Chapter 1: Introduction to Networks

Brendan Shea, PhD

Introduction to Networking

2026

Learning Objectives and Exam Coverage

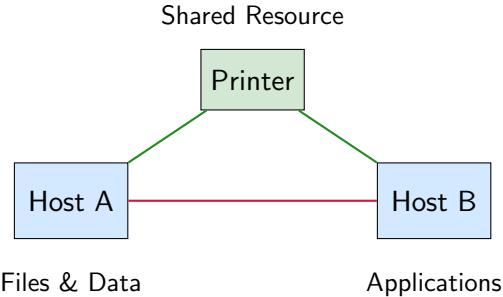
- Students will understand fundamental networking concepts and terminology used in modern computer networks.
- Students will be able to compare and contrast different network topologies and their appropriate use cases.
- Students will identify various network types including LANs, WANs, MANs, and specialized networks.
- Students will analyze network architectures and traffic flow patterns in enterprise environments.

CompTIA Network+ Exam Objective

Domain 1.0 Networking Concepts - 1.6: Compare and contrast network topologies, architectures, and types including mesh, hybrid, star/hub-and-spoke, spine-leaf, point-to-point, three-tier hierarchical model, and traffic flows.

What is a Network? - Basic Definition

- A **network** is defined as "a group or system of interconnected people or things."
- In computing, a network means two or more connected computers that can share resources.
- **Resources** include data, applications, office machines, Internet connections, or combinations thereof.
- Networks enable communication between devices using **binary code** consisting of 1s and 0s in specific patterns.



The Local Area Network (LAN) - Definition and Scope

- A **Local Area Network (LAN)** is restricted to spanning a particular geographic location.
- Examples include office buildings, single departments, or home offices.
- Modern LANs have overcome historical limitations of 30 workstations and distance restrictions.
- **Workgroups** are logical zones that make administration easier by dividing large LANs.

Scooby Doo Gang Network Example

The Mystery Inc. gang sets up their network in their headquarters building. Fred's computer in the main office needs to access files on Velma's computer in the research lab, and Shaggy's laptop in the kitchen needs to print investigation reports on the shared printer in Daphne's room. This entire building network represents their LAN.

Common Network Components Overview

- Networks are composed of three main categories of devices that work together to enable communication.
- **Workstations** are powerful computers that provide resources to other users on the network.
- **Servers** are specialized computers running network operating systems to maintain and control networks.
- **Hosts** refer to any network device with an IP address in TCP/IP terminology.

Key Distinction

The terms workstation, client, and host are often used interchangeably in casual conversation, but they have technical differences. A **client machine** is any device that can request access to resources from servers or workstations.

Workstations vs. Clients - Understanding the Difference

- **Workstations** are powerful computers with multiple CPUs whose resources are available to network users.
- Workstations are often employed as systems that end users operate on a daily basis.
- **Client machines** are any devices that can request access to resources like printers or other hosts.
- The distinction matters technically, though people often use these terms interchangeably in practice.

Scooby Doo Gang Example

Velma's high-powered computer with dual processors serves as a workstation, running complex analysis software while sharing its computational resources with the team. Meanwhile, Shaggy's basic laptop acts as a client machine, requesting access to files stored on Velma's workstation and sending print jobs to the shared printer.

Server Types and Their Functions

- **Servers** get their name because they are "at the service" of the network users.
- Servers run specialized **network operating systems** to maintain and control network operations.
- Dedicated servers optimize performance by handling one specific labor-intensive job.
- Servers require superior CPUs, hard-drive space, and memory compared to client machines.

