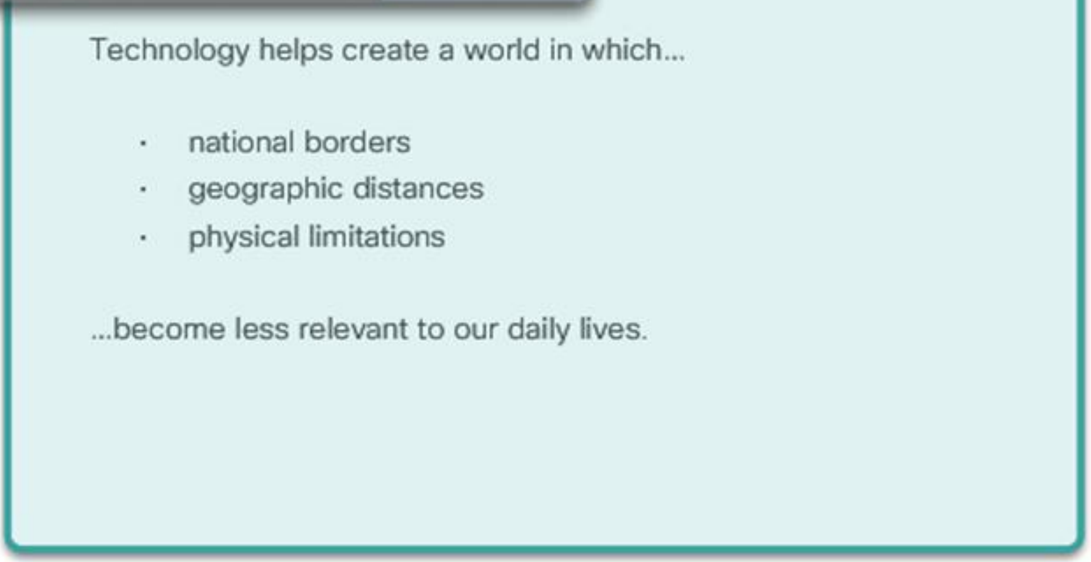
R&S Chapter 1 Exploring the network

This chapter introduces the platform of data networks upon which our social and business relationships increasingly depend. The material lays the groundwork for exploring the services, technologies, and issues encountered by network professionals as they design, build, and maintain the modern network

1.1.0.2 Activity – Draw your own network



Technology helps create a world in which...

- national borders
- geographic distances
- physical limitations

...become less relevant to our daily lives.

Draw Your Concept of the Internet

Draw and label a map of the Internet as you interpret it now. Include your home or school/university location and its respective cabling, equipment, devices, etc. Some items you may wish to include:

- Devices/Equipment
- Media (cabling)
- Link Addresses or Names
- Sources & Destinations
- Internet Service Providers

1.1.1.1 Networks in our Daily Lives

1.1.1.2 Technology Then and Now

1.1.1.3 No Boundaries

Advancements in networking technologies are perhaps the most significant changes in the world today. They are helping to create a world in which national borders, geographic distances, and physical limitations become less relevant presenting ever-diminishing obstacles

1.1.1.4 Networks Support the Way We Learn

1.1.1.5 Networks and Communication

- Texting –.
- Social Media –
- Collaboration Tools –
- Blogs –
- Wikis –
- Podcasting
- Peer-to-Peer (P2P) File Sharing –

1.1.1.6 Networks at Work

In the business world, data networks were initially used by businesses to internally record and manage financial information, customer information, and employee payroll systems. These business networks evolved to enable the transmission of many different types of information services, including email, video, messaging, and telephony

1.1.1.7 Networks in Entertainment

How do you use networks for entertainment?

1.1.1.8 Lab - Researching Network Collaboration Tools

In this lab, you will complete the following objectives:

- **Part 1: Use Collaboration Tools**
- **Part 2: Share Documents with Google Drive**
- **Part 3: Explore Conferencing and Web Meetings**
- **Part 4: Create Wiki Pages**

1.1.2.1 Networks of Many Sizes

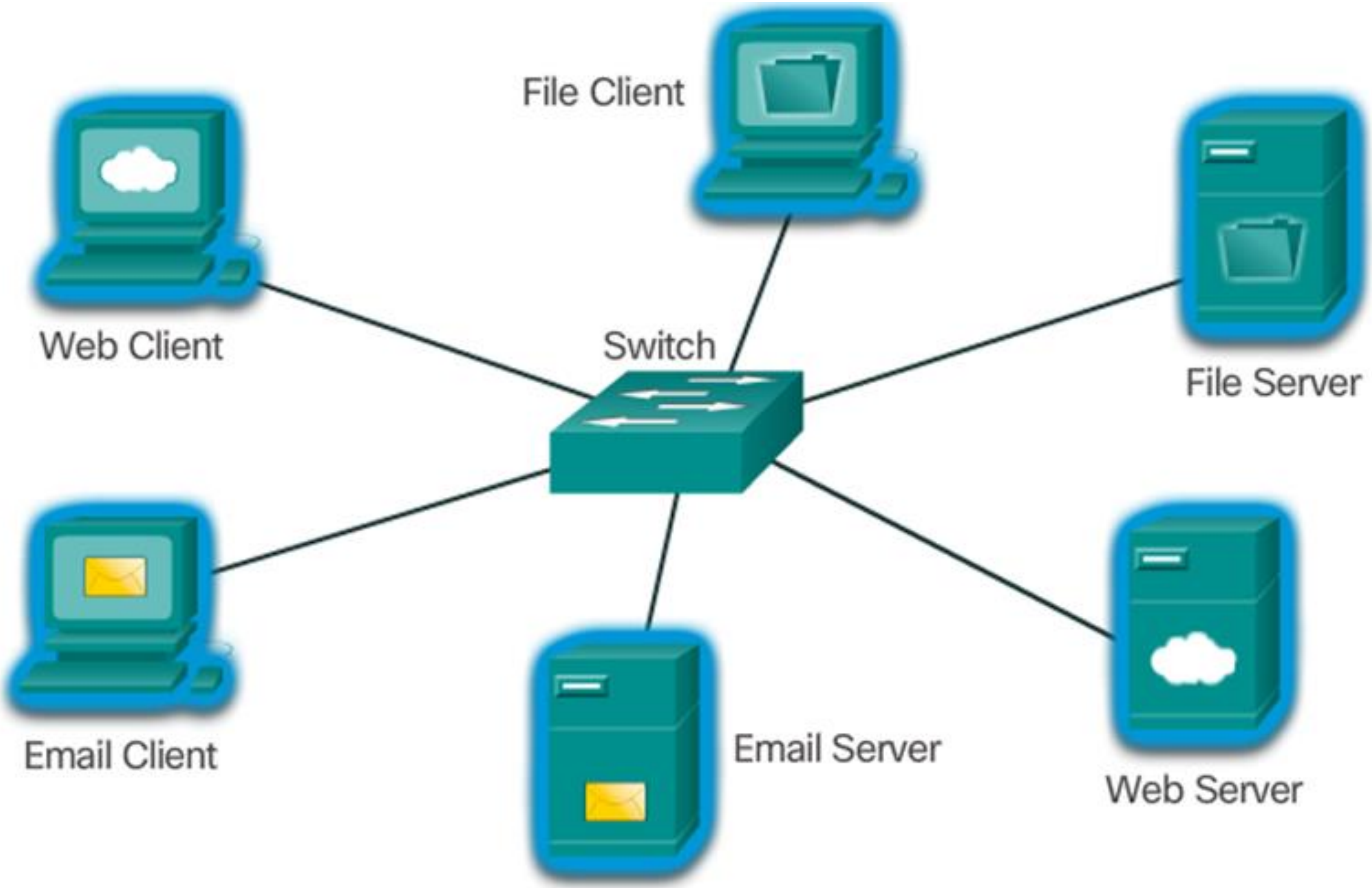
Small Home Networks

Small Office/Home Office Networks

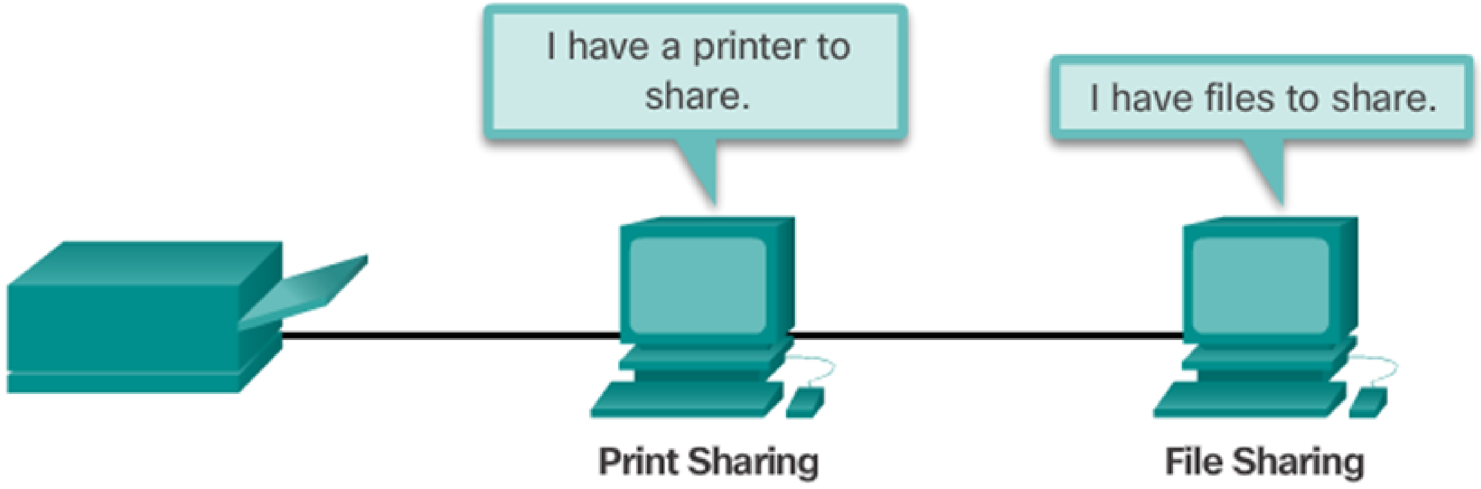
Medium to Large Networks

World Wide Networks

1.1.2.2 Clients and Servers



1.1.2.3 Peer-to-Peer



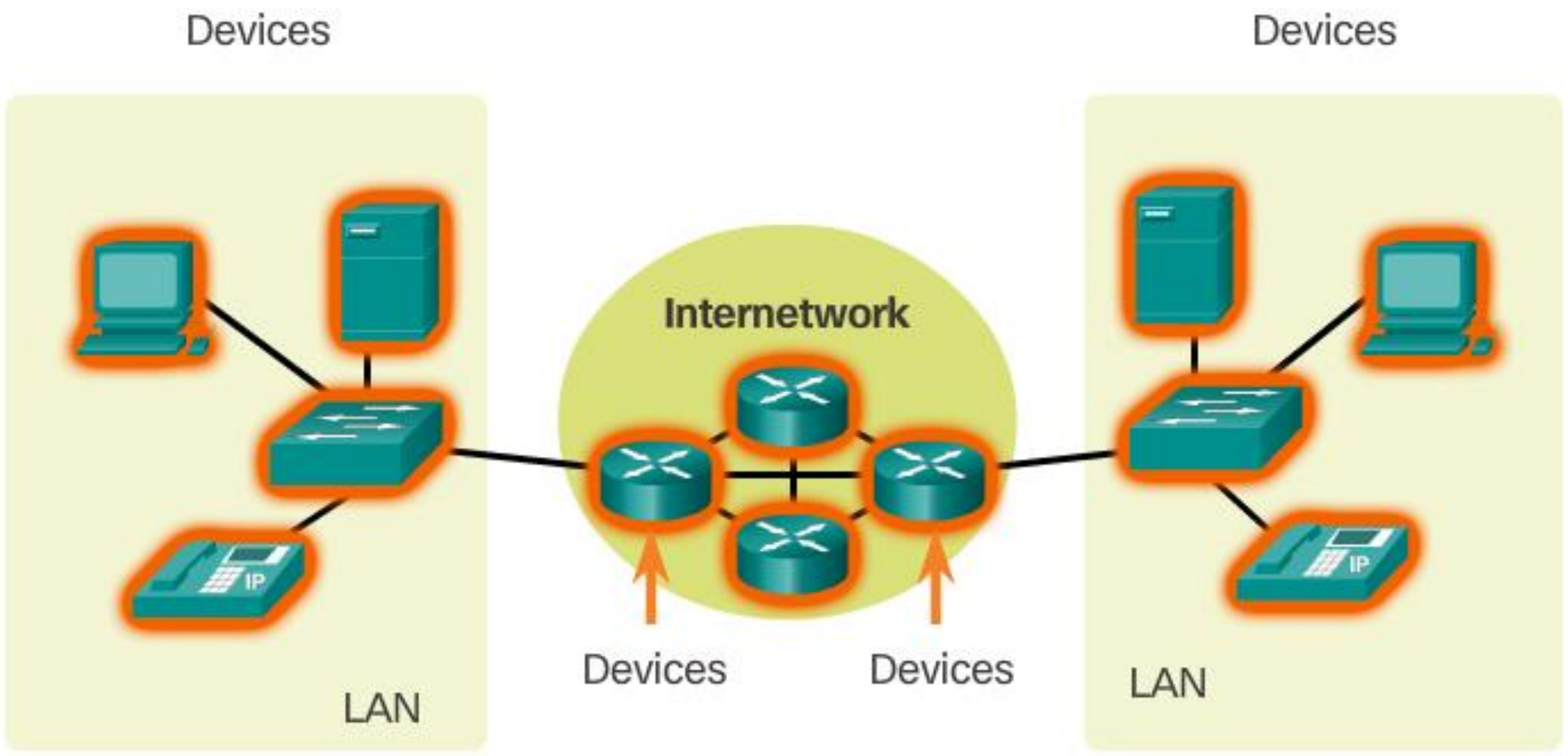
The advantages of peer-to-peer networking:

