Exam Report: 16.1.8 Practice Questions

Date: 12/8/2019 12:53:23 am
Time Spent: 8:34

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 7%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

Which of the following devices accepts incoming client requests and distributes those requests to specific servers?

○ IPS

○ CSU/DSU

○ Caching engine

○ Media converter

➡ ● Load balancer

Explanation

A load balancer is a device that accepts incoming client requests and distributes those requests to multiple servers. One goal of load balancing is to distribute client requests evenly between multiple servers to improve performance.

A CSU/DSU is a device that converts the signal received from the WAN provider into a signal that can be used by equipment at the customer site. An intrusion prevention system (IPS) can detect and respond to security events. A caching engine saves copies of frequently used content, eliminating the need to download the content each time it is requested. A media converter converts signals used on one media type (such as twisted pair Ethernet) to another media type (such as fiber optic).

References

LabSim for Network Pro, Section 16.1.
[netpro18v5_all_questions_en.exm NP09_3-2 #4]

Question 2: Incorrect

Which of the following devices is used on a LAN and offers guaranteed bandwidth to each port?

➡ ○ Switch

● ~~Hub~~

○ Router

○ Bridge

Explanation

A switch offers guaranteed bandwidth to each port.

References

LabSim for Network Pro, Section 16.1.
[netpro18v5_all_questions_en.exm NP05_1-6 #52]

Question 3: Incorrect

Drag the broadcast domain property on the left to the appropriate network device(s) on the right. Each property can be used more than once.

Hub

✓ Single broadcast domain

Unmanaged switch

✓ Single broadcast domain

802.11n wireless access point

~~Multiple broadcast domains~~ Single broadcast domain

Router

✓ Multiple broadcast domains

Bridge

✓ Single broadcast domain

Repeater

✓ Single broadcast domain

Layer 3 switch

✓ Multiple broadcast domains

Explanation

A broadcast domain is a logical division of a network. All network hosts within the same broadcast domain can reach each other using broadcasts at the Data Link layer. All network hosts connected to the following Layer 2 network devices are members of the same broadcast domain:

- Hubs
- Unmanaged switches (because they do not support VLANs)
- 802.11 wireless access points
- Bridges
- Repeaters

Layer 3 devices are used to define boundaries between broadcast domains, such as a router or a layer 3 switch. A managed switch with VLANs implemented also creates separate broadcast domain for each VLAN.

References

LabSim for Network Pro, Section 16.1.
[netpro18v5_all_questions_en.exm D&D1]

Question 4: Incorrect

Match the class of service (COS) priority on the left with its corresponding value on the right.

0

Best effort (default)

1

Background

2

Excellent effort

3

□ Critical applications

4

□ Video (< 100ms latency)

5

□ Voice (< 10ms latency)

6

□ Internetwork control

7

□ Network control

Explanation

Class of service (COS) marks individual frames with a priority value between 0 and 7:

- 0 – Best effort (default)
- 1 – Background
- 2 – Excellent effort
- 3 – Critical applications
- 4 – Video (< 100ms latency)
- 5 – Voice (< 10ms latency)
- 6 – Internetwork control
- 7 – Network control

References

LabSim for Network Pro, Section 16.1.
[netpro18v5_all_questions_en.exm *NP15_OPTIMIZATION_01]

Question 5: Incorrect

Which of the following statements about DSCP are true? (Select two.)

☑ ~~Priority values are assigned by the network switch.~~

☑ ~~A priority value between 0 and 7 is used.~~

➡ □ Classification occurs at Layer 3.

□ Classification occurs at Layer 2.

➡ □ The DiffServ field is used to add precedence values.

Explanation

The Differentiated Services Code Point (DSCP) classification system has the following characteristics:

- Classification occurs at Layer 3.
- Precedence values are inserted in the DiffServ field of an IP packet.
- Up to 64 different classifications are possible, but most networks use only the following classes:
  - Default – best effort
  - Expedited Forwarding (EF) – low loss, low latency
  - Assured Forwarding (AF) – assured delivery under prescribed conditions
  - Class Selector – maintains backward compatibility with IP Precedence field

References

LabSim for Network Pro, Section 16.1.
[netpro18v5_all_questions_en.exm *NP15_OPTIMIZATION_04]

Question 6: Incorrect

Which Class of Service (COS) priority value should be assigned to a video conference call?

