FastEthernet 0/0
RTA(config-if)# encapsulation dot1q
- D. RTA(config)# router eigrp 100
RTA(config-router)# network 10.0.0.0
- E. RTA(config)# route eigrp 100
RTA(config-router)# network 10.1.0.0 255.255.255.0
RTA(config-router)# network 10.1.10.0 255.255.255.0
RTA(config-router)# network 10.1.20.0 255.255.255.0

Answer: B

Explanation:

Interface can be either in Access or trunk mode. Access link can carry the

information of only one VLAN and trunk link can carry the information of more than one VLAN.

Fa0/24 should be in trunk with encapsulation dotq1 so

Interface fa0/24

Switchport trunk encapsulation dotq1 should configured on interface.

QUESTION 432

Some internal BGP neighbors are not coming up within the Certkiller network.

What are the two most likely problems? (Choose two).

- A. There are duplicate IP addresses.
- B. The routes to the neighbors are missing.
- C. An access list blocking external addresses.
- D. The update source interface command is missing in BGP configurations.
- E. There are mismatched subnet masks.
- F. The ebgp-multihop command is missing from the BGP configurations.

Answer: B, D

Explanation:

When two routers establish a TCP enabled BGP connection, they are called neighbors or peers. Each router running BGP is called a BGP speaker. Peer routers exchange multiple messages to open and confirm the connection parameters, such as the version of BGP to be used. If there are any disagreements between the peers, notification errors are sent and the connection fails.

When BGP neighbors first establish a connection, they exchange all candidate BGP routes. After this initial exchange, incremental updates are sent as network information changes. As discussed in earlier modules, incremental updates are more efficient than complete table updates. This is especially true with BGP routers, which may contain the complete Internet routing table.

Peers advertise destinations that are reachable through them by using update messages. These messages contain route prefix, AS path, path attributes such as the degree of preference for a particular route, and other properties.

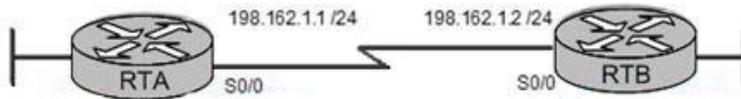
The information for network reachability can change, such as when a route becomes unreachable or a better path becomes available. BGP informs its neighbors of this by withdrawing the invalid routes and injecting the new routing information.

Withdrawn routes are part of the update message. BGP routers keep a table version number that tracks the version of the BGP routing table received from each peer. If the table changes, BGP increments the table version number. A rapidly incrementing table version is usually an indication of instabilities in the network, or a misconfiguration.

If there are no routing changes to transmit to a peer, a BGP speaker will periodically send keepalive messages to maintain the connection. These 19-byte keepalive packets are sent every 60 seconds by default. These packets present a negligible drain on bandwidth and the CPU time on a router.

So Answer B and D are correct.

QUESTION 433



```
RTA# show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
198.162.1.2     1     INIT/          00:00:31   198.162.1.2  Serial0/0
RTA#
```

```
RTB# show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
N/A              1     DOWN/          -           198.162.1.1  Serial0/0
RTB#
```

Refer to the exhibit. The show ip ospf neighbor command reveals a neighbor stuck in the INIT state on router RTA and a neighbor in a DOWN state on router RTB. What is possible cause of this?

- A. The routers do not have Full adjacency with the DR and BDR.
- B. One or both of the OSPF interfaces are configured as passive interfaces.
- C. The keyword "subnets" was omitted from the redistribution command.
- D. The neighboring interfaces are in different OSPF areas.
- E. The dead and hello timers are not the same for the neighboring interfaces.
- F. An ACL that denies incoming multicast traffic is configured on RTB.

Answer: E

Explanation:

OSPF states

OSPF States

The key to effectively designing and troubleshooting OSPF networks is to understand the relationships, or states, that develop between OSPF routers. OSPF interfaces can be in one of seven states. OSPF neighbor relationships progress through these states, one at a time:

1. Down State

In the Down state, the OSPF process has not exchanged information with any neighbor. OSPF is waiting to enter the next state, which is the Init state.

2. InitState

OSPF routers send Type 1 packets, or Hello packets, at regular intervals to establish a relationship with neighbor routers. These intervals are usually ten seconds. When an interface receives its first Hello packet, the router enters the Init state. This means the router knows a neighbor is out there and is waiting to take the relationship to the next step.

The two kinds of relationships are the two-way state and adjacency. A router must receive a Hello from a neighbor before it can establish any relationship.

3. Two-Way State

Using Hello packets, every OSPF router tries to establish a two-way state, or bidirectional communication, with every neighbor router on the same IP network. Among other things, Hello packets include a list of the sender's known OSPF neighbors. A router enters the two-way state when it sees itself in a neighbor's Hello. When RTB learns that RTA knows about RTB, RTB declares a two-way state to exist with RTA.

The two-way state is the most basic relationship that OSPF neighbors can have, but routing information is not shared between routers in this relationship. To learn about the link states of other routers and eventually build a routing table, every OSPF router must form at least one adjacency. An adjacency is an advanced relationship between OSPF routers that involves a series of progressive states that rely not just on Hellos, but also on the other four types of OSPF packets. Routers attempting to become adjacent to one another exchange routing information even before the adjacency is fully established. The first step toward full adjacency is the ExStart state, which is described next.

4. ExStartState

Technically, when a router and its neighbor enter the ExStart state, their conversation is characterized as an adjacency, but they have not become fully adjacent. ExStart is established using Type 2 database description (DBD) packets, also known as DDPs. The two neighbor routers use Hello packets to negotiate who is the "master" and who is the "slave" in their relationship and use DBD packets to exchange databases.

The router with the highest OSPF router ID "wins" and becomes the master. The OSPF router ID is discussed later in this module. When the neighbors establish their roles as master and slave, they enter the Exchange state and begin sending routing information.

5. ExchangeState

In the Exchange state, neighbor routers use Type 2 DBD packets to send each other their link-state information. In other words, the routers describe their link-state databases to each other. The routers compare what they learn with their existing link-state databases. If either of the routers receives information about a link that is not already in its database, the router requests a complete update from its neighbor. Complete routing information is exchanged in the Loading state.

6. LoadingState

After the databases have been described to each router, they may request information that is more complete by using Type 3 packets, link-state requests (LSRs). When a router receives an LSR, it responds with an update by using a Type 4 link-state update (LSU) packet. These Type 4 LSU packets contain the actual link-state advertisements (LSAs), which are the heart of link-state routing protocols. Type 4 LSUs are acknowledged using Type 5 packets, called link-state acknowledgments (LSAcks).

7. Full Adjacency

With the Loading state complete, the routers are fully adjacent. Each router keeps a list of adjacent neighbors, called the adjacency database. Do not confuse the adjacency database with the link-state database or the forwarding database.

For OSPF hello, dead and network types must to same to make adjancies with neighbors.

OSPF routers send Hellos on OSPF enabled interfaces:

- Default every 10 seconds on multi-access and point-to-point segments
- Default every 30 seconds on NBMA segments

Most cases OSPF Hello packets are sent as multicast to ALL SPF Routers (224.0.0.5)

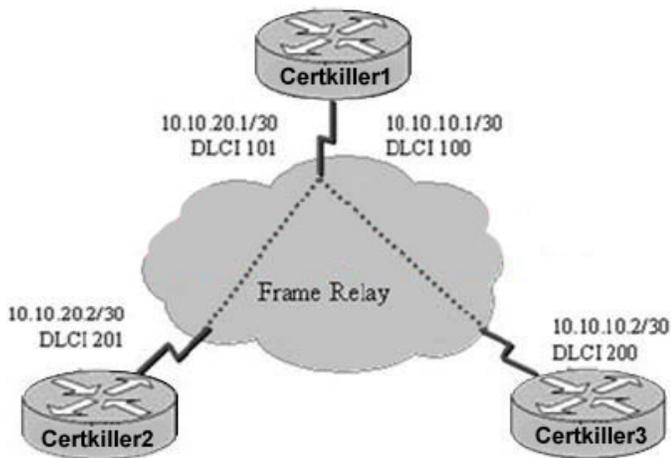
HelloInterval - Cisco default = 10 seconds or 30 seconds and can be changed with the command ip ospf hello-interval.

RouterDeadInterval - The period in seconds that the router will wait to hear a Hello from a neighbor before declaring the neighbor down.

