Module 1: Networking Today

Instructor Materials

Introduction to Networks v7.0
(ITN)

Instructor Materials – Module 1 Planning Guide

This PowerPoint deck is divided in two parts:

- Instructor Planning Guide

  - Information to help you become familiar with the module

  - Teaching aids

- Instructor Class Presentation

  - Optional slides that you can use in the classroom

  - Begins on slide # 12

    Note: Remove the Planning Guide from this presentation before sharing with anyone.

For additional help and resources go to the Instructor Home Page and Course Resources for this course. You also can visit the professional development site on netacad.com, the official Cisco Networking Academy Facebook page, or Instructor Only FB group.

What to Expect in this Module

To facilitate learning, the following features within the GUI may be included in this module:

Feature	Description
Animations	Expose learners to new skills and concepts.
Videos	Expose learners to new skills and concepts.
Check Your Understanding(CYU)	Per topic online quiz to help learners gauge content understanding.
Interactive Activities	A variety of formats to help learners gauge content understanding.
Syntax Checker	Small simulations that expose learners to Cisco command line to practice configuration skills.
PT Activity	Simulation and modeling activities designed to explore, acquire, reinforce, and expand skills.

What to Expect in this Module (Cont.)

To facilitate learning, the following features may be included in this module:

Feature	Description
Hands-On Labs	Labs designed for working with physical equipment.
Class Activities	These are found on the Instructor Resources page. Class Activities are designed to facilitate learning, class discussion, and collaboration.
Module Quizzes	Self-assessments that integrate concepts and skills learned throughout the series of topics presented in the module.
Module Summary	Briefly recaps module content.

Check Your Understanding

- Check Your Understanding activities are designed to let students quickly determine if they understand the content and can proceed, or if they need to review.

- Check Your Understanding activities *do not* affect student grades.

- There are no separate slides for these activities in the PPT. They are listed in the notes area of the slide that appears before these activities.

Module 1: Activities

What activities are associated with this module?

Page #	Activity Type	Activity Name	Optional?
1.1.2	Video	The Cisco Networking Academy Learning Experience	Recommended
1.2.6	Check Your Understanding	Network Components	Recommended
1.3.3	Check Your Understanding	Network Representations and Topologies	Recommended
1.4.5	Check Your Understanding	Common Types of Networks	Recommended
1.5.5	Video	Download and Install Packet Tracer	Recommended
1.5.6	Video	Getting Started in Cisco Packet Tracer	Recommended
1.5.7	Packet Tracer	Network Representation	Recommended
1.6.6	Check Your Understanding	Reliable Networks	Recommended
1.7.5	Video	Cisco WebEx for Huddles	Recommended
1.7.10	Check Your Understanding	Network Trends	Recommended
1.8.3	Check Your Understanding	Network Security	Recommended
1.9.3	Lab	Research IT and Networking Job Opportunities	Recommended

Module 1: Best Practices

Prior to teaching Module 1, the instructor should:

• Review the activities and assessments for this module.

• Try to include as many questions as possible to keep students engaged during classroom presentation.

Topic 1.1

• Ask the class:

  • What wouldn't we have without the internet?

  • What will be possible in the future using the network as the platform?

Module 1: Best Practices (Cont.)

Topic 1.2

- Ask the students what they think of when someone uses the term "host". What is a "host"?

- Discuss the difference between a server client network verses a peer-to-peer (P2P) network. Ask the students what kind of issues we can have with a P2P.

- In a P2P a user may share information with someone who really should not have this right. Remember this is a decentralized model that administers cannot exercise much control.

- Also when a person who is the server is not available (gone to lunch, on vacation, etc.) their resources will not be available to the client. It is important that this is best used on extremely small networks.

Module 1: Best Practices (Cont.)

Topic 1.3

- Create a Packet Tracer demonstration and refer to it throughout the module when referencing concepts introduced in the module (routers, switches, interface, ports, network media connections)

  - Demonstrate a basic topology and some of the key icons

  - Reinforce the differences between the physical and logical topologies

  - Analogies can be good too, when thinking about a street map, a map that shows the physical topology would show where the streets are; whereas a logical map might show which directions the traffic flows on the streets, such as one-way streets or streets in both directions, etc. It is important to know both the physical and the logical, just as it is important to know not only where the streets are, but also which way traffic is allowed to flow on them.

Topic 1.4

- Ask the students what kinds of equipment have on their home networks. Consider that all of these items are on the largest networks. The difference is in ability, quantity, and cost of a companies equipment.

Module 1: Best Practices (Cont.)

Topic 1.5

- Ask the class how they connect to the internet at home.

- Does anyone ever remember connecting via dialup modem?

- Ask the class if any uses a VoIP phone service bundled from their ISP. This would be an example of home converged network.

Topic 1.6

- QoS is the ability to give an advantage to certain kinds of traffic.

  - Ask the class when we like to give advantage to something or someone, but to everyone. If they cannot think of anything, ask if we have an emergency would we want the ambulance, firetruck, etc. to be treated like any other piece of traffic on the highway?

  - Briefly discuss examples of how Confidentiality, Integrity, and Availability are implemented.

    - Confidentiality – Encryption

    - Integrity – checksums or hashing

    - Availability – ensured with redundant hardware, connections, backups, disaster recovery

Module 1: Best Practices (Cont.)

Topic 1.7

- Have students discuss what devices they BYOD to and where.
- Ask students if they use Cloud Computing and what for.
- 1.7.6 – Do some research ahead of time to help describe what a Custom Cloud is
- 1.7.7 – Ask the students to discuss if anyone is currently making use of smart home technology
  - What are various other possibilities besides what is mentioned in the curriculum?

Topic1.8

- Ask the class what kind of internal threats that they might see as a network administrator.
- Ask why internal attacks are as important to address as the obvious external attacks.

Topic 1.9

- Discuss the benefits of obtaining a CCNA certification.
- Have students research current networking job openings that require a CCNA or other Cisco certification.
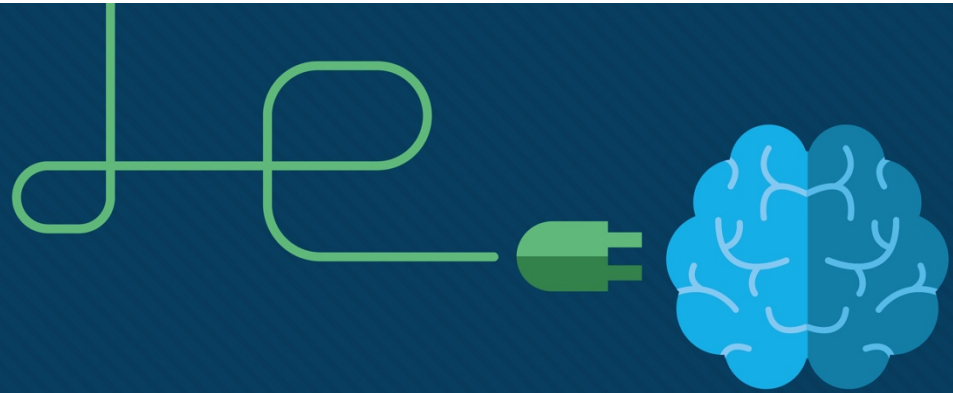
Module 1: Networking Today

Introduction to Networks v7.0
(ITN)

CCNA 7.0 Course Outlines

CCNA v7 Course #1	CCNA v7 Course #2	CCNA v7 Course #3
Networking Today	Basic Device Configuration	Single-Area OSPFv2 Concepts
Basic Switch and End Device Configuration	Switching Concepts	Single-Area OSPFv2 Configuration
Protocol Models	VLANs	WAN Concepts
Physical Layer	Inter-VLAN Routing	Network Security Concepts
Number Systems	STP	ACL Concepts
Data Link Layer	Etherchannel	ACLs for IPv4 Configuration
Ethernet Switching	DHCPv4	NAT for IPv4
Network Layer	SLAAC and DHCPv6 Concepts	VPN and IPsec Concepts
Address Resolution	FHRP Concepts	QoS Concepts
Basic Router Configuration	LAN Security Concepts	Network Management
IPv4 Addressing	Switch Security Configuration	Network Design
IPv6 Addressing	WLAN Concepts	Network Troubleshooting
ICMP	WLAN Configuration	Network Virtualization
Transport Layer	Routing Concepts	Network Automation
Application Layer	IP Static Routing	
Network Security Fundamentals	Troubleshoot Static and Default Routes	
Build a Small Network		

☐ New/significantly changed content

Download Draft Scope and Sequence

Module Objectives

Module Title: Networking Today

Module Objective: Explain the advances in modern technologies.

Topic Title	Topic Objective
Networks Affect our Lives	Explain how networks affect our daily lives.
Network Components	Explain how host and network devices are used.
Network Representations and Topologies	Explain network representations and how they are used in network topologies.
Common Types of Networks	Compare the characteristics of common types of networks.
Internet Connections	Explain how LANs and WANs interconnect to the internet.
Reliable Networks	Describe the four basic requirements of a reliable network.
Network Trends	Explain how trends such as BYOD, online collaboration, video, and cloud computing are changing the way we interact.
Network Security	Identify some basic security threats and solution for all networks.
The IT Professional	Explain employment opportunities in the networking field.

1.1 Networks Affect Our Lives

Networks Connect Us

Communication is almost as important to us as our reliance on air, water, food, and shelter. In today's world, through the use of networks, we are connected like never before.

Video – The Cisco Networking Academy Learning Experience

Cisco Networking Academy: learn how we use technology to make the world a better place.

No Boundaries

- World without boundaries

- Global communities

- Human network

1.2 Network Components

Host Roles

Every computer on a network is called a host or end device.

Servers are computers that provide information to end devices:

- email servers
- web servers
- file server

Clients are computers that send requests to the servers to retrieve information:

- web page from a web server
- email from an email server

Server Type	Description
Email	Email server runs email server software. Clients use client software to access email.
Web	Web server runs web server software. Clients use browser software to access web pages.
File	File server stores corporate and user files. The client devices access these files.

Peer-to-Peer

It is possible to have a device be a client and a server in a Peer-to-Peer Network. This type of network design is only recommended for very small networks.