○ 1

○ 7

○ 6

○ 3

○ 0

➡ ○ 4

○ 5

○ 2

Explanation

A priority value of 4 should be assigned to the video data stream. Each COS priority values specifies a specific traffic type:

- 0 – Best effort (default)
- 1 – Background
- 2 – Excellent effort
- 3 – Critical applications
- 4 – Video (< 100ms latency)
- 5 – Voice (< 10ms latency)
- 6 – Internetwork control
- 7 – Network control

References

LabSim for Network Pro, Section 16.1.
[netpro18v5_all_questions_en.exm *NP15_OPTIMIZATION_06]

Question 7: Incorrect

You have a website that uses multiple servers for different types of transactions. For example, one server is responsible for static web content, while another is responsible for secure transactions.

You would like to implement a device to speed up access to your web content. The device should be able to distribute requests between the various web servers using specialized hardware, and not just a software configuration. In addition, SSL sessions should use the hardware components in the device to create the SSL sessions.

Which type of device should you choose?

○ Proxy server

○ Bandwidth shaper

○ Circuit-level gateway

➡ ○ Content switch

Explanation

Use a content switch to perform these functions. Switches use specialized hardware modules to perform common tasks. For example, you can have a switch with a special hardware module that is used for SSL connections. Using the hardware module in a specialized switch is faster than using the CPU or software in another device.

A bandwidth shaper (also called a traffic shaper) is a device that is capable of modifying the flow of data through a network in response to network traffic conditions. A proxy server is a server that sits between a client and a destination device and can be configured to filter requests based on URL. However, a proxy server uses software, not hardware to perform these tasks. A circuit-level gateway uses the session information to make filtering decisions for allowed or denied traffic.

References

LabSim for Network Pro, Section 16.1.
[netpro18v5_all_questions_en.exm NP09_3-2 #8]

Question 8: Incorrect

Which type of switch optimizes network performance by using ASIC to perform switching at wire speed?

○ Layer 2 switch

➡ ○ Multilayer switch

○ Unmanaged switch

○ Layer 1 switch

Explanation

A multilayer switch uses specialized hardware called an application-specific integrated circuit (ASIC) to perform switching functions in hardware rather than using the CPU and software. ASIC allows switches to perform the switching function at wire speed.

Layer 2 switches use the CPU and software to forward frames. Unmanaged switches are also called Layer 2 switches. A Layer 1 switch is another name for a hub, which does not perform any traffic inspection; received packets are sent out on all ports.

References

LabSim for Network Pro, Section 16.1.
[netpro18v5_all_questions_en.exm *NP15_OPTIMIZATION_10]

Question 9: Incorrect

Which of the following components do switches use to optimizes network performance by performing switching operations in hardware rather than using the CPU and software?

➡ ○ An application-specific integrated circuit

○ Ethernet bonding

○ A traffic shaper

○ A caching engine

Explanation

Switches use specialized hardware called an application-specific integrated circuit (ASIC), which performs switching functions in hardware rather than using the CPU and software. ASIC allows switches to perform the switching function at wire speed.

Caching engines are used to store frequently accessed content for faster access; content is retrieved from the local network instead of the internet. Ethernet bonding is used to create two or more physical connections to the same network by bonding NICs or switch ports together; Ethernet bonding provides increased performance and some fault tolerance. A traffic shaper (also called a bandwidth shaper) is a device that is capable of modifying the flow of data through a network in response to network traffic conditions.

References

LabSim for Network Pro, Section 16.1.
[netpro18v5_all_questions_en.exm *NP15_OPTIMIZATION_12]

Question 10: Incorrect

What is the purpose of using Ethernet bonding? (Select two.)

➡ □ Increases network performance.

➡ □ Provides a failover solution for network adapters.

□ Provides increased bus speeds.

□ Increases read and write operations between the system bus and network adapters.

□ Enables Dual Remote Access (DRA) over a WAN link.