Cisco uses a default of four-times the HelloInterval (4 x 10 sec. = 40 seconds, 120 seconds for NBMA) and can be changed with the command ip ospf dead-interval

To become adjacent, the Hello, DeadInterval and network types must be identical between routers or Hello packets get dropped! No need to change these unless there is some reason for increased performance.

QUESTION 434



```
Certkiller1
!
interface Serial0/0
  encapsulation frame-relay ietf
  frame-relay lmi-type ansi
!
interface Serial0/0.1 point-to-point
  ip address 10.10.20.1 255.255.255.252
  frame-relay interface-dlci 101
interface Serial0/0.2 point-to-point
  ip address 10.10.10.1 255.255.255.252
```

Refer to the exhibit. Router Certkiller 1 has an existing connection to router Certkiller 2 and has been working correctly. The administrator needs to bring up a Frame Relay connection to router Certkiller 3 but the connection is not coming up. What is the problem?

- A. The Frame Relay encapsulation type needs to be changed from IETF to Cisco.
- B. The LMI type needs to be changed from ANSI to Cisco
- C. The command frame-relay map ip 10.10.10.2 200 needs to be added to subinterface

s0/0.2.

D. The command `frame-relay map ip 10.10.10.2 200 broadcast` needs to be added to subinterface s0/0.2.

E. The command `frame-relay interface-dlci 100` needs to be added to subinterface 20/0.2.

F. Inverse ARP needs to be enabled in order for router Certkiller 3 to be able to detect LMI from router Certkiller 1.

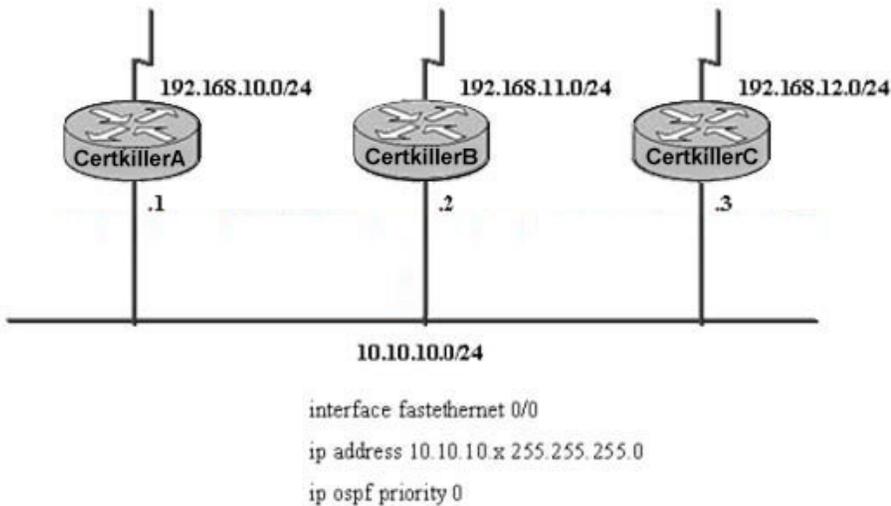
Answer: E

Explanation:

The Frame Relay service provider assigns DLCI numbers for the WAN. Usually, DLCIs 0 to 15 and 1008 to 1023 are reserved for special purposes. Therefore, service providers typically assign DLCIs in the range of 16 to 1007. Multicasts can use DLCI 1019 and 1020. Local Management Interface (LMI) uses DLCI 1023 or 0. Cisco LMI type uses DLCI 1023, and ANSI/ITU-T LMI type uses DLCI 0. DLCI 0 is also used by all Q.933 call control information transmissions to setup, monitor, and terminate SVCs. Some Frame Relay providers may allow their customers to choose their own DLCI numbers, within a specific range, usually between 16 and 1007. You need to assign the proper DLCI number in proper interface using `frame-relay interface-dlci` DLCI number. In the about exhibit no DLCI is configured for serial 0/0.2 sub-interface.

QUESTION 435

Exhibit:



Refer to the exhibit. Which two statements are true? (Choose two.)

- A. The router with the highest IP address will be elected DR on the broadcast segment.
- B. The routers will remain in a 2-way state.
- C. Each router will have two adjacencies.
- D. Certkiller A cannot reach the 192.168.11.0 or 192.168.12.0 network.
- E. The routers will remain in the established state.

Answer: B, D

Explanation:

Because multiaccess networks can support more than two routers, OSPF elects a DR to be the focal point of all link-state updates and LSAs. The role of the DR is critical, therefore a BDR is elected to "shadow" the DR. In the event that the DR fails, the BDR can smoothly take over.

Like any election, the DR/BDR selection process can be rigged to change the outcome. The "ballots" are Hello packets, which contain the ID and priority fields of the router. The router with the highest priority value among adjacent neighbors wins the election and becomes the DR. The router with the second highest priority is elected the BDR. When the DR and BDR have been elected, they keep their roles until one of them fails, even if additional routers with higher priorities show up on the network. Hello packets inform newcomers of the identity of the existing DR and BDR.

By default, all OSPF routers all have the same priority value of 1. A priority number from 0 to 255 can be assigned on any given OSPF interface. A priority of 0 prevents the router from winning any election on that interface. A priority of 255 ensures at least a tie. The Router ID field is used to break ties. If two routers have the same priority, the router with the highest ID will be selected. The router ID can be manipulated by configuring an address on a loopback interface, although that is not the preferred way to control the DR/BDR election process. The priority value should be used instead because each interface can have its own unique priority value. A router can be easily configured to win an election on one interface, and lose an election on another.

QUESTION 436

A network administrator is troubleshooting a host-to-host network communication problem using the divide and conquer approach. The administrator started by using traceroute ip address to verify network layer connectivity between the two hosts that are separated by multiple router hops. The test was successful. Which two assumptions can be made from the success of this test? (Choose two.)

- A. Host A will now be able to transfer files to host B.
- B. The Layer 2 protocols on the network path between hosts are operational.
- C. Layer 1 of the network is operating properly.
- D. The network DNS service is operating properly.

Answer: B, C

Explanation: According to the question that traceroute command is successfully tested it seems that the Layer 2 and Layer 1 Network Operation is running properly.

When the divide and conquer approach is applied towards troubleshooting a networking problem, a layer is selected and tested in both directions from the starting layer. The divide and conquer approach is initiated at a particular layer.

The layer is based on troubleshooter experience level and the symptoms gathered about the problem. Once the direction of the problem is identified, troubleshooting follows that direction until the cause of the problem is identified.

If it can be verified that a layer is functioning, it is typically a safe assumption that the layers below it are functioning as well. If a layer is not functioning properly, gather symptoms of the problem at that layer and work downward to lower layers.

QUESTION 437

Exhibit:

```
PVC Statistics for interface Serial1 (Frame Relay DTE)
```

	Active	Inactive	Deleted	Static
Local	1	0	0	0
Switched	0	0	0	0
Unused	0	0	0	0


```
DLCI = 150  DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial .1
```

input pkts 45	output pkts 48	in pkts 8632
out bytes 6661	dropped pkts 0	in FECN pkts 0
in BECN pkts 0	out FECN pkts 0	out BECN pkts 0
out bcast pkts 31	out bcast bytes 5573	

pvc create time 00:12:12, last time pvc status changed 00:06:23

Refer to the exhibit. Which command would yield the output in the exhibit?

- A. show frame-relay map
- B. show frame-relay lmi
- C. show frame-relay pvc
- D. debug frame-relay pvc
- E. debug frame-relay map

Answer: C

Explanation:

The show frame-relay pvc command displays the status of each configured connection, as well as traffic statistics. This command is also useful for viewing the number of Backward Explicit Congestion Notification (BECN) and Forward Explicit Congestion Notification (FECN) packets received by the router. The command show frame-relay pvc shows the status of all PVCs configured on the router. If a single PVC is specified, only the status of that PVC is shown.

```
Router#show frame-relay pvc 110
```

```
PVC Statistics for interface Serial0 (Frame Relay DTE)
```

```
DLCI = 110, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE,
INTERFACE = Serial0
```

input pkts 14055	output pkts 32795	in bytes 1096228
out bytes 6216155	dropped pkts 0	in FECN pkts 0
in BECN pkts 0	out FECN pkts 0	out BECN pkts 0
in DE pkts 0	out DE pkts 0	
out bcast pkts 32795	out bcast bytes 6216155	

QUESTION 438

A network administrator enters the following commands:

```
Certkiller A(config)# interface fastethernet 0/1
```

```
Certkiller A(config-if)# ip address 172.17.121.2 255.255.255.192
```

The following message appears on the console:

```
% IP addresses may not be configured on L2 links
```

Which Cisco IOS command should the administrator next enter to isolate the problem?

