Chapter 1: Exploring the Network

ITP172 – Networking Fundamentals & Project

Cisco Networking Academy®
Mind Wide Open™

Chapter 1: Objectives

After completing this chapter, students will be able to:

- Explain how multiple networks are used in everyday life.
- Explain the topologies and devices used in a small- to medium-sized business network.
- Explain the basic characteristics of a network that supports communication in a small- to medium-sized business.
- Explain trends in networking that will affect the use of networks in small to medium-sized businesses.

1.1 Globally Connected

Cisco Networking Academy®
Mind Wide Open™

Networking Impacts in Our Daily Lives

- Networks support the way we learn.
- Networks support the way we communicate.
- Networks support the way we work.
- Networks support the way we play.

Networks of Many Sizes

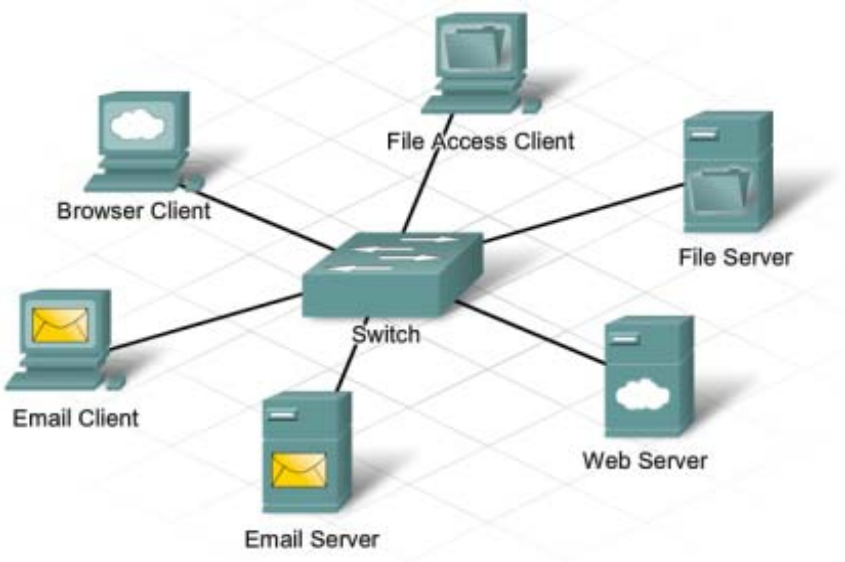
Small Home Networks

Small Office/Home Office Networks **(SOHO)**

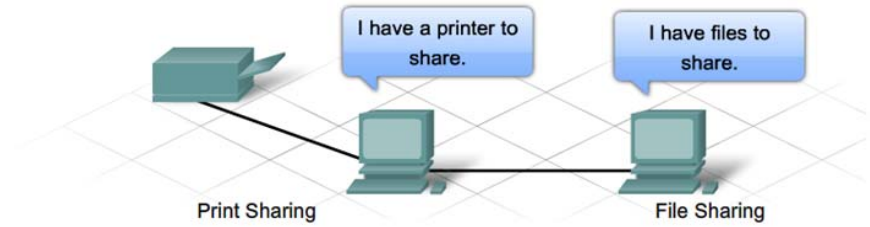
Medium to Large Networks

World Wide Networks

Clients and Servers



Peer-to-Peer



The advantages of peer-to-peer networking:

- Easy to set up
- Less complexity
- Lower cost since network devices and dedicated servers may not be required
- Can be used for simple tasks such as transferring files and sharing printers

The disadvantages of peer-to-peer networking:

- No centralized administration
- Not as secure
- Not scalable
- All devices may act as both clients and servers which can slow their performance

