351-001^{Q&As}

351-001^{Q&As}

CCIE Routing and Switching Written

Pass Cisco 351-001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4lead.com/351-001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

Which two statements about logging are true? (Choose two.)

A. Log messages are sent to the console port by default.

B. Log messages are displayed in a Telnet session by default.

C. Interface status changes are logged at the Notification level.

D. Interface status changes are logged at the Informational level.

E. System restart messages are logged at the Critical level.

F. Reload requests are logged at the Notification level.

Correct Answer: AC

By default, switches send the output from system messages and debug privileged EXEC commands to a logging process. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer,

terminal lines, or a UNIX syslog server, depending on your configuration. The process also sends messages to the console.

Table 29-3 Message Logging Level Keywords

Level Keyword

Level

Description

Syslog Definition

emergencies

System unstable

LOG_EMERG

alerts

Immediate action needed

LOG_ALERT

critical

Critical conditions

LOG_CRIT

errors

Error conditions

LOG_ERR

warnings

Warning conditions

LOG_WARNING

notifications

Normal but significant condition

LOG_NOTICE

informational

Informational messages only

LOG_INFO

debugging

Debugging messages

LOG_DEBUG

The software generates four other categories of messages:

?

Error messages about software or hardware malfunctions, displayed at levels warnings through emergencies. These types of messages mean that the functionality of the switch is affected. For information on how to recover from these

malfunctions, see the system

?

Output from the debug commands, displayed at the debugging level. Debug commands are typically used only by the Technical Assistance Center.

?

Interface up or down transitions and system restart messages, displayed at the notifications level. This message is only for information; switch functionality is not affected.

?

Reload requests and low-process stack messages, displayed at the informational level. This message is only for information; switch functionality is not affected.

References:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2950/software/release/12-
1_9_ea1/configuration/guide/scg/swlog.html
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12- 2_55_se/configuration/

guide/scg_2960/swlog.html

QUESTION 2

Refer to the exhibit.


```
R1(config-if)#ipv6 ospf authentication ipsec spi 256 md5 0 o-routes
```

Which two options are possible states for the interface configured with the given OSPFv3 authentication? (Choose two.)

A. GOING UP

B. DOWN

C. UNCONFIGURED

D. GOING DOWN

Correct Answer: AB

To configure IPsec, you configure a security policy, which is a combination of the security policy index (SPI) and the key (the key is used to create and validate the hash value). IPsec for OSPFv3 can be configured on an interface or on an OSPFv3 area. For higher security, you should configure a different policy on each interface configured with IPsec. If you configure IPsec for an OSPFv3 area, the policy is applied to all of the interfaces in that area, except for the interfaces that have IPsec configured directly. Once IPsec is configured for OSPFv3, IPsec is invisible to you. The secure socket API is used by applications to secure traffic. The API needs to allow the application to open, listen, and close secure sockets. The binding between the application and the secure socket layer also allows the secure socket layer to inform the application of changes to the socket, such as connection open and close events. The secure socket API is able to identify the socket; that is, it can identify the local and remote addresses, masks, ports, and protocol that carry the traffic requiring security. Each interface has a secure socket state, which can be one of the following: NULL: Do not create a secure socket for the interface if authentication is configured for the area. DOWN: IPsec has been configured for the interface (or the area that contains the interface), but OSPFv3 either has not requested IPsec to create a secure socket for this interface, or there is an error condition. GOING UP: OSPFv3 has requested a secure socket from IPsec and is waiting for a CRYPTO_SS_SOCKET_UP message from IPsec. UP: OSPFv3 has received a CRYPTO_SS_SOCKET_UP message from IPsec. CLOSING: The secure socket for the interface has been closed. A new socket may be opened for the interface, in which case the current secure socket makes the transition to the DOWN state. Otherwise, the interface will become UNCONFIGURED. UNCONFIGURED. Authentication is not configured on the interface. OSPFv3 will not send or accept packets while in the DOWN state.