- A. show running-config interface fastethernet 0/1
- B. show ip interface brief
- C. show ip protocols
- D. show spanning-tree

Answer: A

Explanation:

According to output that user tries to assign the IP Address on Layer 2 interface.

Next step of isolating the problem is verify by checking the running configuration of interface.

QUESTION 439

Which statement is true about duplex mismatches and STP?

- A. A switch port that is set to full duplex may not get to transmit BPDUs to its half-duplex neighbor, therefore causing a loop.
- B. The switch port set to half duplex may not get to transmit BPDUs to its full-duplex neighbor, therefore causing a loop.
- C. The switch port set to half duplex may not detect collisions of BPDU frames.
- D. The switch port set to full duplex will detect collisions and will transition to the blocking state.

Answer: B

Explanation:

Duplex plays the vital roles in Spanning tree protocol that port settings the half duplex can't transmit the BPDU's to the full duplex neighbors. You can set using the duplex command in interface configuration mode.

QUESTION 440

Exhibit:

```
092852: Jan 27 22:19:06.713 CST: AAA/AUTHEN (543609479): status = GETPASS
092853: Jan 27 22:19:07.985 CST: AAA/AUTHEN/CONT (543609479): continue_login
(user='dial_tac')
092854: Jan 27 22:19:07.185 CST: AAA/AUTHEN (543609479): status = GETPASS
092855: Jan 27 22:19:07.185 CST: AAA/AUTHEN (543609479): status=ADMIN (tacacs+)
092856: Jan 27 22:19:07.185 CST: AAA/AUTHEN (543609479): statusid=543609479
092857: Jan 27 22:19:08.185 CST: TAC+: ver=192 id=543609479 received AUTHEN status =
092858: Jan 27 22:19:08.185 CST: AAA/AUTHEN (543609479): status = FAIL
092859: Jan 27 22:19:10.185 CST: AAA/MEMORY: free user (0x61D87A70) user='dial tac'
ruser='' port='tty51' rem addr='172.22.2.3' authen type=ASCII service=LOGIN priv=1
```

Refer to the exhibit. Given the output generated by the debug aaa authentication command, which statement is true?

- A. The password is incorrect for authentication.
- B. The NAS was unable to connect to the authentication server.
- C. The user attempted to enter the NAS via the console connection.
- D. The NAS will attempt the next authentication parameter if one is configured.

Answer: A

Explanation:

AAA is an architectural framework for configuring three different security features. Because it uses a single framework, the Cisco IOS can be used to consistently configure authentication, authorization, and accounting.

In this module the terms access server and network access server (NAS) refer to a router connected to the "edge" of a network. This router allows outside users to access the network.

What is meant by authentication, authorization, and accounting? As an example, a user named "flannery" dials into an access server that is configured with CHAP.

The access server will prompt the user for a name and password. The access server authenticates the user's identity by requiring the username and password. This process of verification to gain access is called authentication.

The user may then be able to execute commands on that server once "flannery" has been successfully authenticated. The server uses a process called authorization to determine which commands and resources should be made available to that particular user. Authorization asks the question, "What privileges does this user have?"

Finally, the number of login attempts, the specific commands entered, and other system events can be logged and time-stamped by the accounting process.

Accounting can be used to trace a problem, such as a security breach, or it may be used to compile usage statistics or billing data. The output is generated due to the incorrect password, this authentication was rejected by the AAA server.

QUESTION 441

Which three components should be included in a network topology diagram? (Choose three.)

- A. device names
- B. port speeds
- C. VLANs

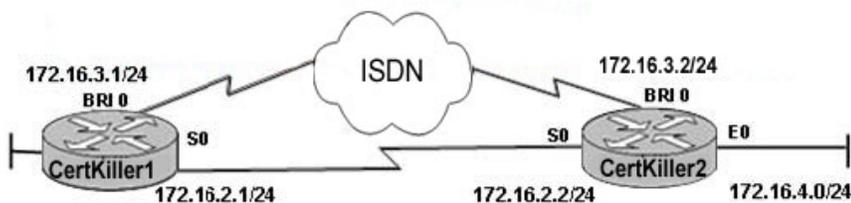
- D. IP addresses
- E. STP settings
- F. etherchannel settings

Answer: A, C, D

Explanation: While designing the Topology diagram, you need to include the device name where which device is suitable, VLAN information need to make the port belong to and IP Address needs to assign on Interfaces.

QUESTION 442

Exhibit:



```

CertKiller1# show_running-config
!
interface Serial0
ip address 172.16.2.1 255.255.255.0
!
interface BRI0
ip address 172.16.3.1 255.255.255.0
encapsulation ppp
dialer idle-timeout 30
dialer watch-disable 15
dialer map ip 172.16.3.2 name R2 broadcast 5552000
dialer map ip 172.16.4.0 name R2 broadcast 5552000
dialer watch-group 1
dialer-group 1
isdn switch-type basic-5ess
ppp multilink
!
router ospf 1
network 172.16.0.0 0.0.255.255 area 0
!
access-list 100 deny ospf any any
access-list 100 permit ip any any
!
dialer-list 1 protocol ip list 100
!
end

```

Refer to the exhibit. Router Certkiller 1 is configured to initiate the ISDN backup connection when the primary link fails using Dialer Watch. The network administrator noticed that when the watched route 172.16.4.0/24 was deleted from the routing table, router Certkiller 1 does not dial the backup link. What statement should be included in the configuration to fix the problem?

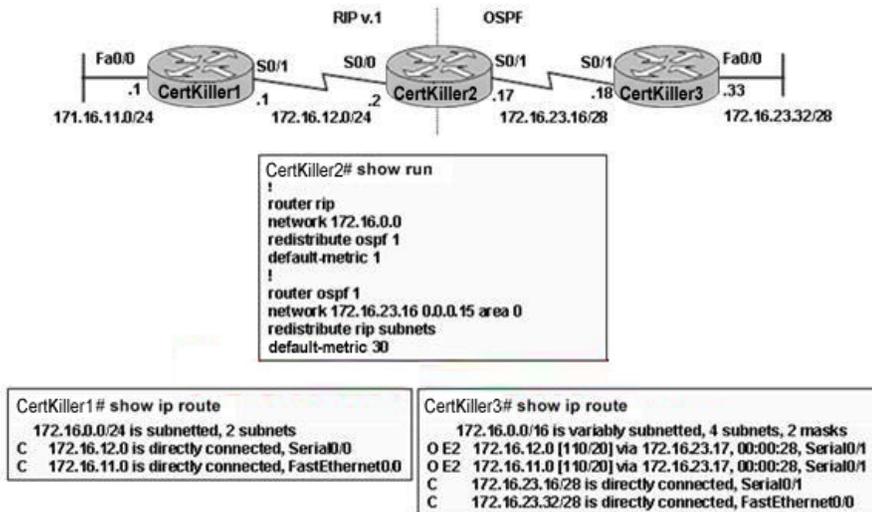
- A. dialer watch-list 1 ip 172.16.0.0 255.255.0.0
- B. dialer watch-list 1 ip 172.16.2.0 255.255.255.0
- C. dialer watch-list 1 ip 172.16.3.0 255.255.255.0
- D. dialer watch-list 1 ip 172.16.4.0 255.255.255.0

Answer: D

Explanation: The dialer watch-list command is the means to detect if the primary interface is up or down. The primary interface is determined to be up when there is an available route with a valid metric to any of the addresses defined in this list, and it point to an interface other then the interface on which the dialer watch-group is defined. The primary interface is determined to be down when there is no available route to any of the address defined in the dialer watch-list command.

QUESTION 443

Exhibit:



RIP and OSPF are configured on the routers as shown in the exhibit. Certkiller 2 is configured with a two-way redistribution between RIP and OSPF domains. All routers can ping each other, but Certkiller 1 cannot see any of the OSPF routes in its routing table. What could the problem be?