- 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

1.2.1.1 Overview of Network Components

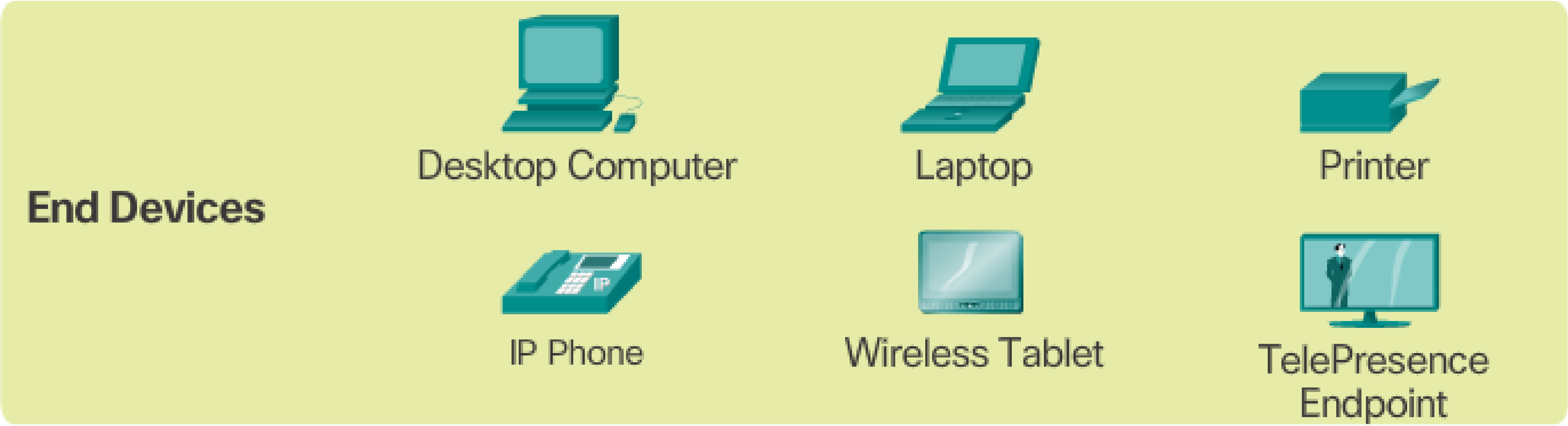


Devices

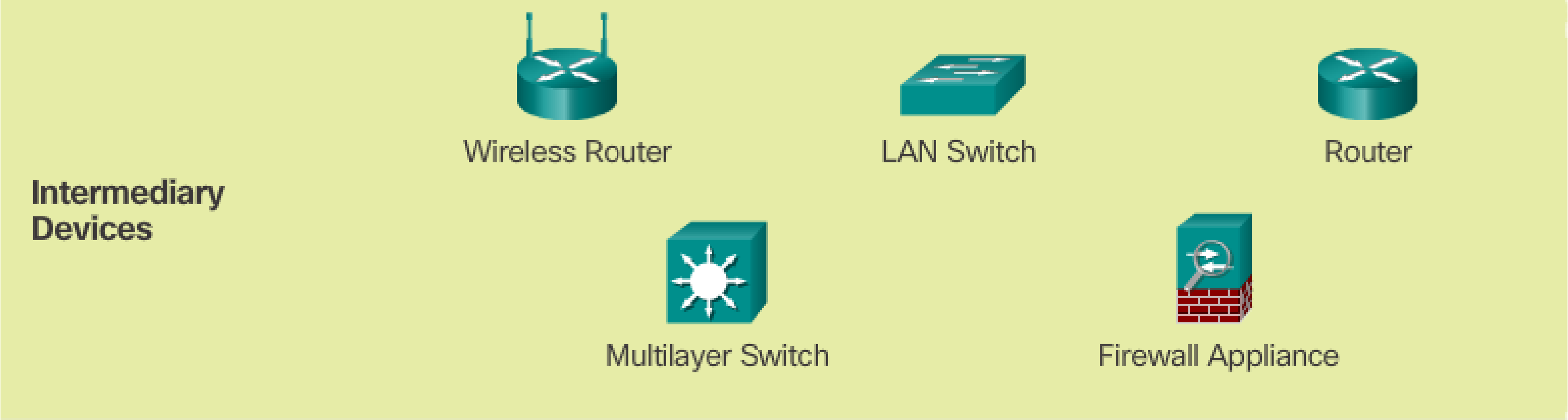
Media

Services

1.2.1.2 End Devices



1.2.1.3 Intermediary Network Devices

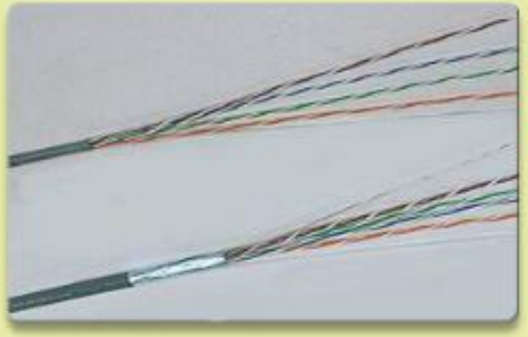


Intermediary network devices perform some or all of these functions:

- Regenerate and retransmit data signals
- Maintain information about what pathways exist through the network and internetwork
- Notify other devices of errors and communication failures
- Direct data along alternate pathways when there is a link failure
- Classify and direct messages according to priorities
- Permit or deny the flow of data, based on security settings

