ITTEST

QUESTION & ANSWER

Guías de estudio precisos, Alta tasa de paso!

Ittest ofrece información actualizada de forma gratuita en un año!

http://www.ittest.es/

Exam : **642-832**

Title : Troubleshooting and maintaing cisco ip networks

Version : Demo

Topic 1, Multiple Choice Questions

1.The following commands are issued on a Cisco Router:

Router (configuration) #access-list 199 permit tcp host 10.1.1.1 host 172.16.1.1

Router (configuration) #access-list 199 permit tcp host 172.16.1.1 host 10.1.1.1

Router (configuration) #exit

Router#debug ip packet 199

What will the debug output on the console show?

A. All IP packets passing through the router

B. Only IP packets with the source address of 10.1.1.1

C. All IP packets from 10.1.1.1 to 172.16.1.1

D. All IP Packets between 10.1.1.1 and 172.16.1.1

Answer: D

Explanation:

In this example, the "debug ip packet" command is tied to access list 199, specifying which IP packets should be debugged. Access list 199 contains two lines, one going from the host with IP address 10.1.1.1 to 172.16.1.1 and the other specifying all TCP packets from host 172.16.1.1 to 10.1.1.1.

2.What level of logging is enabled on a Router where the following logs are seen?

%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

A. alerts

B. critical

C. errors

D. notifications

Answer: D

Explanation:

Cisco routers, switches, PIX and ASA firewalls prioritize log messages into 8 levels (0-7), as shown below:

LevelLevel NameDescription

0 Emergencies System is unusable

1 Alerts Immediate action needed

2 Critical Critical conditions

3 Errors Error conditions

4 Warnings Warning conditions

5 Notifications Informational messages

6 Informational Normal but significant conditions

7 Debugging Debugging messages

When you enable logging for a specific level, all logs of that severity and greater (numerically less) will be logged. In this case we can see that logging level of 3 (as seen by the 3 in "LINK-3UPDOWN") and level 5 (as seen by the 5 in "LINEPROTO-5-UPDOWN") are shown, which means that logging level 5 must have been configured. As shown by the table, logging level 5 is Notifications.

3.You have the followings commands on your Cisco Router:

ip ftp username admin

ip ftp password backup

You have been asked to switch from FTP to HTTP.

Which two commands will you use to replace the existing commands?

A. ip http username admin

B. ip http client username admin

C. ip http password backup

D. ip http client password backup

E. ip http server username admin

F. ip http server password backup

Answer: B,D

Explanation:

Configuring the HTTP Client

Perform this task to enable the HTTP client and configure optional client characteristics.

The standard HTTP 1.1 client and the secure HTTP client are always enabled. No commands exist to disable the HTTP client. For information about configuring optional characteristics for the HTTPS client, see the HTTPS-HTTP Server and Client with SSL 3.0, Release 12.2(15) T, feature module. SUMMARY STEPS

1. enable

2. configure terminal

3. ip http client cache {ager interval minutes | memory {file file-size-limit | pool pool-size-limit}

4. ip http client connection {forceclose | idle timeout seconds | retry count | timeout seconds}

5. ip http client password password

6. ip http client proxy-server proxy-name proxy-port port-number

7. ip http client response timeout seconds

8. ip http client source-interface type number

9. ip http client username username

Reference: HTTP 1.1 Web Server and Client

. http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_http_web.html

4.You have 2 NTP servers in your network - 10.1.1.1 and 10.1.1.2. You want to configure a Cisco router to use 10.1.1.2 as its NTP server before falling back to 10.1.1.1.

Which commands will you use to configure the router?

