Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/24/2022 8:04:11 pm • Time spent: 00:08

Score: 0% Passing Score: 80%

Question 1: ✕ Incorrect

You are adding switches to your network to support additional VLANs. Unfortunately, the new switches are from a different vendor than the current switches.

Which standard do you need to ensure that the switches are supported?

- 802.11
- 802.1x
- 802.1Q
- 802.3

EXPLANATION

If you want to implement VLANs when using multiple vendors in a switched network, be sure each switch supports the 802.1Q standard.

802.1x defines port-based network access controls.

802.11 defines wireless standards.

802.3 defines Ethernet standards.

REFERENCES

5.12.2 VLAN Facts

q_vlan_facts_802_secp7.question.fex

Question 2: ✕ Incorrect

When configuring VLANs on a switch, what is used to identify which VLAN a device belongs to?

- ➡ Switch port
- Host name
- IP address
- MAC address

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

5.12.2 VLAN Facts

q_vlan_facts_port_secp7.question.fex

Question 3: ✕ Incorrect

Which 802.1Q priority is IP phone traffic on a voice VLAN tagged with by default?

- 8
- 3
- 1
- ➡ 5

EXPLANATION

By default, IP phone traffic on a voice VLAN is tagged with an 802.1Q priority of 5.

REFERENCES

5.12.2 VLAN Facts

q_vlan_facts_priority_secp7.question.fex

Question 4: ✕ Incorrect

The IT manager has asked you to create four new VLANs for a new department. As you are going through the VLAN configurations, you find some VLANs numbered 1002-1005. However, they are not in use.

What should you do with these VLANs?

- ➡ Nothing. They are reserved and cannot be used or deleted.
- Configure them so they can be used on the new network.
- Delete them since they are not being used.
- Renumber them and assign them to ports on the switch.

EXPLANATION

You should do nothing and leave these VLANs alone. VLANs 1002 through 1005 are reserved for backward compatibility with old VLAN implementations, which are no longer being used. You cannot use or delete these VLANs.

These VLANs are reserved and cannot be used on the new network.

You cannot edit these VLANs, and you do not want to assign them to ports on the switch since they cannot be used.

REFERENCES

5.12.2 VLAN Facts

q_vlan_facts_reserved_secp7.question.fex

Question 5: ✕ Incorrect

The IT manager has asked you to create a separate VLAN to be used exclusively for wireless guest devices to connect to.

Which of the following is the primary benefit of creating this VLAN?

- You can control broadcast traffic and create a collision domain for just the wireless guest devices.
- You can load-balance wireless guest network traffic to have a lower priority than the rest of the traffic on the network.
- ➡ You can control security by isolating wireless guest devices within this VLAN.
- You can create a wireless guest network more affordably with a VLAN than you can with a router.

EXPLANATION

The primary benefit of creating a VLAN for wireless guest devices to connect to is it allows you to control security by isolating wireless guest devices within this VLAN. Devices on this VLAN cannot communicate with other devices in other VLANs unless you allow traffic to get through with a router or Layer 3 switch. In this case, you would likely keep this wireless guest VLAN isolated from the rest of your network and only allow traffic from this VLAN to communicate with the internet.

The following are also benefits of creating VLANs in general (but these are not the primary benefit of creating a wireless guest VLAN):

- You can create virtual LANs based on criteria other than physical location (such as workgroup, protocol, or service).
- You can simplify device moves (devices are moved to new VLANs by modifying the port assignment).
- You can control broadcast traffic and create collision domains based on logical criteria.
- You can load-balance network traffic (divide traffic logically rather than physically).

REFERENCES

5.12.2 VLAN Facts

q_vlan_facts_security_secp7.question.fex

Question 6: ✕ Incorrect

A virtual LAN can be created using which of the following?

- Router
- Gateway
- Hub
- Switch

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

5.12.2 VLAN Facts

q_vlan_facts_switch_secp7.question.fex

Question 7: ✕ Incorrect

Which of the following is an appropriate definition of a VLAN?

- A device used to filter WAN traffic.
- ➡ A logical grouping of devices based on service need, protocol, or other criteria.
- A device used to route traffic between separate networks.
- A physical collection of devices that belong together and are connected to the same wire or physical switch.

EXPLANATION

A virtual LAN (VLAN) can be defined as the following:

- A logical collection of devices that belong together and act as if they are connected to the same wire or physical switch.
- A logical grouping of devices based on service need, protocol, or other criteria rather than physical proximity.

REFERENCES

5.12.2 VLAN Facts

q_vlan_facts_vlan_01_secp7.question.fex

Question 8: ✕ 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 RJ-45 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?

- NAT
- Port authentication
- ➡ VLANs
- DMZ

EXPLANATION

Use VLANs to segregate hosts based on switch ports. You could 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 this would not restrict access once authenticated or provide any type of access if not authenticated.

A demilitarized zone is a buffer network, or subnet, that sits between a 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 to another. 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

5.12.2 VLAN Facts

q_vlan_facts_vlan_02_secp7.question.fex

Question 9: ✕ 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.

What should you use for this situation?

- Port security
- VPN
- ➡ VLAN
- Spanning Tree Protocol

EXPLANATION

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 Protocol 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

5.12.2 VLAN Facts

q_vlan_facts_vlan_03_secp7.question.fex

Question 10: ✕ Incorrect

You are creating a VLAN for voice over IP (VoIP). Which command should you use?

- **switchport voice vlan [*number*]**
- **switchport vlan voip [*number*]**
- **switchport vlan voice [*number*]**
- **switchport voip vlan [*number*]**

EXPLANATION

To create a voice VLAN, use the **switchport voice vlan [*number*]** command.

REFERENCES

5.12.2 VLAN Facts

9.9.5 Embedded and Specialized Systems Facts

q_vlan_facts_voip_secp7.question.fex