1.2.1.4 Network Media

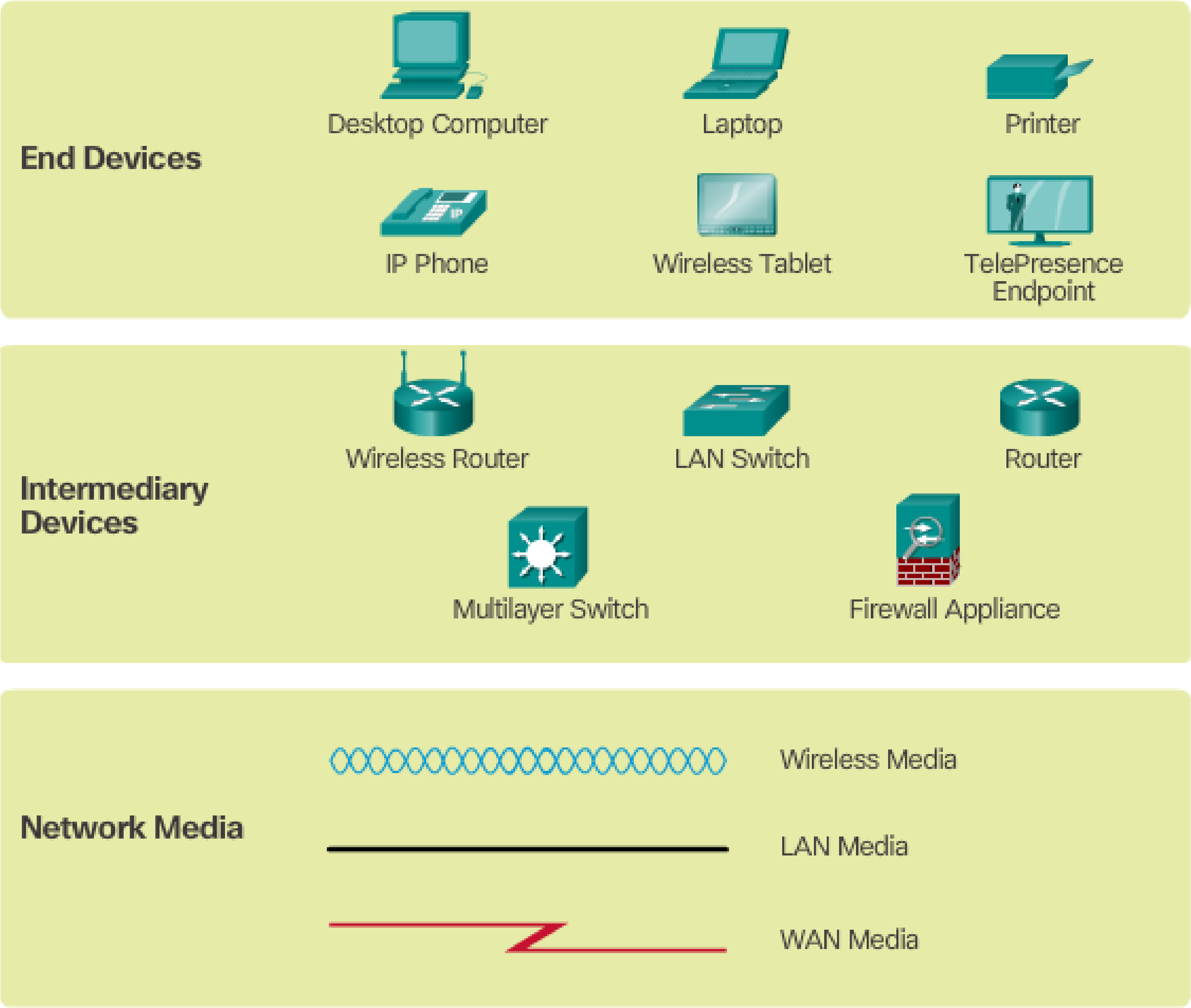
Copper



Fiber Optic

Wireless

1.2.1.5 Network Representations



End Devices

Desktop Computer

Laptop

Printer

IP Phone

Wireless Tablet

TelePresence Endpoint

Intermediary Devices

Wireless Router

LAN Switch

Router

Multilayer Switch

Firewall Appliance

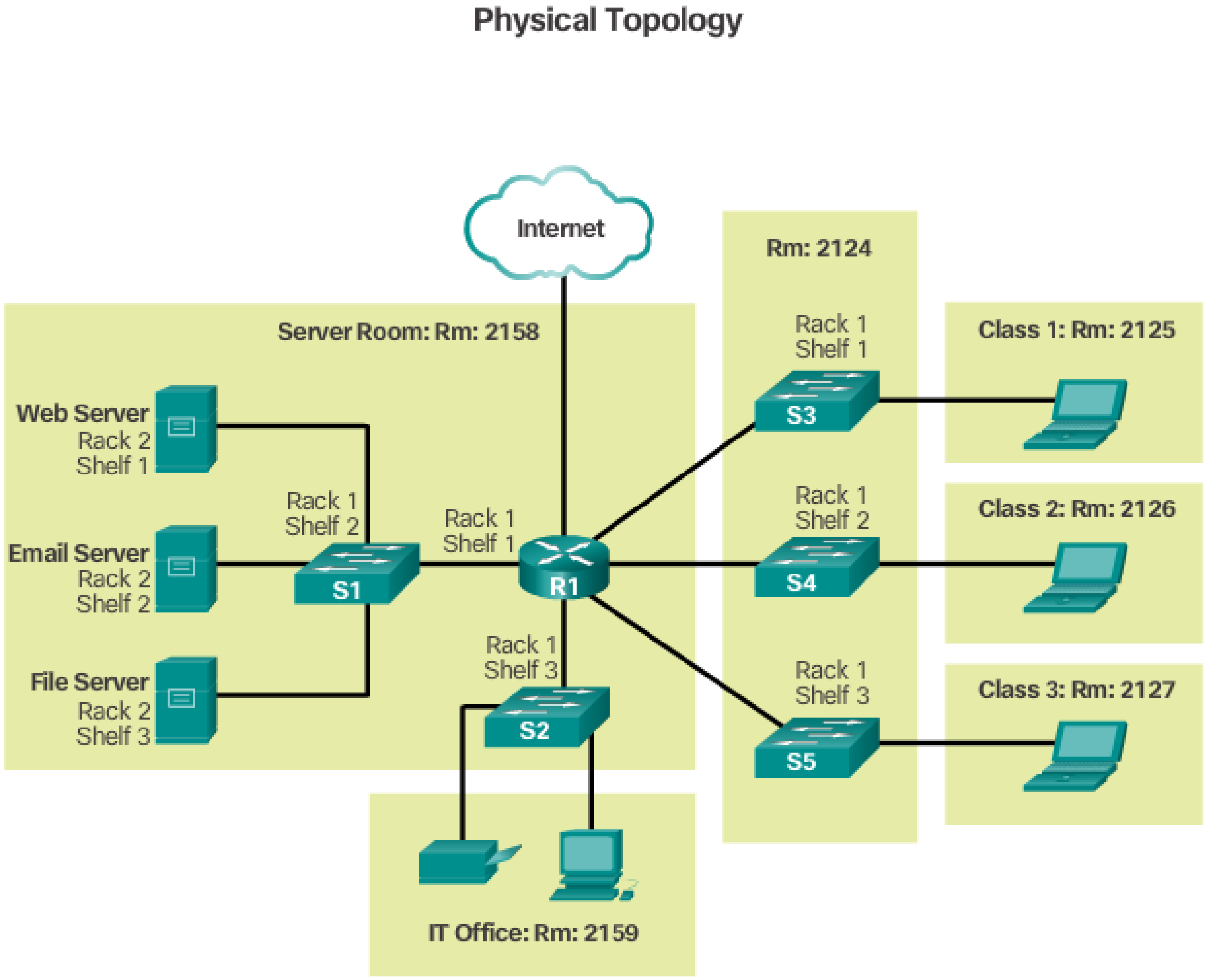
Network Media

Wireless Media

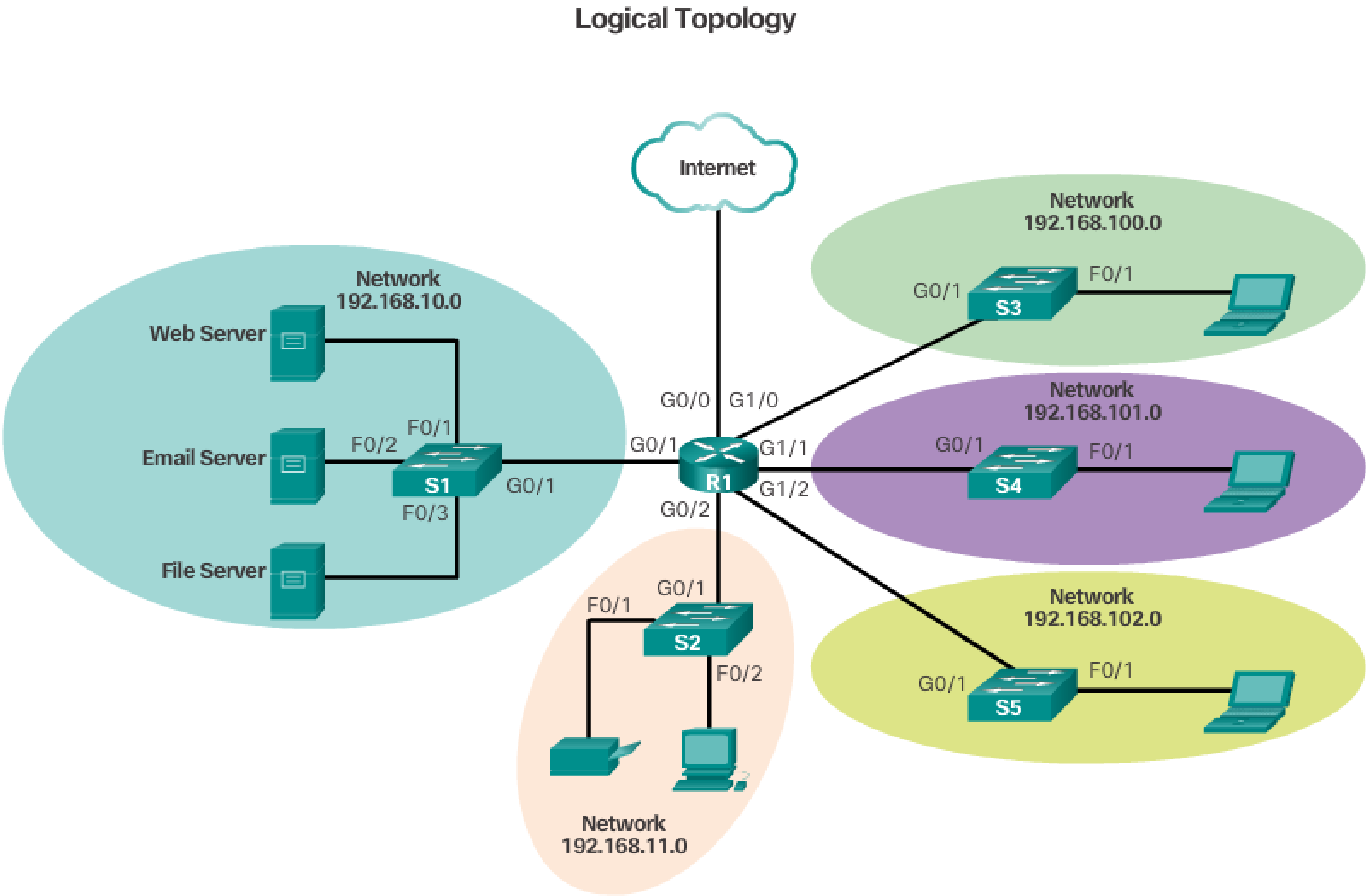
LAN Media

WAN Media

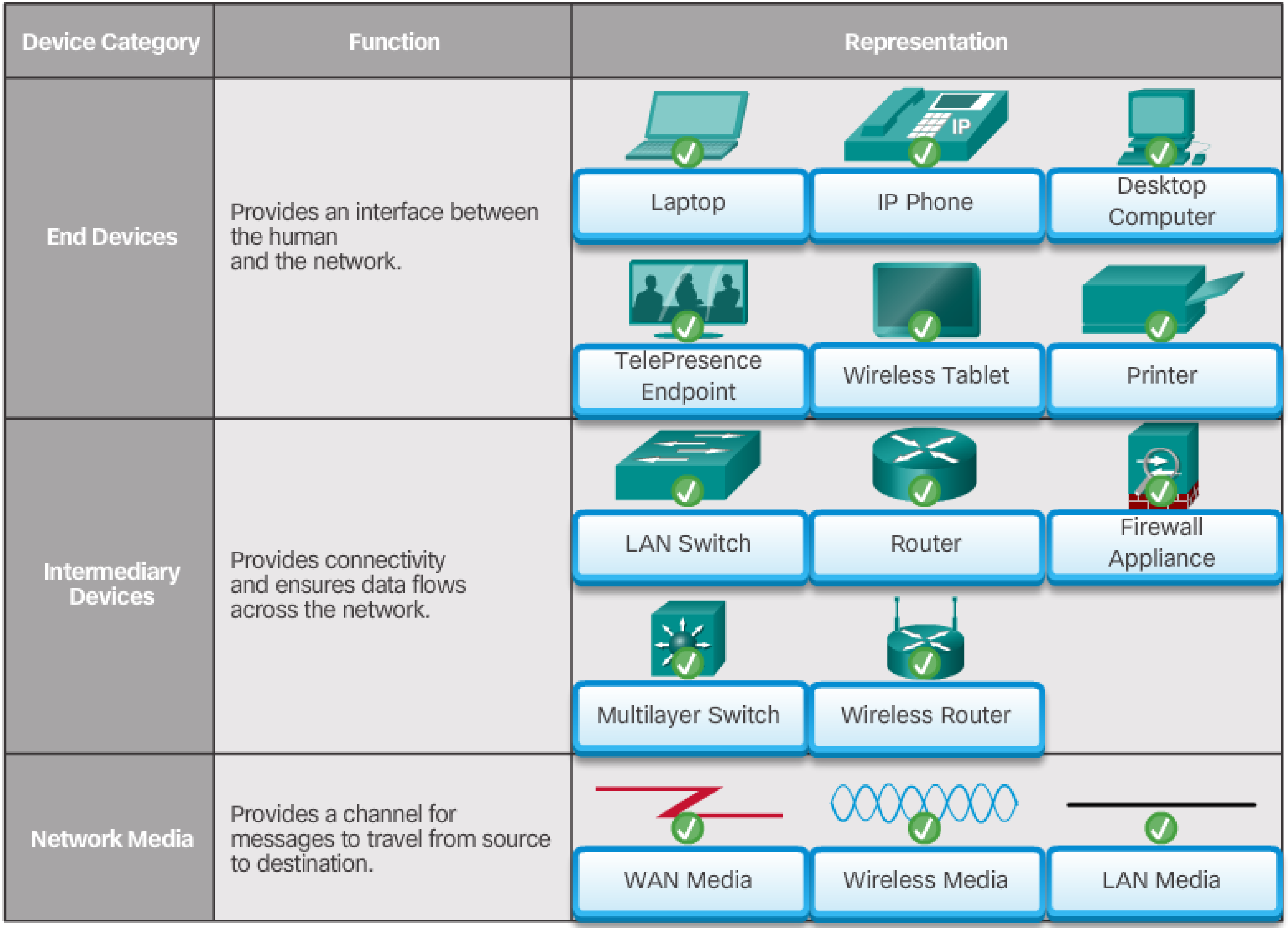
1.2.1.6 Topology Diagrams



1.2.1.6 Topology Diagrams

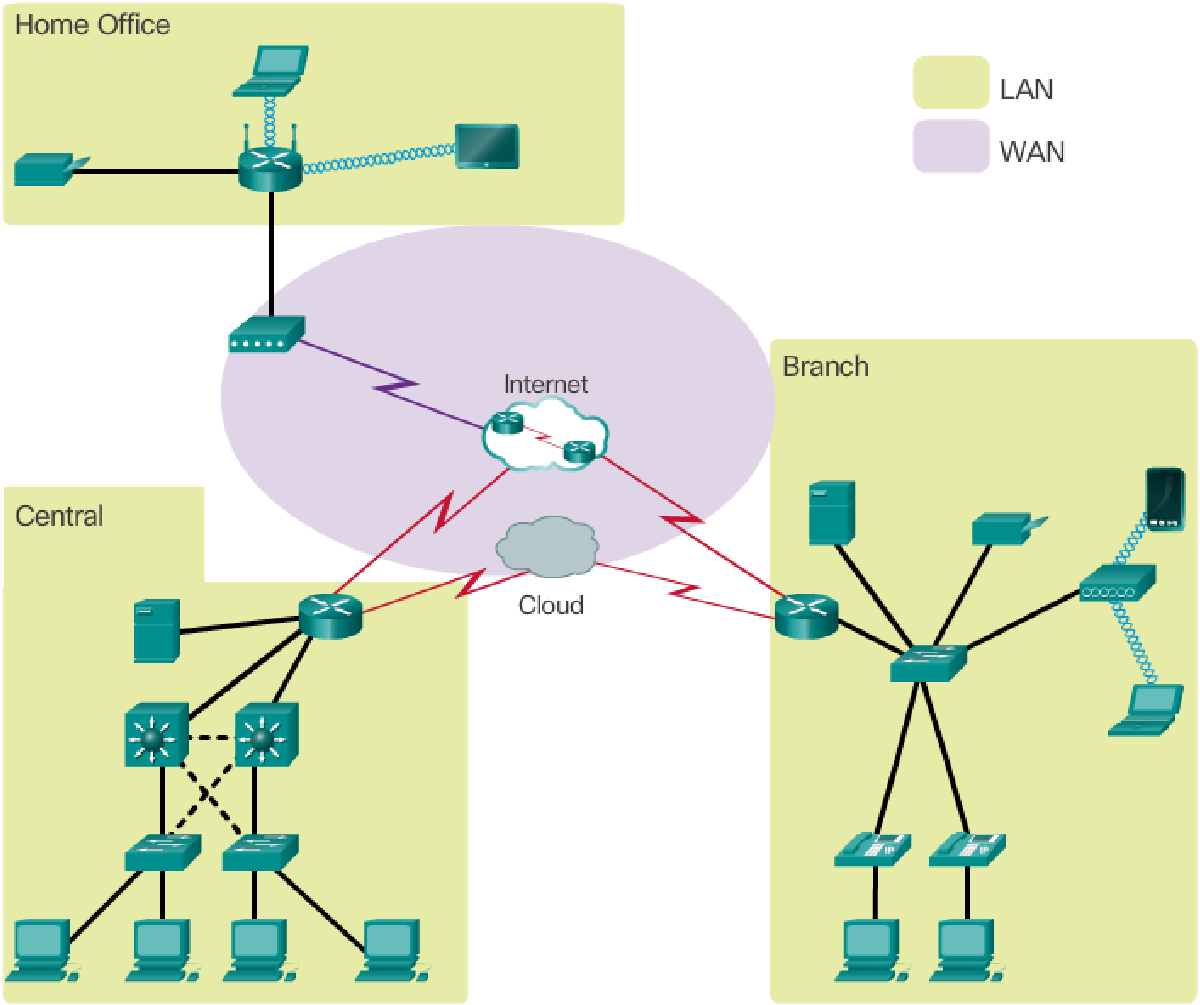


1.2.1.7 Activity - Network Component Representations and Functions



Device Category	Function	Representation
End Devices	Provides an interface between the human and the network.	Laptop IP Phone Desktop Computer TelePresence Endpoint Wireless Tablet Printer
Intermediary Devices	Provides connectivity and ensures data flows across the network.	LAN Switch Router Firewall Appliance Multilayer Switch Wireless Router
Network Media	Provides a channel for messages to travel from source to destination.	WAN Media Wireless Media LAN Media

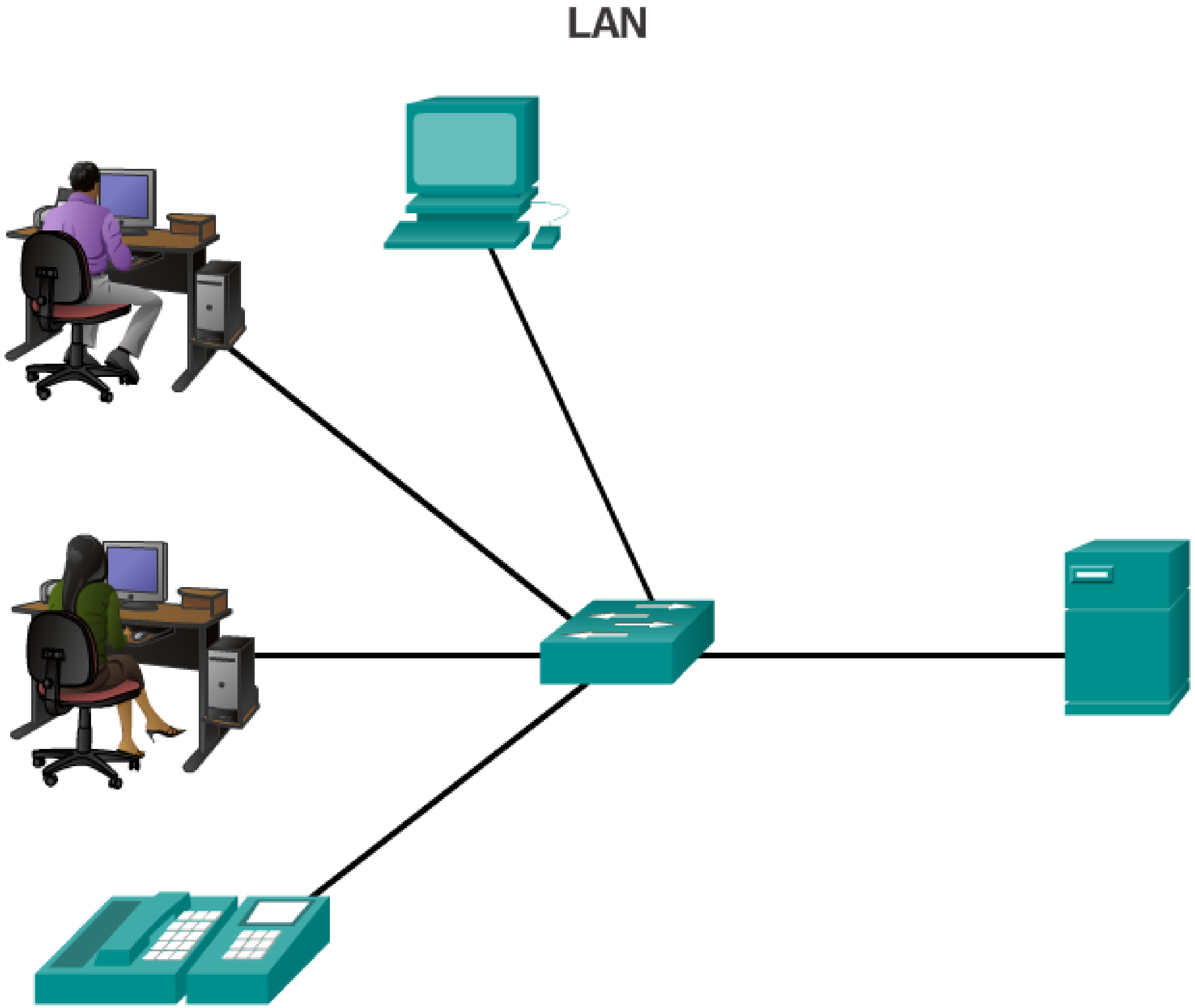
1.2.2.1 Types of Networks



Network infrastructures can vary greatly in terms of:

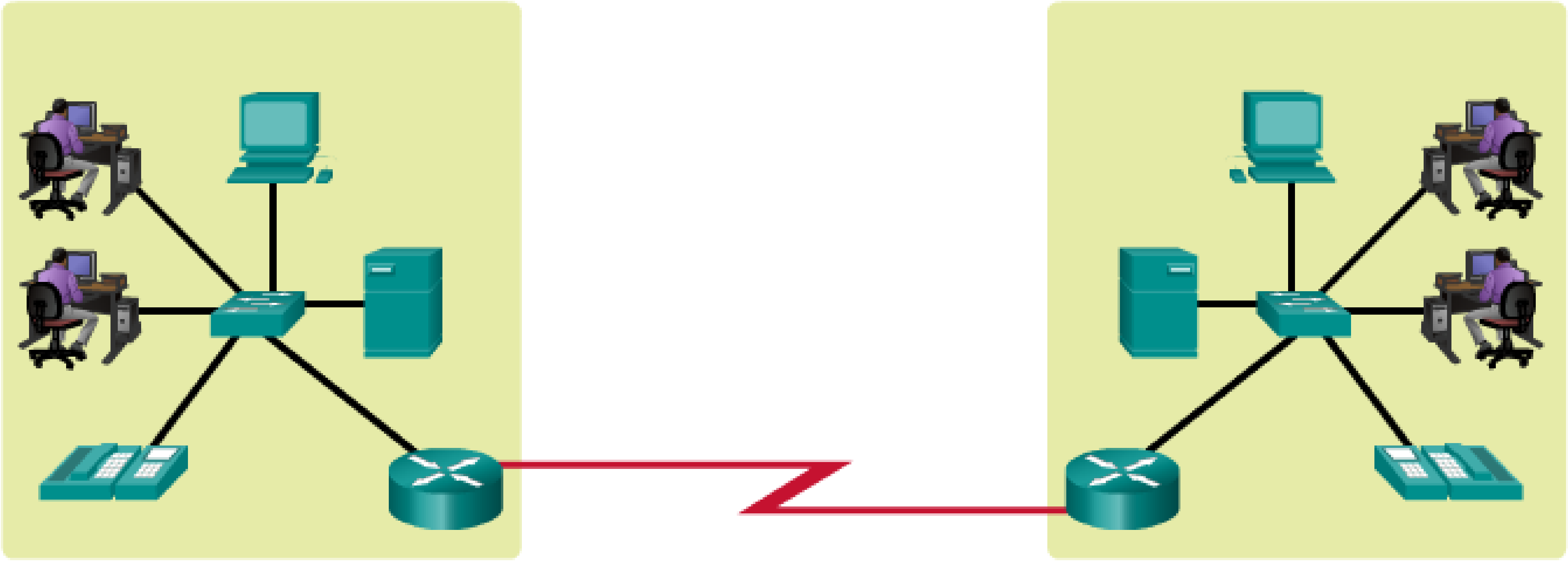
- Size of the area covered
- Number of users connected
- Number and types of services available
- Area of responsibility