CISCO

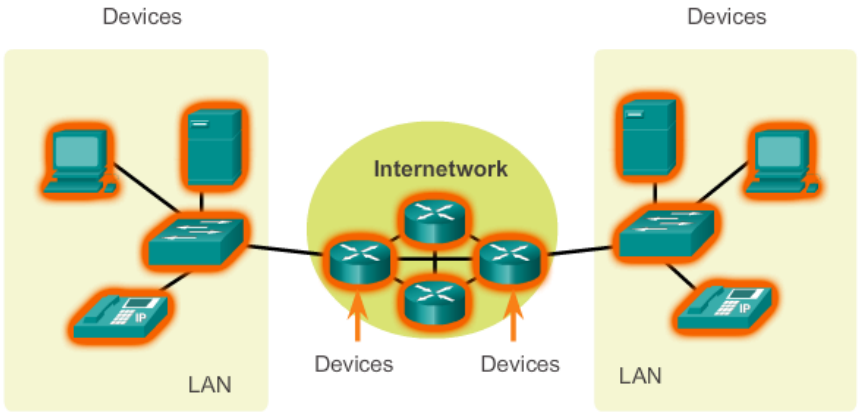
1.2 LANs, WANs, and the Internet

Cisco Networking Academy®
Mind Wide Open™

Components of a Network

There are three categories of network components:

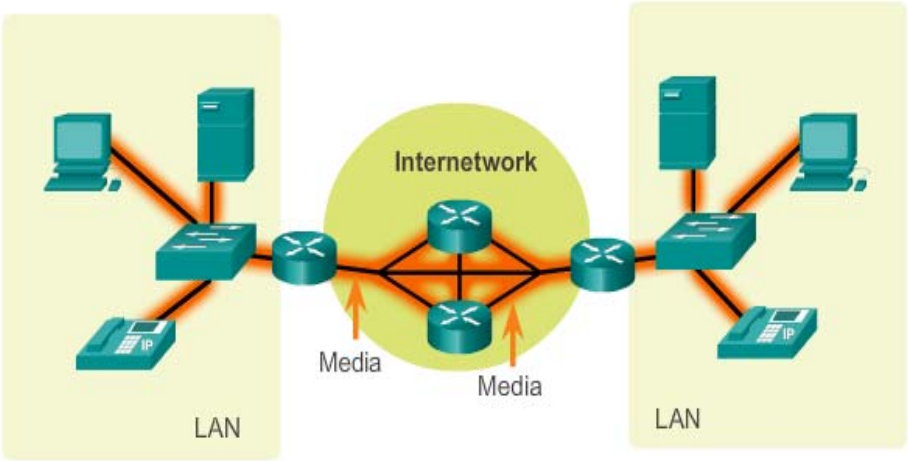
- **Devices**
- **Media**
- **Services**



9

Components of a Network

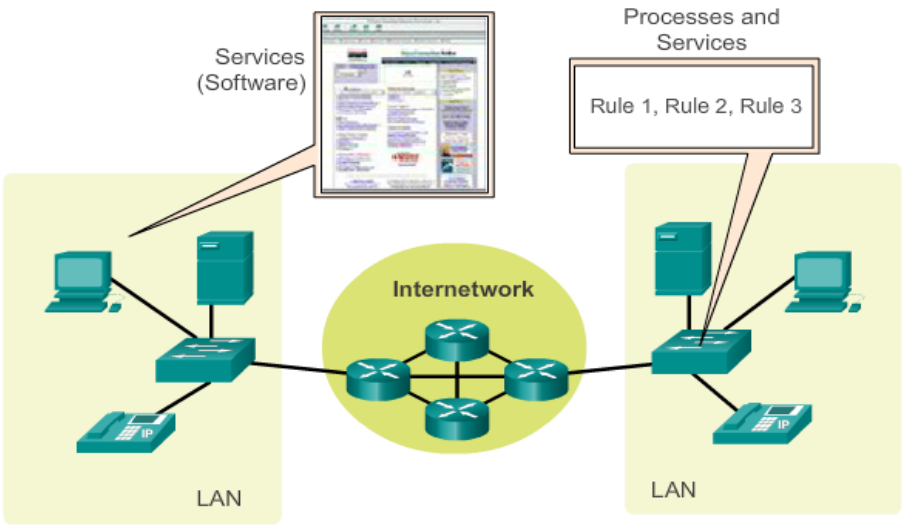
Media



10

Components of a Network

Services (Software)