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15- sy/iro-15-sy-book/ip6-route-ospfv3-auth-ipsec.html
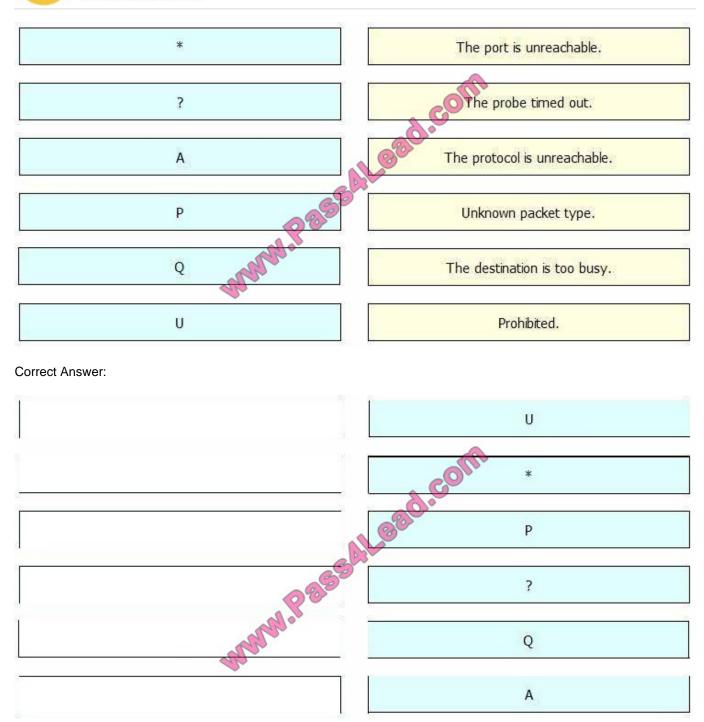

QUESTION 3

DRAG DROP

Drag each traceroute text character on the left to its meaning on the right.

Select and Place:

*		The port is unreachable.	
?		The probe timed out.	
A		The protocol is unreachable.	
P		Unknown packet type.	
Q		The destination is too busy.	
U		Prohibited.	

Correct Answer:

		U	
		*	
		P	
		?	
		Q	
		A	

QUESTION 4

Which action must you take to configure encryption for a dynamic VPN?

A. Configure an FQDN peer in the crypto profile.

B. Configure an FQDN identity in the crypto keyring.

C. Configure an FQDN in the crypto keyring.

D. Configure an FQDN on the router.
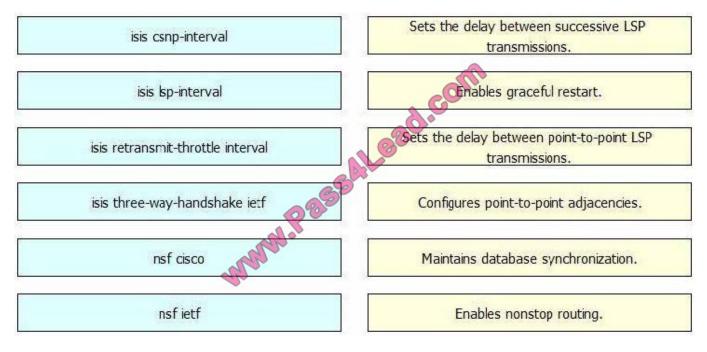
Correct Answer: A

QUESTION 5

DRAG DROP

Drag each IS-IS command on the left to its effect on the right.

Select and Place:

Commands	Effects
isis csnp-interval	Sets the delay between successive LSP transmissions.
isis lsp-interval	Enables graceful restart.
isis retransmit-throttle interval	Sets the delay between point-to-point LSP transmissions.
isis three-way-handshake ietf	Configures point-to-point adjacencies.
nsf cisco	Maintains database synchronization.
nsf ietf	Enables nonstop routing.

Correct Answer:

	isis lsp-interval
	nsf ietf
	isis retransmit-throttle interval
	isis three-way-handshake ietf
	isis csnp-interval
	nsf cisco

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.pass4lead.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: