2.1.4 Networking Facts

A *network* is a group of computers that can share information through interconnections.

This lesson covers the following topics:

- Network components
- Network benefits
- Network classification
- Dynamic Multipoint Virtual Private Networks (DMVPNs)

Network Components

A network is made up of the following components:

- Computers - these are often called nodes or hosts.
- Transmission media - a path for electrical signals between devices.
- Network interfaces - devices that send and receive electrical signals.
- Protocols - rules or standards that describe how hosts communicate and exchange data.

Network Benefits

Despite the costs of implementation and maintenance, networks save organizations money by allowing them to:

- Consolidate (centralize) data storage.
- Share peripheral devices (such as printers).
- Increase internal and external communications.
- Increase productivity and collaboration.

Network Classification

There are several ways to classify networks. The following table lists several ways to identify networks by types and classifications.

Type	Classification	Description
Host role	Peer-to-peer	In a *peer-to-peer* network, each host can provide network resources to other hosts or use resources located on other hosts. Each host providing resources controls access to the resources. Advantages of peer-to-peer networks include: • Easy implementation • Inexpensive Disadvantages of peer-to-peer networks include: • Difficult to expand (not scalable) • Difficult to support • Lack centralized control • No centralized storage
	Client-server	In a *client-server* network, hosts have specific roles. For example, some hosts are assigned server roles that allow them to provide network resources to other hosts. Other hosts are assigned client roles that allow them to consume network resources. Advantages of client-server networks include the following: • Easy to expand (scalable) • Easy to support • Centralized services • Easy to back up Disadvantages of client-server networks include the following: • Expensive server operating systems

- Extensive advanced planning required

Geography	Personal area network (PAN)	A *personal area network* is a small network used for communicating between personal devices. For example, a PAN may include a notebook computer, a wireless headset, a wireless printer, and a smart phone. A PAN is limited in range to only a few feet. A PAN is typically created using Bluetooth wireless technologies.
	Local area network (LAN)	A *local area network* is a network in a small geographic area, like an office. A LAN typically uses wires to connect systems together.
	Wireless local area network (WLAN)	A *wireless LAN* covers an area that is roughly the same size as a standard LAN. However, it uses radio signals instead of wires to connect systems together.
	Wide area network (WAN)	A *wide area network* is a group of LANs that are geographically isolated and connected to form a large internetwork.
	Metropolitan area network (MAN)	A *metropolitan area network* is a network that covers an area as small as a few city blocks to as large as an entire metropolitan city. MANs are typically owned and managed by a city as a public utility. Be aware that many IT professionals do not differentiate between a wide area network and a MAN as they use the same network technologies.
	Campus area network (CAN)	A *campus area network* is a computer network made up of an interconnection of local area networks within a limited geographical area, such as a university's campus. Most of the networking components, such as the transmission media, switches, and routers are owned by the campus tenant.
Software-defined wide	SD-WAN	A *software-defined wide area network* is a virtual WAN network that uses software to control connectivity, management and services between data centers and remote branches as well as the cloud.

area network (SD-WAN)		It allows any combination of transport services such as Long Term Evolution (LTE), Multiprotocol Label Switching (MPLS), and broadband internet services, to securely connect users to applications. SD-WAN is based on the same methodology as software-defined networking (SDN) which separates the control plane from the data plane to make networking more intelligent.
Management	Network	The term *network* often describes a computer system controlled by a single organization. This could be a local area network at a single location or a wide area network used by a single business or organization. If two companies connect their internal networks to share data, you could call it one network. However, it is two networks because each network is managed by a different company.
	Subnet	A *subnet* is a portion of a network with a common network address. • All devices on the subnet share the same network address, but they have unique host addresses. • Each subnet in a larger network has a unique subnet address. • Devices connected through hubs or switches are on the same subnet. Routers are used to connect multiple subnets.
	Internetwork	An *internetwork* has geographically dispersed WAN connections that connect multiple LANs. Connecting two networks under different management is a form of internetworking because data must travel between two networks.
Participation	Internet	The *internet* is a large world-wide public network. The internet is public because virtually anyone can connect to it. • Users and organizations connect to the internet through an internet service provider (ISP).

- The internet uses a set of communication protocols (TCP/IP) for providing services.
- Individuals and organizations can make services (such as a website) available to other users on the internet.

Intranet	An *intranet* is a private network that uses internet technologies. Services on an intranet are available only to hosts that are connected to the private network. For example, your company might have a website that only employees can access.
Extranet	An *extranet* is a private network that uses internet technologies, but its resources are made available only to external, trusted users. For example, you might create a website on a private network that only users from a partner company can access.

Dynamic Multipoint VPNs

Dynamic Multipoint VPN (DMVPN) is a Cisco software solution for building multiple VPNs in an easy, dynamic, and scalable manner. You use a DMVPN when you need to add more sites, but other VPN types are not sufficient.

- DMVPN uses a hub-and-spoke configuration to establish a full mesh topology. This simplifies the VPN tunnel configuration and provides a flexible option to connect to the central site.
- Each site uses Multipoint Generic Routing Encapsulation (mGRE). The mGRE tunnel interface allows a single GRE interface to dynamically support multiple IPsec tunnels.
- Spoke sites can also obtain information about each other and alternatively build direct tunnels between themselves (spoke-to-spoke tunnels).