End Devices

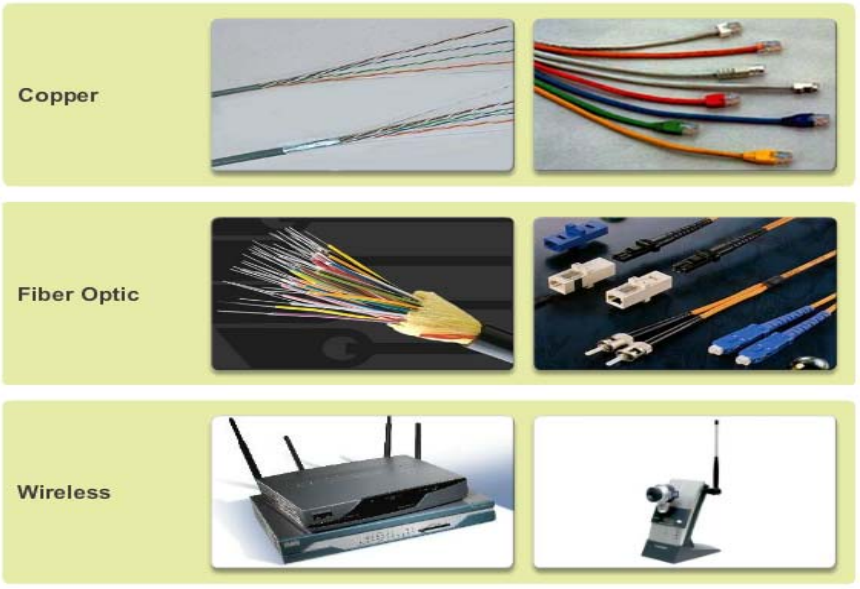
Some examples of end devices are:

- Computers (work stations, laptops, file servers, web servers)
- Network printers
- VoIP phones
- TelePresence endpoint
- Security cameras
- Mobile handheld devices (such as smart phones, tablets, PDAs, and wireless debit / credit card readers and barcode scanners)

Examples of intermediary network devices are:

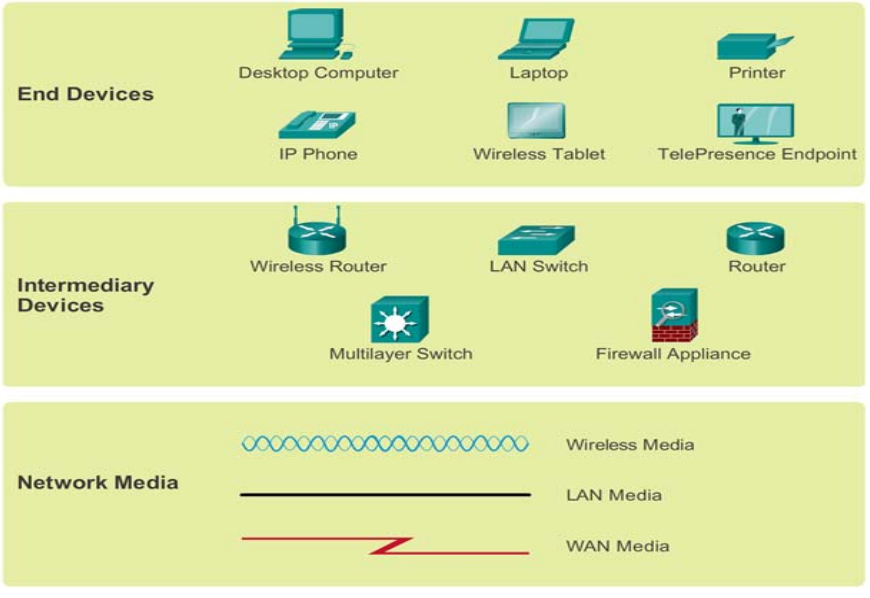
- Network Access Devices (switches, and wireless access points)
- Internetworking Devices (routers)
- Security Devices (firewalls)

Network Media



13

Network Representations



14

Types of Networks

The two most common types of network infrastructures are:

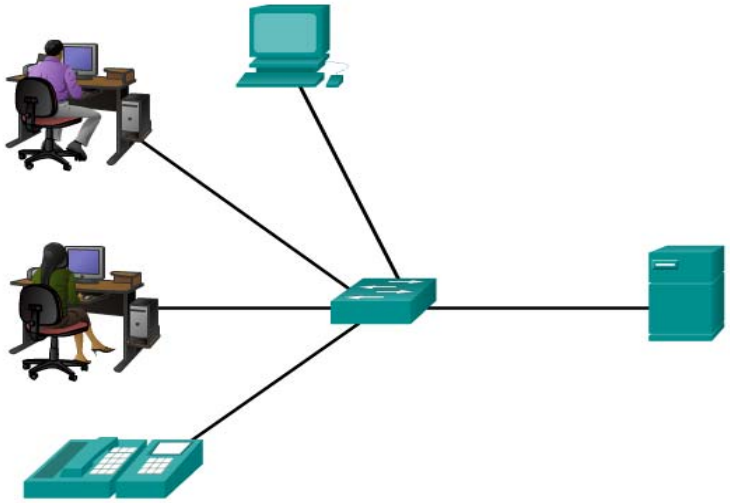
- Local Area Network (LAN)
- Wide Area Network (WAN)

Other types of networks include:

- Metropolitan Area Network (MAN)
- Wireless LAN (WLAN)
- Storage Area Network (SAN)

15

Local Area Networks (LAN)

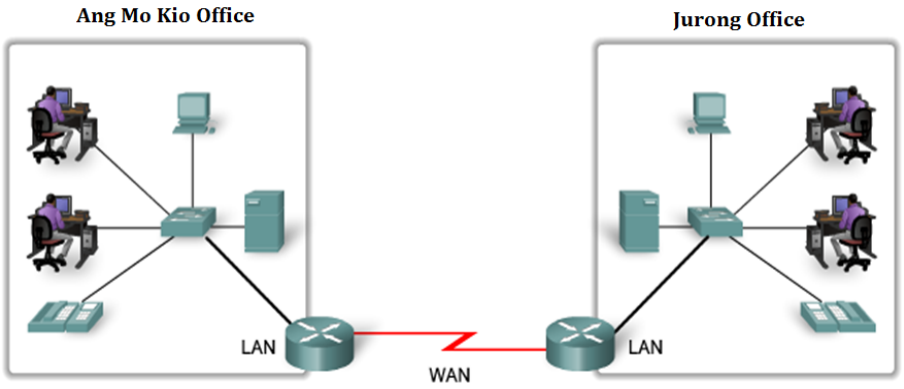


A network serving a home, building, or campus is considered a LAN.

16

Wide Area Networks (WAN)

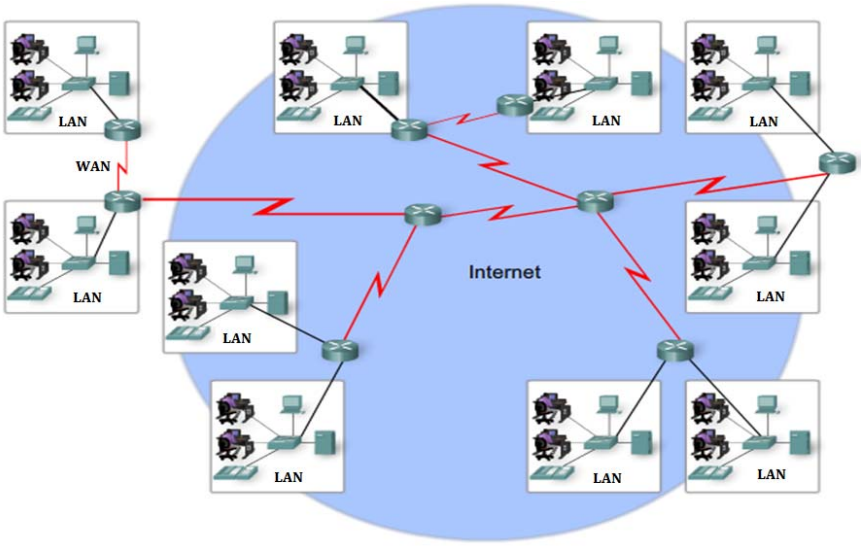
LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN).



17

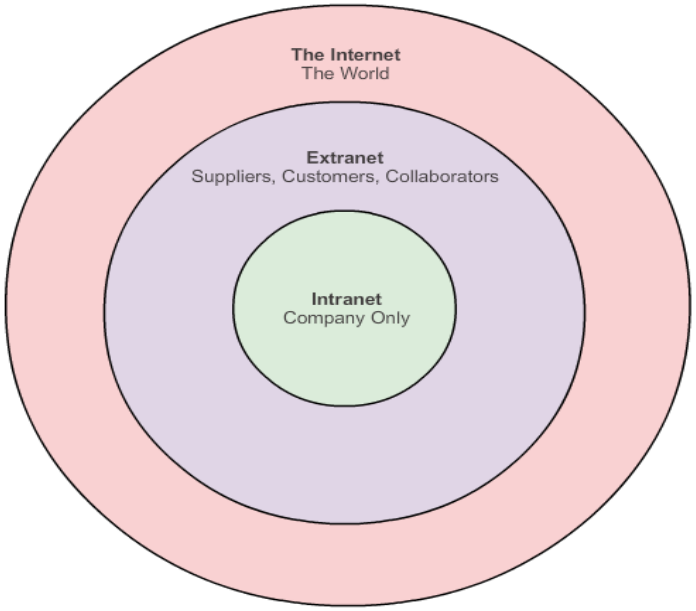
The Internet – Network of (many) networks

LANs and WANs may be connected into internetworks.



18

Intranet and Extranet

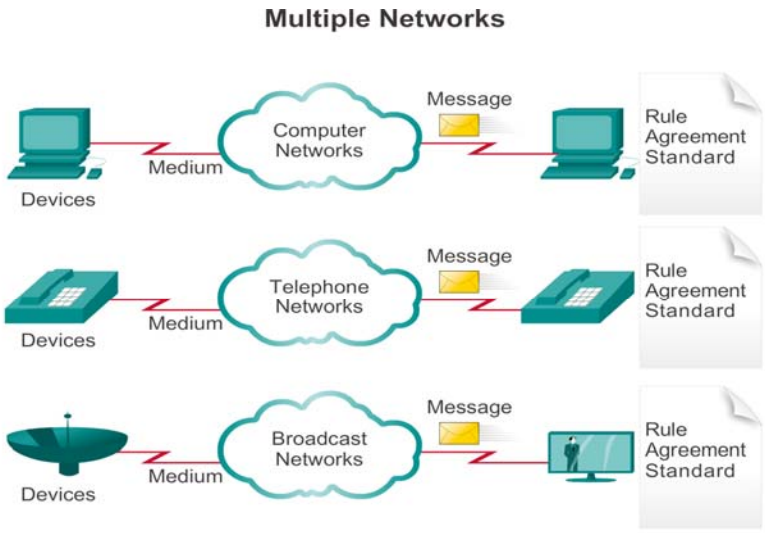


19

1.3 The Network as a Platform

Cisco Networking Academy®
Mind Wide Open™

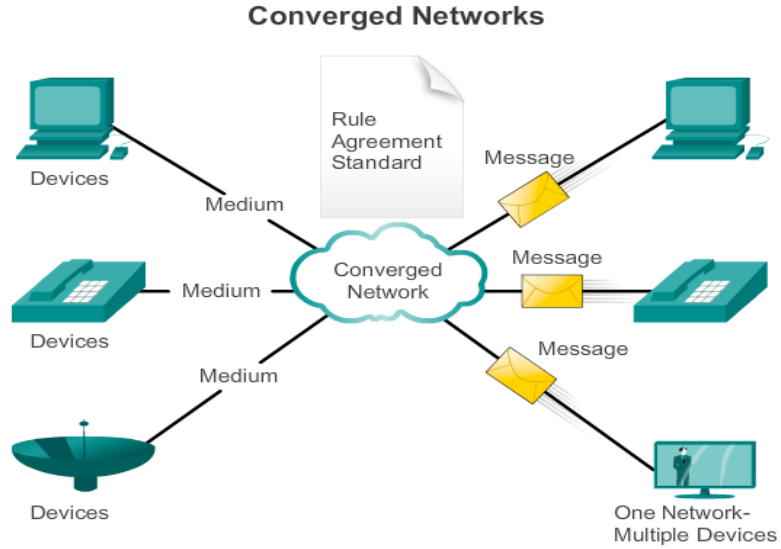
The Converging Network



Multiple services are running on multiple networks.

