Chapter 1 B:
Exploring the Network

Types of Networks

The two most common types of network infrastructures are:

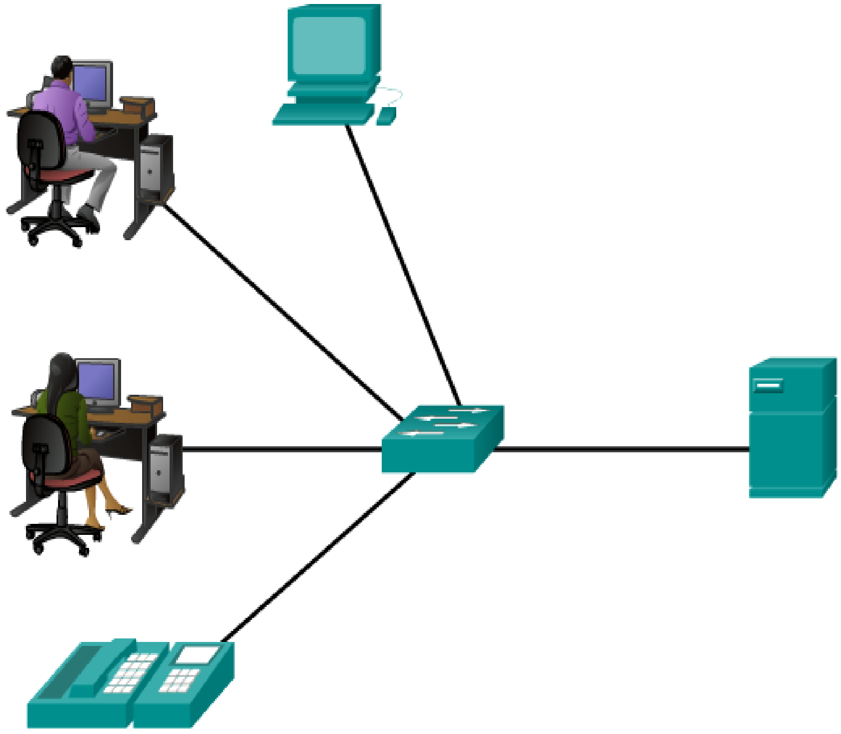
- Local Area Network (LAN)
- Wide Area Network (WAN).

Other types of networks include:

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

LANs and WANs

Local Area Networks (LAN)



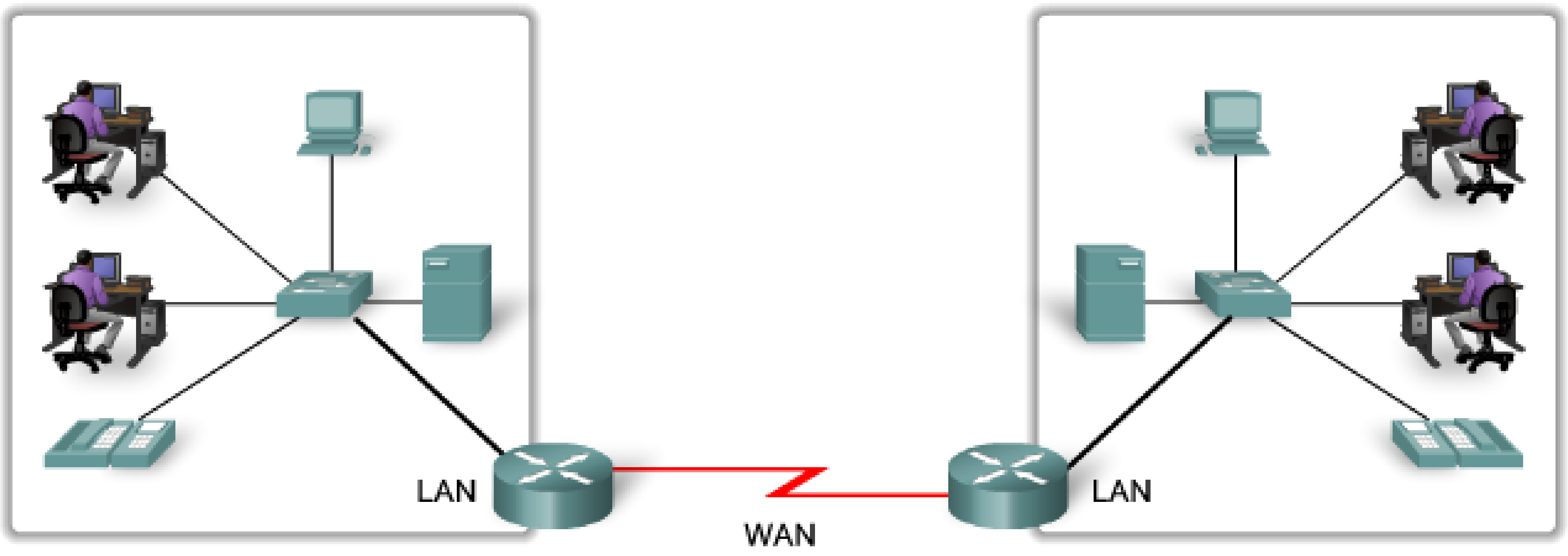
A network serving a home, building, or campus is considered a LAN.