Server Type	**Function**
File Server	Stores and dispenses files
Mail Server	Handles email functions
Print Server	Manages network printers
Web Server	Manages web content via HTTPS
Application Server	Manages network applications
Proxy Server	Handles tasks for other machines

Hosts - The TCP/IP Perspective

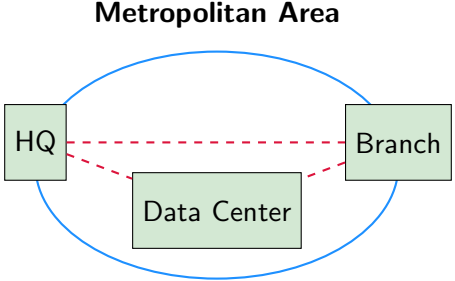
- The term **host** can refer to almost any type of networking device in modern usage.
- In TCP/IP terminology, a host specifically means any network device with an IP address.
- The term originates from the era when only mainframes were considered intelligent network devices.
- Today, hosts include workstations, servers, routers, and any device that can communicate using TCP/IP.

Historical Context

In networking's "Jurassic period," mainframes were the only intelligent devices on networks and were called hosts. Everything else was considered "dumb terminals" without IP addresses. The term has evolved but retains its connection to devices capable of independent network communication.

Metropolitan Area Network (MAN)

- A **Metropolitan Area Network (MAN)** covers a metropolitan area to interconnect buildings and facilities.
- MANs typically operate over **carrier provider networks** using leased network connections.
- These networks can be thought of as concentrated WANs with high-speed interconnections.
- MANs often use in-ground fiber optics and provide cost-effective high-speed interconnects.



Wide Area Network (WAN) - Spanning the Distance

- A **Wide Area Network (WAN)** spans large geographic areas and links disparate locations.
- WANs usually employ routers and public links as defining criteria for their classification.
- The Internet is the largest example of a WAN, connecting networks worldwide.
- WANs can be **distributed** (interconnected computers in many places) or **centralized** (remote connections to a main location).

Key WAN Characteristics

- Usually need router ports for connectivity
- Span larger geographic areas than LANs
- Generally slower than LANs
- Allow selective connection timing and duration
- Can utilize private or public data transport media

Personal Area Network (PAN) - Close Proximity Connections

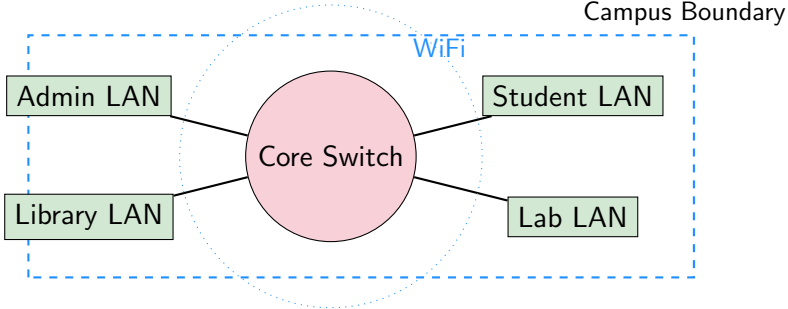
- A **Personal Area Network (PAN)** enables close proximity connections between devices.
- PANs are commonly seen with smartphones and laptops in conference rooms for collaboration.
- While PANs can use wired connections like Ethernet or USB, wireless is more common.
- Typical wireless technologies include **Bluetooth**, **infrared**, and **ZigBee**.

Scooby Doo Gang PAN Example

During a mystery investigation meeting, Fred uses Bluetooth to connect his smartphone to the conference room projector to display clues. Simultaneously, Velma's laptop connects to Daphne's tablet via Bluetooth to share forensic analysis data. These short-range connections (a few meters) form their PAN for the meeting.

Campus Area Network (CAN)

- A **Campus Area Network (CAN)** covers a limited geographical area such as a college or corporate campus.
- CANs typically interconnect LANs in various buildings and offer Wi-Fi components for roaming users.
- These networks are larger than LANs but smaller than MANs or WANs in scope.
- Most CANs provide Internet connectivity as well as access to data center resources.



Peer-to-Peer Networks - Decentralized Authority

- In **peer-to-peer networks**, computers have no central or special authority and are all equals.
- The authority to perform security checks lies with the computer that has the desired resource.
- Computers can simultaneously act as both client machines requesting resources and server machines providing resources.
- This architecture works well for small numbers of users with local backups and minimal security requirements.