Explanation

In a true fault tolerant strategy, all system components must be considered. Ethernet bonding (also called adapter teaming) is a fault tolerant strategy that uses multiple network adapters configured in a failover solution. In the event of a NIC failure, other adapters will automatically provide link redundancy. Multiple adapters can also increase performance by distributing the network load between adapters.

References

LabSim for Network Pro, Section 16.1.
[netpro18v5_all_questions_en.exm NP05_3-11 #130]

▼ **Question 11:** Incorrect

A web server on your network hosts the public website for your company. You want to make sure that a failure of the NIC in the server does not prevent the website from being accessible on the internet.

Which solution should you implement?

○ Spanning tree

○ Traffic shaping

○ QoS

➡ ○ Ethernet bonding

Explanation

Ethernet bonding (also called NIC teaming) logically groups two or more physical connections to the same network. If one NIC fails, the second NIC with a connection to the same network can still be used.

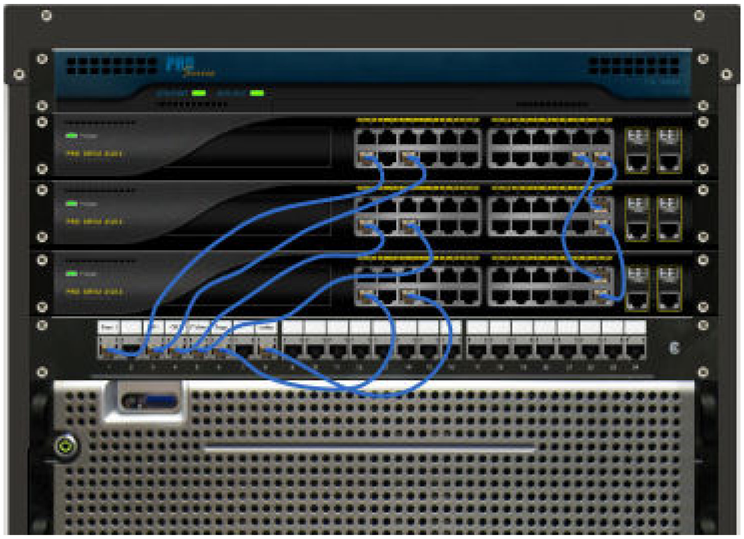
Spanning tree is a protocol on a switch that allows the switch to maintain multiple paths between switches within a subnet. A traffic shaper (also called a bandwidth shaper) is a device that is capable of modifying the flow of data through a network in response to network traffic conditions. Quality of Service (QoS) refers to a set of mechanisms that try to guarantee timely delivery or minimal delay of important or time-sensitive communications. QoS is particularly important when implementing Voice over IP (VoIP), Video over IP, or online gaming, where delay or data loss make the overall experience unacceptable.

References

LabSim for Network Pro, Section 16.1.
[netpro18v5_all_questions_en.exm NP09_4-5 #MCS1]

▼ **Question 12:** Incorrect

This question includes an image to help you answer the question. Close



A new assistant network administrator was recently hired by your organization to relieve some of your workload.

You assigned the assistant network administrator to replace a defective patch cable that connected port 1 on your patch panel to one of your network switches. You noticed that it took him an unusually long time to complete this task. Once done, users almost immediately began to report that the network had gone down.

Upon entering the server room, you see that the assistant administrator has configured your network rack as shown in the Exhibit.

What should you do? (Choose two. Each response is a complete solution.)

□ Enable port security on each switch port.

□ Connect the patch panel to the switches with red cross-over cables.

□ Replace the patch cables connecting the switches together with red cross-over cables.

□ Consolidate all patch cables from the patch panel to a single switch.

➡ □ Enable STP on each switch.

➡ □ Remove the patch cable connecting the first switch to the third switch.

Explanation

The assistant administrator in the scenario appears to have connected the switches together in a way that creates a bridge loop (sometimes called a switching loop). Notice the following:

- Switch1 is connected to Switch2 and Switch3
- Switch2 is connected to Switch1 and Switch3
- Switch3 is connected to Switch1 and Switch2

A bridge loop occurs when there are multiple Layer 2 paths between two network hosts. This usually results in a broadcast storm as the switches repeatedly rebroadcast all broadcast messages, flooding the network.