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

LANs and WANs

Wide Area Networks (WAN)

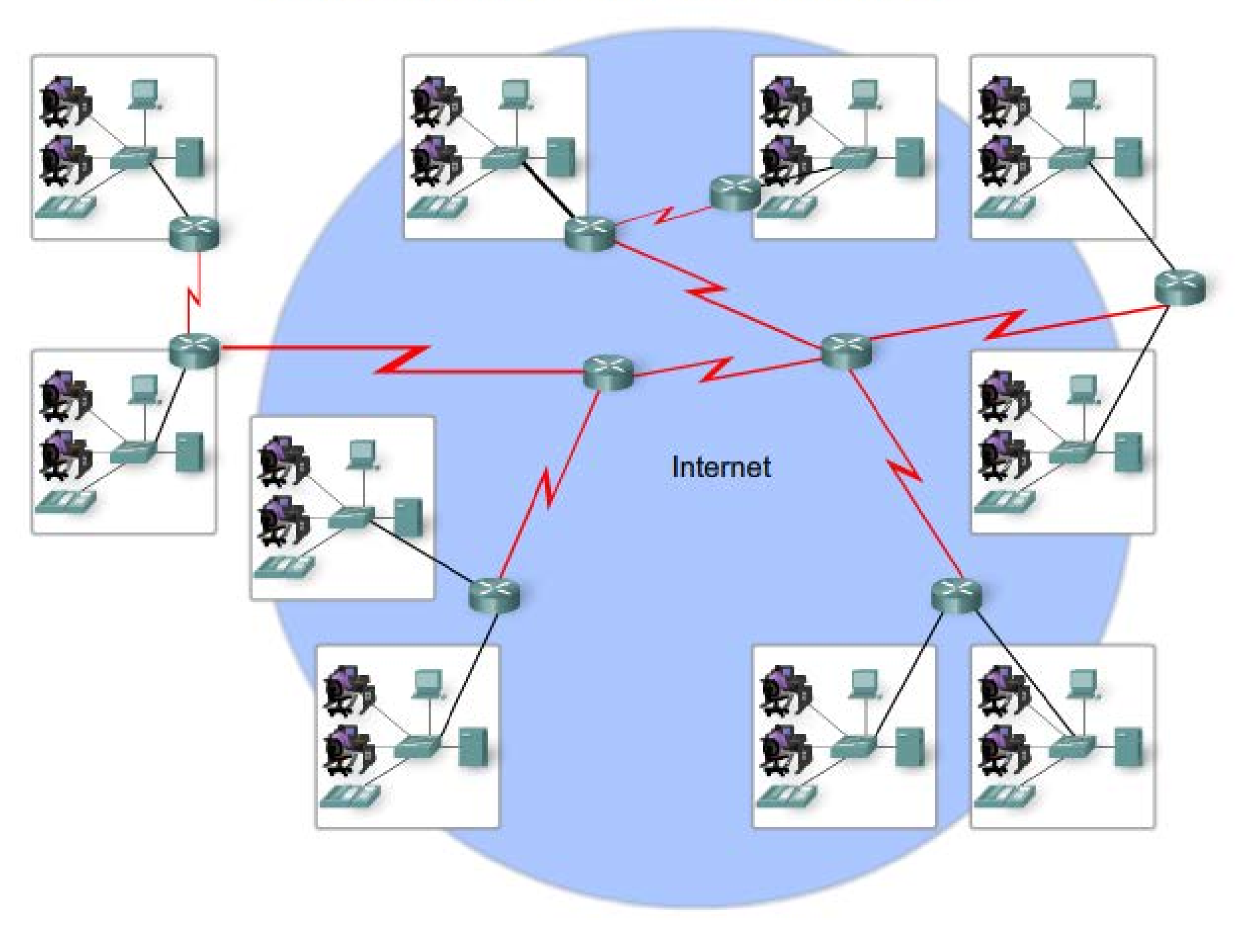
LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN).