- A. OSPF and RIP use the same major network 172.16.0.0. Therefore, the keyword subnets is not required to redistribute protocols into OSPF.
- B. The process of redistribution of RIP into OSPF does not require any metric conversion, so there is no need to define the metric using the default-metric command during the redistribution.
- C. Because OSPF has a longer mask for the same major network than RIP and because RIP version 1 is being used, none of the routes learned from OSPF will be advertised into RIP.
- D. The metric for the OSPF routes that are redistributed into RIP is too low, a fact that prevents OSPF routes from being advertised into RIP.

Answer: C

Explanation:

To support multiple routing protocols within the same internetwork efficiently,

routing information must be shared among the different routing protocols. For example, routes learned from a RIP process may need to be imported into an IGRP process. This process of exchanging routing information between routing protocols is called route redistribution. Such redistribution can be one-way or two-way. One-way routes are where one protocol receives the routes from another. Two-way routes are where both protocols receive routes from each other. Routers that perform redistribution are called boundary routers because they border two or more autonomous systems or routing domains. This section examines route redistribution in detail, including the use of administrative distance, guidelines for redistribution implementation, and issues with redistribution configuration. Although the redistribution command is available for all IP routing protocols, it behaves differently depending on the actual IP routing protocols involved. However, the underlying principles are the same. Therefore, the examples in this section can be used as a starting point for any redistribution scheme.

Syntax of Redistribute

```
Router(config-router)#redistribute protocol [process-id] {level-1 | level-1-2 | level-2} [metric metric-value][metric-type type-value] [match {internal | external 1 | external 2}][tag tag-value] [route-map map-tag][weight weight] [subnets]
```

```
RTB(config)#router rip
RTB(config-router)#network 172.16.0.0
RTB(config-router)#router eigrp 24
RTB(config-router)#network 172.24.0.0
RTB(config-router)#redistribute rip metric 10000 100
255 1 1500
```

In Re-distribution RIP v1 is configured so it doesn't support the Subnet, VLSM etc so unable to learn from OSPF.

QUESTION 444

Exhibit:



```

CertKillerA# show cdp entry CertKiller1
-----
Device ID: CertKiller1
Entry address(es):
  IP address: 10.1.1.2
Platform: cisco WS-C3560-24PS, Capabilities: Switch IGMP
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime : 134 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C3560 Software (C3560-I9-M), Version 12.2(20)SE4, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Sat 08-Jan-05 23:06 by antonino

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27,
  value=00000000FFFFFFFFF010221FF00000000000000137F30E600FF0000
VTP Management Domain: ''
Native VLAN: 1
Duplex: full
  
```

Refer to the exhibit. From router Certkiller A, the administrator can telnet to switch Certkiller 2, but cannot telnet to switch Certkiller 1. On the basis of the information that is generated by the show cdp entry command, which layer-model troubleshooting statement is true?

- A. The problem resides at Layer 1.
- B. The problem resides at Layer 2.
- C. The problem resides at Layer 3.
- D. The problem resides at Layer 4 or higher.
- E. There is an application layer problem with the Telnet program.

Answer: D

Explanation: Answer D is correct because show cdp neighbors is working properly as well as layer 3 address is displaying correctly. It means that problem occurred either in layer 4 or higher layers.

The transport layer provides end-to-end traffic accountability. Layer 4 technologies ensure reliable data delivery using acknowledgments, sequence numbers, and flow control mechanisms. The transport layer is the first layer that provides end-user functions.

Problems at the transport layer can present symptoms ranging from sub-optimal network operation to complete network communications failure. There are at least 35 recognized transport layer protocols. Some of the more common of these are:

1. User Datagram Protocol (UDP)
2. Transport Control Protocol (TCP)
3. Sequenced Packet Exchange (SPX)
4. AppleTalk Transaction Protocol (ATP)
5. NetBIOS

This section will discuss the characteristics of these protocols and related transport

layer technologies.

A specific network protocol can communicate with another network protocol at the layer above or below it. Within the TCP/IP protocol suite, Layer 4 operations are primarily handled by UDP and TCP. UDP and TCP rely on IP at the network layer and use port numbers to identify what higher layer application traffic is contained in the packet. ICMP is a protocol from the TCP/IP suite that operates at the network layer and it too relies on IP. Unlike UDP and TCP, ICMP does not carry user data. ICMP is primarily used by network devices for self-management and self-tuning functions and by network engineers for troubleshooting network problems. UDP, TCP, and ICMP are all used heavily on the Internet, supporting a wide variety of traffic types and applications.

The Network Basic Input/Output System (NetBIOS) was developed for IBM in 1983 by Sytek Corporation and officially defines a session level interface and a data transport protocol. NetBIOS was extended by IBM in 1985 to create the NetBIOS Extended User Interface (NetBEUI) protocol. NetBEUI supports NetBIOS operations at the network layer. NetBEUI and NetBIOS are commonly used in Microsoft and IBM LANs.

NetBEUI operates at the network layer and interfaces directly with ISO's Logical Link Control 2 (LLC2) at the data-link layer. NetBIOS interfaces with NetBEUI and with IBM's Server Message Block (SMB) protocol at the application layer. Together, NetBIOS and NetBEUI can be considered to be operating from the network layer through to the presentation layer. Because both NetBIOS and NetBEUI are non-hierarchical broadcast-based protocols, they depend on other hierarchical protocols, such as IP or IPX, to operate in a routed network.

Novell's proprietary protocol suite uses Sequenced Packet Exchange (SPX) at the transport layer to implement reliable data delivery. In the early days of local area networking, Novell's suite of protocols was commonly implemented. Until version 5 of Novell's network operating system, IPX/SPX was the default protocol suite installed for Novell networks.

Because IPX is not compatible with IP, networks running the Novell protocols are unable to communicate with the Internet without being translated. Due to the growing need for corporate, academic, and government networks to be connected to the Internet, almost all Novell network installations now use the TCP/IP protocol suite. This has led to the steady decline of the number of new network installations using the IPX/SPX protocol suite.

AppleTalk Transaction Protocol (ATP) is used at the transport layer of legacy AppleTalk networks and relies on AppleTalk's Datagram Delivery Protocol (DDP) at the network layer. Because ATP is incompatible with IP, new Mac networks usually use the TCP/IP protocol suite in preference to using the AppleTalk protocol suite.

Although legacy networks using IPX/SPX and AppleTalk still exist, troubleshooting these protocol suites is not in the scope of this course and will not be discussed further in this curriculum.

QUESTION 445

Exhibit:

CertKiller1# show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
10	DATA	suspended	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6
20	MANAGEMENT	active	
25	VOICE	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

<Output omitted>

Refer to the exhibit. Interfaces FastEthernet 0/7 to 0/12 must be assigned to the MANAGEMENT VLAN. Which command sequence will accomplish this task?

- A. Certkiller 1(config)# interface range FastEthernet 0/7 - 12
Certkiller 1(config-if-range)# switchport mode access
Certkiller 1(config-if-range)# switchport access vlan 20
- B. Certkiller 1(config)# interface range FastEthernet 0/7 - 12
Certkiller 1(config-if-range)# switchport mode access
Certkiller 1(config-if-range)# switchport access vlan MANAGEMENT
- C. Certkiller 1(config)# interface range FastEthernet 0/7 - 12
Certkiller 1(config-if-range)# switchport mode trunk
Certkiller 1(config-if-range)# switchport trunk vlan 20
- D. Certkiller 1(config)# interface range FastEthernet 0/7 - 12
Certkiller 1(config-if-range)# switchport mode trunk
Certkiller 1(config-if-range)# switchport trunk vlan MANAGEMENT

Answer: A

Explanation:

Static VLANs are ports on a switch that are manually assigned to a VLAN by using a VLAN management application or by working directly within the switch. These ports maintain their assigned VLAN configuration until an administrator changes them. Although static VLANs require manual entry changes, they are secure, easy to configure, and straightforward to monitor. This type of VLAN works well in networks where moves are controlled and managed. It is also appropriate for networks that employ robust VLAN management software to configure the ports. Static VLANs are also a consideration if it is not desirable to assume the additional overhead required when maintaining end-station MAC addresses and custom filtering tables.