1.2.2.2 Local Area Networks



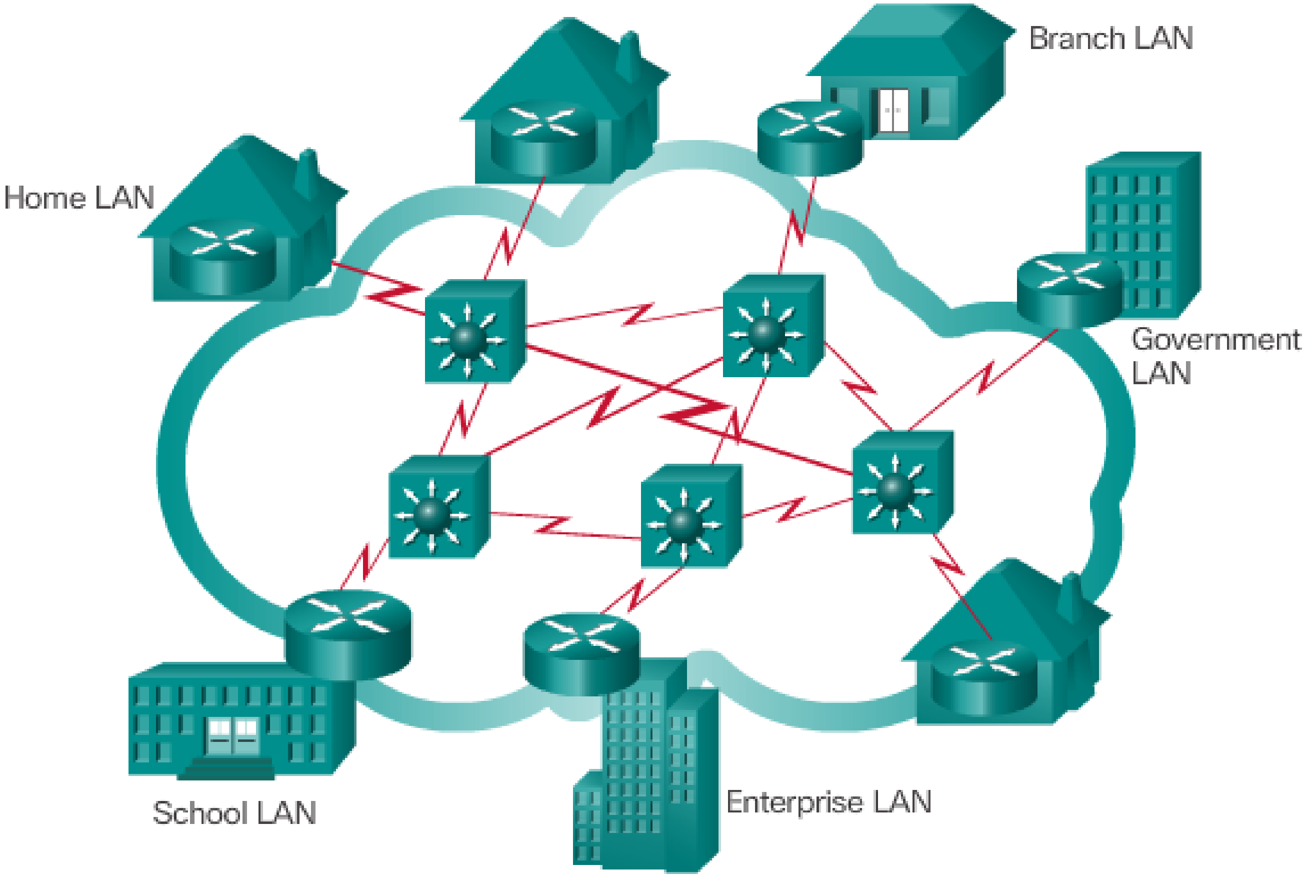
1.2.2.3 Wide Area Networks

WAN



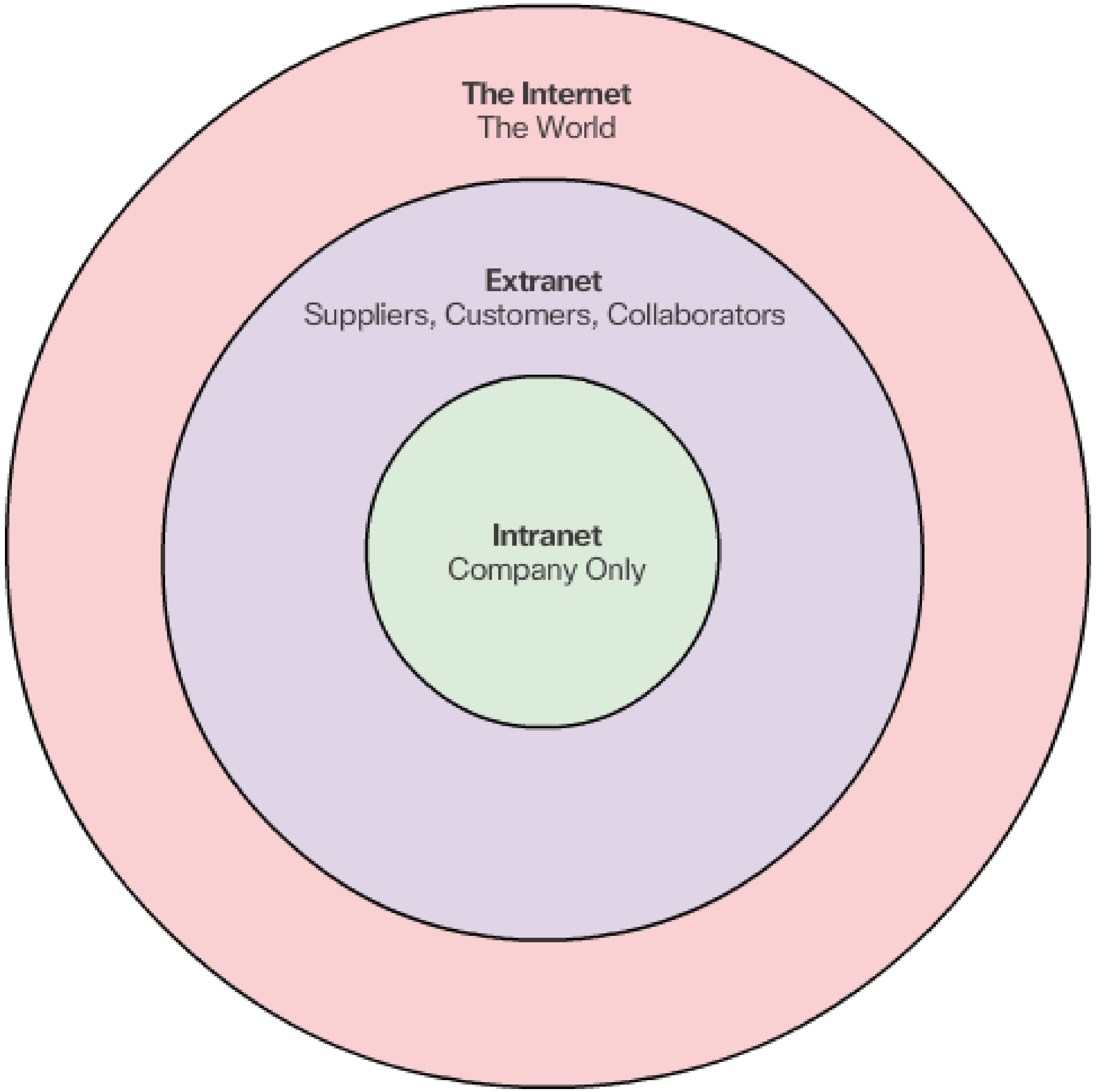
1.2.3.1 The Internet

Collection of Interconnected LANs and WANs



LANs use WAN services to interconnect.

1.2.3.2 Intranets and Extranets



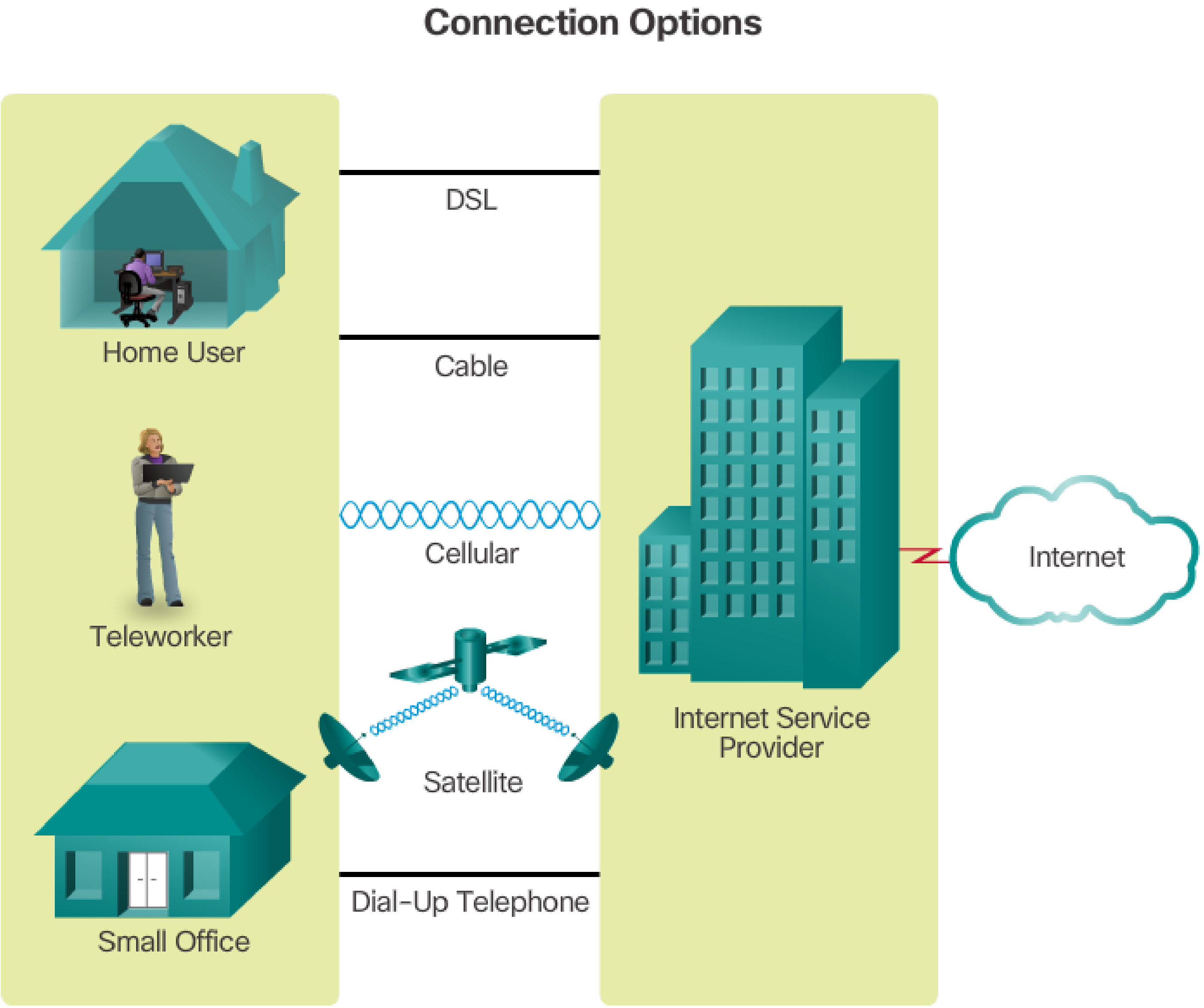
An organization may use an extranet to provide secure and safe access to individuals who work for a different organization, but require access to the organization's data. Examples of extranets include:

- A company that is providing access to outside suppliers and contractors.
- A hospital that is providing a booking system to doctors so they can make appointments for their patients.
- A local office of education that is providing budget and personnel information to the schools in its district.

1.2.4.1 Internet Access Technologies

There are many different ways to connect users and organizations to the Internet.

1.2.4.2 Home and Small Office Internet Connections



Cable -.

DSL –

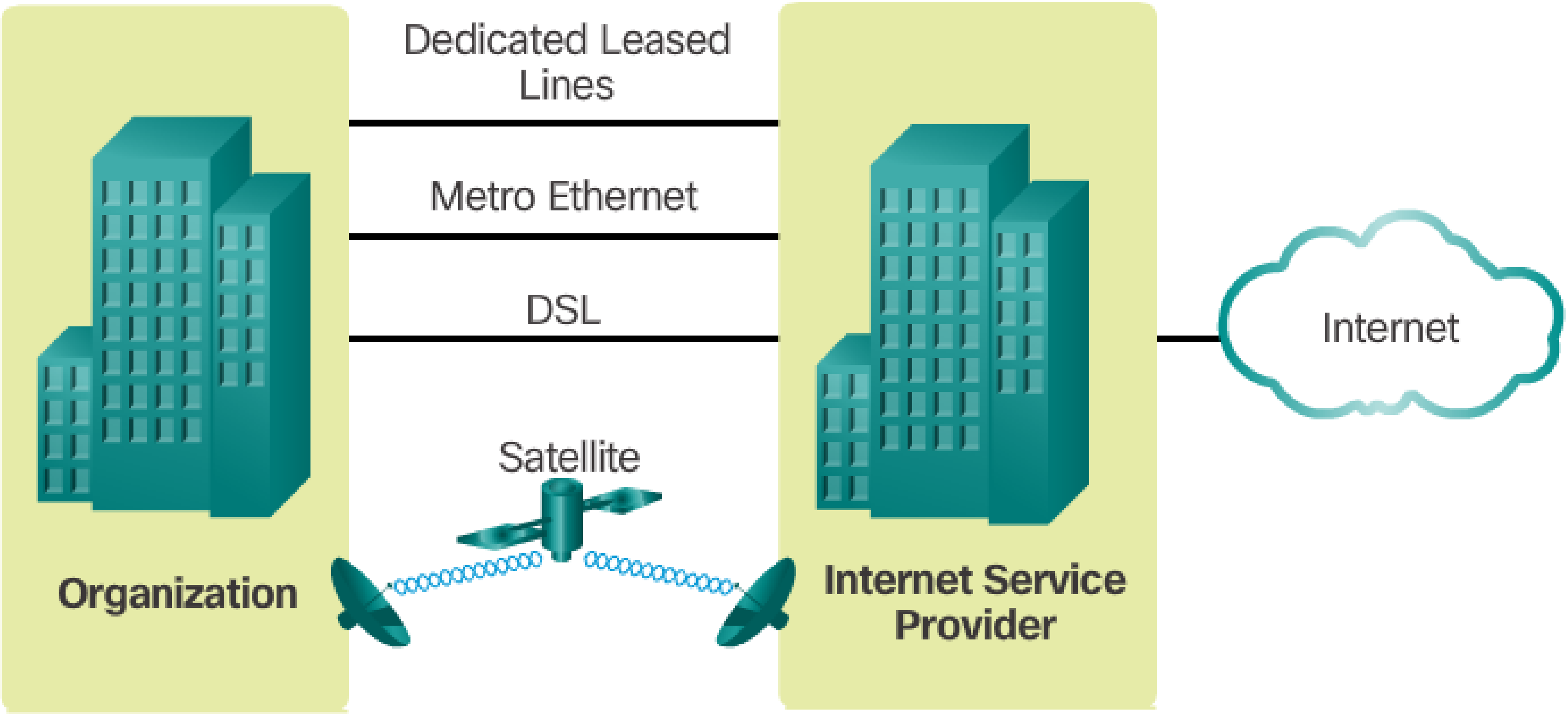
Cellular -.

