9.4.5 Virtual Networking Facts

Virtualized networks allow virtual servers and desktops to communicate with each other. They can also be configured to allow communications with devices on the physical network. The following table describes the components of a virtual network.

Implementation	Description
Virtual Network Interfaces	Within each virtual machine, you can configure one or more virtual network interfaces, which function in much the same manner as 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 for the best possible driver support by the operating system within the virtual machine. ▪ A MAC address. Most hypervisors automatically assign a MAC address to each virtual network interface. However, 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.
Virtual Switches	A virtual switch allows one virtual machine to communicate with another in much the same way that a physical switch allows physical hosts to communicate with each other. Virtual switches are typically implemented in two ways: ▪ As software that is integrated within the hypervisor. This is sometimes called software-defined networking (SDN). ▪ Within the firmware of the hypervisor hardware. A virtual switch functions in the same manner as a physical switch. After initially coming online, a virtual switch floods each frame it receives until it builds a table that identifies which MAC addresses are connected to each port. When the table is done, the switch can intelligently forward frames to the port where the destination host is connected.
Virtual VLANs	Most virtual switch implementations support VLANs. You can define VLANs within the virtual switch and associate specific hosts with a specific VLAN. However, because virtual hosts are not physically connected to the switch with cables, VLAN membership is defined within the configuration of each virtual machine. The VLAN configuration of most virtual switches is compatible with the VLAN configuration used by most hardware switches. This allows VLAN information to be trunked from the virtual switch to switches on the physical network, enabling a VLAN to span both physical and virtual networks.
Virtual Routers	You can use virtualization technology to create virtual routers. To do this, a router must support virtual routing and forwarding (VRF) technology. VRF allows a router to host multiple routing tables simultaneously. A physical router can support only a single network on each router interface. However, a virtual router can support multiple networks on each router interface. A different routing table is used for each network. This is useful in situations where multiple virtual networks exist on the same physical network. As with physical routers, a routing protocol is used by the virtual router to route data between networks.
Virtual Firewalls	Virtualized hosts are susceptible to the same network exploits as physical network hosts and need to be protected by a firewall. Protecting communications between virtual hosts is challenging because the data never leaves the virtual network, so it can't be protected with a physical firewall. One strategy for protecting virtual machines with a firewall is to route virtual machine-to-virtual machine traffic out of the virtual network and onto the physical network, where a physical firewall can be used to filter the traffic. A better strategy is to implement a virtual firewall within the hypervisor itself to monitor and filter traffic on the virtual network as it flows between virtual machines.
Jumbo Frames	*Jumbo frames* are Ethernet frames with more than 1500 bytes of payload. Jumbo frames can carry up to 9000 bytes of payload, but variations exist. Many Gigabit Ethernet switches and Gigabit Ethernet network interface cards support jumbo frames. Each Ethernet frame received requires that the network hardware and software process it. Increasing the frame size makes a large amount of data transferable with less effort, reducing CPU utilization and increasing throughput by reducing the number of frames needing processing and reducing the total overhead byte count of all the frames sent.