The creation of a VLAN on a switch is a very straightforward and simple task. If using a Cisco IOS -based switch, get to interface configuration mode and issue the switchport command. The switchport mode command can be used to set the

interface to access, dynamic or trunk.

```
Certkiller (config-if)#switchport mode [access | dynamic | trunk]
```

To statically associate an interface with a VLAN, use the following commands:

```
Certkiller (config-if)#switchport mode access
```

```
Certkiller (config-if)#switchport access vlan number
```

Interface FastEthernet 0/3 on the switch is being set to access mode with the switchport mode command. The port is then put into VLAN 2 with the switchport access vlan command as shown using the show running-config command. The switchport mode access command is the default mode for switch interfaces and is not shown in the running-config.

Unlike the earlier 2900XL switch, the 2950 and 3550 switches have an interface range that enables a range of interfaces to be identified for a subsequent operation. For example, several ports can be assigned to a VLAN with one switchport command.

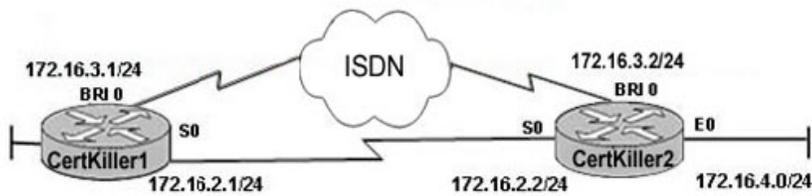
```
Certkiller (config)#interface range fa0/1 - 6
```

```
Certkiller (config-if-range)#switchport access vlan 10
```

This command will assign ports 1 through 6 to vlan 10 in one command sequence. Ports on Cisco switches usually default to the DTP mode of dynamic desirable. This means that another switch connected to this port can cause trunking to occur on this interface. It is recommended that all non-trunking switch ports be configured as access ports with the command switchport mode access. This will help prevent certain man-in-the-middle attacks from occurring within the network. There are also other reasons why it is important not to have rogue switches attaching to the network in regards to Spanning-Tree Protocol (STP). These issues are discussed in the Spanning-Tree Protocol module.

QUESTION 446

Exhibit:



```

CertKiller1# show running-config
!
interface Serial0
ip address 172.16.2.1 255.255.255.0
!
interface BRI0
ip address 172.16.3.1 255.255.255.0
encapsulation ppp
dialer idle-timeout 30
dialer watch-disable 15
dialer map ip 172.16.3.2 name R2 broadcast 5552000
dialer watch-group 8
dialer-group 1
isdn switch-type basic-5ess
ppp multilink
!
router ospf 1
network 172.16.0.0 0.0.255.255 area 0
!
dialer watch-list 8 ip 172.16.4.0 255.255.255.0
!
access-list 100 deny ospf any any
access-list 100 permit ip any any
!
dialer-list 1 protocol ip list 100
!
end

```

Refer to the exhibit and the partial output taken from router Certkiller 1. Router Certkiller 1 is configured to use Dialer Watch to initiate the ISDN backup connection when the primary link fails. The network administrator noticed that when the watched route 172.16.4.0/24 was deleted from the routing table, router Certkiller 1 does not dial the backup link. What should be done to fix the problem?

- A. The backup interface command should be configured under the BRI interface.
- B. A static route should be configured pointing to the watched network.
- C. A second map statement should be configured pointing to the watched network.
- D. OSPF should be defined as interesting traffic.

Answer: C

Explanation: The dialer watch-list command is the means to detect if the primary interface is up or down. The primary interface is determined to be up when there is an available route with a valid metric to any of the addresses defined in this list, and it point to an interface other than the interface on which the dialer watch-group is defined. The primary interface is determined to be down when there is no available route to any of the address defined in the dialer watch-list command.

QUESTION 447

Exhibit:

```
CertKiller1# show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
10 VLAN0010	act/lshut	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6
20 DATA	active	
25 VOICE	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

<Output omitted>

Refer to the exhibit. The status lights over the switchports FastEthernet 0/1 through 0/6 are amber and the ports do not forward any frames. Given the information provided in the exhibit, what would correct the problem?

- A. Certkiller 1(config)# interface range FastEthernet 0/1 - 6
Certkiller 1(config-if-range)# no shut
- B. Certkiller 1(config)# interface range FastEthernet 0/1 - 6
Certkiller 1(config-if-range)# timeout absolute 20
- C. Certkiller 1(config)# interface range FastEthernet 0/1 - 6
Certkiller 1(config-if-range)# power inline auto
- D. Certkiller 1(config)# vlan 1
Certkiller 1(config-if-range)# no shut
- E. Certkiller 1(config)# vlan 10
Certkiller 1(config-if-range)# no shut

Answer: E

Explanation :In Output status of VLAN 10 is shutdown so not forwarding any frames through this port. So you need to bring the status of interface into active by using no shutdown command in vlan interface configuration mode. Interface fa0/1 to 6 belongs to vlan 10, when you shutdown the vlan 10 it downs all interfaces belongs to this vlan.

QUESTION 448

Which general troubleshooting approach typically works better for complex problems?

- A. top down

- B. bottom up
- C. divide and conquer
- D. split and test

Answer: B

Explanation:

When applying a bottom-up approach towards troubleshooting a networking problem, the examination starts with the physical components of the network and then is worked up through the layers of the OSI model until the cause of the problem is identified. It is a good approach for a troubleshooter to use when the problem is suspected to be physical. Most networking problems reside at the lower levels, so implementing the bottom-up approach will often result in effective results. The downside to selecting this approach is that it requires checking of every device and interface on the network until the possible cause of the problem is found. It is a requirement to document each conclusion and possibility. The challenge is to determine which devices to start with.

In many cases, problems within the first four layers can be determined by entering a ping or traceroute command. If the connection is successful, then the cause is likely at the application level. Otherwise, a closer look at the lower levels will be needed to locate the problem.

Verify that Internet control message protocol (ICMP) echo request and echo reply are enabled on the network in order for commands such as ping and traceroute to work. This action should include authorization from the network administrator and documentation of that authorization. If ping has been disabled on the network, it is a result of the implementation of policy. Document in a station log or your personal work log that ping, or any command that was initially disabled, was enabled for network testing and subsequently disabled. This is important should there be an unauthorized intrusion into the network while you are troubleshooting the network. If disabled, the failure of a ping or traceroute command can easily be mistaken for a loss of connectivity

QUESTION 449

Exhibit:



```

CertKillerA# debug ip packet
IP packet debugging is on

CertKillerA# telnet 10.1.1.2
Trying 10.1.1.2 ...
*Mar 1 04:35:50.882: IP: tableid=0, s=10.1.1.1 (local), d=10.1.1.2 (FastEthernet0/0), routed via FIB
*Mar 1 04:35:50.882: IP: s=10.1.1.1 (local), d=10.1.1.2 (FastEthernet0/0), len 44, sending
*Mar 1 04:35:50.886: IP: s=10.1.1.2 (FastEthernet0/0), d=10.1.1.1, len 44, access denied
*Mar 1 04:35:50.886: IP: tableid=0, s=10.1.1.1 (local), d=10.1.1.2 (FastEthernet0/0), routed via FIB
*Mar 1 04:35:50.886: IP: s=10.1.1.1 (local), d=10.1.1.2 (FastEthernet0/0), len 56, sending
*Mar 1 04:35:52.882: IP: tableid=0, s=10.1.1.1 (local), d=10.1.1.2 (FastEthernet0/0), routed via FIB
*Mar 1 04:35:52.882: IP: s=10.1.1.1 (local), d=10.1.1.2 (FastEthernet0/0), len 44, sending
*Mar 1 04:35:52.882: IP: s=10.1.1.2 (FastEthernet0/0), d=10.1.1.1, len 44, access denied

