9.3.3 SDN Facts

This lesson covers the following topics:

- Software defined networking (SDN)
- SDN advantages and disadvantages

Software Defined Networking (SDN)

Software defined networking (SDN) is a recent technology that allows network and security professionals to manage, control, and make changes to a network. The idea is that network engineers are able to use software to configure and intelligently control the network rather than relying on the individual static configuration files that are located on each network device.

SDN uses a controller to manage the devices. The controller is software that is able to inventory hardware components in the network, gather network statistics, make routing decisions based on gathered data, and facilitate communication between devices from different vendors. It can also be used to make wide-spread configuration changes on just one device.

The SDN architecture consists of three layers. The table below shows the functions:

SDN Layer	Function
Application layer	The Application layer communicates with the Control layer through what is called the northbound interface. These are sometimes called northbound APIs.
Control layer	The Control layer receives its requests from the Application layer and then provides the Physical layer with its configuration and instructions.
Physical layer	The Physical layer, also known as the Infrastructure layer, communicates to the Control layer through the southbound interface. The individual networking devices use southbound APIs to communicate with the control plane and vice versa. Even though this layer is called the Physical layer, it is where both physical and virtual network devices sit.

SDN Advantages and Disadvantages

Some advantages of SDN include:

- Centralized management
- More granular control
- Lower overall cost and labor
- Give new life to old networking hardware
- Gather network information and statistics
- Facilitate communication between hardware from different vendors

Some disadvantages of SDN include:

- Is currently a new technology
- Lack of vendor support

- Standards are still being developed
- Centralized control opens a new target for security threats