

Overall Performance



View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

Question 1: Incorrect

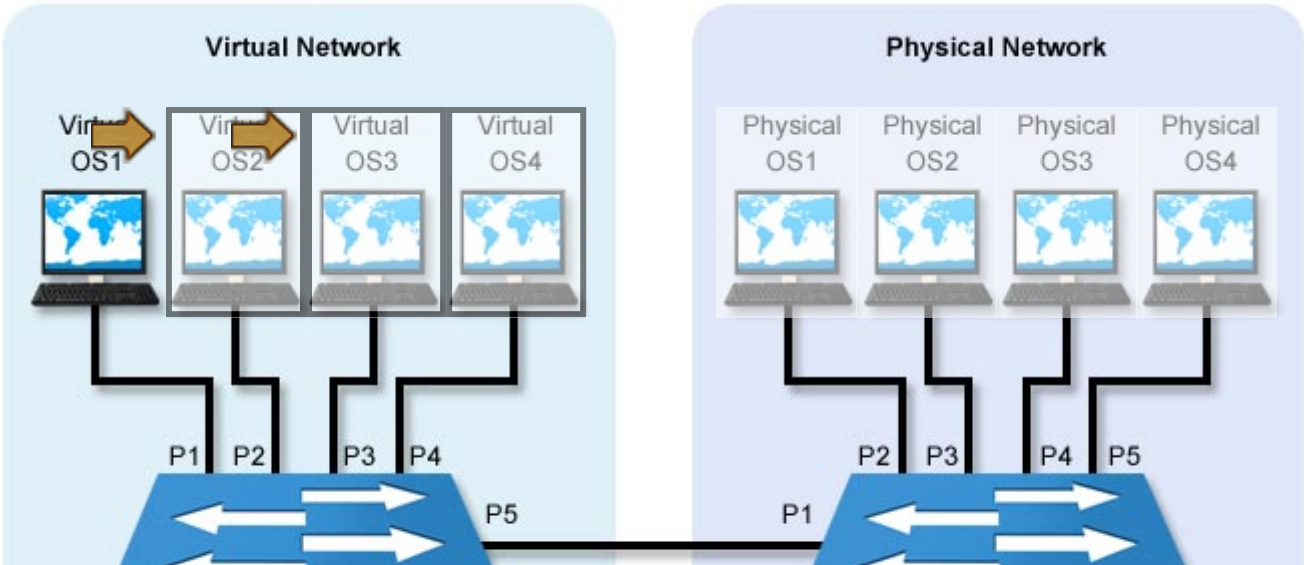
You have configured a virtual network that includes the following virtual components:

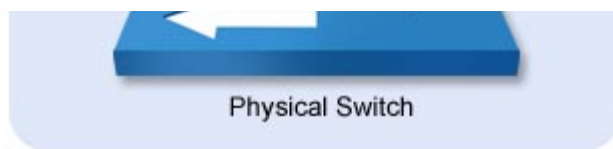
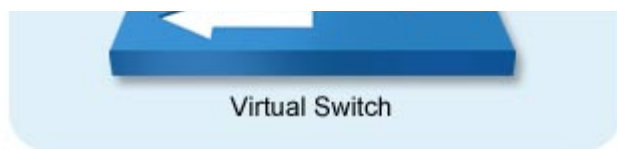
- Four virtual machines (Virtual OS1, Virtual OS2, etc.)
- One virtual switch

The virtual switch is connected to a physical network to allow the virtual machines to communicate with the physical machines out on the physical network.

Given the port configuration for the virtual switch and the physical switch in the table below, click on all of the virtual and physical machines that Virtual OS1 can communicate with.

Device	Port	Port Assignment
Virtual Switch	P1	Virtual Network1
	P2	Virtual Network1
	P3	Virtual Network1
	P4	Physical Network
	P5	Physical Network
Physical Switch	P1	Physical Network
	P2	Physical Network
	P3	Physical Network
	P4	Physical Network
	P5	Physical Network





Explanation

Virtual OS1 can communicate with the following machines:

- Virtual OS2
- Virtual OS3

The virtual switch port configuration allows these three virtual machines to communicate as if the machines were part of a real physical network. Virtualized networks allow virtual servers and desktops to communicate with each other and can also allow communication with network devices out on the physical network via the host operating system. Virtual networks typically include the following components:

- Virtual switches allow multiple virtual servers and/or desktops to communicate on virtual network segments and/or the physical network. Virtual switches are often configured in the hypervisor.
- Virtual network adapters are created and assigned to a desktop or server in the hypervisor.
- Multiple network adapters can be assigned to a single virtual machine.
- Each network adapter has its own MAC address.
- Each network adapter is configured to connect to only one network at a time (meaning a virtual network or the physical network, but not both).