21

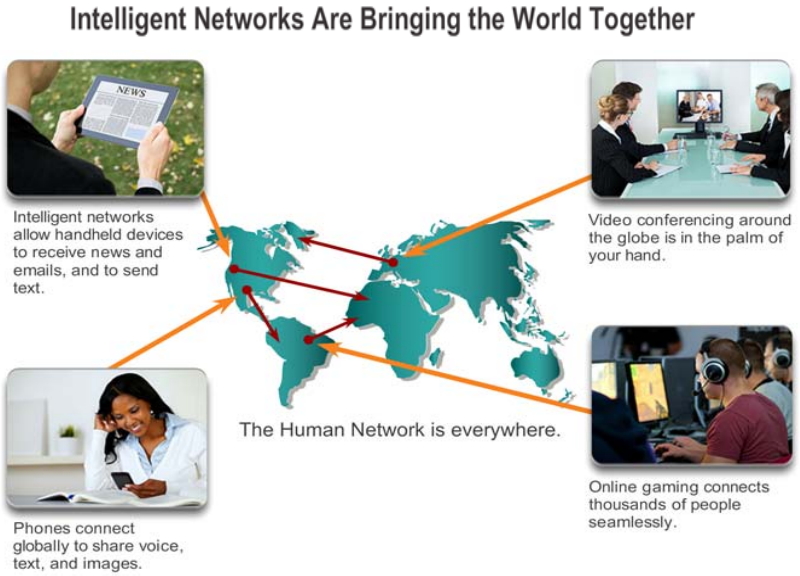
The Converging Network



Converged data networks carry multiple services on one network.

22

Planning for the Future



23

Supporting Network Architecture

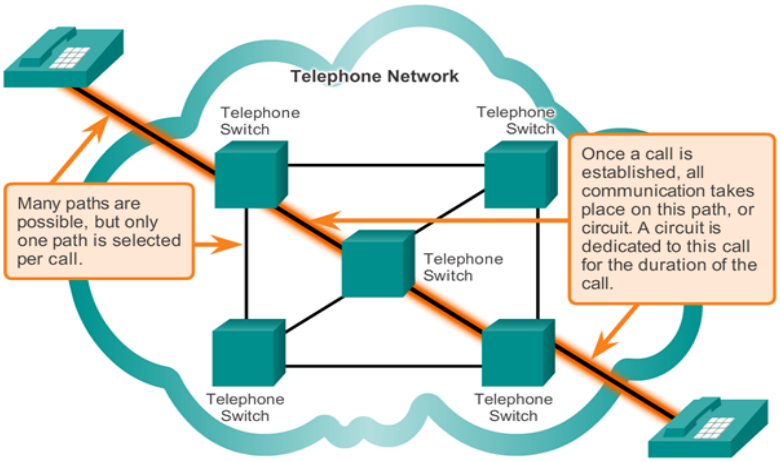
As networks evolve, we are discovering that there are four basic characteristics that the underlying architectures need to address in order to meet user expectations:

- Fault Tolerance
- Scalability
- Quality of Service (QoS)
- Security

24

Fault Tolerance in Circuit Switched Network

Circuit Switching in a Telephone Network



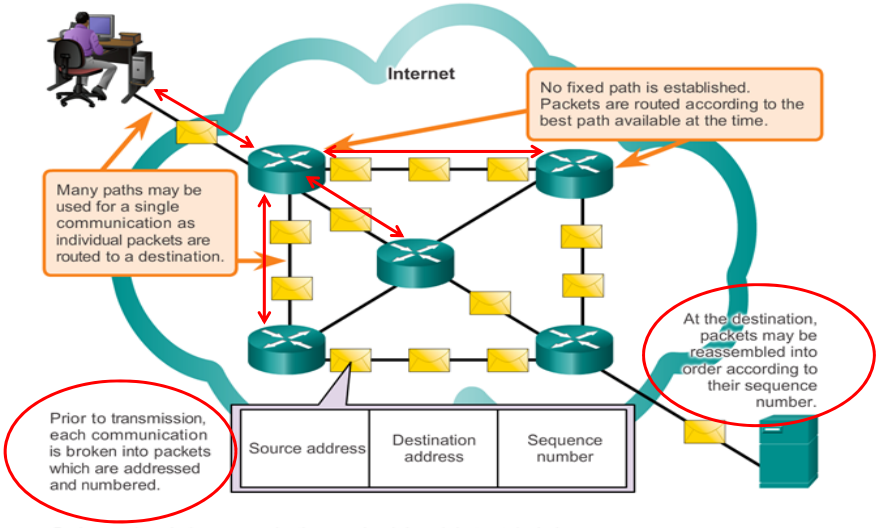
The circuit stays active, even if no one is speaking.

There are many, many circuits, but a finite number. During peak periods, some calls may be denied.

25

Packet-Switched Networks

Packet Switching in a Data Network



During peak periods, communication may be delayed, but not denied.

26

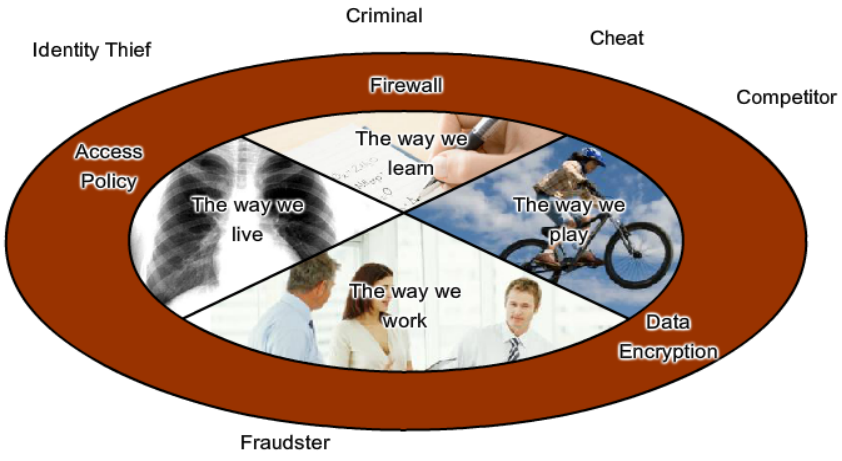
Providing QoS

Examples of priority decisions for an organization might include:

- **Time-sensitive** communication - increase priority for services like telephony or video distribution.
- **Non time-sensitive** communication - decrease priority for web page retrieval or email.
- **High importance to organization** - increase priority for production control or business transaction data.
- **Undesirable communication** - decrease priority or block unwanted activity, like peer-to-peer file sharing or live entertainment.

27

Providing Network Security



The communication and information that we would like to be private is protected from those who would make unauthorized use of it.

28

1.4 The Changing Network Environment

Cisco Networking Academy®
Mind Wide Open™

New trends

Some of the top trends include:

- Bring Your Own Device (BYOD)
- Online collaboration
- Video
- Cloud computing

Bring Your Own Device (BYOD)