I have a printer to share	I have files to share
Print Sharing	File Sharing
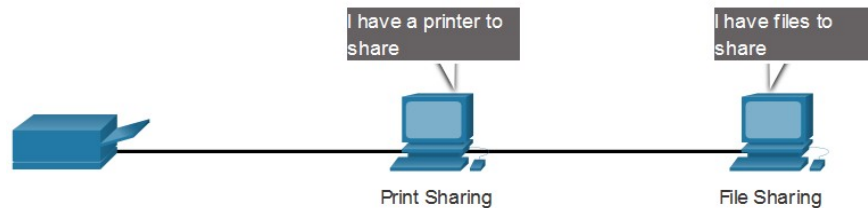
Advantages	Disadvantages
Easy to set up	No centralized administration
Less complex	Not as secure
Lower cost	Not scalable
Used for simple tasks: transferring files and sharing printers	Slower performance

End Devices

An end device is where a message originates from or where it is received. Data originates with an end device, flows through the network, and arrives at an end device.
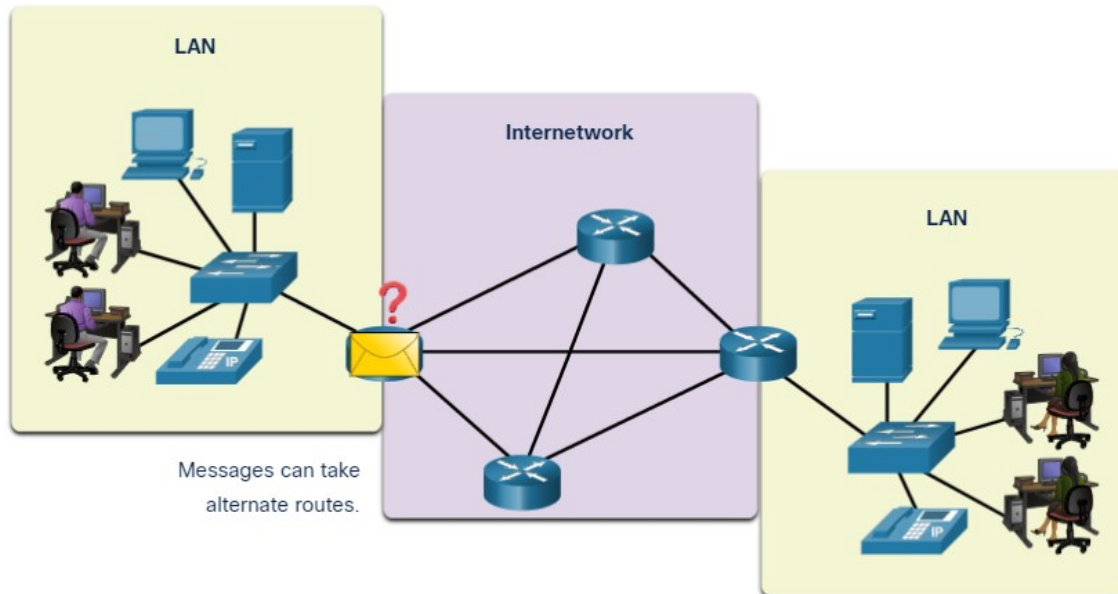
Intermediary Network Devices

An intermediary device interconnects end devices. Examples include switches, wireless access points, routers, and firewalls.

Management of data as it flows through a network is also the role of an intermediary device, including:

- Regenerate and retransmit data signals.
- Maintain information about what pathways exist in the network.
- Notify other devices of errors and communication failures.

Intermediary Devices

Wireless Router   LAN Switch   Router

Multilayer Switch   Firewall Appliance
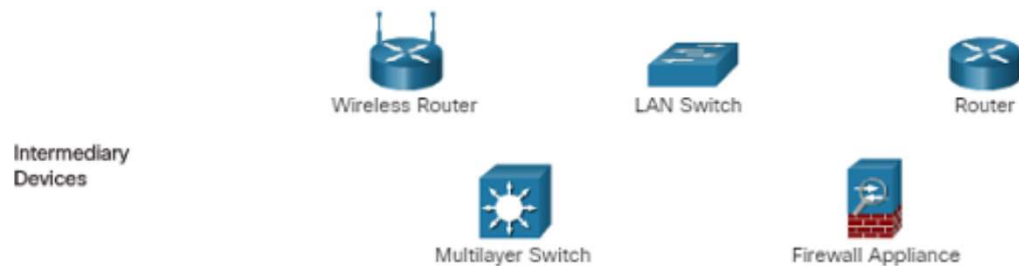
Network Media

Communication across a network is carried through a medium which allows a message to travel from source to destination.

Media Types	Description
Metal wires within cables	Uses electrical impulses
Glass or plastic fibers within cables (fiber-optic cable)	Uses pulses of light.
Wireless transmission	Uses modulation of specific frequencies of electromagnetic waves.

Copper
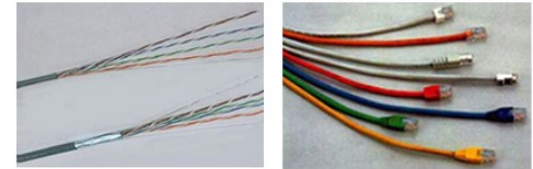
Fiber-optic

Wireless

1.3 Network Representations and Topologies

Network Representations

Network diagrams, often called topology diagrams, use symbols to represent devices within the network.

Important terms to know include:

- Network Interface Card (NIC)
- Physical Port
- Interface

Note: Often, the terms port and interface are used interchangeably

End Devices	Desktop Computer	Laptop	Printer
	IP Phone	Wireless Tablet	TelePresence Endpoint

Intermediary Devices	Wireless Router	LAN Switch	Router
	Multilayer Switch	Firewall Appliance	

Network Media	Wireless Media
	LAN Media
	WAN Media
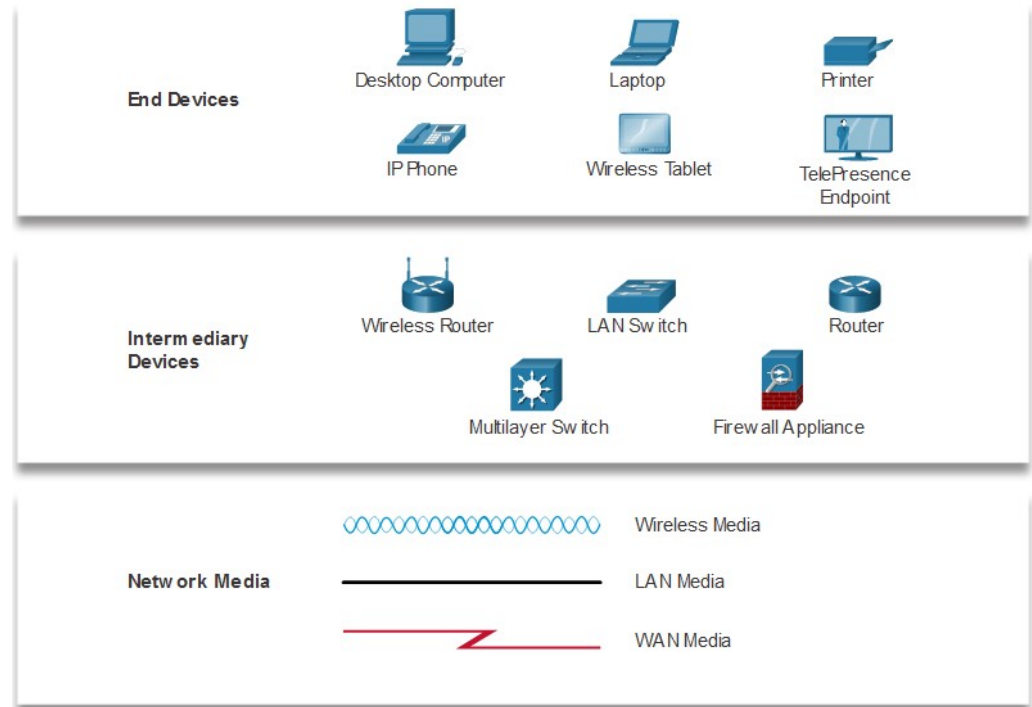
Topology Diagrams

Physical topology diagrams illustrate the physical location of intermediary devices and cable installation.
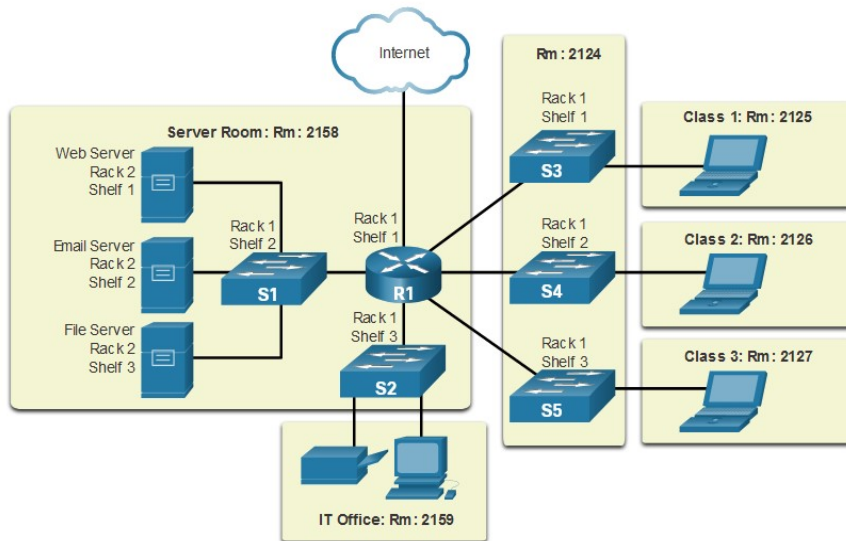
Logical topology diagrams illustrate devices, ports, and the addressing scheme of the network.
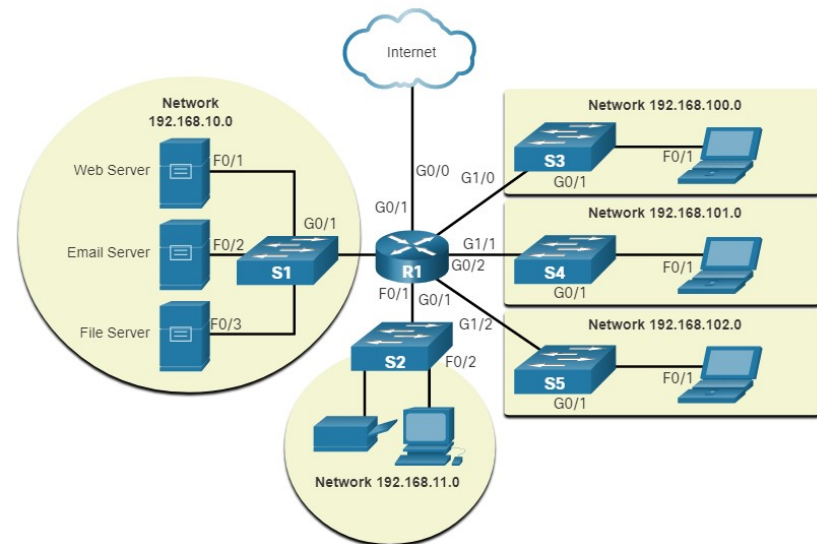
1.4 Common Types of Networks