<Output omitted>

```

Refer to the exhibit. From router Certkiller A, the administrator can telnet to switch CK2 , but cannot telnet to switch CK1 . On the basis of the information that is generated by the debug ip packet command, which layer-model troubleshooting statement is true?

- A. The problem resides at Layer 1
- B. The problem resides at Layer 2
- C. The problem resides at Layer 3
- D. The problem resides at Layer 4
- E. There is an application Layer problem with the Telnet program.

Answer: D

Explanation: Answer D is correct because show cdp neighbors is working properly as well as layer 3 address is displaying correctly. It means that problem occurred either in layer 4 or higher layers.

The transport layer provides end-to-end traffic accountability. Layer 4 technologies ensure reliable data delivery using acknowledgments, sequence numbers, and flow control mechanisms. The transport layer is the first layer that provides end-user functions.

Problems at the transport layer can present symptoms ranging from sub-optimal network operation to complete network communications failure. There are at least 35 recognized transport layer protocols. Some of the more common of these are:

1. User Datagram Protocol (UDP)
2. Transport Control Protocol (TCP)
3. Sequenced Packet Exchange (SPX)
4. AppleTalk Transaction Protocol (ATP)
5. NetBIOS

This section will discuss the characteristics of these protocols and related transport layer technologies.

A specific network protocol can communicate with another network protocol at the

layer above or below it. Within the TCP/IP protocol suite, Layer 4 operations are primarily handled by UDP and TCP. UDP and TCP rely on IP at the network layer and use port numbers to identify what higher layer application traffic is contained in the packet. ICMP is a protocol from the TCP/IP suite that operates at the network layer and it too relies on IP. Unlike UDP and TCP, ICMP does not carry user data. ICMP is primarily used by network devices for self-management and self-tuning functions and by network engineers for troubleshooting network problems. UDP, TCP, and ICMP are all used heavily on the Internet, supporting a wide variety of traffic types and applications.

The Network Basic Input/Output System (NetBIOS) was developed for IBM in 1983 by Sytek Corporation and officially defines a session level interface and a data transport protocol. NetBIOS was extended by IBM in 1985 to create the NetBIOS Extended User Interface (NetBEUI) protocol. NetBEUI supports NetBIOS operations at the network layer. NetBEUI and NetBIOS are commonly used in Microsoft and IBM LANs.

NetBEUI operates at the network layer and interfaces directly with ISO's Logical Link Control 2 (LLC2) at the data-link layer. NetBIOS interfaces with NetBEUI and with IBM's Server Message Block (SMB) protocol at the application layer. Together, NetBIOS and NetBEUI can be considered to be operating from the network layer through to the presentation layer. Because both NetBIOS and NetBEUI are non-hierarchical broadcast-based protocols, they depend on other hierarchical protocols, such as IP or IPX, to operate in a routed network.

Novell's proprietary protocol suite uses Sequenced Packet Exchange (SPX) at the transport layer to implement reliable data delivery. In the early days of local area networking, Novell's suite of protocols was commonly implemented. Until version 5 of Novell's network operating system, IPX/SPX was the default protocol suite installed for Novell networks.

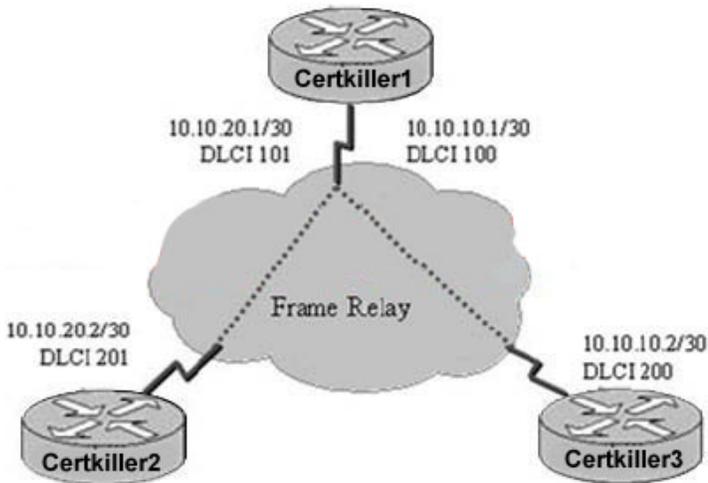
Because IPX is not compatible with IP, networks running the Novell protocols are unable to communicate with the Internet without being translated. Due to the growing need for corporate, academic, and government networks to be connected to the Internet, almost all Novell network installations now use the TCP/IP protocol suite. This has led to the steady decline of the number of new network installations using the IPX/SPX protocol suite.

AppleTalk Transaction Protocol (ATP) is used at the transport layer of legacy AppleTalk networks and relies on AppleTalk's Datagram Delivery Protocol (DDP) at the network layer. Because ATP is incompatible with IP, new Mac networks usually use the TCP/IP protocol suite in preference to using the AppleTalk protocol suite.

Although legacy networks using IPX/SPX and AppleTalk still exist, troubleshooting these protocol suites is not in the scope of this course and will not be discussed further in this curriculum.

QUESTION 450

Exhibit:



```

Certkiller1
!
interface Serial0/0
!
interface Serial0/0.2 point-to-point
ip address 10.10.10.1 255.255.255.252
frame-relay interface-dlci 101

```

Refer to the exhibit. Hosts connected to router Certkiller 1 are unable to reach hosts connected to routers Certkiller 2 and Certkiller 3. The results from the show interface serial 0/0 command show that the interface is up, line protocol down. What is the problem?

- A. Frame Relay LMI is misconfigured.
- B. Frame Relay is not configured on routers Certkiller 2 and Certkiller 3.
- C. The Frame Relay switch is not properly configured.
- D. Frame Relay for router Certkiller 1 is uses Cisco encapsulation. Frame Relay for routers Certkiller 2 and Certkiller 3 use IETF encapsulation.
- E. The DLCIs are configured for the wrong subinterfaces.

Answer: E

Explanation:

The Frame Relay service provider assigns DLCI numbers for the WAN. Usually, DLCIs 0 to 15 and 1008 to 1023 are reserved for special purposes. Therefore, service providers typically assign DLCIs in the range of 16 to 1007. Multicasts can use DLCI 1019 and 1020. Local Management Interface (LMI) uses DLCI 1023 or 0. Cisco LMI type uses DLCI 1023, and ANSI/ITU-T LMI type uses DLCI 0. DLCI 0 is also used by all Q.933 call control information transmissions to setup, monitor, and terminate SVCs. Some Frame Relay providers may allow their customers to

choose their own DLCI numbers, within a specific range, usually between 16 and 1007. You need to assign the proper DLCI number in proper interface using frame-relay interface-dlci DLCI number. In the about exhibit wrong DLCI is configured for serial 0/0.2 sub-interface.

QUESTION 451

Refer to the Exhibit: The user who is connected to interface fastethernet 0/1 is on VLAN 10 and cannot access network resources. On the basis of the information in the exhibit, which command sequence would correct the problem?

```
CertKiller1# show interfaces fastethernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation is negotiate
Negotiation of Trunking. off
Access Mode VLAN: 10 (DATA)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Private VLANs Enabled: 2-10-1
Capture Mode Disabled: ALL
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
CertKiller1#
```

- A. Certkiller 1(config)# interface fa0/1
Certkiller 1(config)# no shutdown
- B. Certkiller 1(config)# interface fastethernet 0/1
Certkiller 1(config)# switchport mode access
- C. Certkiller 1(config)# vlan 10
Certkiller 1(config)# no shutdown
- D. Certkiller 1(config)# vlan 10
Certkiller 1(config)# state active

Answer: A

Explanation:

In Exhibit, fa0/1 interface operational mode is in down state. To bring into operational mode needs to use no shutdown.

1. Go to the interface configuration mode
2. Type no shutdown command

QUESTION 452

Which logging procedure requires the least system overhead on a Cisco router ?

- A. login to the console
- B. logging to the internal buffer
- C. logging to the syslog server
- D. logging to a virtual terminal over WAN

Answer: B

Explanation:

Logging Messages to an Internal Buffer

The default logging device is the console; all messages are displayed on the console unless otherwise specified. To log messages to an internal buffer, use the logging buffered router configuration command. The full syntax of this command follows:

logging buffered

no logging buffered

The logging buffered command copies logging messages to an internal buffer instead of writing them to the console. The buffer is circular in nature, so newer messages overwrite older messages. To display the messages that are logged in the buffer, use the privileged EXEC command show logging. The first message displayed is the oldest message in the buffer.

The no logging buffered command cancels the use of the buffer and writes messages to the console (the default).

QUESTION 453

Refer to the exhibit: Which two problems are the most likely cause of the exhibit output ?

(Choose all that apply)

```
Vlan8 - Group 8
Local state is Active, priority 110, may preempt
Hellotime 3 hold time 10
Next hello sent in 00:00:01.168
Hot standby IP address is 10.1.2.2 configured
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac08
5 state changes, last state change 00:05:03
```

- A. Spanning tree issues
- B. HSRP misconfiguration
- C. VRRP misconfiguration
- D. Physical Layer Issue

E. Transport Layer Issue

Answer: A, D

Explanation:

Spanning-Tree Protocol (STP) is a Layer 2 protocol that utilizes a special-purpose algorithm to discover physical loops in a network and effect a logical loop-free topology. STP creates a loop-free tree structure consisting of leaves and branches that span the entire Layer 2 network. The actual mechanics of how bridges communicate and how the STP algorithm works will be discussed at length in the following topics. Note that the terms bridge and switch are used interchangeably when discussing STP. In addition, unless otherwise indicated, connections between switches are assumed to be trunks.

QUESTION 454

Refer to the exhibit: What are two important facts in interpreting the output of the show ip pim interface command (Choose Two).