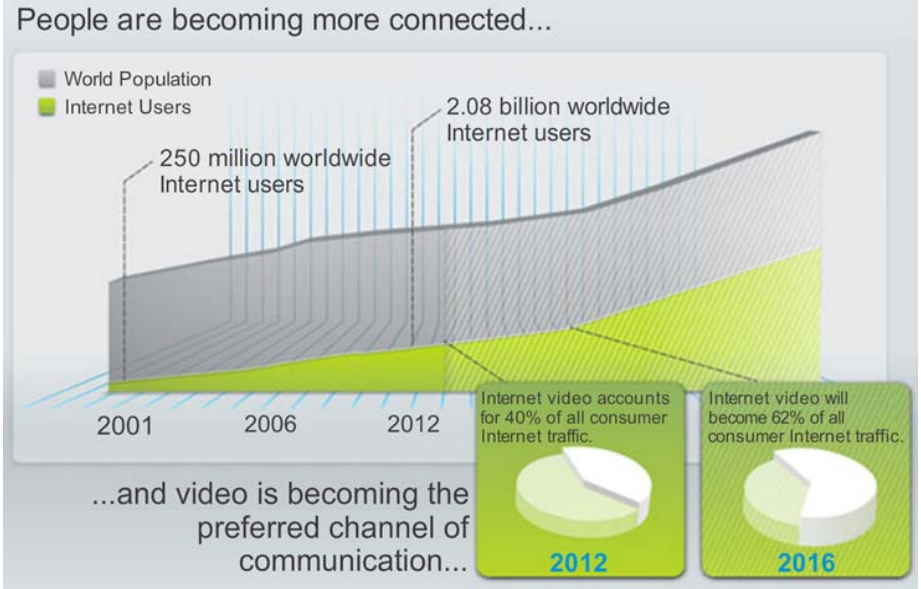
The concept of any device, to any content, in anyway is a major global trend that requires significant changes to the way devices are used. This trend is known as Bring Your Own Device (BYOD).

31

Online Collaboration – working together

32

Video Communication



33

Cloud Computing

Cloud computing offers the following potential benefits:

- Organizational flexibility
- Agility and rapid deployment
- Reduced cost of infrastructure
- Refocus of IT resources
- Creation of new business models

34

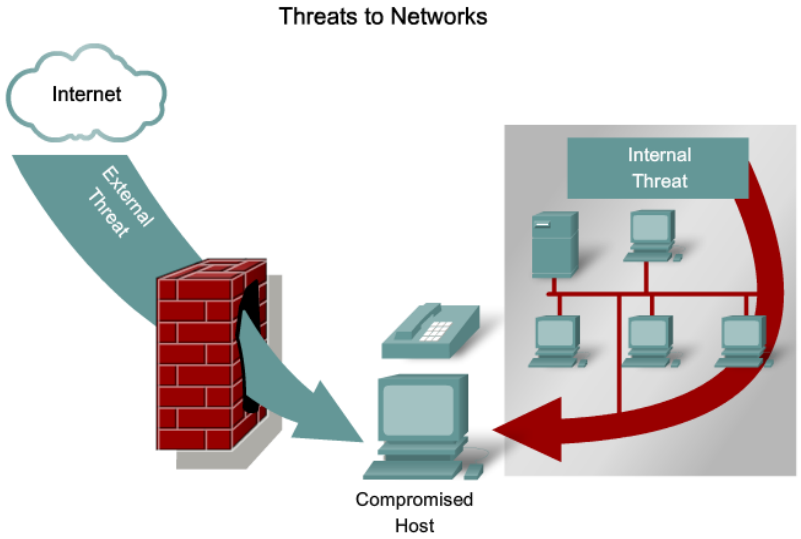
Data Centers

A data center is a facility used to house computer systems and associated components including:

- High-speed virtual servers
  (sometimes referred to as server farms or server clusters)
- Storage systems (typically uses SAN technology)
- Backup power supplies
- Redundant data communications connections
- Environmental controls
  (e.g., air conditioning, fire suppression)
- Security devices

35

Network Security



36

Security Threats

The most common external threats to networks include:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks, also called zero-hour attacks
- Hacker attacks
- Denial of service (DoS) attacks
- Data interception and theft
- Identity theft

37

Security Solutions

Network security components often include:

- Antivirus and antispyware
- Firewall filtering
- Dedicated firewall systems
- Access control lists (ACL)
- Intrusion prevention systems (IPS)
- Virtual Private Networks (VPNs)

38

Summary

In this chapter, you learned:

- Networks and the Internet have changed the way we communicate, learn, work, and even play.
- The Internet is the largest network in existence. In fact, the term Internet means a “network of networks”.
- Network infrastructure is made up of network components such as intermediate and end devices and network media.
- Network security is an important part of computer networks, regardless of whether it is a small home network or a large corporation with thousands of users.
- The network infrastructure must grow and adjust to support the way the network is used.
- The routing and switching platform is the foundation of any network infrastructure.