

Section 2

Securing the Perimeter

Question 1

Which enable password is cryptographically most secure?

Question 2

Which router vty line configuration commands must be run to enable successful Telnet sessions to the router?

Question 3

What does AAA stand for?

Question 1 Answer

Enable secret passwords are stored as an MD5 hash, which is more secure than the legacy enable password. The legacy enable password should be disabled when not needed.

Question 2 Answer

The commands **login** and **password** must run at the **router(config-line)#** prompt for a remote Telnet connection to work. Note that Telnet is insecure and that SSH is the recommended command-line interface access protocol because of its inherent security.

Question 3 Answer

Authentication, Authorization, and Accounting

Question 4

Which part of AAA determines what activities are allowed for the user?

Question 5

Name two two-factor authentication technologies.

Question 6

What is packet mode access?

Question 4 Answer

Authorization

Question 5 Answer

Token card and soft tokens

Question 6 Answer

Packet mode access is remote network access by users, such as a PPP dial-in connection to an ISP's system.

Question 7

Name the two types of AAA server protocols.

Question 8

List three user accounts database types CSACS can interact with.

Question 9

How does an administrator log into and control a CSACS?

Question 7 Answer

RADIUS and TACACS+

Question 8 Answer

Windows SAM (Windows NT), Windows Active Directory (Windows 2000 and newer), ODBC, LDAP, and Novell NDS

Question 9 Answer

CSACS is managed through a web browser interface either directly on the local CSACS host or over a network.

Question 10

Which global command disables source routing, an IP feature allowing packets with a predefined route to override local routes?

Question 11

Which command disables a router's SNMP process?

Question 12

Which interface command disables ICMP notifications of unreachable networks?

Question 10 Answer

The `router(config)#no ip source-route` command

Question 11 Answer

The `router(config)#no snmp-server` command

Question 12 Answer

`router(config)#no ip unreachable`

Question 13

What are the valid numbering ranges of extended ACLs?

Question 14

What type of ACL creates openings during specified time slots?

Question 15

After an ACL is created, what is the next step to place it into production?

Question 13 Answer

100 to 199 and 2000 to 2699

Question 14 Answer

Time-based

Question 15 Answer

Apply it to an interface with the `ip access-group` interface configuration command or the `access-class` line configuration command.

Question 16

Which type of management network separates management traffic from general user and system traffic?

Question 17

Which command-line access application is discouraged?

Question 18

Which IOS command generates a crypto keypair for use with SSH?

Question 16 Answer

Out-of-band (OOB)

Question 17 Answer

Telnet. Use SSH whenever possible.

Question 18 Answer

The crypto key generate {options} command

Question 19

What are the three SNMP security model versions?

Question 20

What are the three SNMP security levels?

Question 21

What does Cisco recommend for securing trunks?

Question 19 Answer

SNMP version 1, version 2c, and version 3

Question 20 Answer

noauth, auth, priv

Question 21 Answer

Allow only the VLANs that must traverse the trunk to be configured on the trunk. Prune all other VLANs. Assign dedicated VLAN numbers as the native VLAN number.

Question 22

Which IOS switch command controls the number of allowable MAC addresses on a port?

Question 23

What are the three switchport violation modes?

Question 24

Which IOS command prevents a port from sending or receiving bridge protocol data units (BPDUs) to mitigate spanning tree protocol attacks?

Question 22 Answer

The switchport port-security maximum *{number}* command

Question 23 Answer

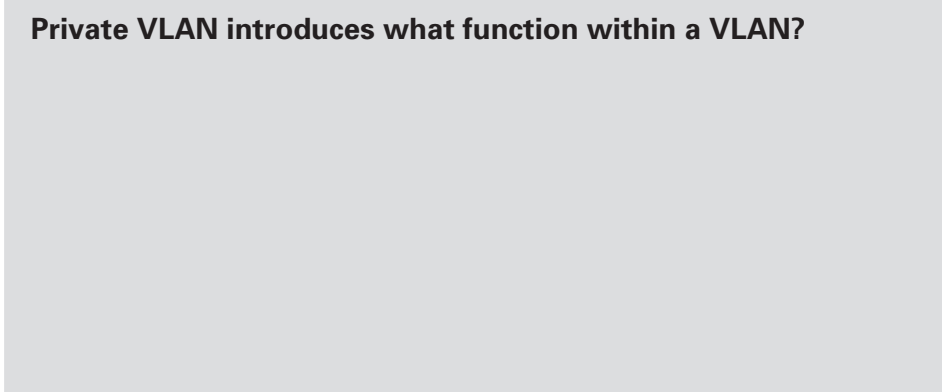
Protect, restrict, and shut down.

Question 24 Answer

The spanning-tree bpdudfilter enable command

Question 25

Private VLAN introduces what function within a VLAN?



Question 26

What is the main objective of a VLAN proxy attack?



Question 25 Answer

Promiscuous, Isolated, and Community ports that control intra-segment communication.

Question 26 Answer

A VLAN proxy attack is an attempt to circumvent private VLAN controls.