```
#CertKiller1 show ip pim interface
```

Address	Interface	Version/Mode	Nbr Count	Query Intvl
192.168.10.1	Ethernet0	v2/Sparse-Dense	1	30
192.168.9.3	Ethernet1	v2/Sparse-Dense	1	30

- A. Multiaccess Segments elect a DR based on lowest IP Address
- B. Multiaccess segments elect a DR based on highest IP Address
- C. Multiaccess multicast segments do not elect a DR
- D. The RP is only seen in version 2 of Sparse-Dense Mode
- E. Point-to-Pont links do not displays DR Information

Answer: A, E

Explanation:

Protocol Independent Multicast (PIM) is a routing protocol that can be used for forwarding multicast traffic. PIM operates independent of any particular IP routing protocol. Therefore, PIM makes use of the IP unicast routing table and does not keep a separate multicast routing table.

PIM can operate in two modes, depending on the density of the recipients in a multicast group. Cisco

has developed a third hybrid mode, as well. The PIM modes are as follows:

1. PIM Dense Mode
2. PIM Sparse Mode
3. PIM Sparse-Dense Mode

PIM selects the DR from the segments having lowest IP Address and point-to-point links do not displays DR information.

QUESTION 455

Refer to the exhibit: While troubleshooting intermittently lost packets within the

network, the network administrator issued the show policy-map command on router 7206 in the network. Which statement is true about the exhibit output?

```
CertKiller1# show policy-map interface atm 1/0.1
ATM1/0.1: VC 0/100 -
  Service-policy output: cbwfq (1283)
  Class-map: A (match-all) (1285/2)
    28621 packets, 7098008 bytes
    5 minute frtered rate 10000 bps, drop rate 0 bps
  Match: access-group 10 (1285)
  Weighted Fair Queueing
    Output Queue: Conversation 73
    Bandwidth 500 (kbps) Max Threshold 64 (packets)
    (pkts matched/bytes matched) 28621/7098008
    (depth/total drops/no-buffer drops) 0/0/0
  Class-map: B (match-all) (1301/4)
    2058 packets, 148176 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
  Match: access-group 103 (1305)
  Weighted Fair Queueing
    Output Queue: Conversation 75
    Bandwidth 500 (kbps) Max Treshold 64 (packets)
    (pkts matched/bytes matched) 0/0
    (depth/total drops/no-buffer drops) 0/0/0
  Class-map: class-default (match-any) (1309/0)
    19 packets, 968 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
  Match: any (1313)
```

- A. The default class of packets has experienced 1313 dropped packets
- B. This interface has experienced congestion with all classes of traffic.
- C. None of the classes of traffic has caused congestion
- D. Only traffic matching class-map A was being transmitted when congestion occurred on this router.

Answer: B

Explanation:

This table illustrates when packets sit in the L3 queue. Locally generated packets are always process-switched and are delivered first to the L3 queue before they are passed on to the interface driver. Fast-switched and Cisco Express Forwarding (CEF)-switched packets are delivered directly to the transmit ring and sit in the L3 queue only when the transmit ring is full.

Packet Type	Congestion	Non-Congestion
Locally-generated packets, which includes Telnet packets and pings	Yes	Yes
Other packets that are process-switched	Yes	Yes

[642-831](#)

Packets that are CEF- or fast-switched	Yes	No
--	-----	----

This example shows these guidelines applied to the show policy-map interface output (the four key counters are in bold):

```
7206# show policy-map interface atm 1/0.1ATM1/0.1: VC 0/100 -Service-policy output:
cbwfq (1283)Class-map: A (match-all) (1285/2)28621 packets, 7098008 bytes5 minute
offered rate 10000 bps, drop rate 0 bpsMatch: access-group 101 (1289)Weighted Fair
QueueingOutput Queue: Conversation 73Bandwidth 500 (kbps) Max Threshold 64
(pkts matched/bytes matched) 28621/7098008(depth/total drops/no-buffer
drops) 0/0/0Class-map: B (match-all) (1301/4)2058 packets, 148176 bytes5 minute
offered rate 0 bps, drop rate 0 bpsMatch: access-group 103 (1305)Weighted Fair
QueueingOutput Queue: Conversation 75Bandwidth 50 (kbps) Max Threshold 64
(pkts matched/bytes matched) 0/0(depth/total drops/no-buffer drops)
0/0/0Class-map: class-default (match-any) (1309/0)19 packets, 968 bytes5 minute
offered rate 0 bps, drop rate 0 bpsMatch: any (1313)This table defines the bolded
counters:
```

Counter	Explanation
28621 packets, 7098008 bytes	The number of packets which match the criteria of the class. This counter increments whether or not the interface is congested.
(pkts matched/bytes matched) 28621/7098008	The number of packets which match the criteria of the class when the interface was congested. In other words, the interface transmit ring was full, and the driver and the L3 processor system worked together to queue the excess packets in the L3 queues, where the service policy applies. Packets that are process-switched always go through the L3 queuing system and thus increment the "packets matched" counter.
Class-map: B (match-all) (1301/4)	These numbers define an internal ID used with the CISCO-CLASS-BASED-QOS-MIB Management Information Base (MIB). They no longer appear in the show policy-map output in current releases of Cisco IOS.

5 minute offered rate 0 bps, drop rate 0 bps	Use the load-interval command to change this value and make it a more instantaneous value. The lowest value is 30 seconds; however, statistics displayed in the show policy-map interface output are updated every 10 seconds. Since the command effectively provides a snapshot at a specific moment, the statistics may not reflect a temporary increase in queue size.
--	---

Without congestion, there is no need to queue any excess packets. With congestion, packets, which includes CEF- and fast-switched packets, may go into the L3 queue. Refer back to how the Cisco IOS configuration guide defines congestion: "If you use congestion management features, packets accumulating at an interface are queued until the interface is free to send them; they are then scheduled according to their assigned priority and the queuing mechanism configured for the interface."

Normally, the "packets" counter is much larger than the "pkts matched" counter. If the values of the two counters are nearly equal, then the interface currently receives a large number of process-switched packets or is heavily congested. Both of these conditions should be investigated to ensure optimal packet forwarding.

How Are Conversation Numbers Allocated? This section explains how your router allocates conversation numbers for the queues created when the service policy is applied.