Networks of Many Sizes

Small Home

SOHO
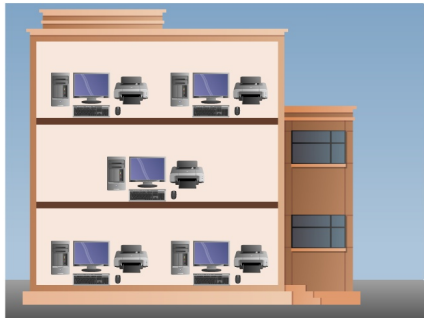
Medium/Large

World Wide

- Small Home Networks – connect a few computers to each other and the Internet

- Small Office/Home Office – enables computer within a home or remote office to connect to a corporate network

- Medium to Large Networks – many locations with hundreds or thousands of interconnected computers

- World Wide Networks – connects hundreds of millions of computers world-wide – such as the internet

Common Types of Networks
LANs and WANs

Network infrastructures vary greatly in terms of:

- Size of the area covered
- Number of users connected
- Number and types of services available
- Area of responsibility

Two most common types of networks:

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

LANs and WANs (cont.)

A LAN is a network infrastructure that spans a small geographical area.
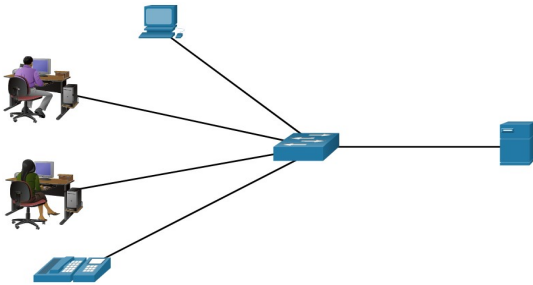
A WAN is a network infrastructure that spans a wide geographical area.
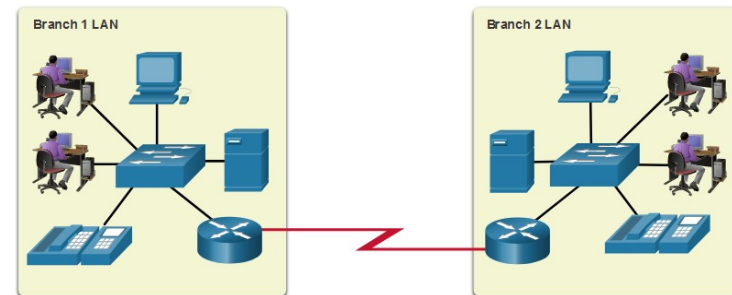
LAN	WAN
Interconnect end devices in a limited area.	Interconnect LANs over wide geographical areas.
Administered by a single organization or individual.	Typically administered by one or more service providers.
Provide high-speed bandwidth to internal devices.	Typically provide slower speed links between LANs.

The Internet

The internet is a worldwide collection of interconnected LANs and WANs.

- LANs are connected to each other using WANs.

- WANs may use copper wires, fiber optic cables, and wireless transmissions.

The internet is not owned by any individual or group. The following groups were developed to help maintain structure on the internet:

- IETF

- ICANN

- IAB

Hospital LAN

Home LAN

Government LAN

School LAN

Business LAN
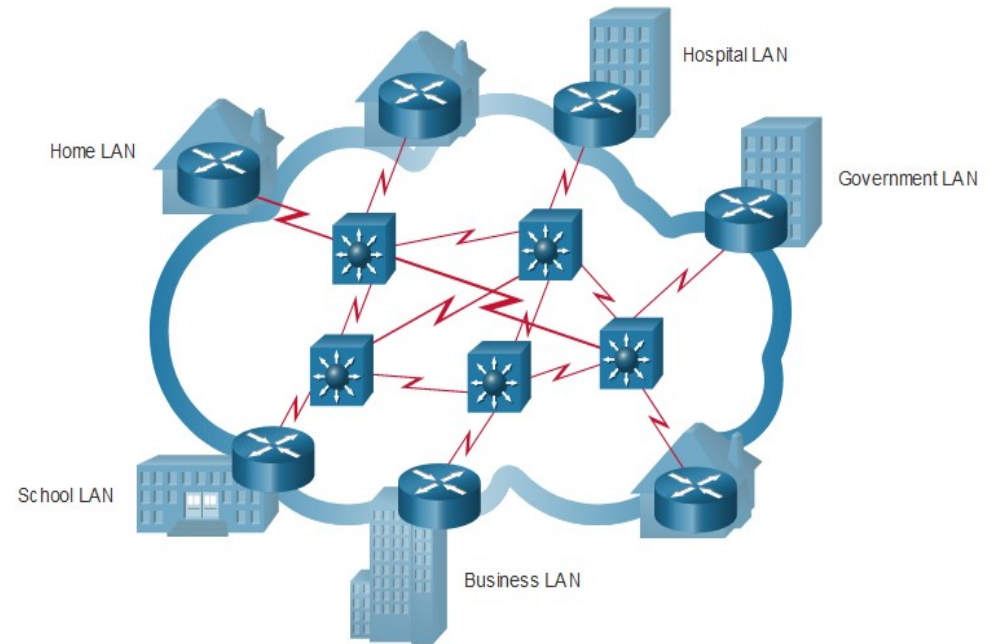
Intranets and Extranets
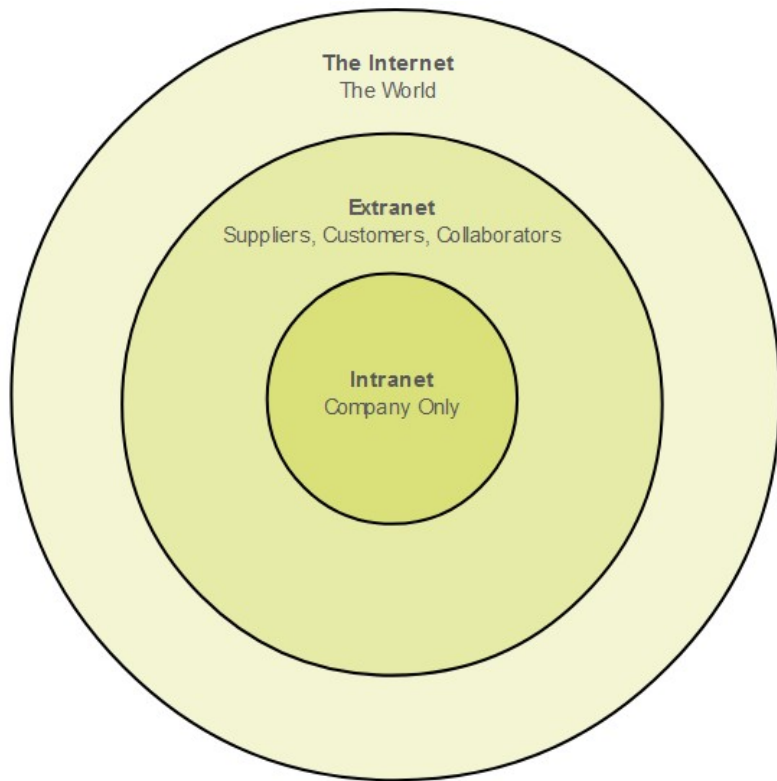
An intranet is a private collection of LANs and WANs internal to an organization that is meant to be accessible only to the organizations members or others with authorization.

An organization might use an extranet to provide secure access to their network for individuals who work for a different organization that need access to their data on their network.

1.5 Internet Connections

Internet Access Technologies

There are many ways to connect users and organizations to the internet:

- Popular services for home users and small offices include broadband cable, broadband digital subscriber line (DSL), wireless WANs, and mobile services.

- Organizations need faster connections to support IP phones, video conferencing and data center storage.

- Business-class interconnections are usually provided by service providers (SP) and may include: business DSL, leased lines, and Metro Ethernet.

Home and Small Office Internet Connections
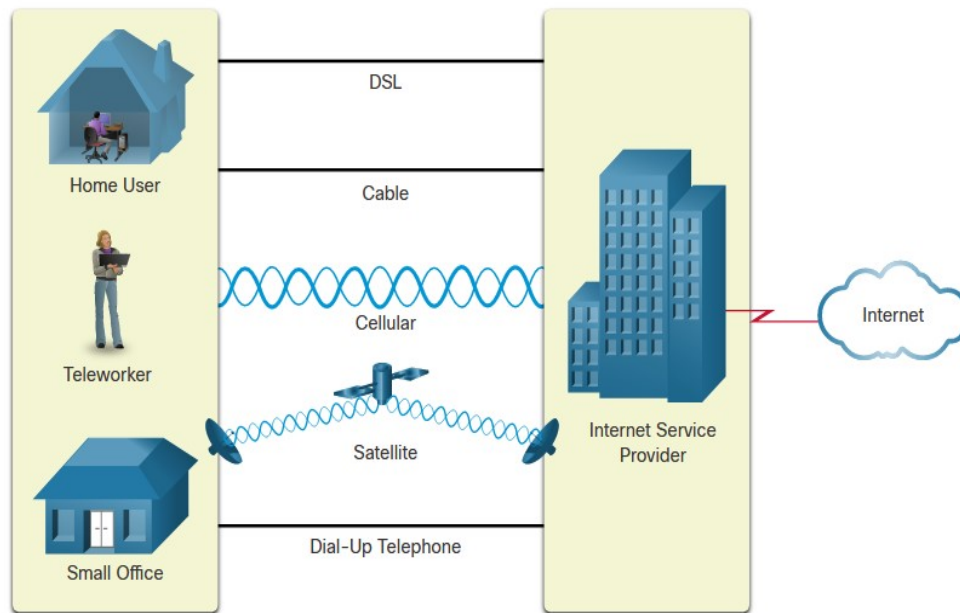
Connection	Description
Cable	high bandwidth, always on, internet offered by cable television service providers.
DSL	high bandwidth, always on, internet connection that runs over a telephone line.
Cellular	uses a cell phone network to connect to the internet.
Satellite	major benefit to rural areas without Internet Service Providers.
Dial-up telephone	an inexpensive, low bandwidth option using a modem.