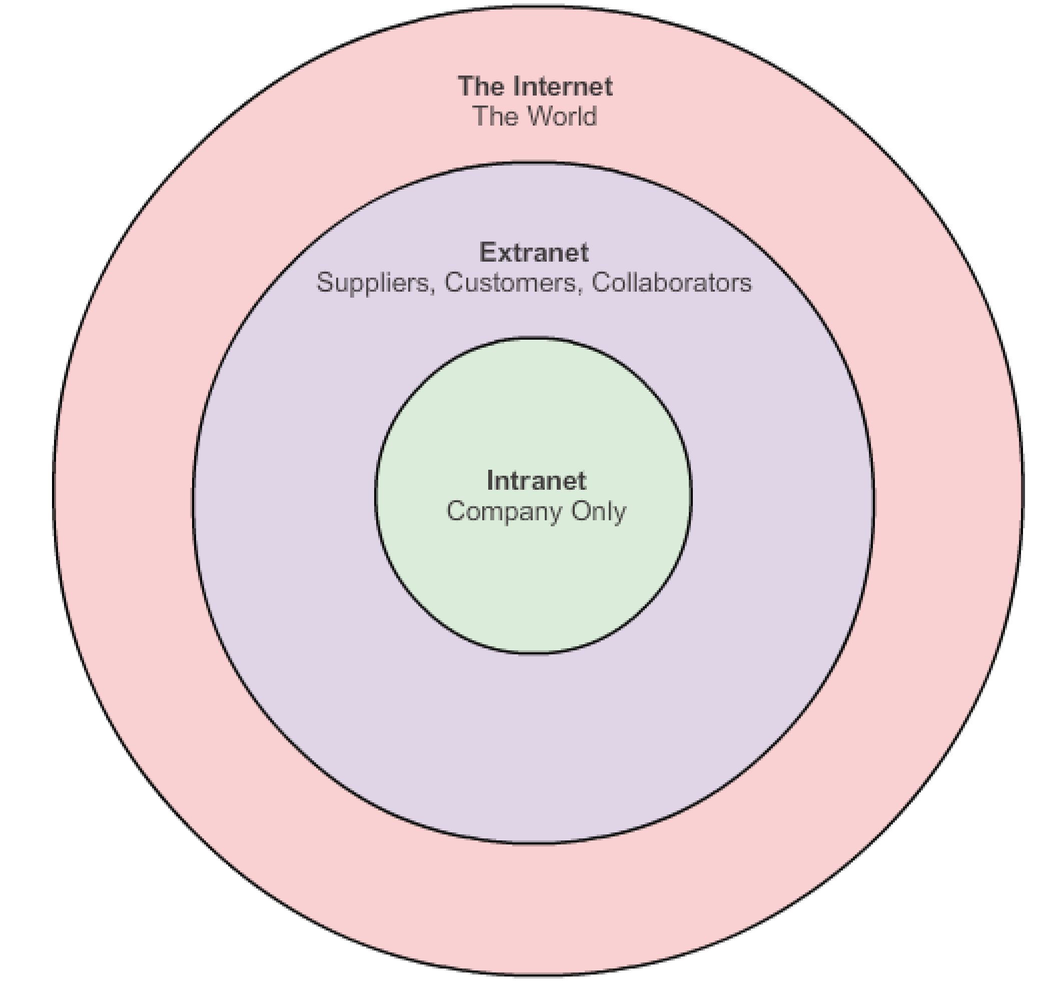
Two or more LANs can be connected by a WAN