To fix this issue, you can do one of the following:

- Remove the patch cable connecting the first switch to the third switch. This will break the switching loop and stop the broadcast storm.
- Enable STP on each switch. STP ensures there is only one active path between switches. Switch ports that are part of that path are placed in a forwarding state. Switch ports that are part of redundant but unused paths are placed in a blocking (non-forwarding) state. When an active path goes down, the STP automatically recovers and activates the backup ports necessary to provide continued connectivity.

Consolidating all patch cable from the patch panel to a single switch will not break the bridge loop, nor would enabling port security on each switch port. It is not necessary to replace the patch cables connecting the switches together with cross-over cables, as most switches have Auto-MDIX enabled by default.

References

LabSim for Network Pro, Section 16.1.
[netpro18v5_all_questions_en.exm MCM1]

▼ **Question 13:** Incorrect

Your company leases a very fast internet connection and pays for it based on usage. You have been asked by the company president to reduce internet line lease costs. You want to reduce the amount of web pages that are downloaded over the leased connection without decreasing performance.

What is the best way to do this?

➡ ○ Install a proxy server.

○ Install a packet-filtering firewall.

○ Install modems in employees' computers.

○ Implement NAT.

Explanation

A proxy server caches frequently visited websites in its cache. It can fulfill client requests from its cache instead of retrieving the information from the internet.

References

LabSim for Network Pro, Section 16.1.
[netpro18v5_all_questions_en.exm NP05_3-6 #17]

▼ **Question 14:** Incorrect

Your organization uses a time-keeping application that only runs on Windows 2000 and does not run on newer OS versions. Because of this, there are several Windows 2000 workstations on your network.

Last week you noticed unusual activity on your network coming from the Windows 2000 workstations. After further examination, you discover that the Windows 2000 workstations were the victim of a malicious attack and were being used to infiltrate the network.

You find out that the attackers were able to gain access to the workstations because of the legacy operating system being used. The organization still needs to use the Windows 2000 workstations, which need to be connected to the internet, but you want to make sure the network is protected from future events.

Which solution should you implement to protect the network while also allowing operations to continue as normal?

○ Create a dedicated network for the Windows 2000 workstations that is completely isolated from the rest of the network, including a separate internet connection.

○ Install anti-virus software on the Windows 2000 workstations and configure Windows to automatically download and install updates.

➡ ○ Configure VLAN membership so that the Windows 2000 workstations are on their own VLAN.

○ Implement a host-based firewall on each Windows 2000 workstation and configure Windows to automatically download and install updates.

Explanation

The best solution is to place the Windows 2000 workstations in their own VLAN. If you use VLAN network segmentation, the workstations will still have access to the internet, but network access can be heavily restricted. This greatly reduces the damage a workstation can cause if it were to become compromised again.

Legacy operating systems, such as Windows 2000, are easy targets for attackers. This is because legacy operating systems use outdated protocols and have known exploits. Installing an anti-virus or host-based firewall would do very little to protect the entire network. In addition, legacy operating system are no longer supported with updates or patches, so enabling automatic updates would offer no benefit. Creating a dedicated network for the workstations would affect normal operations and also increase network management load.

References

LabSim for Network Pro, Section 16.1.
[netpro18v5_all_questions_en.exm *NP15_NETWORK_SEGMENTATION_01]

▼ **Question 15:** Incorrect

You are in the process of implementing a network access protection (NAP) infrastructure to increase your network's security.

You are currently configuring the remediation network that non-compliant clients will connect to in order to become compliant. The remediation network needs to be isolated from the secure network.

Which technology should you implement to accomplish this task?

○ Virtual private networking (VPN)

○ Port security

○ Data encryption using PKI

➡ ○ Network segmentation

Explanation

Implementing network segmentation would isolate the remediation server from the rest of the network while still allowing the remediation server to contact the NAP infrastructure.

Virtual private networking (VPN) is used to create a secure connection between two hosts or two sites over an unsecured network. Encrypting data transmissions using PKI would only protect transmitted data, not isolate the remediation network. Port security is used to identify allowed and denied devices that connect to a switch port and would not isolate the remediation network.

References

LabSim for Network Pro, Section 16.1.
[netpro18v5_all_questions_en.exm *NP15_NETWORK_HARDENING_03]