Businesses Internet Connections

Corporate business connections may require:

- higher bandwidth
- dedicated connections
- managed services
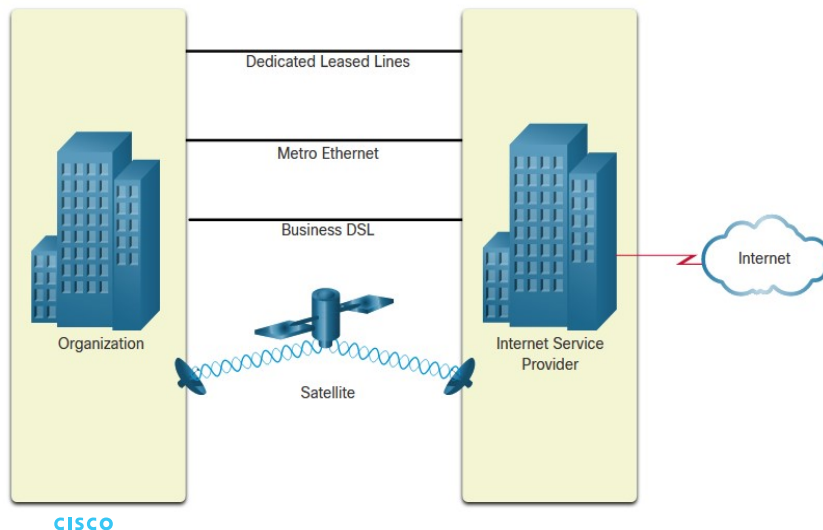
Type of Connection	Description
Dedicated Leased Line	These are reserved circuits within the service provider's network that connect distant offices with private voice and/or data networking.
Ethernet WAN	This extends LAN access technology into the WAN.
DSL	Business DSL is available in various formats including Symmetric Digital Subscriber Lines (SDSL).
Satellite	This can provide a connection when a wired solution is not available.

The Converging Network

Before converged networks, an organization would have been separately cabled for telephone, video, and data. Each of these networks would use different technologies to carry the signal.

Each of these technologies would use a different set of rules and standards.
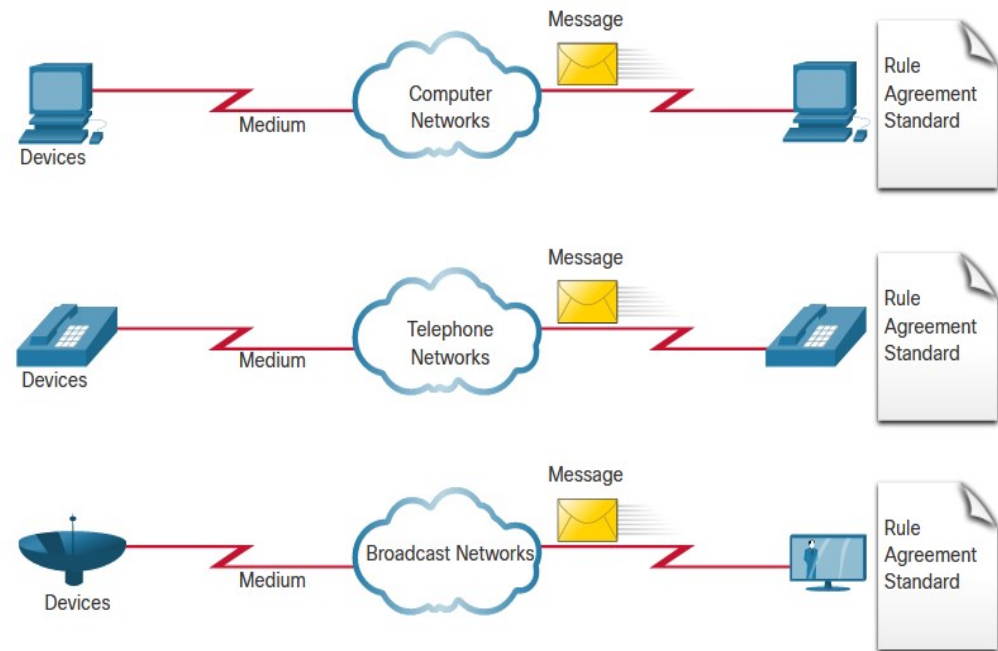
The Converging Network (Cont.)

Converged data networks carry multiple services on one link including:

- data
- voice
- video

Converged networks can deliver data, voice, and video over the same network infrastructure. The network infrastructure uses the same set of rules and standards.
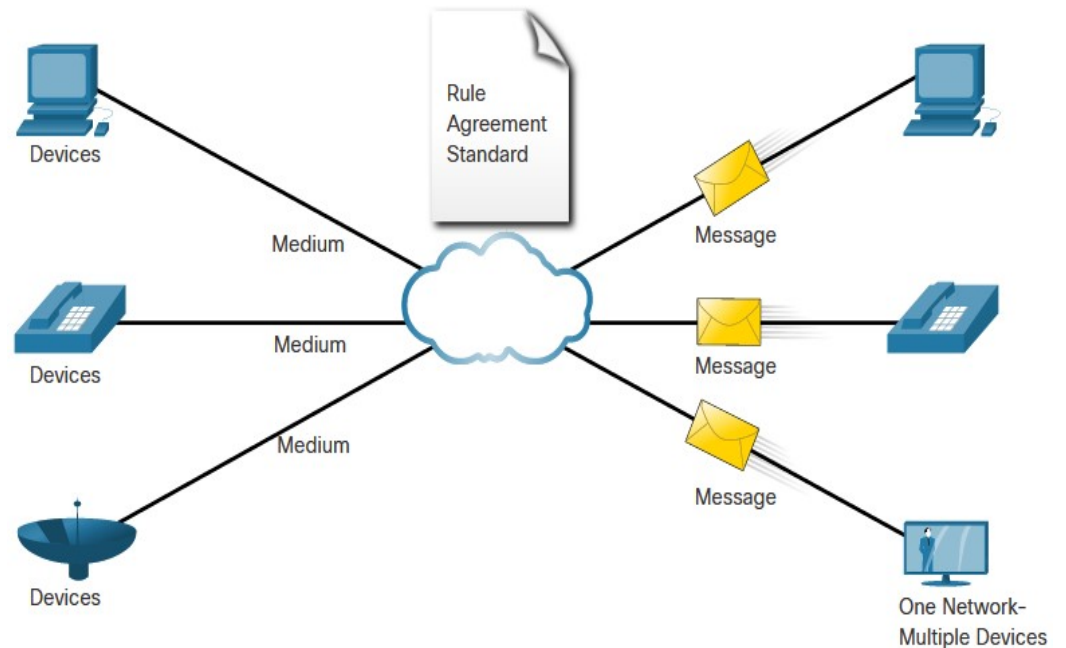
Internet Connections
Video – Download and Install Packet Tracer

This video will demonstrate the download and install process of Packet Tracer.

Video – Getting Started in Cisco Packet Tracer

This video will cover the following:

- Navigate the Packet Tracer interface
- Customize the Packet Tracer Interface

Packet Tracer – Network Representation

In this Packet tracer you will do the following:

- The network model in this activity incorporates many of the technologies that you will master in your CCNA studies.

Note: It is not important that you understand everything you see and do in this activity.

1.6 Reliable Networks

Network Architecture
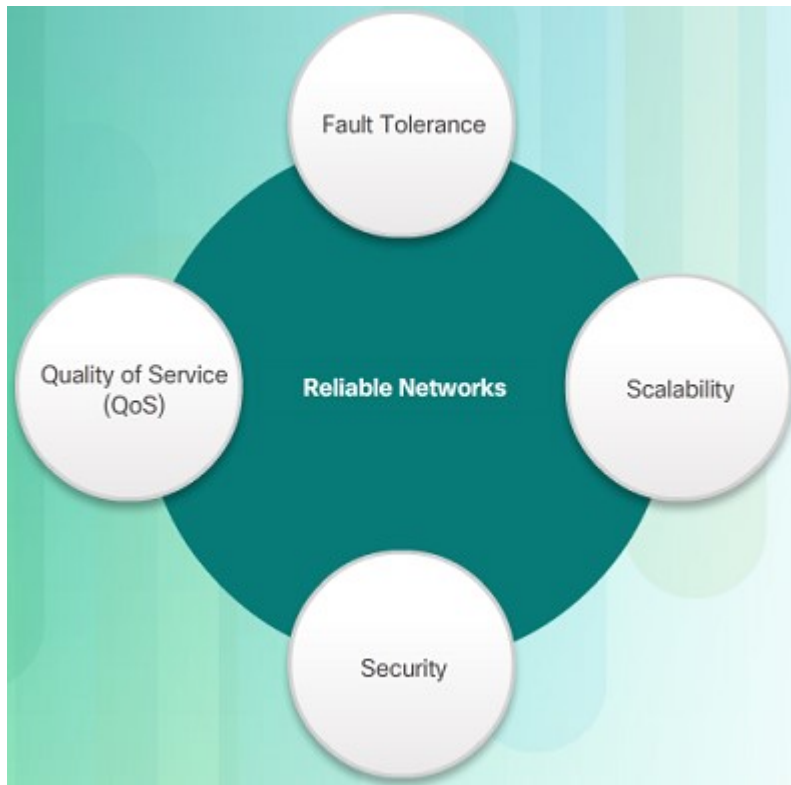
Network Architecture refers to the technologies that support the infrastructure that moves data across the network.

There are four basic characteristics that the underlying architectures need to address to meet user expectations:

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

Fault Tolerance

A fault tolerant network limits the impact of a failure by limiting the number of affected devices. Multiple paths are required for fault tolerance.

Reliable networks provide redundancy by implementing a packet switched network:

- Packet switching splits traffic into packets that are routed over a network.
- Each packet could theoretically take a different path to the destination.

This is not possible with circuit-switched networks which establish dedicated circuits.

Internet

Redundant connections allow for alternative paths if a device or a link fails. The user experience is unaffected.