Satellite –

Dial-up Telephone -

1.2.4.3 Businesses Internet Connections

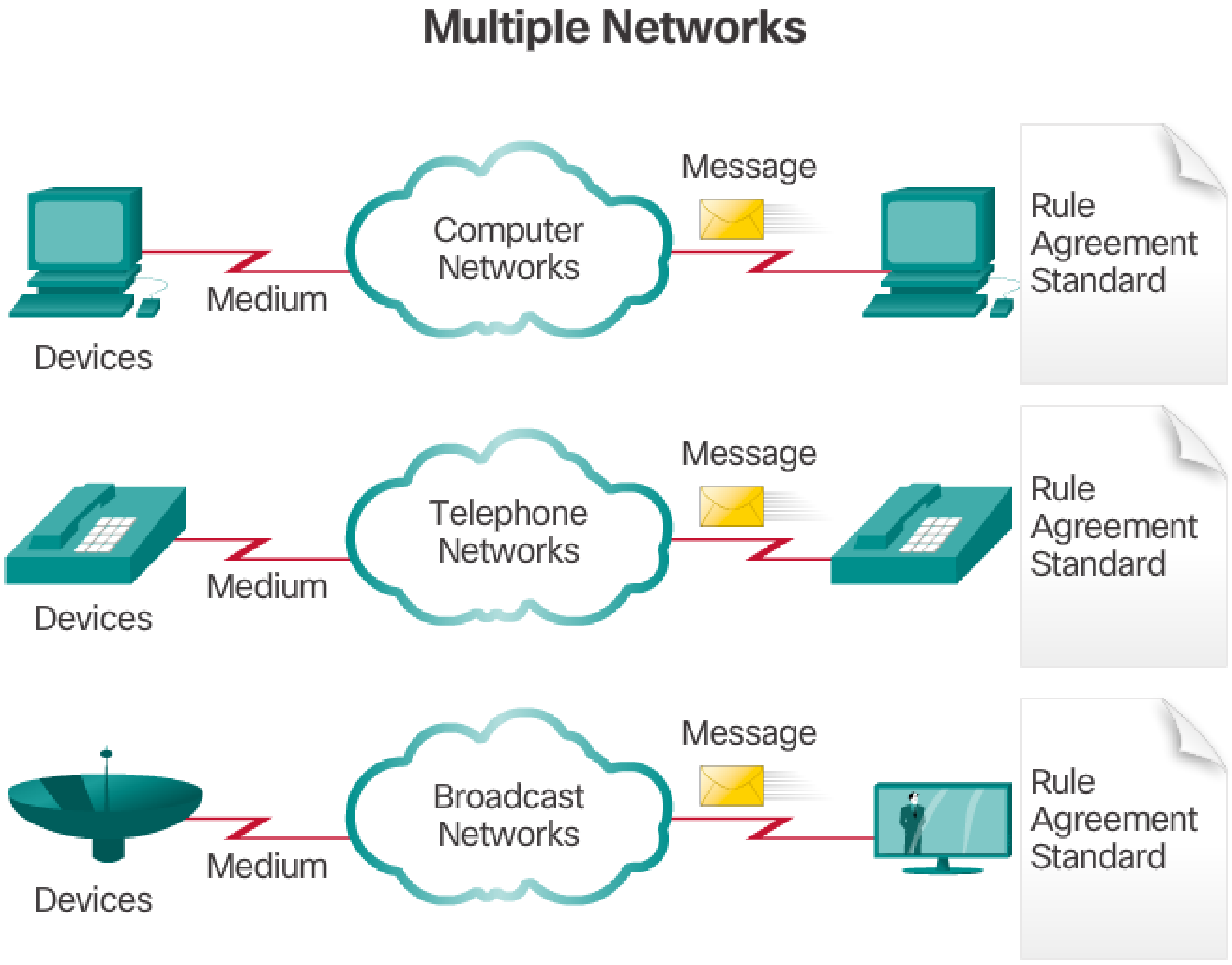
Connection Options



1.2.4.4 Packet Tracer - Help and Navigation Tips

1.2.4.5 Packet Tracer - Network Representation

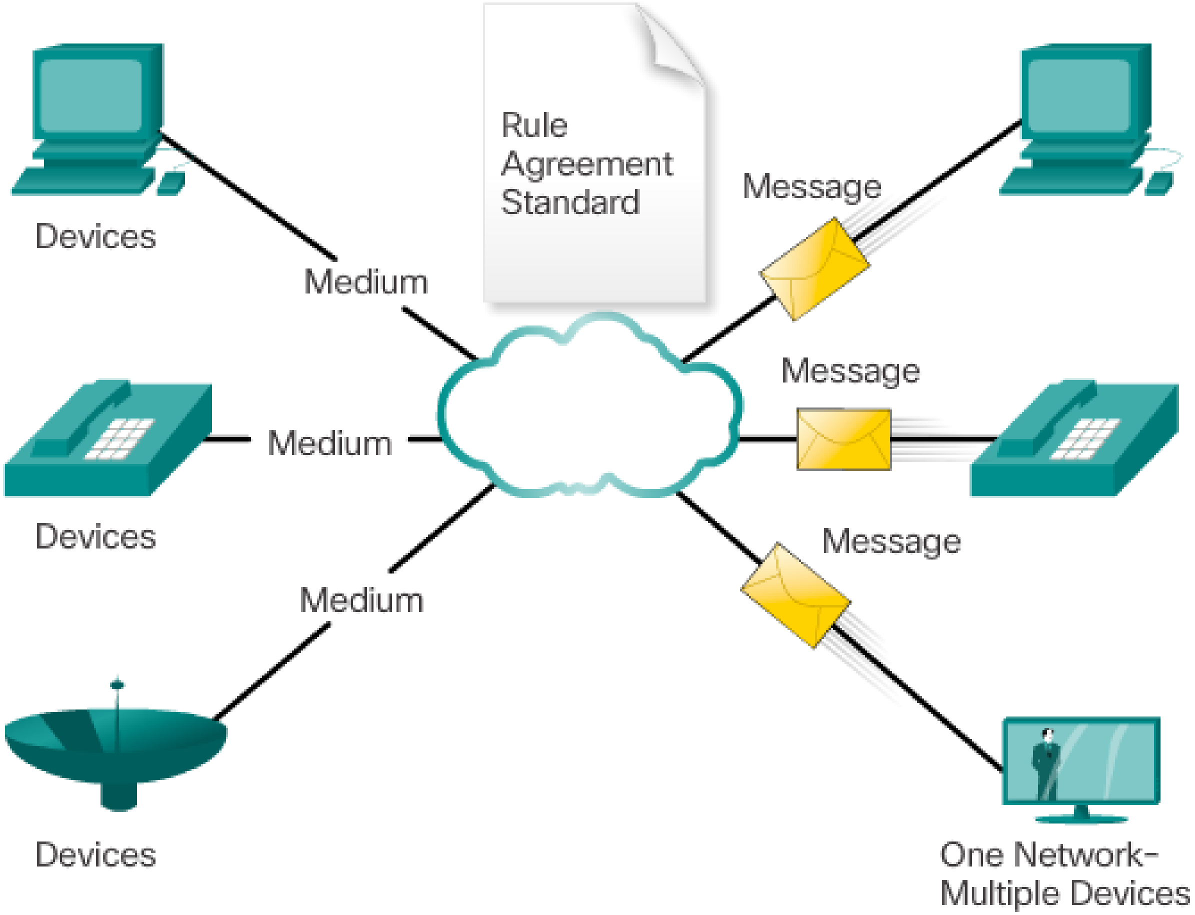
1.3.1.1 Traditional Separate Networks



Multiple services are running on multiple networks.

1.3.1.2 The Converging Network

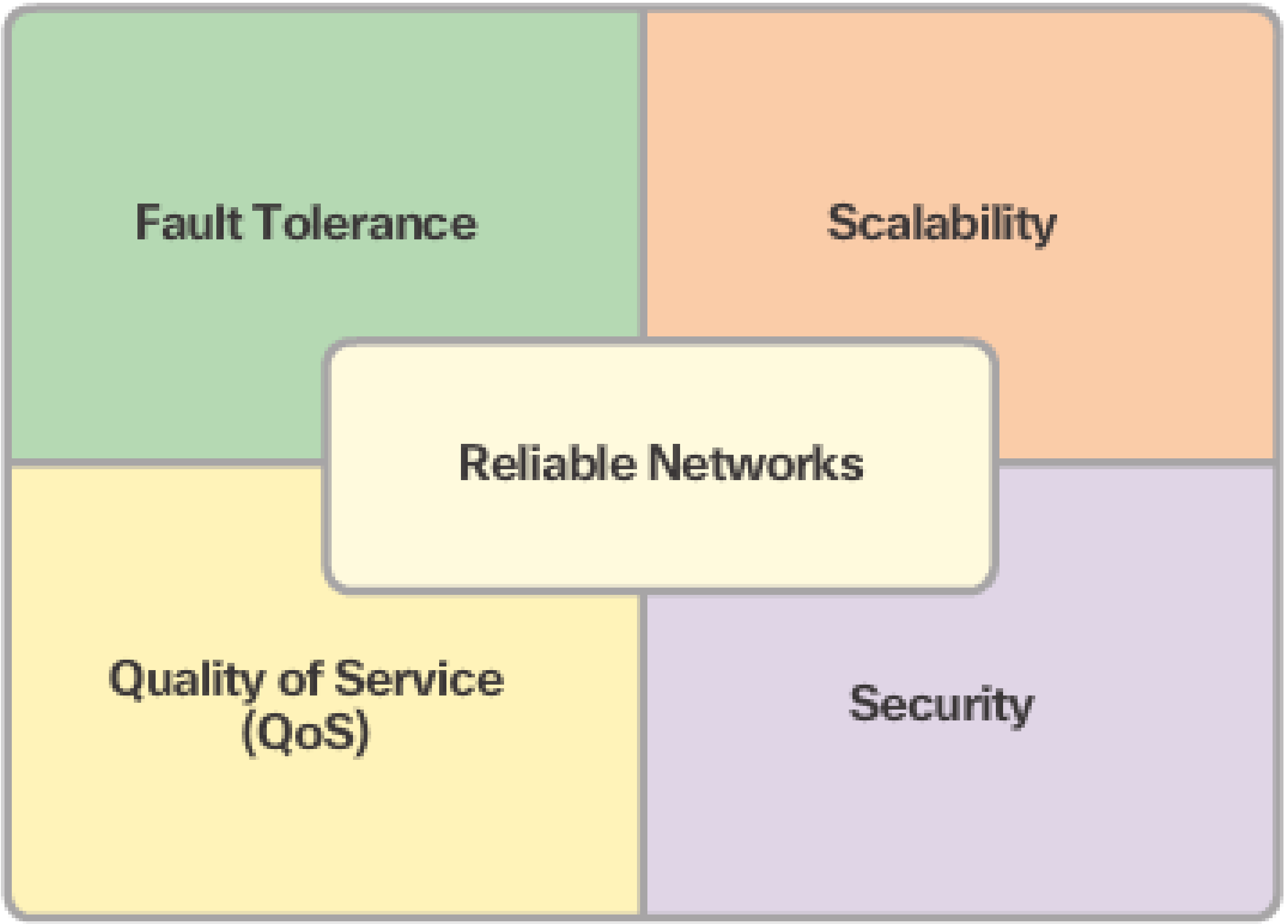
Converged Networks



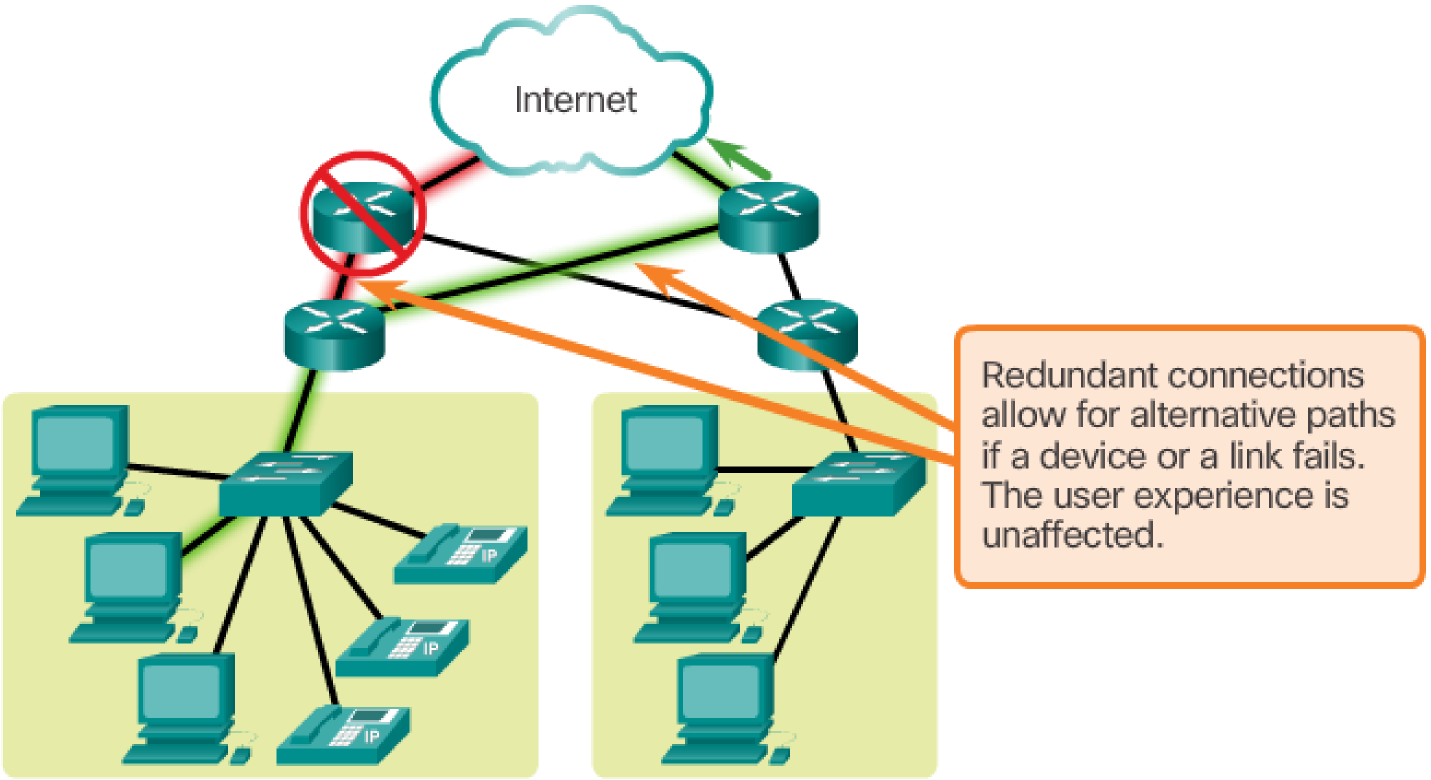
Converged data networks carry multiple services on one network.