Virtual OS4 and all of the other Physical OS machines are configured to communicate on the physical network.

References

LabSim for Network Pro, Section 9.4.

[netpro18v5_all_questions_en.exm NP15_VIRTUALIZATION_03]

▼ Question 2: Correct

You need to provide DHCP and file share services to a physical network. These services should be deployed using virtualization. Which type of virtualization should you implement?

- ☐ Virtual networks
- ☐ Virtual desktops
- ➡ ☒ Virtual servers
- ☐ Network as a service (NaaS)

Explanation

Server virtualization runs multiple instances of a server operating system on a single physical computer. With server virtualization, you can migrate servers on older hardware to newer computers or add virtual servers to computers with extra unused hardware resources.

Virtual desktops do not provide DHCP services. Virtual networks allow virtual servers and desktops to communicate with each other, and they can also allow communication with network devices out on the physical network via the host operating system. Network as a service (NaaS) servers and desktops that are all virtualized and managed by a contracted third party.

References

LabSim for Network Pro, Section 9.4.

[netpro18v5_all_questions_en.exm NP15_VIRTUAL_NETWORKING_01]

Question 3: Incorrect

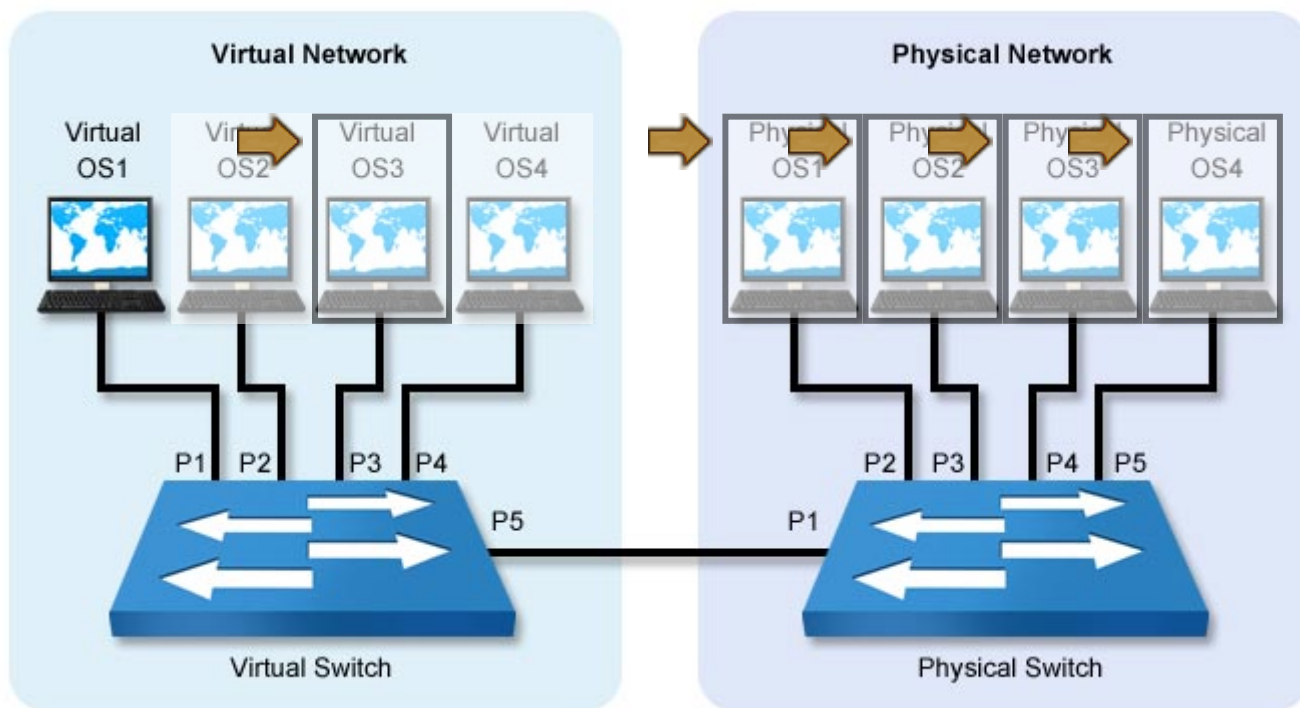
You have configured a virtual network that includes the following virtual components:

- Four virtual machines (Virtual OS1, Virtual OS2, etc.)
- One virtual switch

The virtual switch is connected to a physical network to allow the virtual machines to communicate with the physical machines out on the physical network.

