Exam Report: 6.4.7 Practice Questions

Date: 10/15/2019 8:14:15 pm
Time Spent: 3:23

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 8%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Incorrect

You need to keep users in all other departments from accessing the servers used by the finance department.

Which of the following technologies should you use to logically isolate the network?

➡ ○ VLANs

● ~~Subnetting~~

○ NIC teaming

○ MAC filtering

Explanation

A virtual LAN (VLAN) uses switch ports to define a broadcast domain. When you define a VLAN, you assign devices on different switch ports to a separate logical, or virtual, LAN.

NIC teaming is used to combine two or more physical connections into one logical connection and does not isolate networks. While MAC filtering could be used to control access, it is easily bypassed by MAC spoofing. Subnetting is used to divide large networks into smaller networks. Subnetting can be used to isolate sensitive systems, but a subent is not as secure as a VLAN.

References

LabSim for Network Pro, Section 6.4.
[netpro18v5_all_questions_en.exm *NP15_VIRTUAL_LANS_01]

Question 2: Correct

Which of the following are reasons to configure VLANs on a switch as opposed to using switches without VLANs? (Select two.)

□ Increased number of collision domains

➡ ☑ Increased number of broadcast domains

□ Allowing broadcast traffic between subnets

□ Redundant paths between two hosts

➡ ☑ Increased security

Explanation

Create VLANs to increase the number of broadcast domains and implement security. Each

VLAN is in its own broadcast domain. Broadcast traffic within the VLAN goes only to the members of the VLAN. Members of one VLAN can only communicate with members in the same VLAN through the switch. A router or a Layer 3 switch is required to enable inter-VLAN communication.

Using switches increases the number of collision domains because each switch port is its own collision domain. Using VLANs does not offer this additional advantage. Spanning tree lets you have loop-free redundant paths through a switched network. Broadcast traffic does not travel between routers.

References

LabSim for Network Pro, Section 6.4.
[netpro18v5_all_questions_en.exm C802_208 MULTIPLE CHOICE [122]]

▼ Question 3: Incorrect

Which of the following statements describe how VLANs affect broadcast traffic within an internetwork? (Select two.)

□ Broadcast traffic is transmitted to all devices on all VLANs.

□ Devices on separate VLANs share the same subnet address.

➡ □ Broadcast traffic is transmitted only within a VLAN.

□ Broadcast traffic is only transmitted on VLAN1.

➡ □ Devices on the same VLAN have the same subnet address.

Explanation

VLANs allow computers to be grouped into a common broadcast domain regardless of their physical location on the network. Broadcast traffic is seen only by computers belonging to the same VLAN. Devices sharing a VLAN ID must also share the same subnet address so that traffic can be routed between VLANs.

Broadcast traffic is only transmitted to devices belonging to the same VLAN as the device that sent the broadcast. Broadcast traffic is not forwarded to the other VLANs.

References

LabSim for Network Pro, Section 6.4.
[netpro18v5_all_questions_en.exm C802_209 C801 403-29 [33]]

▼ Question 4: Incorrect

Which of the following are true regarding using multiple VLANs on a single switch? (Select two.)

➡ □ The number of broadcast domains increases.

□ The number of broadcast domains decreases.

□ The number of broadcast domains remains the same.

➡ □ The number of collision domains remains the same.

□ The number of collision domains increases.

□ The number of collision domains decreases.

Explanation

When you configure multiple VLANs on a single switch, the number of broadcast domains increases. Each VLAN will be placed in its own broadcast domain. The number of collision domains remains the same. Each switch port is its own collision domain regardless of the number of VLANs configured on the switch.

References

LabSim for Network Pro, Section 6.4.
[netpro18v5_all_questions_en.exm C802_209 C801 403-124 [42]]

▼ Question 5: Incorrect

You can create a virtual LAN using which of the following?

○ Gateway

➡ ○ Switch

○ Router

○ Hub

Explanation

Use a switch to create virtual LANs (VLANs). The various ports on a switch can be assigned to a specific VLAN to create logically distinct networks on the same physical network topology.

Routers, gateways, and hubs are common network devices, but they do not support the creation of VLANs.

References

LabSim for Network Pro, Section 6.4.
[netpro18v5_all_questions_en.exm SP02_3-3 [13]]

▼ Question 6: Incorrect

You manage a network that uses a single switch. All ports within your building connect through the single switch.

In the lobby of your building are three RJ45 ports connected to the switch. You want to allow visitors to plug into these ports to gain internet access, but they should not have access to any other devices on your private network. Employees connected throughout the rest of your building should have both private and internet access.

Which feature should you implement?

○ Port authentication

➡ ○ VLANs

○ NAT

○ DMZ

Explanation

Use VLANs to segregate hosts based on switch ports. You can define two VLANs, one for employees connected throughout the building, and another for the ports in the lobby. The ports in the lobby would have only internet access, while devices connected to ports in the rest of the building could communicate with other devices within the same VLAN.

Use port authentication to control access to the network based on things such as username and password. Port authentication would allow or deny access, but would not restrict access once authenticated or provide any type of access if not authenticated.

A demilitarized zone (DMZ) is a buffer network (or subnet) that sits between the private network and an untrusted network (such as the internet). Network address translation (NAT) modifies the IP addresses in packets as they travel from one network (such as a private network) to another (such as the internet). NAT allows you to connect a private network to the internet without obtaining registered addresses for every host. Hosts on the private network share the registered IP addresses.