Peer-to-Peer Challenges

Security presents major challenges because each user must maintain usernames and passwords on every machine. Passwords for the same user often change across different machines, creating a management nightmare. Backing up critical data becomes difficult without centralized storage.

Client-Server Networks - Centralized Management

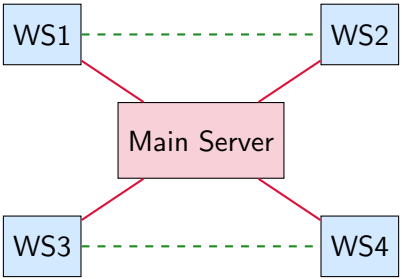
- **Client-server networks** use a single server with a network operating system to manage the entire network.
- Client requests for resources go to the main server, which handles security and directs clients to desired resources.
- This architecture provides better organization because all files are stored in one centralized location.
- Security is tighter because all usernames and passwords are maintained on the dedicated server.

Scooby Doo Gang Client-Server Example

Mystery Inc. sets up a client-server network where Velma's dedicated server computer stores all case files, clue databases, and monster identification records. When Fred needs to access witness statements from his laptop (client), he authenticates through Velma's server, which verifies his permissions and grants access to the appropriate files.

Hybrid Network Architectures

- Many modern networks are a healthy blend of peer-to-peer and client-server architectures.
- **Hybrid networks** have specified servers while permitting simultaneous resource sharing from workstations.
- Supporting machines run server services reasonably well despite handling fewer inbound connections.
- Well-designed mixed environments benefit from the positive aspects of both architectural worlds.



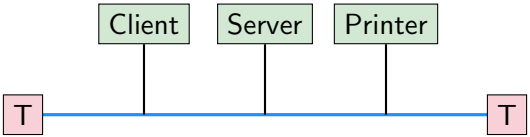
Network Architecture Comparison

- Network architecture choice depends on organization size, security needs, and administrative requirements.
- **Scalability** differs significantly between peer-to-peer and client-server implementations.
- Performance optimization varies based on centralized versus distributed resource management approaches.
- Cost considerations include both initial setup expenses and ongoing maintenance requirements.

Factor	**Peer-to-Peer**	**Client-Server**
Security	Decentralized	Centralized
Scalability	Limited	Excellent
Cost	Low initial	Higher initial
Administration	Complex	Simplified
Performance	Variable	Optimized
Fault Tolerance	Distributed	Single point

Bus Topology - Linear Connections

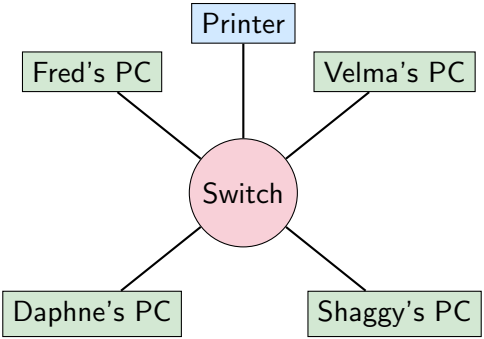
- **Bus topology** is the most basic topology, consisting of two distinct and terminated ends.
- Each computer connects to one unbroken cable running the entire length of the network.
- Modern implementations use drop cables or "T" connectors instead of direct wire taps.
- All computers see all data flowing through the cable, but only the addressed computer receives it.



Main Bus Cable with Terminators

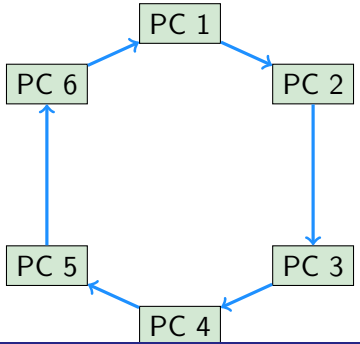
Star (Hub-and-Spoke) Topology

- **Star topology** connects computers to a central point with individual cables or wireless connections.
- The central device is typically a hub, switch, or access point managing all connections.
- Cable failure affects only the specific machine or segment, providing better fault tolerance.
- This topology offers excellent scalability by simply adding new cables to the central device.