Scalability

Internet

Additional users and whole networks can be connected to the Internet without degrading performance for existing users.
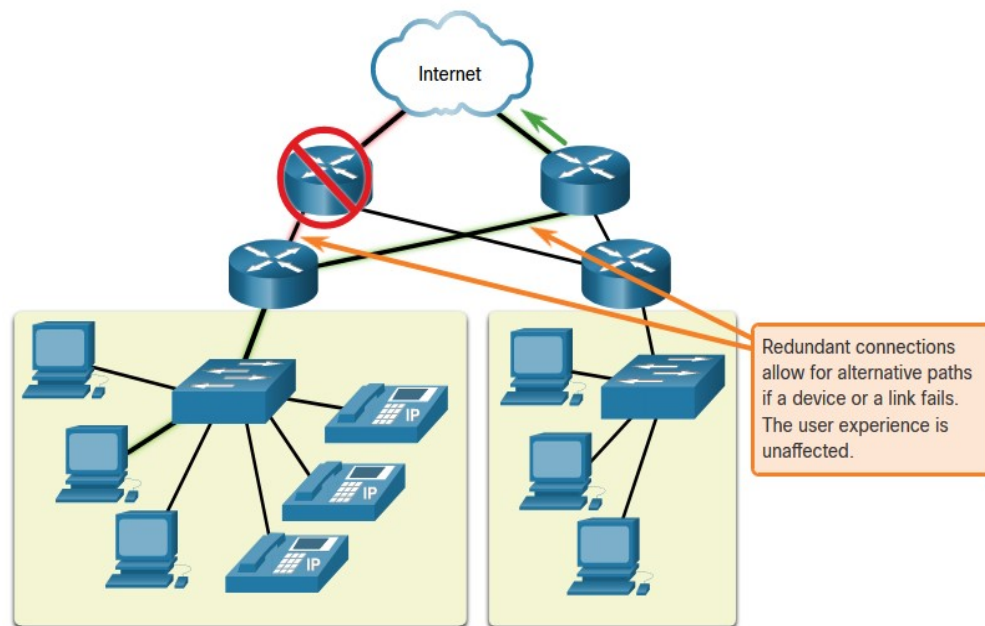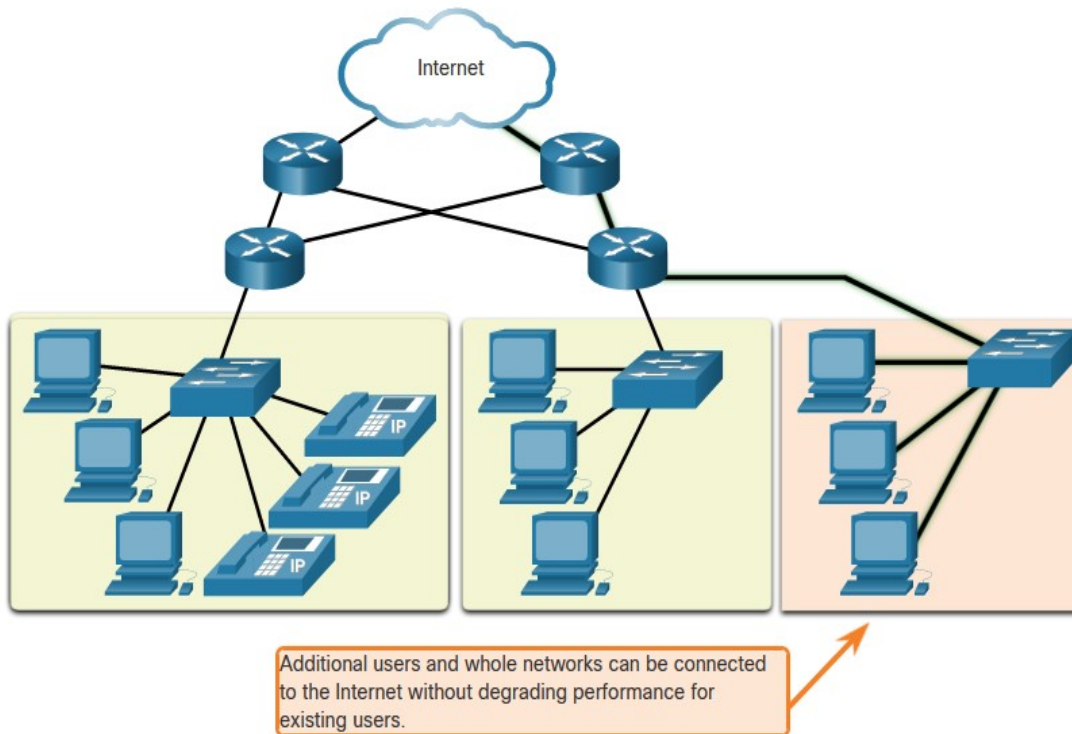
A scalable network can expand quickly and easily to support new users and applications without impacting the performance of services to existing users.

Network designers follow accepted standards and protocols in order to make the networks scalable.
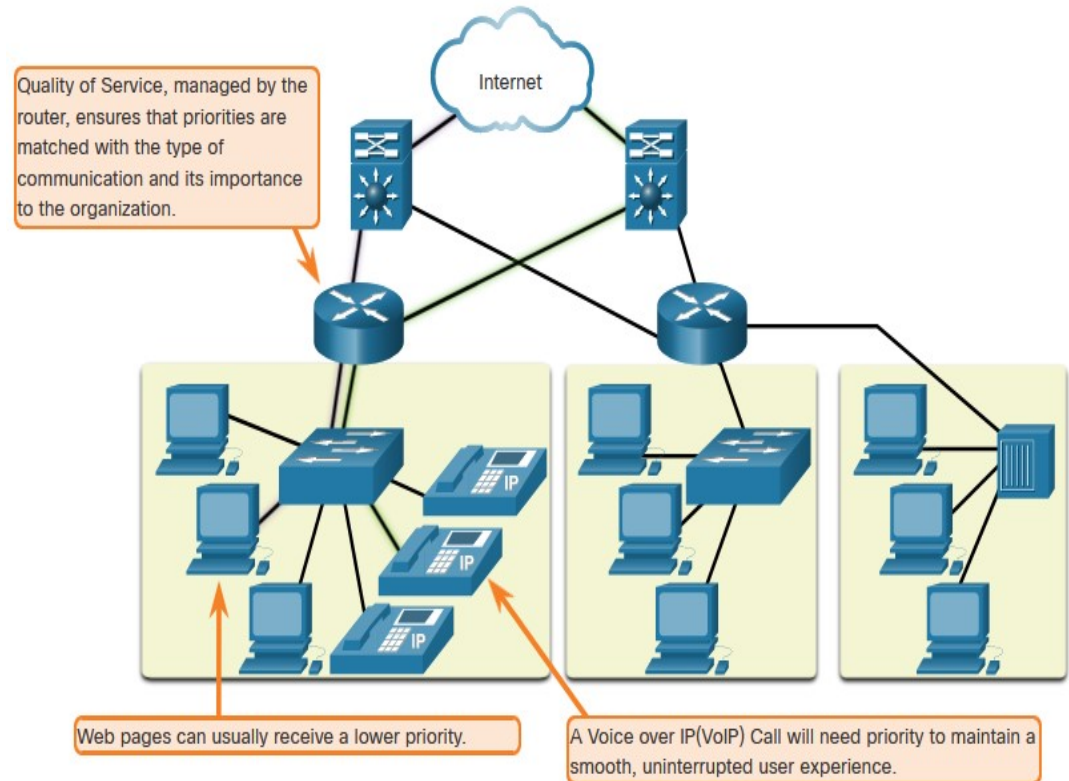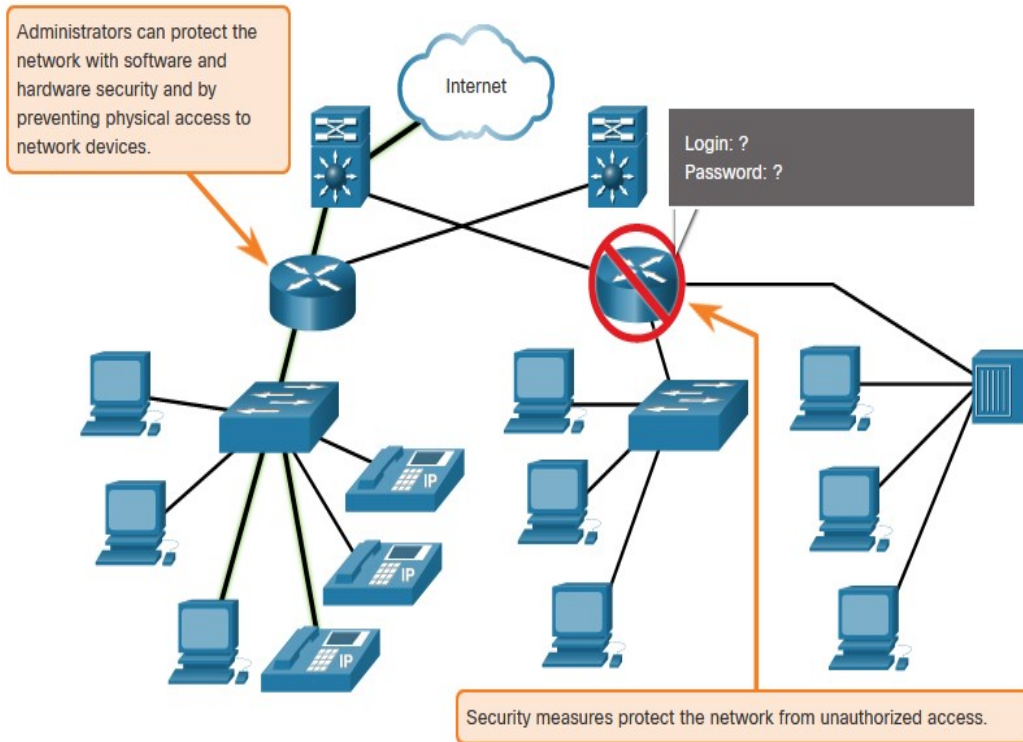
Quality of Service

Voice and live video transmissions require higher expectations for those services being delivered.

Have you ever watched a live video with constant breaks and pauses? This is caused when there is a higher demand for bandwidth than available – and QoS isn't configured.

- Quality of Service (QoS) is the primary mechanism used to ensure reliable delivery of content for all users.

- With a QoS policy in place, the router can more easily manage the flow of data and voice traffic.

Quality of Service, managed by the router, ensures that priorities are matched with the type of communication and its importance to the organization.

Internet

Web pages can usually receive a lower priority.

A Voice over IP(VoIP) Call will need priority to maintain a smooth, uninterrupted user experience.

Network Security

Administrators can protect the network with software and hardware security and by preventing physical access to network devices.

Internet

Login: ?
Password: ?

Security measures protect the network from unauthorized access.