```
Router# show policy-map interface s1/0.1 dlc1 100Serial1/0.1: DLCI 100 -output :
mypolicyClass voiceWeighted Fair QueueingStrict PriorityOutput Queue: Conversation
72Bandwidth 16 (kbps) Packets Matched 0(pkts discards/bytes discards) 0/0Class
immediate-dataWeighted Fair QueueingOutput Queue: Conversation 73Bandwidth 60
(%) Packets Matched 0(pkts discards/bytes discards/tail drops) 0/0/0mean queue depth:
0drops: class random tail min-th max-th mark-prob0 0 64 128 1/101 0 0 71 128 1/102 0
0 78 128 1/103 0 0 85 128 1/104 0 0 92 128 1/105 0 0 99 128 1/106 0 0 106 128 1/107 0
0 113 128 1/10rsvp 0 0 120 128 1/10Class priority-dataWeighted Fair QueueingOutput
Queue: Conversation 74Bandwidth 40 (%) Packets Matched 0 Max Threshold 64
(packets)(pkts discards/bytes discards/tail drops) 0/0/0Class class-defaultWeighted Fair
QueueingFlow Based Fair QueueingMaximum Number of Hashed Queues 64 Max
Threshold 20 (packets)The class-default class is the default class to which traffic is
directed, if that traffic does not satisfy the match criteria of other classes whose policy is
defined in the policy map. The fair-queue command allows you to specify the number of
dynamic queues into which your IP flows are sorted and classified. Alternately, your
router allocates a default number of queues derived from the bandwidth on the interface
or VC. Supported values in either case are a power of two, in a range from 16 to 4096.
This table lists the default values for interfaces and for ATM permanent virtual circuits
(PVCs):
```

Default Number of Dynamic Queues as a Function of Interface Bandwidth

BandwidthRange	Number of Dynamic Queues
Less than or equal to 64 kbps	16

More than 64 kbps and less than or equal to 128 kbps	32
More than 128 kbps and less than or equal to 256 kbps	64
More than 256 kbps and less than or equal to 512 kbps	128
More than 512 kbps	256

Default Number of Dynamic Queues as a Function of ATM PVC Bandwidth

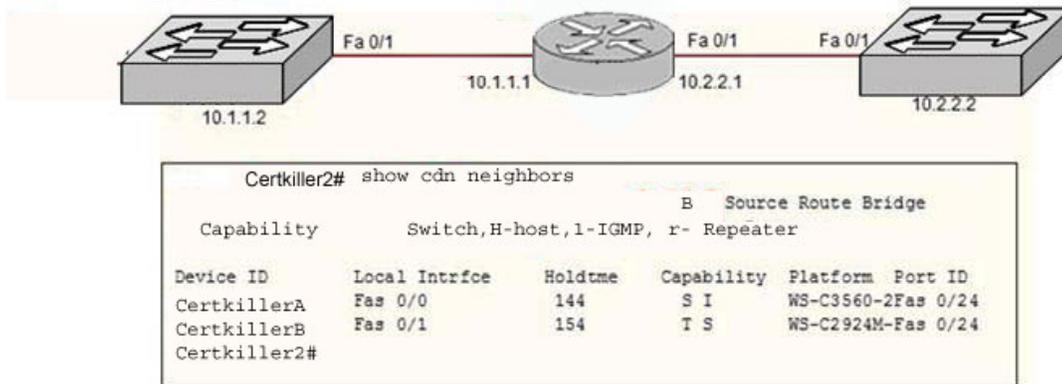
BandwidthRange	Number of Dynamic Queues
Less than or equal to 128 kbps	16
More than 128 kbps and less than or equal to 512 kbps	32
More than 512 kbps and less than or equal to 2000 kbps	64
More than 2000 kbps and less than or equal to 8000 kbps	128
More than 8000 kbps	256

Based on the number of reserved queues for weighted fair queuing, Cisco IOS assigns a conversation or queue number as shown in this table:

Conversation / Queue Number	Type of Traffic
1 - 256	General flow-based traffic queues. Traffic that does not match to a user-created class will match to class-default and one of the flow-based queues.
257 - 263	Reserved for Cisco Discovery Protocol (CDP) and for packets marked with an internal high-priority flag.
264	Reserved queue for the priority class (classes configured with the priority command). Look for the "Strict Priority" value for the class in the show policy-map interface output. The priority queue uses a conversation ID equal to the number of dynamic queues plus eight.
265 and higher	Queues for user-created classes.

QUESTION 456

Network topology exhibit:



You work as a network administrator at Certkiller .com. Study the exhibit carefully. From Certkiller 2 you can ping IP address 10.2.2.2 of switch Certkiller B, but is unable to ping IP address 10.1.1.2 of switch Certkiller A

- A. On the basis of the exhibited output of the show cdp neighbors command, which two statements are true? Select two.
- A. The problem is with an access list blocking all traffic to the 10.0.0.0/8 network.
 - B. This is an example of using the divide-and-conquer approach to the troubleshooting a network problem
 - C. The problem has been isolated at Layer 3 or higher.
 - D. This is an example of using the bottom-up to troubleshooting a network problem.
 - E. This is an example of using the top-down to troubleshooting a network problem.

Answer: A,B

Explanation:

When the divide and conquer approach is applied towards troubleshooting a networking problem, a layer is selected and tested in both directions from the starting layer. The divide and conquer approach is initiated at a particular layer. The layer is based on troubleshooter experience level and the symptoms gathered about the problem. Once the direction of the problem is identified, troubleshooting follows that direction until the cause of the problem is identified.

If it can be verified that a layer is functioning, it is typically a safe assumption that the layers below it are functioning as well. If a layer is not functioning properly, gather symptoms of the problem at that layer and work downward to lower layers.

QUESTION 457

Exhibit:

```

Certkiller# debug ip igmp
12:32:51:065: IGMP: Send v2 Query on Ethernet1 to 224.0.0.1
12:32:51:069: IGMP: Set report delay time to 9.4 seconds for 224.0.1.40 on Ethernet1
12:32:56:089 I GMP: Recieved V1 Report from 192.168.9.1 (Ethernet1) for 239.255.0.1
12:32:069:I GMP:Standing V1 host present timer for 239.255.0.1 on Ethernet1
12:33:01:065: IGMP: send V2 Report for 224.0.1.40 on Ethernet1
12:33:01:069: IGMP: Received v2 Report from 192.168.9.4 (Ethernet1) for 224.0.1.40
12:33:51:065: IGMP: Send v2 Query on Ethernet1 to 224.0.0.1
  
```

You work as a network administrator at Certkiller .com. Study the exhibit carefully. What can be said from the output displayed in the exhibit? Select two.

- A. IP RIM PR mapping is static.
- B. The IP multicast groups are 224.0.0.1, 224.0.1.40, and 239.255.0.1
- C. Certkiller A received an IGMP report version 1 from host 192.168.9.1.
- D. Reverse Path Forwarding (RPF) is enabled for 224.0.1.40.
- E. The router sent an IGMP version 2 query out interface Ethernet1 at multicast address 224.0.0.1
- F. Reverse Path Forwarding (RPF) is enabled for 192.168.9.4

Answer: B,C

Explanation:

How does a router know of the recipients in a multicast group, much less of their locations? To receive multicast traffic from a source, both the source and every recipient must first join a common multicast group. This group is also known by its multicast IP address. A host can join a multicast group by sending a request to its local router. This is done through the Internet Group Management Protocol (IGMP). IGMPv1 is defined in RFC 1112, and its successor, IGMPv2, in RFC 2236. When several hosts join a group by contacting their local routers, it is the multicast routing protocol (such as PIM) that "connects the dots" and forms the multicast tree between routers.

IGMPv1

To join a multicast group, a host can dynamically send a Membership Report IGMP message to its local router. This message tells the router what multicast address (group) the host is joining. The multicast address is used as the destination IP address, as well as the group address listed in the message.

Every 60 seconds, one router on each network segment queries all hosts to see if they are interested in receiving multicast traffic. This router is known as the IGMPv1 Querier and functions simply to invite hosts to join a group. Queries are sent to the 224.0.0.1 all-hosts multicast address for quick distribution. If a host is interested in joining a group, or if it wants to continue receiving a group that it has already joined, it must respond with a membership report.

QUESTION 458

While verifying a Frame Relay connection on a Certkiller router you enter the command:

```
debug frame-relay lmi
```

From this, you notice this line in your output:

```
type 0 status field reads 0x00.
```

What is the status this LMI connection?

- A. Added/active
- B. Added/inactive
- C. Deleted
- D. Disabled

E. None of the above

Answer: B

Explanation:

LMI is a signaling standard between the DTE and the Frame Relay switch. LMI is responsible for managing the connection and maintaining the status between devices.

LMI includes support for the following:

1. A keepalive mechanism - This verifies that data is flowing.
2. A status mechanism - These messages provide communication and synchronization between the network and the user device. They periodically report the existence of new PVCs and the deletion of already existing PVCs. They also generally provide information about PVC integrity. VC status messages prevent the sending of data into black holes, which are PVCs that no longer exist.
3. A multicast mechanism - Multicasting allows a sender to transmit a single frame that can be delivered by the network to multiple recipients. Multicasting supports the efficient delivery of routing protocol messages and address resolution procedures that typically must be sent to many destinations simultaneously.
4. Global addressing - This gives connection identifiers global rather than local significance. This allows them to be used to identify a specific interface to the Frame Relay network. Global addressing makes the Frame Relay network resemble a LAN in terms of addressing. Therefore, address resolution protocols perform over Frame Relay exactly as they do over a LAN. The Frame Relay switch uses LMI to report the status of configured PVCs. The three possible PVC states are as follows:
 1. Active state - Indicates that the connection is active and that routers can exchange data.
 1. Inactive state - Indicates that the local connection to the Frame Relay switch is working, but the remote router connection to the Frame Relay switch is not working.
 2. Deleted state - Indicates that no LMI is being received from the Frame Relay switch, or that there is no service between the CPE router and Frame Relay switch.