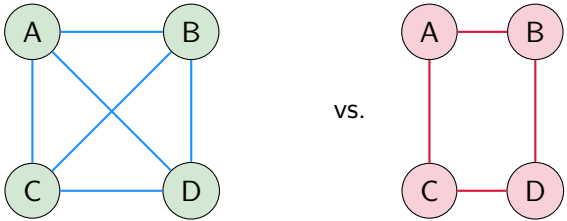
Ring Topology - Circular Data Flow

- **Ring topology** connects each computer directly to other computers in a circular formation.
- Network data flows from computer to computer around the ring back to the source.
- Adding new devices requires breaking the cable ring, likely bringing down the entire network.
- This topology is expensive, difficult to reconfigure, and not fault-tolerant for LANs.



Mesh Topology - Multiple Redundant Paths

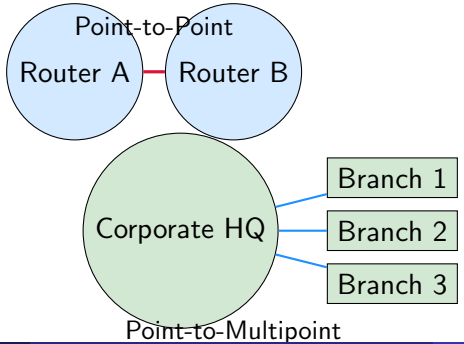
- **Mesh topology** provides a path from every machine to every other machine in the network.
- Full mesh requires n(n-1)/2 connections, where n is the number of devices.
- **Partial mesh** provides some redundancy without connecting every device to every other device.
- This topology offers excellent fault tolerance but creates significant complexity and cost.



4 devices = 4(4-1)/2 = 6 connections Partial mesh = 4 connections

Point-to-Point and Point-to-Multipoint Topologies

- **Point-to-point topology** provides a direct connection between two routers or switches.
- This creates one communication path that can be physical (serial cable) or logical (circuit within Frame Relay/MPLS).
- **Point-to-multipoint topology** connects one interface on a router to multiple destination routers.
- All routers and interfaces in point-to-multipoint connections are part of the same network.



Hybrid Topology - Combining Multiple Types

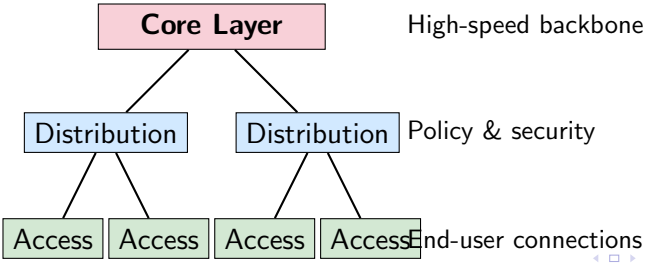
- **Hybrid topology** combines two or more types of physical or logical network topologies.
- This approach allows networks to leverage the advantages of different topologies in appropriate areas.
- Common implementations include star networks connected via mesh backbones or ring WANs.
- Hybrid designs provide flexibility to optimize performance, cost, and fault tolerance for specific needs.

Scooby Doo Gang Hybrid Network Example

Mystery Inc. uses a hybrid topology where their local headquarters uses star topology (all computers connected to a central switch), but their remote investigation sites connect back to headquarters using a partial mesh WAN topology. This gives them reliable local connectivity and redundant paths between field offices, combining the cost-effectiveness of star topology with the fault tolerance of mesh topology.