Given the port configuration for the virtual switch and the physical switch in the table below, click on all of the virtual and physical machines that Virtual OS1 can communicate with.

Device	Port	Port Assignment
Virtual Switch	P1	Virtual Network1
	P2	Virtual Network2
	P3	Virtual Network1
	P4	Virtual Network2
	P5	Physical Network, Virtual Network1
Physical Switch	P1	Physical Network
	P2	Physical Network
	P3	Physical Network
	P4	Physical Network
	P5	Physical Network

**Explanation**

Virtual OS1 can communicate with the following machines:

- Virtual OS3
- Physical OS1

- Physical OS3
- Physical OS4

The virtual switch port configuration allows Virtual OS1 to communicate with machines on Virtual Network1 and the physical network. P5 on the virtual switch is configured to allow communication between the virtual and physical machines as if they were on the same real physical network.

Virtualized networks allow virtual servers and desktops to communicate with each other, and can also allow communication with network devices out on the physical network via the host operating system. Virtual networks typically include the following components:

- Virtual switches allow multiple virtual servers and/or desktops to communicate on virtual network segments and/or the physical network. Virtual switches are often configured in the hypervisor.
- Virtual network adapters are created and assigned to a desktop or server in the hypervisor.
- Multiple network adapters could be assigned to a single virtual machine.
- Each network adapter has its own MAC address.
- Each network adapter is configured to connect to only one network at a time (meaning a virtual network or the physical network, but not both).

Virtual OS2 and Virtual OS4 belong to Virtual Network2 and are only able to communicate with each other.

References

LabSim for Network Pro, Section 9.4.

[netpro18v5_all_questions_en.exm NP15_VIRTUAL_NETWORKING_03]

▼ Question 4: Correct

You are an application developer. You use a hypervisor with multiple virtual machines installed to test your applications on various operating system versions and editions.

Currently, all of your testing virtual machines are connected to the production network through the hypervisor's network interface. You are concerned that the latest application you are working on could adversely impact other network hosts if errors exist in the code.

To prevent problems, you decide to isolate the virtual machines from the production network. However, they still need to be able to communicate directly with each other.

What should you do? (Select two. Each response is one part of the complete solution.)

- ➡ ☒ Connect the virtual network interfaces in the virtual machines to the virtual switch.
- ☐ Disable the switch port that the hypervisor's network interface is connected to.
- ☐ Disconnect the network cable from the hypervisor's network interface.
- ☐ Create a new virtual switch configured for bridged (external) networking.
- ➡ ☒ Create a new virtual switch configured for host-only (internal) networking.
- ☐ Create MAC address filters on the network switch that block each virtual machine's virtual network interfaces.

Explanation

To allow the virtual machines to communicate with each other while isolating them from the production network, complete the following:

- Create a new virtual switch configured for host-only (internal) networking.
- Connect the virtual network interfaces in the virtual machines to the virtual switch.

Creating a bridged virtual switch would still allow the virtual machines to communicate on the production network through the hypervisor's network interface. Disconnecting the hypervisor's network cable, blocking the virtual machine's MAC addresses, or disabling the hypervisor's switch port would isolate the virtual machines from the production network, but would also prevent them from communicating with each other.

References

LabSim for Network Pro, Section 9.4.

[netpro18v5_all_questions_en.exm NP15_VIRTUAL_NETWORKING_04]

▼ Question 5: Correct

Match the virtualization feature on the right with the appropriate description on the left.

Flexibility

✓ Moving virtual machines between hypervisor hosts.

Testing

✓ Verifying that security controls are working as designed.

Server consolidation

✓ Performing a physical-to-virtual migration (P2V).

Sandboxing

✓ Isolating a virtual machine from the physical network.

Explanation

Some of the advantages and features of virtualization include the following:

- Flexibility: Because they are self-contained, virtual machines are easy to move between hypervisor hosts as needed.
- Testing: Virtual machines can be configured in a lab environment that mirrors your production network for testing purposes, such as testing security controls to verify that they are working as designed.
- Server consolidation: Server consolidation allows you to move physical systems onto just a few hypervisors with many virtual machines. A physical-to-virtual migration (P2V) moves an operating system off physical hardware and onto a virtual machine.
- Isolation: A sandboxed virtual machine is isolated from the physical network to allow testing to be performed without impacting the production environment.

References

LabSim for Network Pro, Section 9.4.