References

LabSim for Network Pro, Section 6.4.
[netpro18v5_all_questions_en.exm SP08_2-2 1]

Question 7: Incorrect

You want to reduce collisions by creating separate collision domains and virtual LANs. Which of the following devices should you choose?

○ Router

○ Bridge

➡ ○ Switch

○ Active hub

Explanation

Use a switch to create additional collision domains on a LAN. A switch filters an entire network and creates virtual LANs inside it rather than dividing it into separate internetworks as a router does.

References

LabSim for Network Pro, Section 6.4.
[netpro18v5_all_questions_en.exm NP05_1-6 #36]

Question 8: Incorrect

Your company is a small start-up that has leased office space in a building shared by other businesses. All businesses share a common network infrastructure. A single switch connects all devices in the building to the router that provides internet access.

You would like to make sure that your computers are isolated from computers used by other companies. Which feature should you request to have implemented?

○ Spanning tree

○ Port security

➡ ○ VLAN

○ VPN

Explanation

You should define virtual LANs (VLANs) on the switch. With a VLAN, a port on the switch is associated with a VLAN. Only devices connected to ports that are members of the same VLAN can communicate with each other. Routers are used to allow communication between VLANs if necessary.

Use virtual private network (VPN) to connect two hosts securely through an unsecured network (such as the internet). VPN tunneling protocols protect data as it travels through the unsecured network. Spanning tree is a switch feature that allows for redundant paths between switches. Port security is a method of requiring authentication before a network connection is allowed.

References

LabSim for Network Pro, Section 6.4.
[netpro18v5_all_questions_en.exm NP09_2-7 #MCS2]

Question 9: Incorrect

Which of the following best describes the concept of a VLAN?

➡ ○ Devices on the same network logically grouped as if they were on separate networks.

○ Devices connected by a transmission medium other than cable (such as microwave or radio transmissions).

○ Devices on different networks that can receive multicast packets.

○ Devices connected through the internet that can communicate without using a network address.

○ Devices in separate networks (which means they have different network addresses) logically grouped as if they were in the same network.

Explanation

A VLAN is created by identifying a subset of devices on the same network and logically identifying them as if they were on separate networks. Think of a VLAN as a subdivision of a LAN.

References

LabSim for Network Pro, Section 6.4.
[netpro18v5_all_questions_en.exm NP05_3-8 #7]

▼ Question 10: Incorrect

Which of the following connectivity hardware is used to create a VLAN?

○ Bridge

➡ ○ Switch

○ Hub

○ Router

Explanation

Specialized switches are used to create virtual LANs. The switch must be capable of appending and reading VLAN IDs.

References

LabSim for Network Pro, Section 6.4.
[netpro18v5_all_questions_en.exm NP05_3-8 #24]

▼ Question 11: Incorrect

When you configure VLANs on a switch, which of the following is used to identify a device's VLAN membership?

○ IP address

➡ ○ Switch port

○ MAC address

○ Host name

Explanation

VLAN membership is configured by assigning a switch port to a VLAN. A switch can have multiple VLANs configured on it, but each switch port can only be a member of a single VLAN. All devices connected to a switch port are members of the same VLAN.

References

LabSim for Network Pro, Section 6.4.

[netpro18v5_all_questions_en.exm NP09_3-3 #10]

Question 12: Incorrect

You manage a network with two switches. The switches are connected together through their Gigabit Ethernet uplink ports.

You define VLAN 1 and VLAN 2 on each switch. A device on the first switch in VLAN 1 needs to communicate with a device on the same switch which is in VLAN 2.

What should you configure so that the two devices can communicate?

○ Spanning tree

○ Trunking

○ Mirroring

➡ ○ Routing

○ PoE

Explanation

In a typical configuration with multiple VLANs and a single or multiple switches, workstations in one VLAN will not be able to communicate with workstations in other VLANs. To enable inter-VLAN communication, you will need to use a router (or a Layer 3 switch).

Trunking is used to configure switch ports to carry VLAN traffic between switches or between a router and a switch. If you configured a single router to connect to the switch with a single physical interface, you would have to configure trunking on that interface in addition to routing. Trunking by itself would not enable the two devices to communicate.

Spanning tree is a protocol on a switch that allows the switch to maintain multiple paths between switches within a subnet. The spanning tree protocol runs on each switch and is used to select a single path between any two switches. Mirroring sends traffic from all switch ports to a switch port you designate as the mirrored port. Power over Ethernet (PoE) supplies power to end devices through the RJ45 Ethernet switch port.

References

LabSim for Network Pro, Section 6.4.
[netpro18v5_all_questions_en.exm NP09_3-3 #9]

Question 13: Incorrect

You run a small network for your business that has a single router connected to the internet and a single switch. You keep sensitive documents on a computer that you would like to keep isolated from other computers on the network. Other hosts on the network should not be able to communicate with this computer through the switch, but you still need to access the network through the computer.

Which of the following should you use in this situation?

○ VPN

○ Spanning tree

○ Port security

➡ ○ VLAN

Explanation

You should define virtual LANs (VLANs) on the switch. With a VLAN, a port on the switch is associated with a VLAN. Only devices connected to ports that are members of the same VLAN can communicate with each other. Routers are used to allow communication between VLANs if necessary.

Use a virtual private network (VPN) to connect two hosts securely through an unsecured network (such as the internet). VPN tunneling protocols protect data as it travels through the unsecured network. Spanning tree is a switch feature that allows for redundant paths between switches. Port security is a method of requiring authentication before a network connection is allowed.

References

LabSim for Network Pro, Section 6.4.
[netpro18v5_all_questions_en.exm NP09 2-7 1]