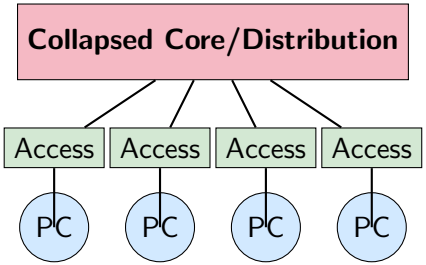
Three-Tiered Network Model (Core, Distribution, Access)

- The **three-tiered model** was introduced by Cisco over 20 years ago as the gold standard for network design.
- **Core layer** serves as the network backbone, providing high-speed routing and switching between geographic areas.
- **Distribution layer** (workgroup/aggregation layer) handles packet filtering, security policies, and VLAN routing.
- **Access layer** (edge layer) connects end-user hosts and provides local switching, collision domains, QoS, and PoE.



Collapsed-Core Model - Cost-Effective Design

- The **collapsed-core model** combines core and distribution layer functions into a single tier.
- This design reduces cost and complexity in small to midsize networks while maintaining functionality.
- Modern powerful switching equipment can support both core routing and distribution-layer services effectively.
- The collapsed-core still performs the same functions as separate core and distribution layers.

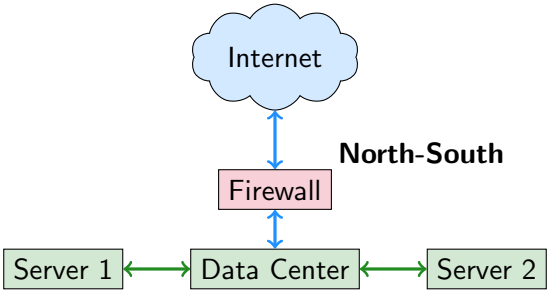


Combined functions

End-user connections

Traffic Flow Analysis - North-South vs. East-West

- Understanding traffic flow is essential for network security and performance optimization.
- **North-south traffic** flows between your internal network and external Internet connections.
- **East-west traffic** represents lateral movement between servers, data centers, and internal network segments.
- Security monitoring must address both traffic types, with increasing focus on east-west due to insider threats.



Virtual Networking and Network Function Virtualization (NFV)

- **Virtual networking** provides networking services through software rather than dedicated hardware devices.
- **Virtual switches (vSwitch)** operate on hypervisors, eliminating the need for external networking hardware.
- **Virtual Network Interface Cards (vNIC)** connect virtual machines to the hypervisor and network.
- **Network Function Virtualization (NFV)** runs routers, switches, firewalls, and load balancers as software on single devices.

Scooby Doo Gang Virtual Network Example

Mystery Inc. virtualizes their entire network infrastructure on a single powerful server. Instead of buying separate physical routers, switches, and firewalls, they run virtual versions of each device as software. Fred's virtual machine connects through a vNIC to a virtual switch, which routes traffic through a virtual firewall before reaching Velma's analysis server - all running on the same physical hardware managed by the hypervisor.

Chapter Summary and Key Takeaways

- Networks enable resource sharing between connected devices using various topologies and architectures.
- Physical topologies (bus, star, ring, mesh) each offer distinct advantages and trade-offs for different scenarios.
- Network types range from small PANs to global WANs, with specialized networks like SANs for storage.
- Modern network design emphasizes virtualization, software-defined approaches, and hierarchical models for scalability.

Essential Network Concepts

- **Fault tolerance** vs. **cost** considerations in topology selection
- **Centralized** (client-server) vs. **decentralized** (peer-to-peer) architectures
- **Three-tier model**: Core (backbone), Distribution (policy), Access (end-users)
- **Traffic flow**: North-south (external) and east-west (internal) security implications

Review Questions and Exam Preparation

- Which topology provides the highest fault tolerance but requires the most connections?
- What are the three layers of the hierarchical network model and their primary functions?
- How do peer-to-peer and client-server architectures differ in terms of security and scalability?
- What is the difference between north-south and east-west traffic flow patterns?

Study Focus Areas	**Key Terms**
Network Components	Workstation, Server, Host, Client
Topologies	Bus, Star, Ring, Mesh, Hybrid
Network Types	LAN, WAN, MAN, PAN, CAN, SAN
Architectures	Peer-to-peer, Client-server
Design Models	Three-tier, Collapsed-core, Spine-leaf
Advanced Concepts	MPLS, SDWAN, NFV, Traffic flow