A. ntp server 10.1.1.1

ntp server 10.1.1.2

B. ntp server 10.1.1.1

ntp server 10.1.1.2 primary

C. ntp server 10.1.1.1

ntp server 10.1.1.2 prefer

D. ntp server 10.1.1.1 fallback

ntp server 10.1.1.2

Answer: C

Explanation:

A router can be configured to prefer an NTP source over another. A preferred server's responses are

discarded only if they vary dramatically from the other time sources. Otherwise, the preferred server is used for synchronization without consideration of the other time sources. Preferred servers are usually specified when they are known to be extremely accurate. To specify a preferred server, use the prefer keyword appended to the ntp server command.

The following example tells the router to prefer TimeServerOne over TimeServerTwo:

Router#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router (config) #ntp server TimeServerOne prefer

Router (config) #ntp server TimeServerTwo

Router (config) #^Z

5.The following command is issued on a Cisco Router:

Router (configuration) #logging console warnings

Which alerts will be seen on the console?

A. Warnings only

B. debugging, informational, notifications, warnings

C. warnings, errors, critical, alerts, emergencies

D. notifications, warnings, errors

E. warnings, errors, critical, alerts

Answer: C

Explanation:

Cisco routers prioritize log messages into 8 levels (0-7), as shown below:

LevelLevel NameDescription

0 Emergencies System is unusable

1 Alerts Immediate action needed

2 Critical Critical conditions

3 Errors Error conditions

4 Warnings Warning conditions

5 Notifications Informational messages

6 Informational Normal but significant conditions

7 Debugging Debugging messages

When you enable logging for a specific level, all logs of that severity and greater (numerically less) will be logged. In this case, when you enable console logging of warning messages (level 4), it will log levels 0-4, making the correct answer warnings, errors, critical, alerts, and emergencies.

6.Which two of the following options are categories of Network Maintenance tasks?

A. Firefighting

B. Interrupt-driven

C. Policy-based

D. Structured

E. Foundational

Answer: B,D

Explanation:

Proactive Versus Reactive Network Maintenance:

Network maintenance tasks can be categorized as one of the following:

- Structured tasks: Performed as a predefined plan.

- Interrupt-driven tasks: Involve resolving issues as they are reported.

Reference: CCNP TSHOOT Official Certification Guide, Kevin Wallace, Chapter 1, p.7

7.You enabled CDP on two Cisco Routers which are connected to each other. The Line and Protocol status for the interfaces on both routers show as UP but the routers do not see each other a CDP neighbors.

Which layer of the OSI model does the problem most likely exist?

A. Physical

B. Session

C. Application

D. Data-Link

E. Network

Answer: D

Explanation:

CDP is a protocol that runs over Layer 2 (the data link layer) on all Cisco routers, bridges, access servers, and switches. CDP allows network management applications to discover Cisco devices that are neighbors of already known devices, in particular, neighbors running lower-layer, transparent protocols. With CDP, network management applications can learn the device type and the SNMP agent address of neighboring devices. This feature enables applications to send SNMP queries to neighboring devices. In this case, the line protocol is up which means that the physical layer is operational (layer 1) but the data link layer is not.

Reference: "Configuring CDP"

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.1E/native/configuration/guide/c dp.html

8.FCAPS is a network maintenance model defined by ISO.

It stands for which of the following?

A. Fault Management

B. Action Management

C. Configuration Management

D. Protocol Management

E. Security Management

Answer: A,C,E

Explanation:

The FCAPS maintenance model consists of the following:

FCAPS Maintenance Tasks:

9.Which three management categories are contained in the FCAPS network maintenance model? (Choose three.)

A. Config

B. Fault

C. Storage

D. Accounting

E. Redundancy

F. Telecommunications

Answer: A,B,D

10.What is the result of configuring the logging console warning command?

A. Messages with a severity level of 4 and higher will be logged to all available TTY lines.

B. Only warning messages will be logged on the console.

C. Warning, error, critical, and informational messages will be logged on the console.

D. Warning, critical, alert, and emergency messages will be logged on the console.

E. The logging console warning command needs to be followed in the configuration with logging buffered byte size to specify the message buffer size for the console.

Answer: D