There are two main types of network security that must be addressed:

- Network infrastructure security
  - Physical security of network devices
  - Preventing unauthorized access to the devices
- Information Security
  - Protection of the information or data transmitted over the network

Three goals of network security:

- Confidentiality – only intended recipients can read the data
- Integrity – assurance that the data has not be altered with during transmission
- Availability – assurance of timely and reliable access to data for authorized users

1.7 Network Trends

Recent Trends

The role of the network must adjust and continually transform in order to be able to keep up with new technologies and end user devices as they constantly come to the market.

Several new networking trends that effect organizations and consumers:

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

Bring Your Own Device
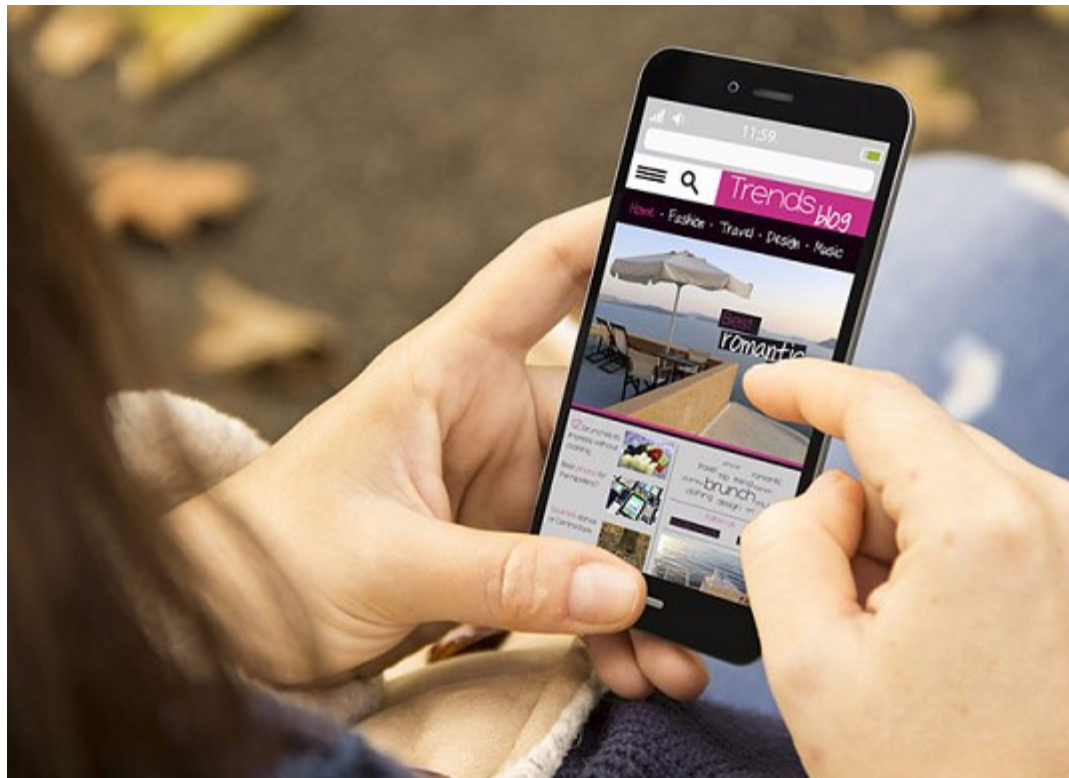
Bring Your Own Device (BYOD) allows users to use their own devices giving them more opportunities and greater flexibility.

BYOD allows end users to have the freedom to use personal tools to access information and communicate using their:

- Laptops
- Netbooks
- Tablets
- Smartphones
- E-readers

BYOD means any device, with any ownership, used anywhere.

Online Collaboration
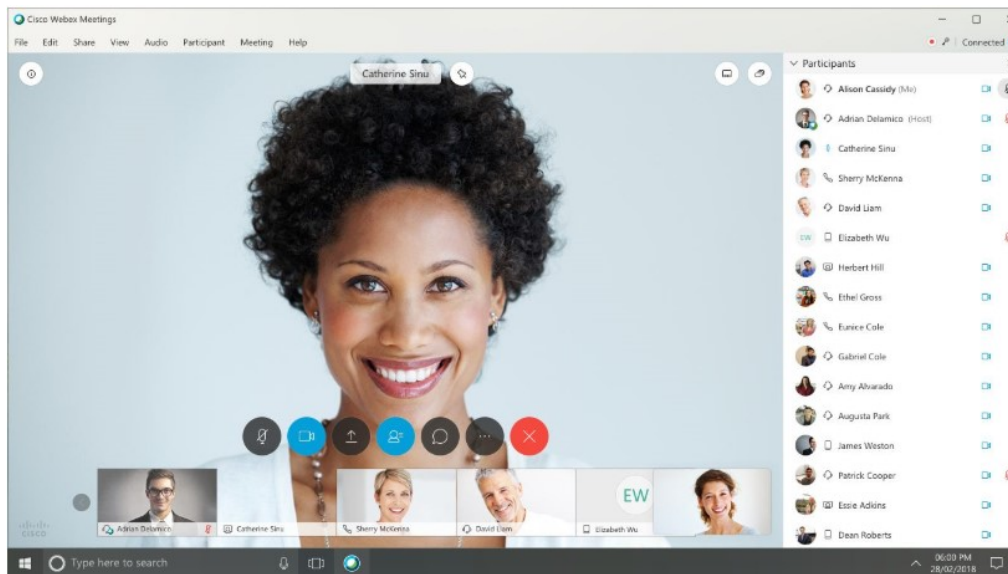
- Collaborate and work with others over the network on joint projects.

- Collaboration tools including Cisco WebEx (shown in the figure) gives users a way to instantly connect and interact.

- Collaboration is a very high priority for businesses and in education.

- Cisco Webex Teams is a multifunctional collaboration tool.

  - send instant messages
  - post images
  - post videos and links

Video Communication

- Video calls are made to anyone, regardless of where they are located.

- Video conferencing is a powerful tool for communicating with others.

- Video is becoming a critical requirement for effective collaboration.

- Cisco TelePresence powers is one way of working where everyone, everywhere.

Network Trends
Video – Cisco WebEx for Huddles

54
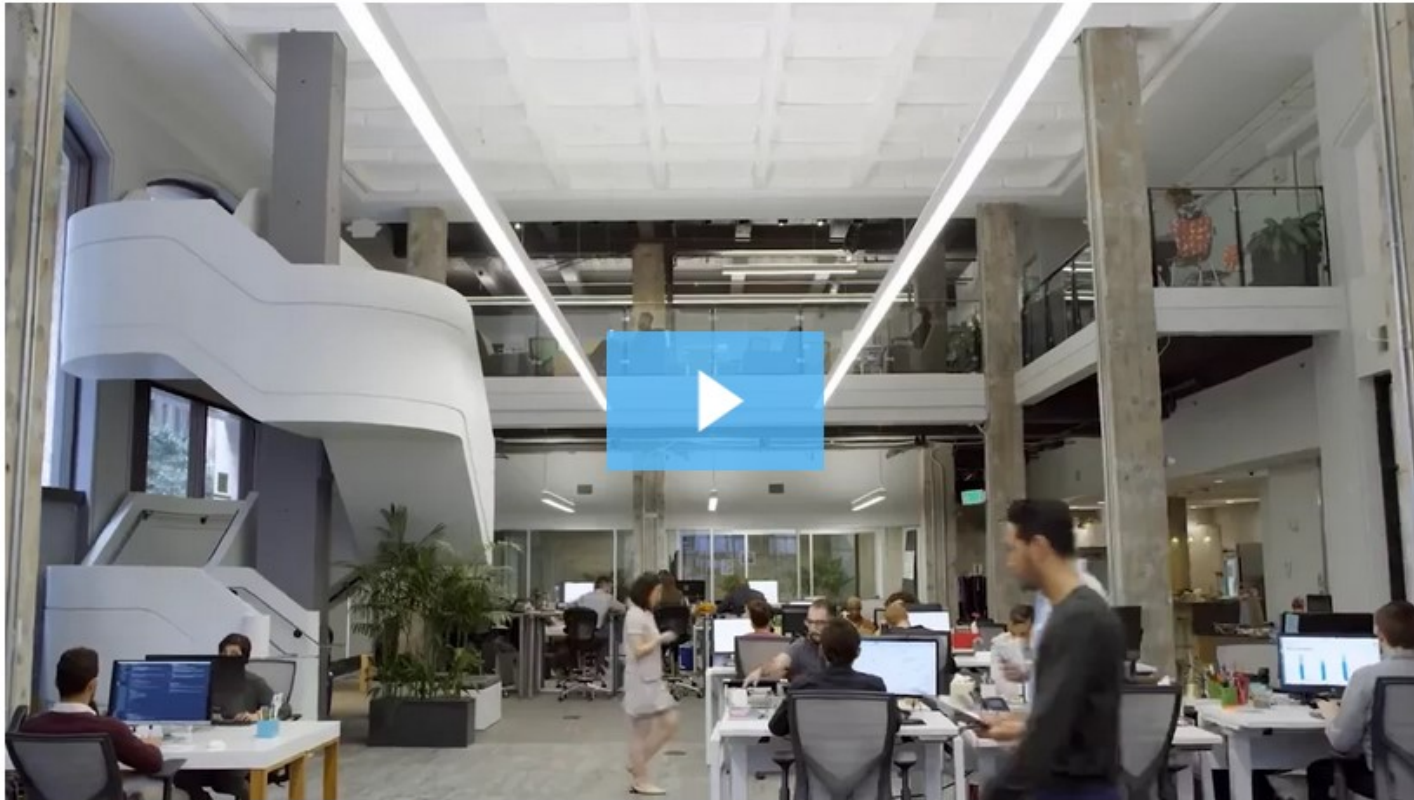
Cloud Computing

Cloud computing allows us to store personal files or backup our data on servers over the internet.

- Applications can also be accessed using the Cloud.
- Allows businesses to deliver to any device anywhere in the world.

Cloud computing is made possible by data centers.

- Smaller companies that can't afford their own data centers, lease server and storage services from larger data center organizations in the Cloud.

Cloud Computing (Cont.)

Four types of Clouds:

- Public Clouds
  - Available to the general public through a pay-per-use model or for free.
- Private Clouds
  - Intended for a specific organization or entity such as the government.
- Hybrid Clouds
  - Made up of two or more Cloud types – for example, part custom and part public.
  - Each part remains a distinctive object but both are connected using the same architecture.
- Custom Clouds
  - Built to meet the needs of a specific industry, such as healthcare or media.
  - Can be private or public.