[netpro18v5_all_questions_en.exm NP15_VIRTUAL_NETWORKING_05]

▼ Question 6: Correct

You are responsible for maintaining Windows workstation operating systems in your organization. Recently, an update from Microsoft was automatically installed on your workstations that caused an in-house application to stop working.

To keep this from happening again, you decide to test all updates on a virtual machine before allowing them to be installed on production workstations.

Currently, none of your testing virtual machines has a network connection. However, they need to be able to connect to the update servers at Microsoft to download and install updates.

What should you do? (Select two. Each response is one part of the complete solution.)

☐ Disable the switch port that the hypervisor's network interface is connected to.

➡ ☒ Create a new virtual switch configured for bridged (external) networking.

☐ Create a new virtual switch configured for host-only networking.

☐ Create a new virtual switch configured for internal networking.

➡ ☒ Connect the virtual network interfaces in the virtual machines to the virtual switch.

Explanation

To allow the virtual machines to communicate with the Microsoft update servers on the internet, complete the following:

- Create a new virtual switch configured for bridged (external) networking.
- Connect the virtual network interfaces in the virtual machines to the virtual switch.

Creating an internal or host-only virtual switch would not allow the virtual machines to communicate on the production network through the hypervisor's network interface. Disabling the hypervisor's switch port would also isolate the virtual machines from the production network.

References

LabSim for Network Pro, Section 9.4.

[netpro18v5_all_questions_en.exm NP15_VIRTUAL_NETWORKING_06]

▼ Question 7: Correct

What key advantage does a virtual router have over a physical router?

☐ Allows the virtual router redundancy protocol (VRRP) to be used.

➡ ☒ Multiple networks can be connected to a single interface.

☐ Faster routing performance.

☐ Routing protocols are not necessary for routing data between networks.

Explanation

The key advantage of a virtual router is that it can support multiple networks on a single router interface. It does this by using a different routing table for each network. Physical routers are limited to a single network on each interface.

Like physical routers, virtual routers use routing protocols to route data between networks. The virtual router redundancy protocol is used by physical routers to specify backup routers in the case of a failure. Virtual routers do not offer significant performance increases.

References

LabSim for Network Pro, Section 9.4.

[netpro18v5_all_questions_en.exm *NP15_VIRTUAL_NETWORKING_07]

▼ Question 8: Correct

You want to be able to monitor and filter VM-to-VM traffic within a virtual network.

What should you do?

☐ Define VLAN memberships on each VM.

☐ Create a virtual router with VRF technology.

➡ ☒ Implement a virtual firewall within the hypervisor.

☐ Route VM-to-VM traffic through a physical firewall and back to the virtual network.

Explanation

Virtualized hosts are susceptible to the same network exploits as physical network hosts and need to be protected by a firewall. By implementing a virtual firewall within the hypervisor itself, you can monitor and filter traffic on the virtual network as it flows between virtual machines.

While routing VM-to-VM traffic through a physical firewall would work, it is very inefficient. A virtual router with VRF is used to create multiple networks from a single router interface.

Configuring VLAN membership would not allow you to monitor and filter traffic.

References

LabSim for Network Pro, Section 9.4.

[netpro18v5_all_questions_en.exm *NP15_VIRTUAL_NETWORKING_08]

▼ Question 9: Correct

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

- ☐ The type of NIC installed in the physical machine determines the type of virtual NIC that is emulated.
- ➡ ☒ Multiple virtual NICs can be added to a virtual machine.
- ☐ Virtual NICs don't have a MAC address.
- ➡ ☒ Virtual NICs need the appropriate driver installed to function.
- ☐ Virtual NICs can only communicate with other virtual NICs.

Explanation

Within each virtual machine, you can configure one or more virtual network interfaces, which function similarly to physical network interfaces. Virtual interfaces use Ethernet standards to transmit and receive frames on the network. The operating system within the virtual machine must have the appropriate driver installed to support the virtual network interface, just as with a physical network interface.

When you configure a virtual network interface within a virtual machine's configuration, you can specify:

- The type of physical network interface to emulate. This allows the best possible driver support from the operating system within the virtual machine.
- A MAC address. Most hypervisors automatically assign a MAC address to each virtual network interface. Some hypervisors allow you to use a custom MAC address if needed.
- The network to connect to. Most hypervisors allow you to define many different virtual networks.
- When you configure a virtual network interface, you will select which virtual network you want it to be connected to.

References

LabSim for Network Pro, Section 9.4.

[netpro18v5_all_questions_en.exm *NP15_VIRTUAL_NETWORKING_09]