1.3.1.3 Lab – Researching Converged Network Services

1.3.2.1 Network Architecture



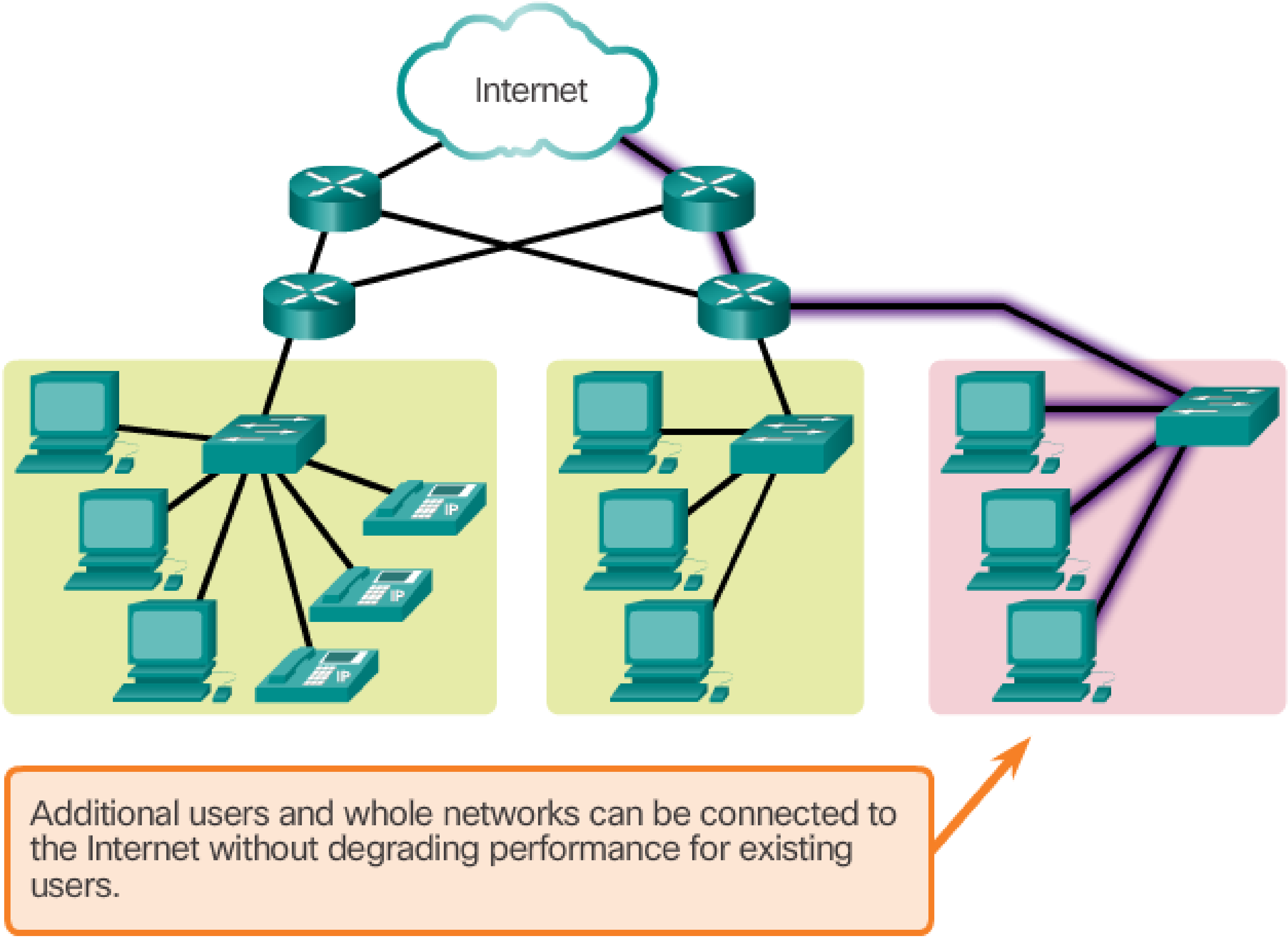
1.3.2.2 Fault Tolerance



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

A fault tolerant network is one that limits the impact of a failure, so that the fewest number of devices are affected. It is also built in a way that allows quick recovery when such a failure occurs. These networks depend on multiple paths between the source and destination of a message. If one path fails, the messages can be instantly sent over a different link. Having multiple paths to a destination is known as redundancy

1.3.2.3 Scalability

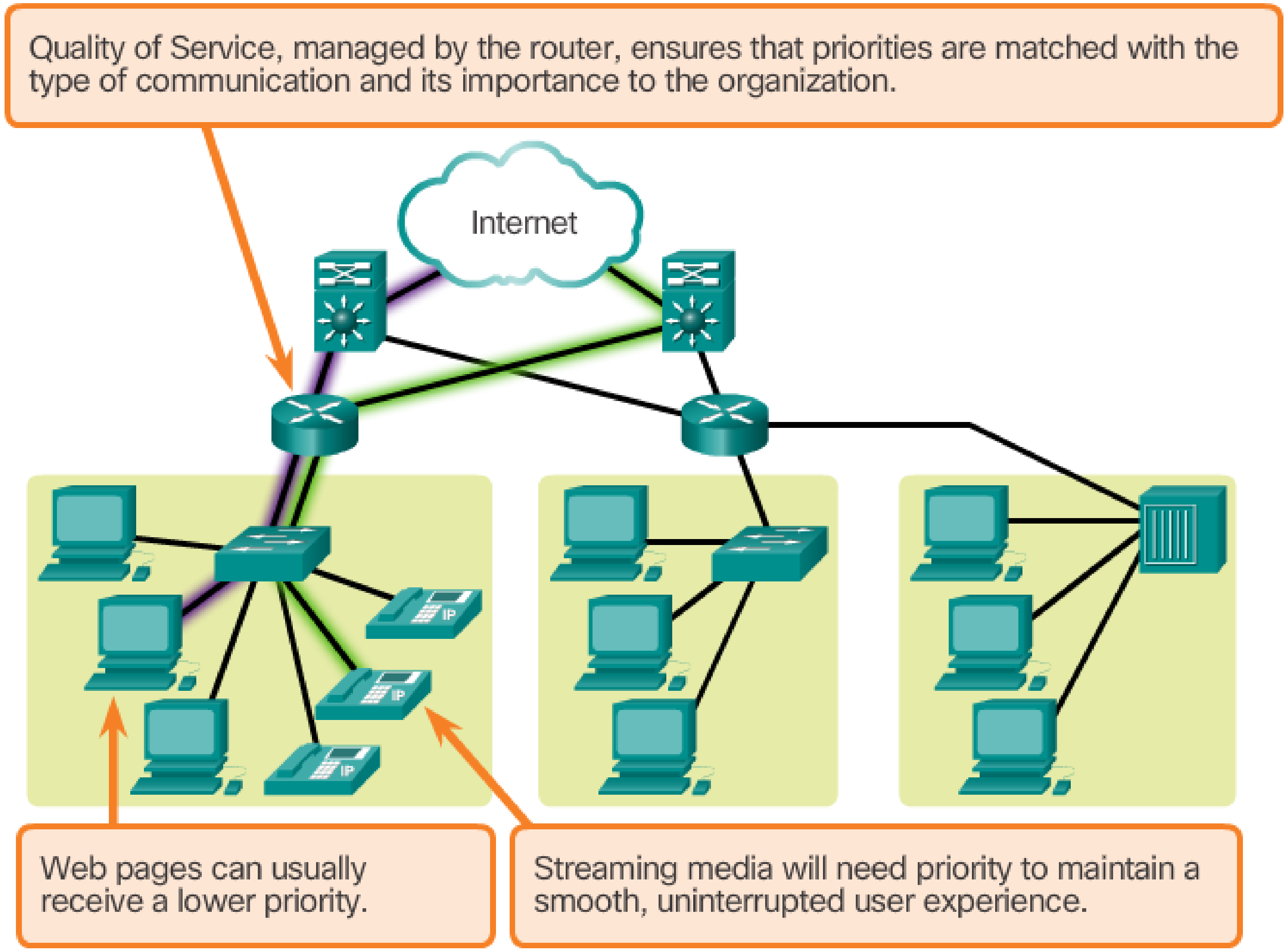


Additional users and whole networks can be connected to the Internet without degrading performance for existing users.

A scalable network can expand quickly to support new users and applications without impacting the performance of the service being delivered to existing users.

1.3.2.4 Quality of Service

Quality of Service (QoS)



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

Web pages can usually receive a lower priority.

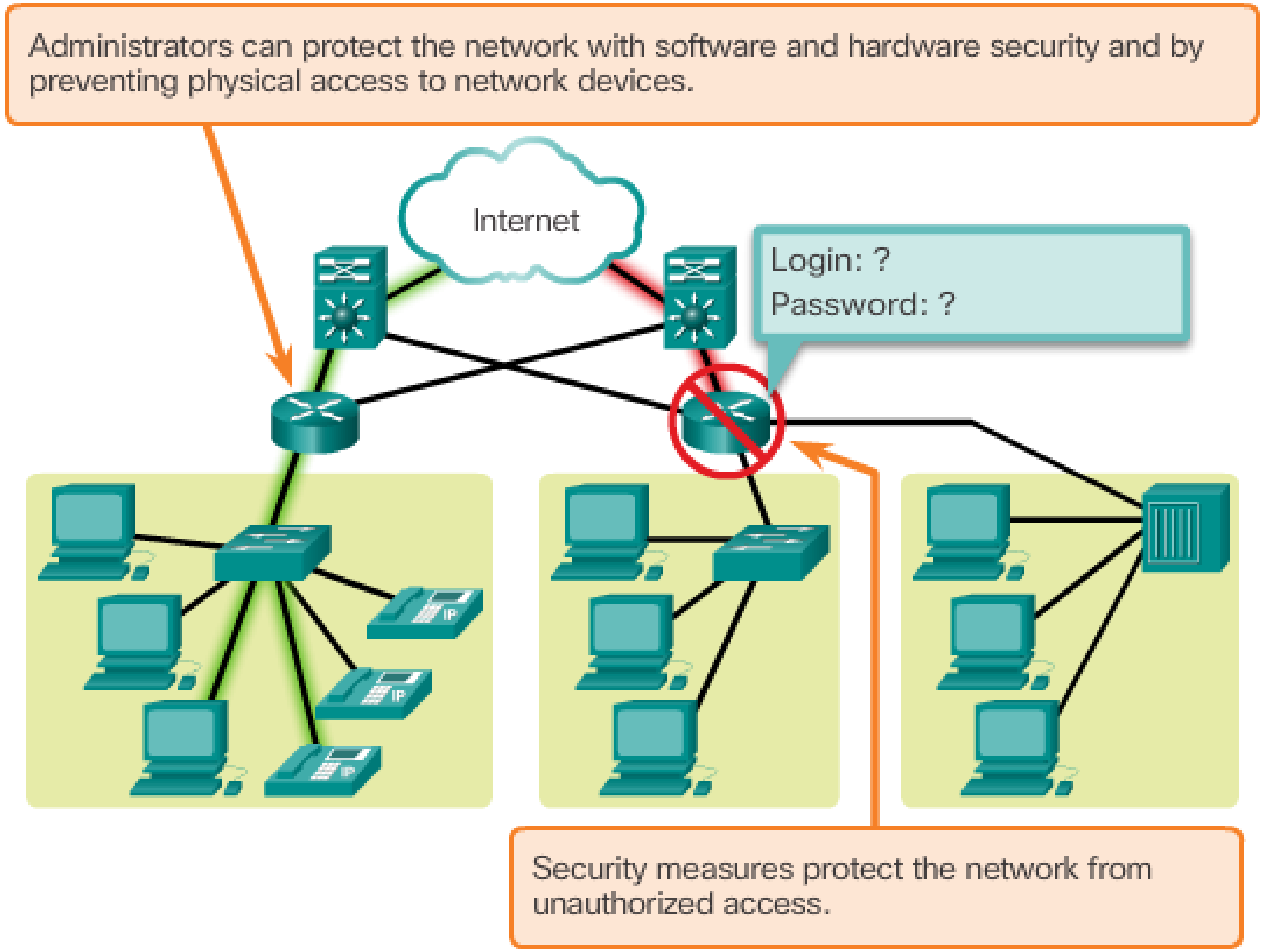
Streaming media will need priority to maintain a smooth, uninterrupted user experience.

New applications available to users over internetworks, such as voice and live video transmissions, create higher expectations for the quality of the delivered services.

As data, voice, and video content continue to converge onto the same network, QoS becomes a primary mechanism for managing congestion and ensuring reliable delivery of content to all users.

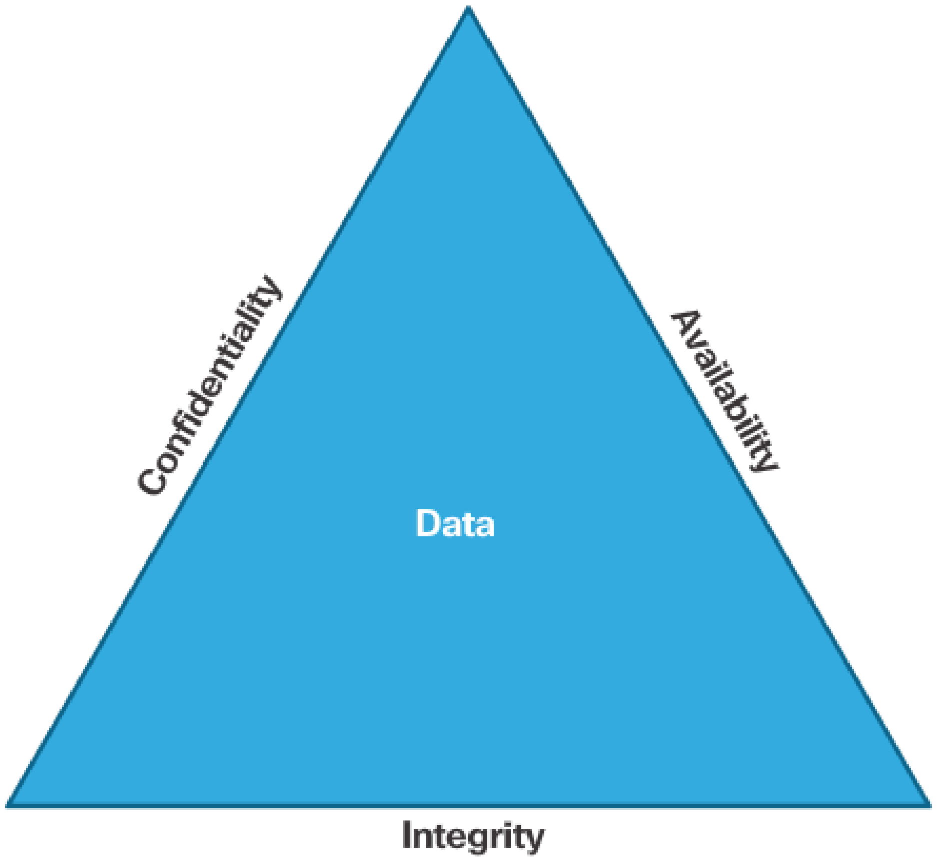
1.3.2.5 Security

Security

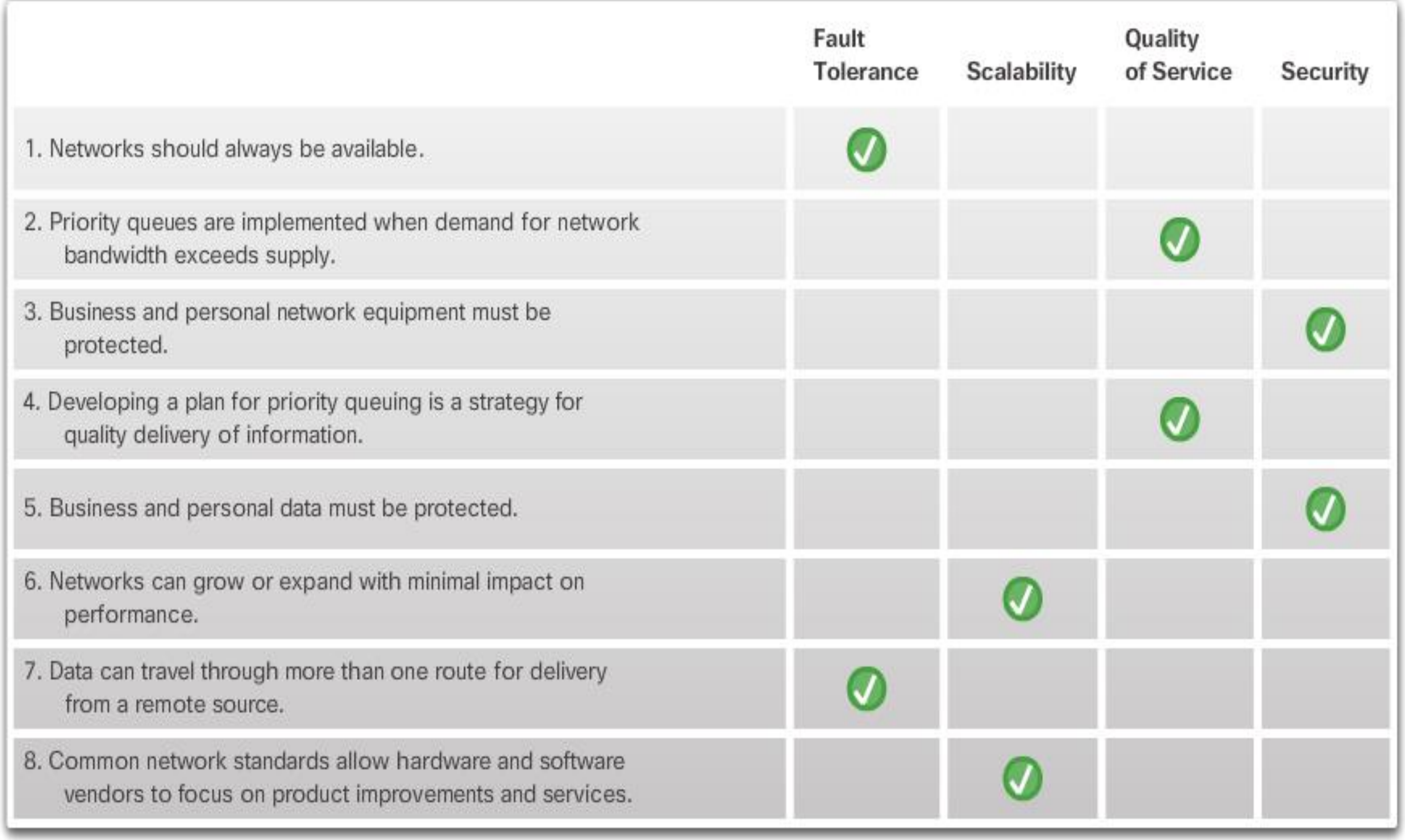


Administrators can protect the network with software and hardware security and by preventing physical access to network devices.