Technology Trends in the Home
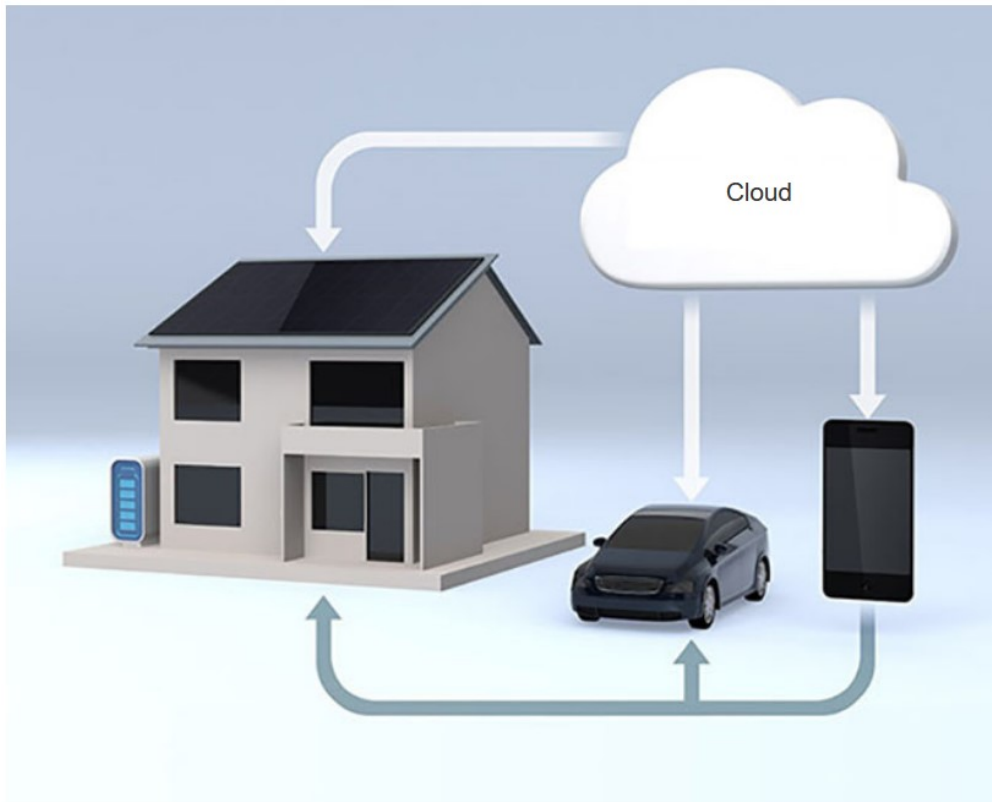
- Smart home technology is a growing trend that allows technology to be integrated into every-day appliances which allows them to interconnect with other devices.

- Ovens might know what time to cook a meal for you by communicating with your calendar on what time you are scheduled to be home.

- Smart home technology is currently being developed for all rooms within a house.

Network Trends
Powerline Networking

PLEK400
4-Port Powerline Adapter

Wireless-N Router

PLE400

PLSK400
4-Port Powerline Adapter

Powerline Connection ————

Wired Connection ————
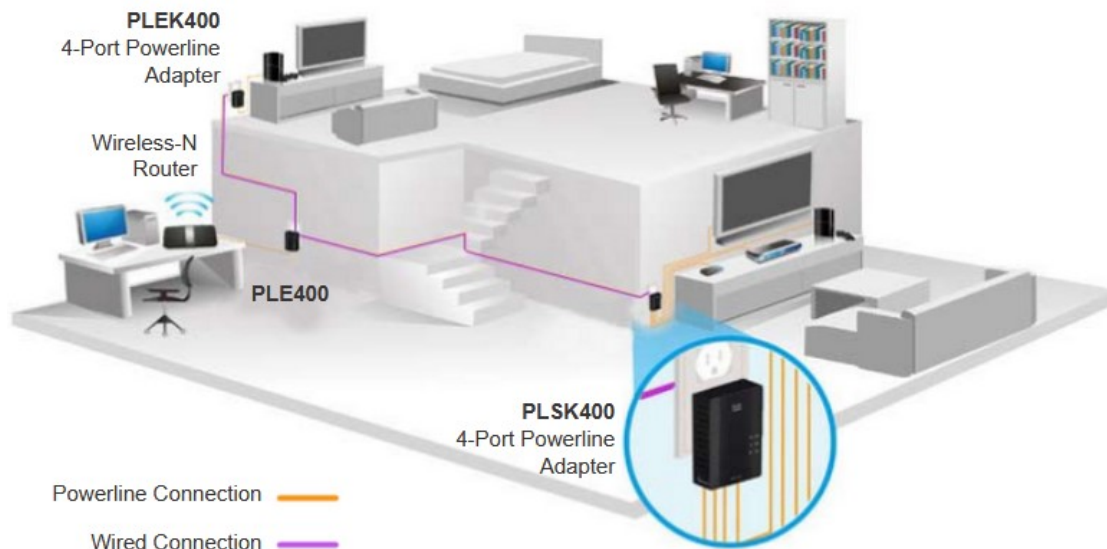
- Powerline networking can allow devices to connect to a LAN where data network cables or wireless communications are not a viable option.

- Using a standard powerline adapter, devices can connect to the LAN wherever there is an electrical outlet by sending data on certain frequencies.

- Powerline networking is especially useful when wireless access points cannot reach all the devices in the home.

Wireless Broadband

Wireless Broadband Service
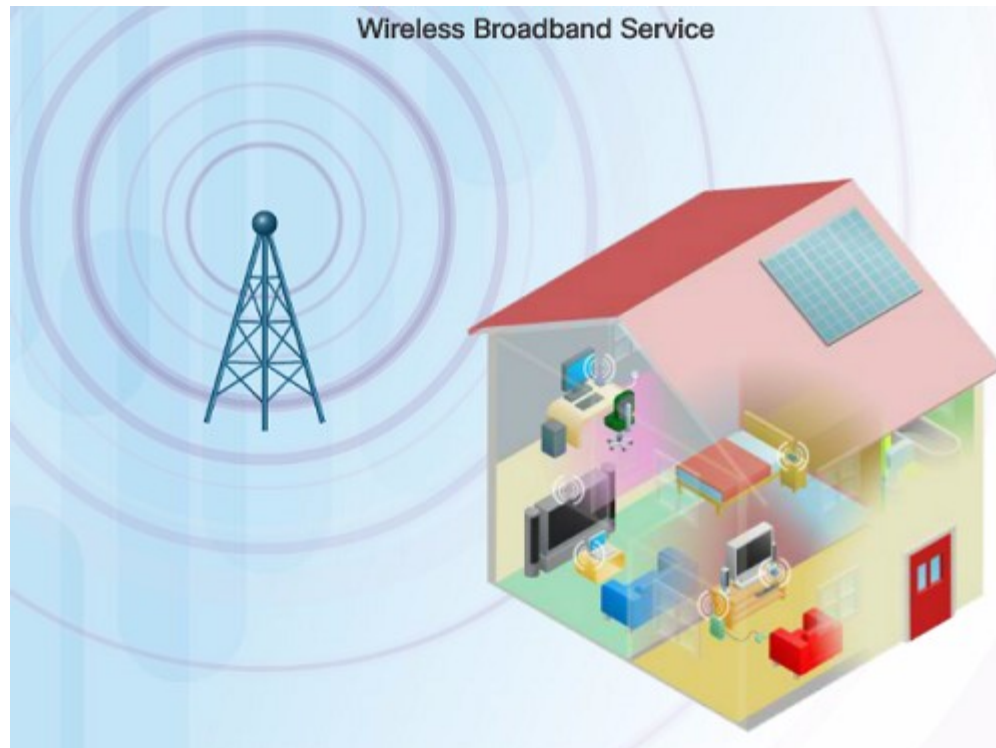
In addition to DSL and cable, wireless is another option used to connect homes and small businesses to the internet.

- More commonly found in rural environments, a Wireless Internet Service Provider (WISP) is an ISP that connects subscribers to designated access points or hotspots.

- Wireless broadband is another solution for the home and small businesses.

  - Uses the same cellular technology used by a smart phone.

  - An antenna is installed outside the house providing wireless or wired connectivity for devices in the home.

1.8 Network Security

Security Threats
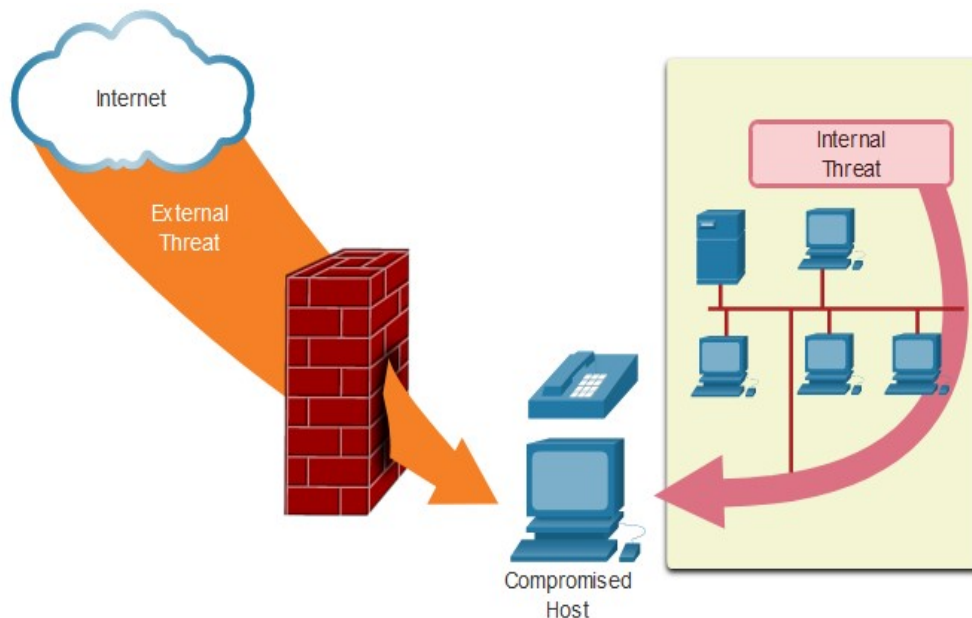
- Network security is an integral part of networking regardless of the size of the network.

- The network security that is implemented must take into account the environment while securing the data, but still allowing for quality of service that is expected of the network.

- Securing a network involves many protocols, technologies, devices, tools, and techniques in order to secure data and mitigate threats.

- Threat vectors might be external or internal.

Security Threats (Cont.)
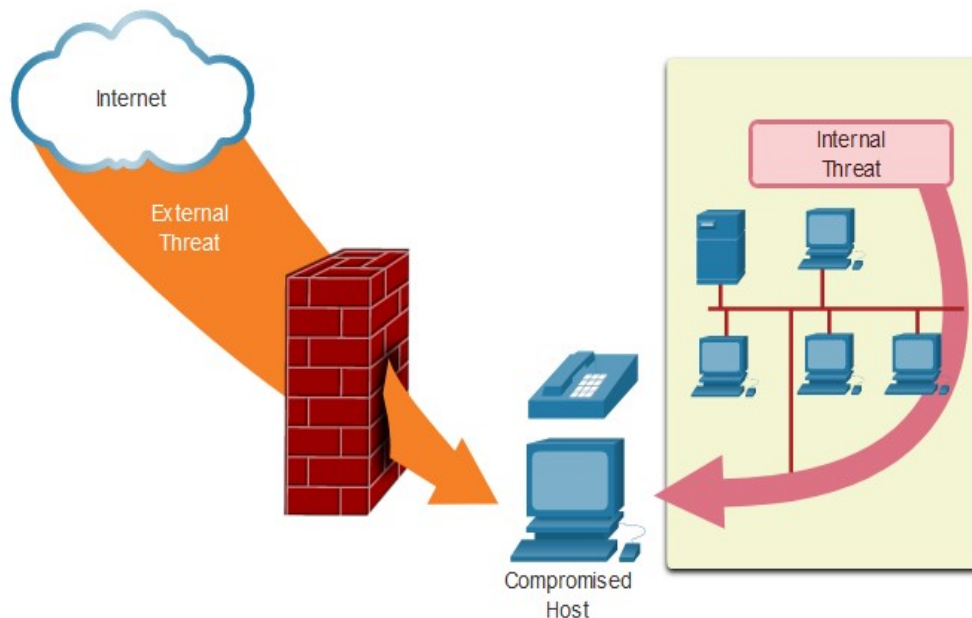
External Threats:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks
- Threat Actor attacks
- Denial of service attacks
- Data interception and theft
- Identity theft

Internal Threats:

- lost or stolen devices
- accidental misuse by employees
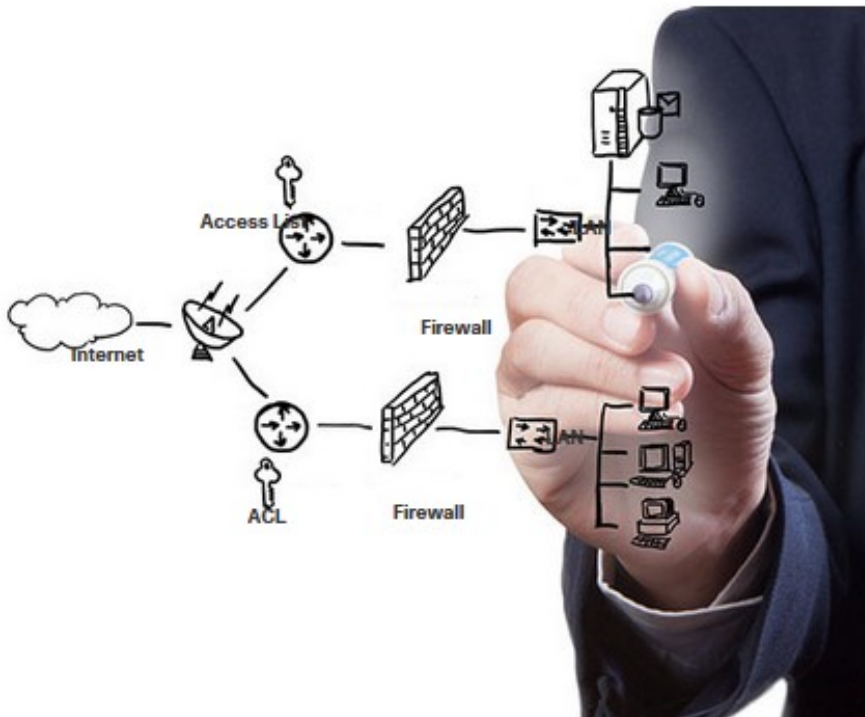- malicious employees

Security Solutions

Security must be implemented in multiple layers using more than one security solution.

Network security components for home or small office network:

- Antivirus and antispyware software should be installed on end devices.

- Firewall filtering used to block unauthorized access to the network.

Security Solutions (Cont.)

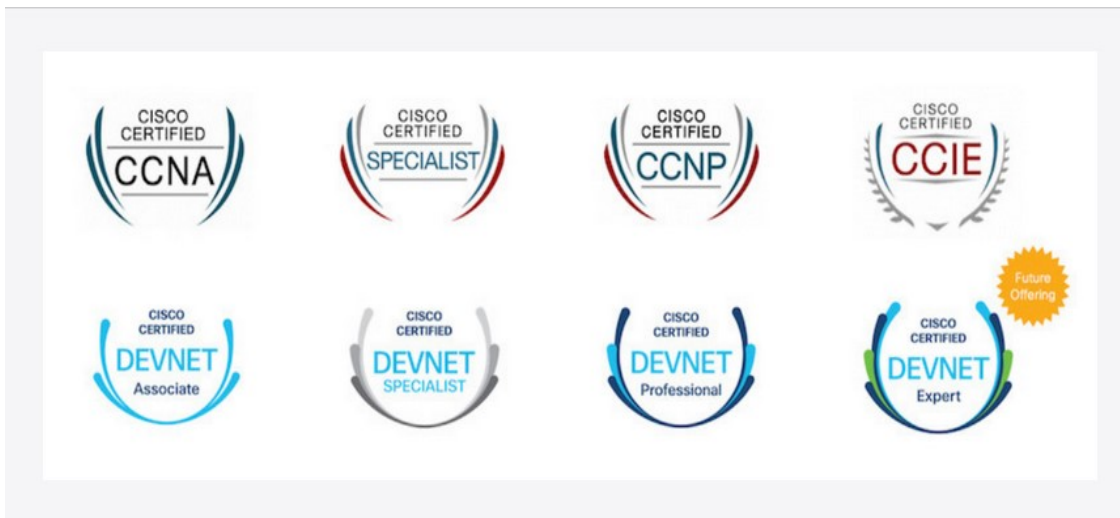Larger networks have additional security requirements:

- Dedicated firewall system
- Access control lists (ACL)
- Intrusion prevention systems (IPS)
- Virtual private networks (VPN)

The study of network security starts with a clear understanding of the underlying switching and routing infrastructure.

1.9 The IT Professional

The IT Professional
CCNA

The Cisco Certified Network Associate (CCNA) certification:

- demonstrates that you have a knowledge of foundational technologies
- ensures you stay relevant with skills needed for the adoption of next-generation technologies.

The new CCNA focus:

- IP foundation and security topics
- Wireless, virtualization, automation, and network programmability.

New DevNet certifications at the associate, specialist and professional levels, to validate your software development skills.

Specialist certification validate your skills in line with your job role and interests.

The IT Professional
Networking Jobs

Employment Opportunities
Discover career possibilities and options from our Talent Bridge employment program.

Talent Bridge Matching Engine
Find employment opportunities where you live with the new pilot program, the Talent Bridge Matching Engine. Search for jobs with Cisco as well as Cisco partners and distributors seeking Cisco Networking Academy students and alumni. Register now to complete your profile. Must be 18 years of age or older to register and participate in the Matching Engine.

Be Part of Our Dream Team
We offer opportunities to gain hands-on experiences throughout the year. These are specific projects that we invite students to participate in as a Dream Team member. Learn more about this experience and how you can participate.

Your Career, our Talent Bridge Resources
Learn about the resources we have to offer that can help you on your journey to becoming gainfully employed.

Match with Jobs

Connect with Peers

Enroll in a Career Preparation Workshop

At www.netacad.com you can click the Careers menu and then select Employment opportunities.

- Find employment opportunities by using the Talent Bridge Matching Engine.

- Search for jobs with Cisco, Cisco partners and distributors seeking Cisco Networking Academy students and alumni.

The IT Professional
Lab – Researching IT and Networking Job Opportunities

In this lab, you will complete the following objectives:

- Research Job Opportunities
- Reflect on Research

1.10 Module Practice and Quiz

What did I learn in this module?

- Through the use of networks, we are connected like never before.
- All computers that are connected to a network and participate directly in network communication are classified as hosts.
- Diagrams of networks often use symbols to represent the different devices and connections that make up a network.
- A diagram provides an easy way to understand how devices connect in a large network.
- The two types of network infrastructures are Local Area Networks (LANs), and Wide Area Networks (WANs).
- SOHO internet connections include cable, DSL, Cellular, Satellite, and Dial-up telephone.
- Business internet connections include Dedicated Leased Line, Metro Ethernet, Business DSL, and Satellite.

What did I learn in this module? (Cont.)

- Network architecture refers to the technologies that support the infrastructure and the programmed services and rules, or protocols, that move data across the network.

- There are four basic characteristics of network architecture: Fault Tolerance, Scalability, Quality of Service (QoS), and Security.

- Recent networking trends that affect organizations and consumers: Bring Your Own Device (BYOD), online collaboration, video communications, and cloud computing.

- There are several common external and internal threats to networks.

- Larger networks and corporate networks use antivirus, antispyware, and firewall filtering, but they also have other security requirements: Dedicated firewall systems, Access control lists (ACL), Intrusion prevention systems (IPS), and Virtual private networks (VPN)

- The Cisco Certified Network Associate (CCNA) certification demonstrates your knowledge of foundational technologies.

New Terms and Commands

- Peer-to-Peer File Sharing
- Small Office/Home Office or SOHO
- Medium to large network
- Server
- Client
- Peer-to-Peer network
- End device
- Intermediary device
- Medium
- Network Interface Card (NIC)
- Physical Port
- Interface
- Physical topology diagram

- Logical topology diagram
- Local Area Network (LAN)
- Wide Area Network (WAN)
- Internet
- Intranet
- Extranet
- Internet Service Provider (ISP)
- Converged networks
- Network architecture
- Fault tolerant network
- Packet-switched network
- Circuit-switched network
- Scalable network
- Quality of Service (Qos)

- Network bandwidth
- Bring Your Own Device (BYOD)
- Collaboration
- Cloud computing
- Private clouds
- Hybrid clouds
- Public clouds
- Custom clouds
- Data center
- Smart home technology
- Powerline networking
- Wireless Internet Service Provider (WISP)
- Network architecture