Security measures protect the network from unauthorized access.



1.3.2.6 Activity - Reliable Networks

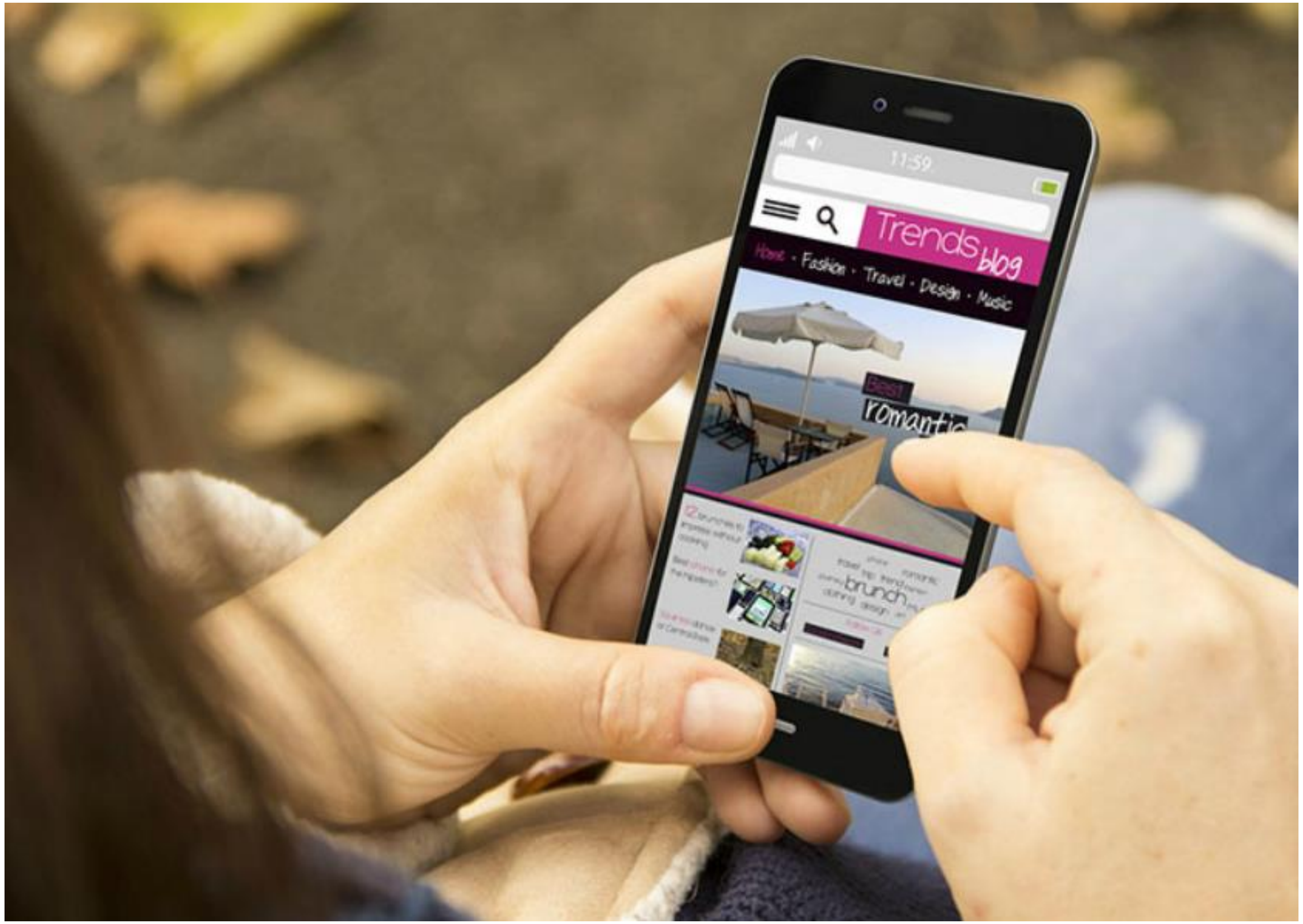


	Fault Tolerance	Scalability	Quality of Service	Security
1. Networks should always be available.	✓			
2. Priority queues are implemented when demand for network bandwidth exceeds supply.			✓	
3. Business and personal network equipment must be protected.				✓
4. Developing a plan for priority queuing is a strategy for quality delivery of information.			✓	
5. Business and personal data must be protected.				✓
6. Networks can grow or expand with minimal impact on performance.		✓		
7. Data can travel through more than one route for delivery from a remote source.	✓			
8. Common network standards allow hardware and software vendors to focus on product improvements and services.		✓		

1.4.1.1 New Trends

As new technologies and end user devices come to market, businesses and consumers must continue to adjust to this ever-changing environment. The role of the network is transforming to enable the connections between people, devices, and information

1.4.1.2 Bring Your Own Device



The concept of any device, to any content, in any manner, 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).

BYOD is about end users having the freedom to use personal tools to access information and communicate across a business or campus network.

1.4.1.3 Online Collaboration

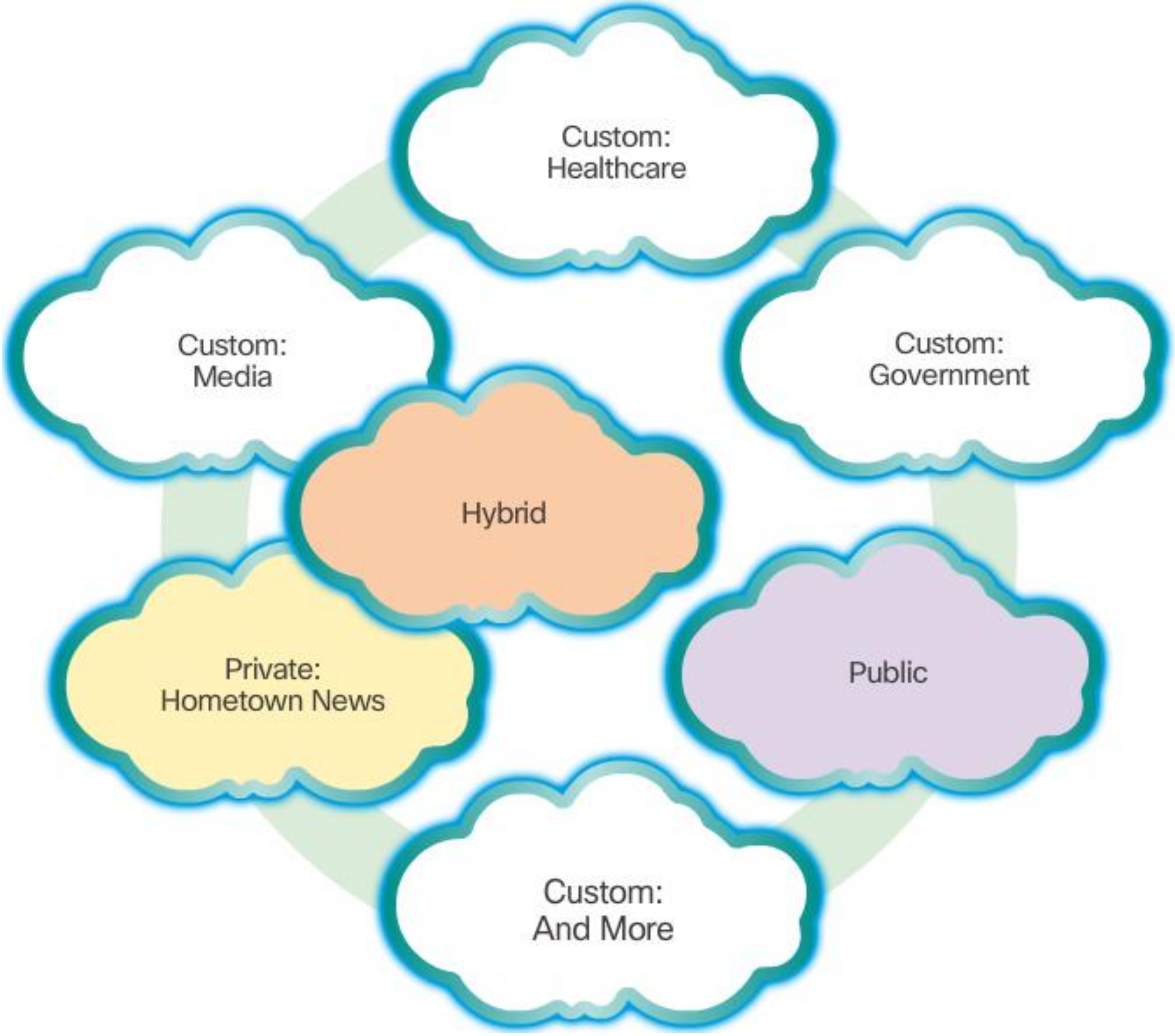
For businesses, collaboration is a critical and strategic priority that organizations are using to remain competitive. Collaboration is also a priority in education. Students need to collaborate to assist each other in learning, to develop team skills used in the work force, and to work together on team-based projects

1.4.1.4 Video Communication

. Video is being used for communications, collaboration, and entertainment. Video calls can be made to and from anywhere with an Internet connection.

Video conferencing is a powerful tool for communicating with others at a distance, both locally and globally. Video is becoming a critical requirement for effective collaboration as organizations extend across geographic and cultural boundaries

1.4.1.5 Cloud Computing

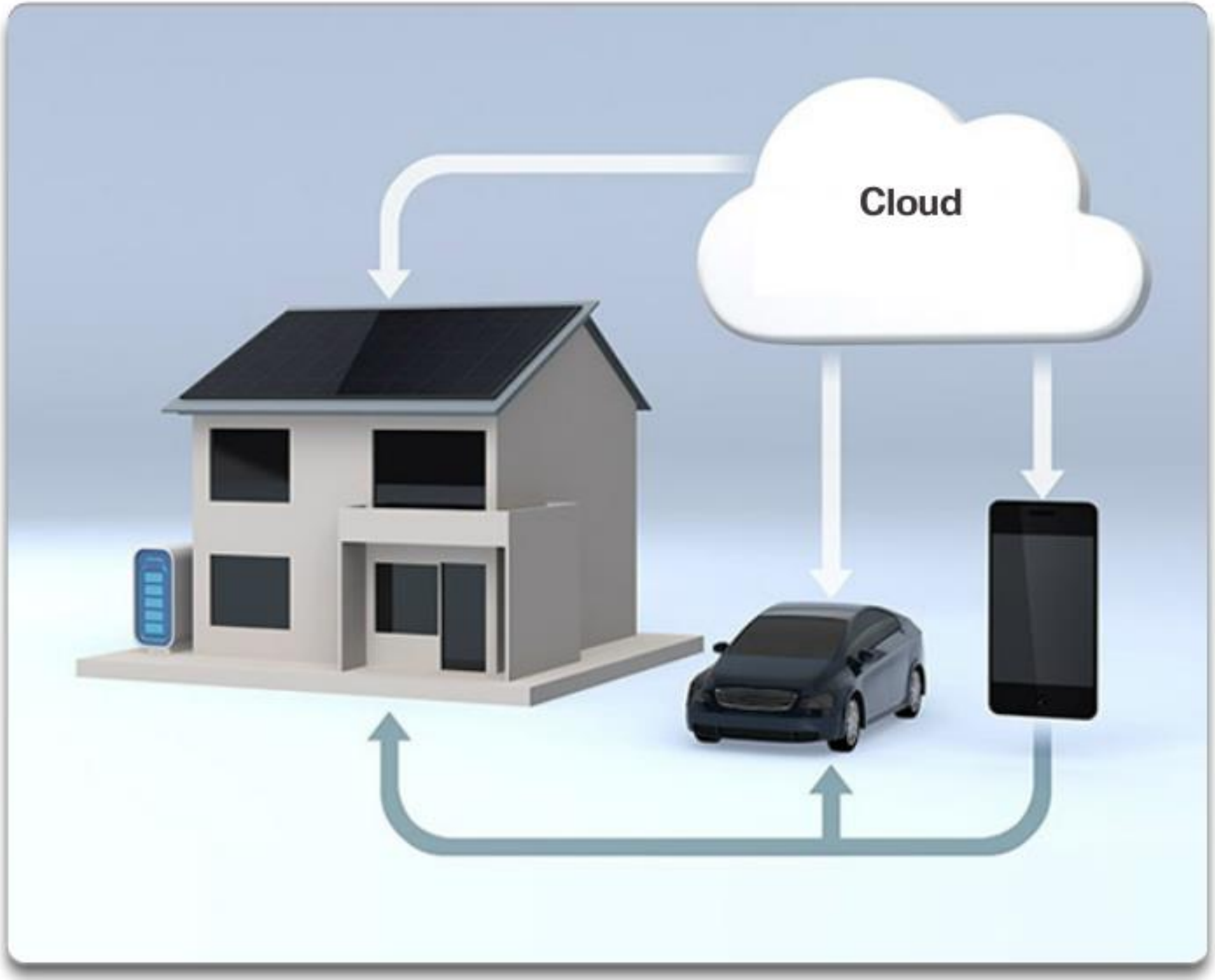


. Cloud computing allows us to store personal files, even backup our entire hard disk drive on servers over the Internet. Applications such as word processing and photo editing can be accessed using the Cloud.

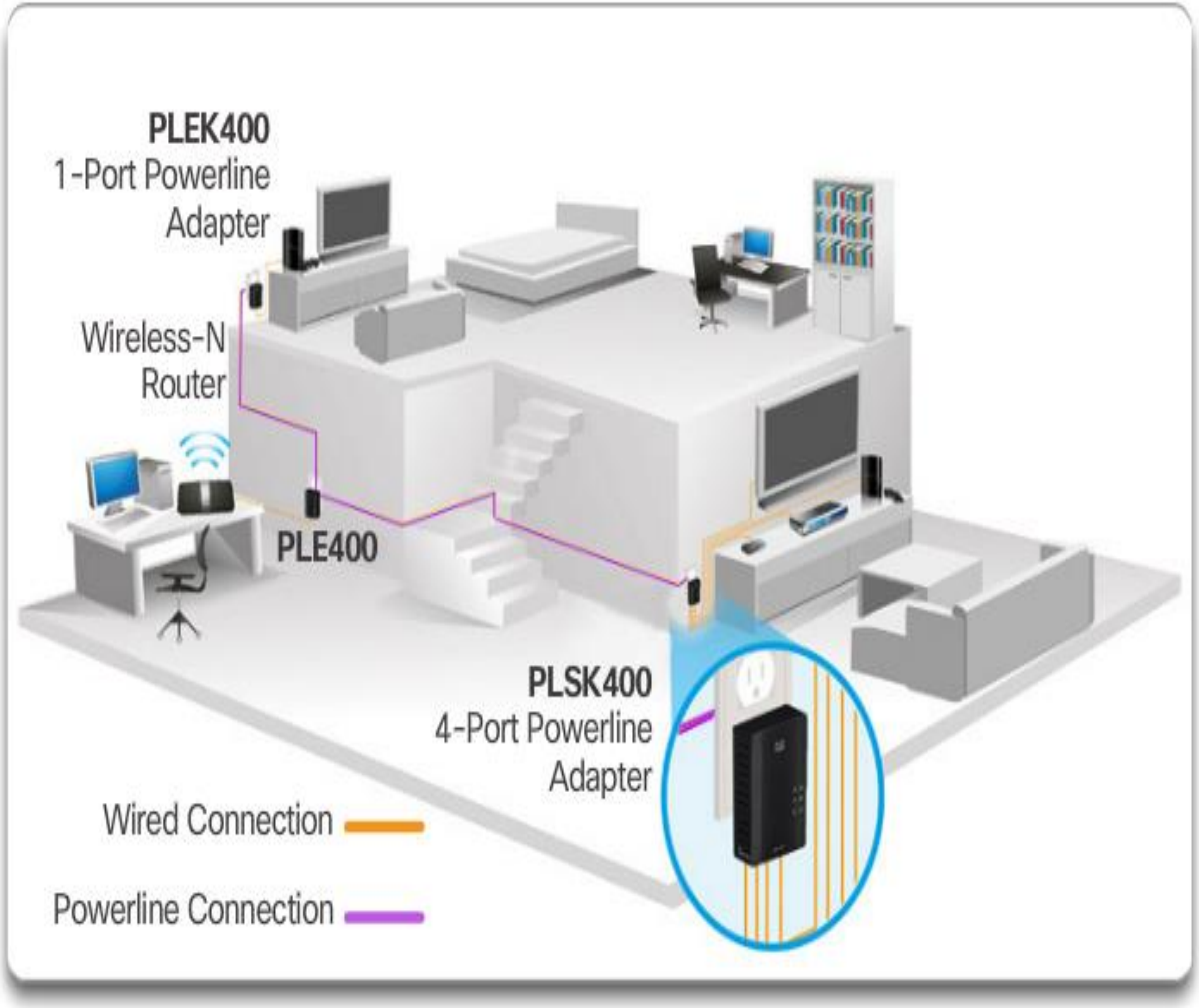
For businesses, Cloud computing extends IT's capabilities without requiring investment in new infrastructure, training new personnel, or licensing new software. These services are available on demand and delivered economically to any device anywhere in the world without compromising security or function.

1.4.2.1 Technology Trends in the Home

Smart Home Technology



1.4.2.2 Powerline Networking



Powerline Networking

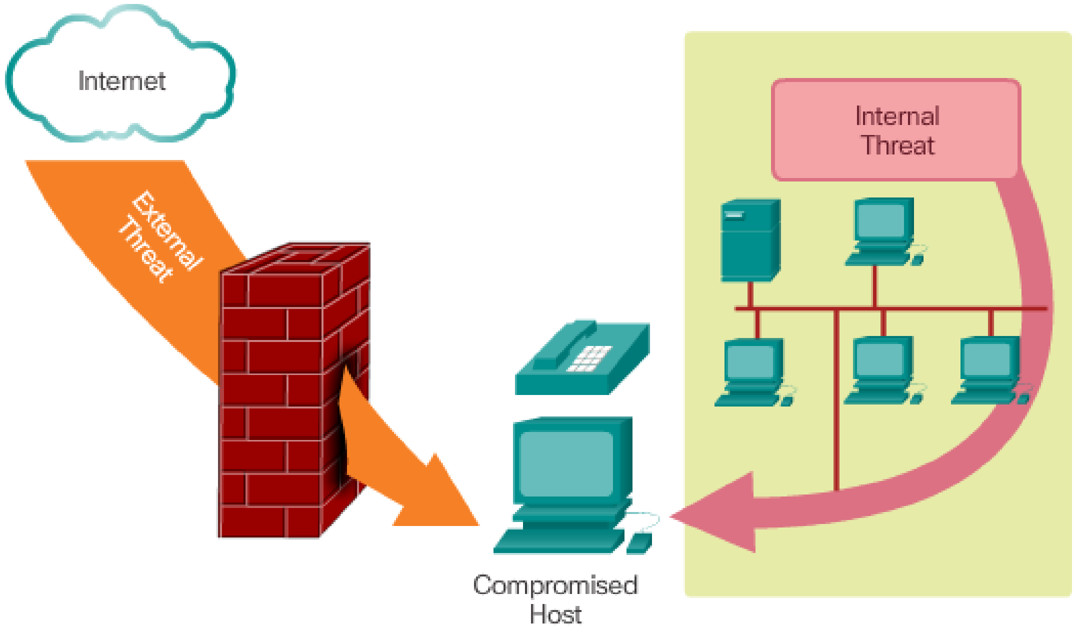
Powerline networking is an emerging trend for home networking that uses existing electrical wiring to connect devices, as shown in the figure. The concept of “no new wires” means the ability to connect a device to the network wherever there is an electrical outlet

1.4.2.3 Wireless Broadband

Wireless Broadband

Connecting to the Internet is vital in smart home technology. DSL and cable are common technologies used to connect homes and small businesses to the Internet. However, wireless may be another option in many areas.

1.4.3.1 Security Threats

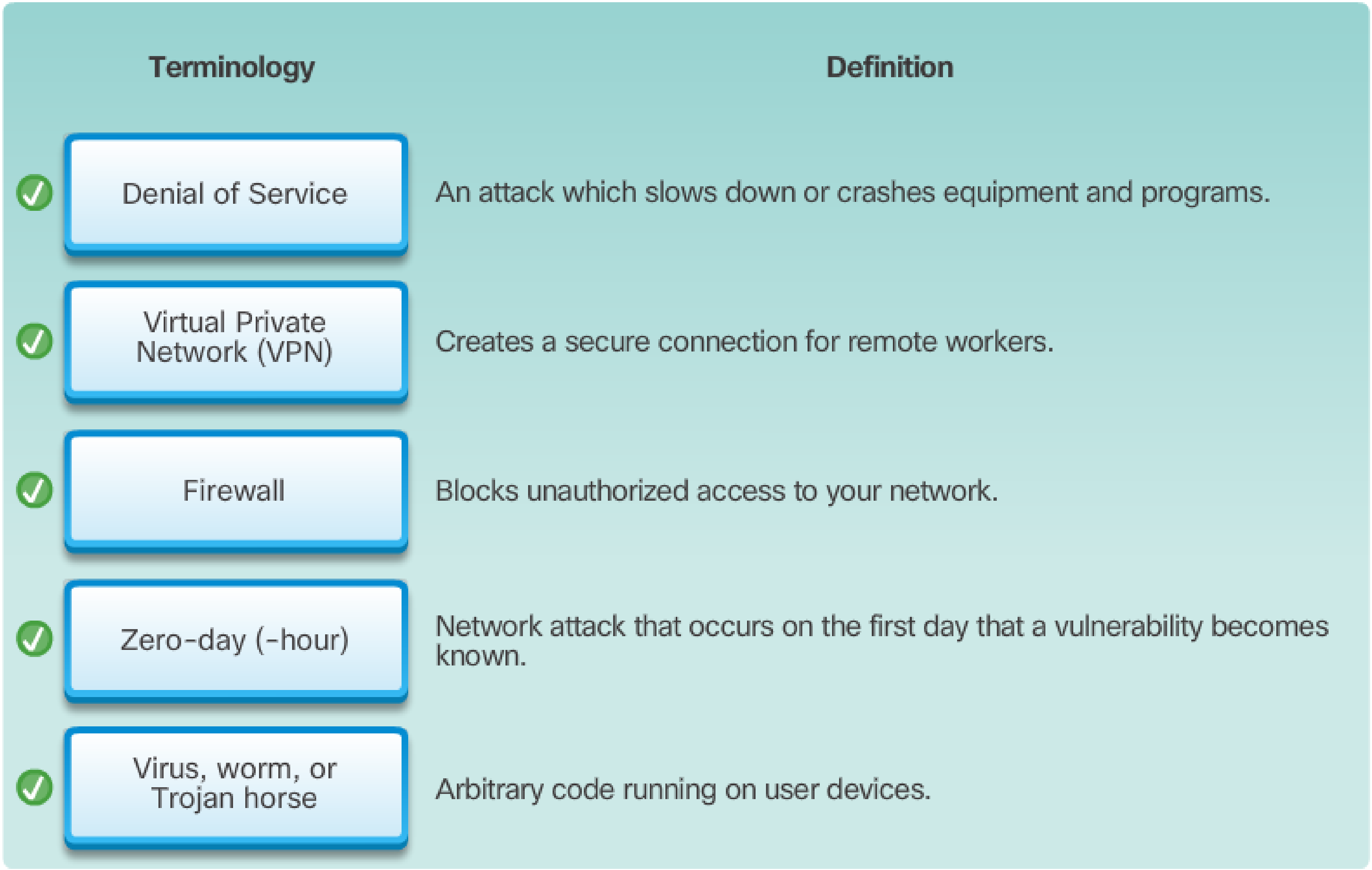


- **Viruses, worms, and Trojan horses** - malicious software and arbitrary code running on a user device
- **Spyware and adware** - software installed on a user device that secretly collects information about the user
- **Zero-day attacks, also called zero-hour attacks** - an attack that occurs on the first day that a vulnerability becomes known
- **Hacker attacks** - an attack by a knowledgeable person to user devices or network resources
- **Denial of service attacks** - attacks designed to slow or crash applications and processes on a network device
- **Data interception and theft** - an attack to capture private information from an organization's network
- **Identity theft** - an attack to steal the login credentials of a user in order to access private data

1.4.3.2 Security Solutions

- **Antivirus and antispyware** – These are used to protect end devices from becoming infected with malicious software.
- **Firewall filtering** – This is used to block unauthorized access to the network. This may include a host-based firewall system that is implemented to prevent unauthorized access to the end device, or a basic filtering service on the home router to prevent unauthorized access from the outside world into the network.
- **Dedicated firewall systems** – These are used to provide more advanced firewall capabilities that can filter large amounts of traffic with more granularity.
- **Access control lists (ACL)** – These are used to further filter access and traffic forwarding.
- **Intrusion prevention systems (IPS)** – These are used to identify fast-spreading threats, such as zero-day or zero-hour attacks.
- **Virtual private networks (VPN)** – These are used to provide secure access to remote workers.

1.4.3.3 Activity - Network Security Terminology

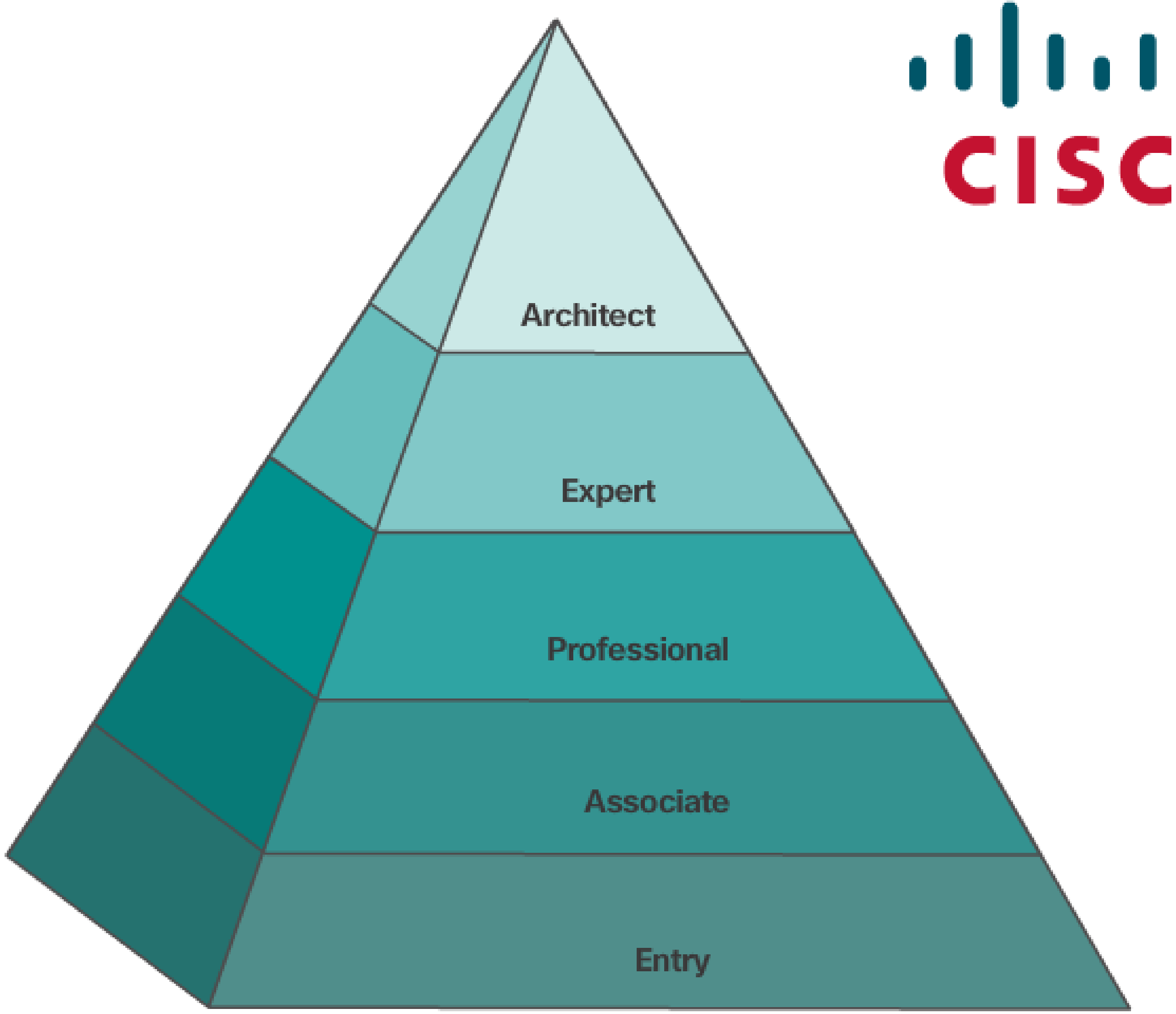


	Terminology	Definition
✓	Denial of Service	An attack which slows down or crashes equipment and programs.
✓	Virtual Private Network (VPN)	Creates a secure connection for remote workers.
✓	Firewall	Blocks unauthorized access to your network.
✓	Zero-day (-hour)	Network attack that occurs on the first day that a vulnerability becomes known.
✓	Virus, worm, or Trojan horse	Arbitrary code running on user devices.

1.4.4.1 Cisco Network Architecture

The role of the network has changed from a data-only network to a system that enables the connections of people, devices, and information in a media rich, converged network environment. In order for networks to function efficiently and grow in this type of environment, the network must be built upon a standard network architecture

1.4.4.2 CCNA



1.4.4.3 Lab - Researching IT and Networking Job Opportunities

Lab | Researching IT and Networking Job Opportunities

1.5.1.1 Class Activity – Draw Your Concept of the Internet Now

Exploring the Network...

- Communicating in a Network-Centric World
- The Network as a Platform
- LANs, WANs, and the Internet
- The Changing Network Environment

1.5.1.2 Warriors of the Net

To view the video, Warriors of the Net, go to:
http://www.warriorsofthe.net

1.5.1.3 Chapter 1: Exploring the Network

Summary | Chapter 1