The Internet

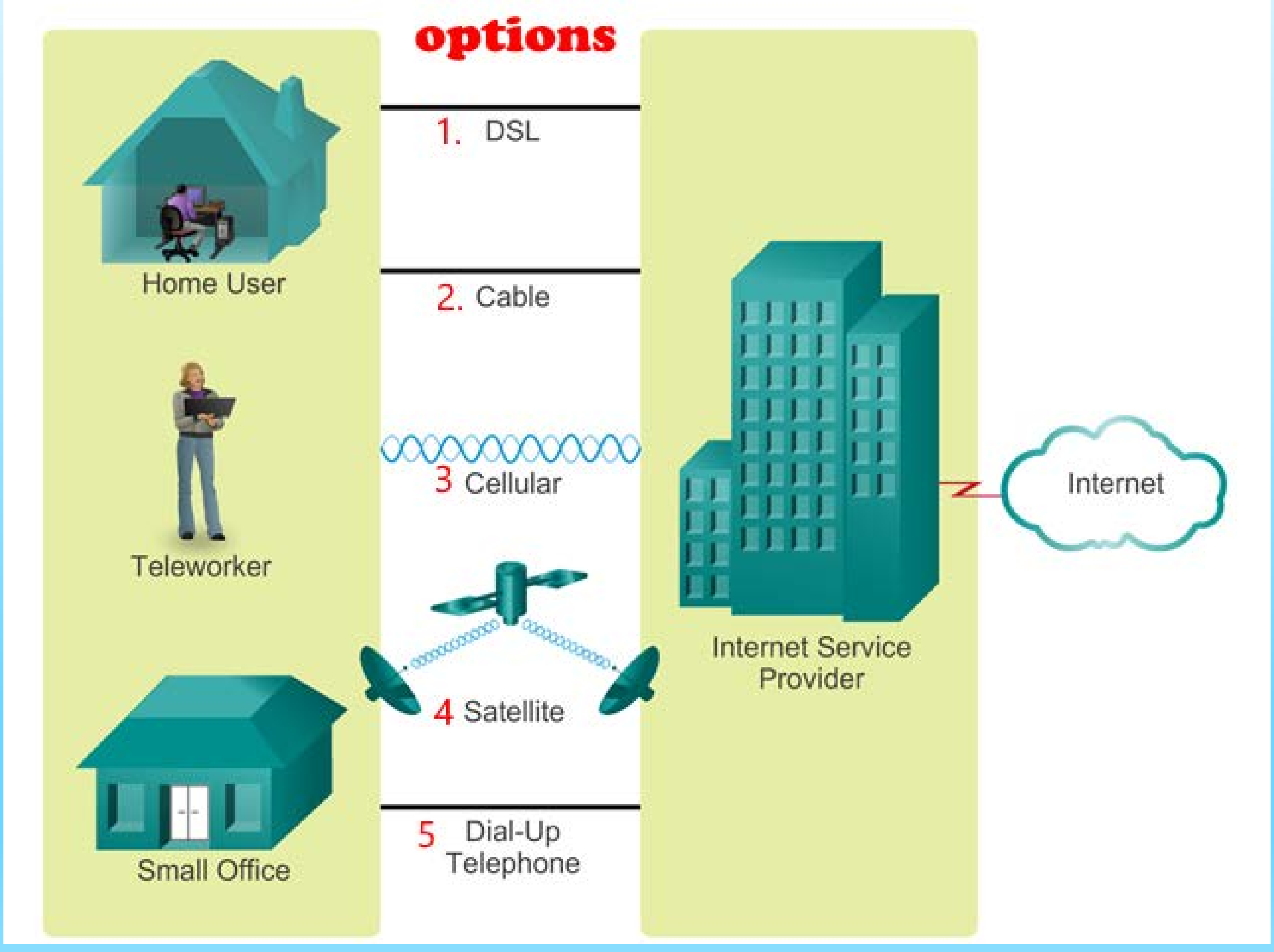
LANs and WANs can be connected by internetworks



Intranet and Extranet

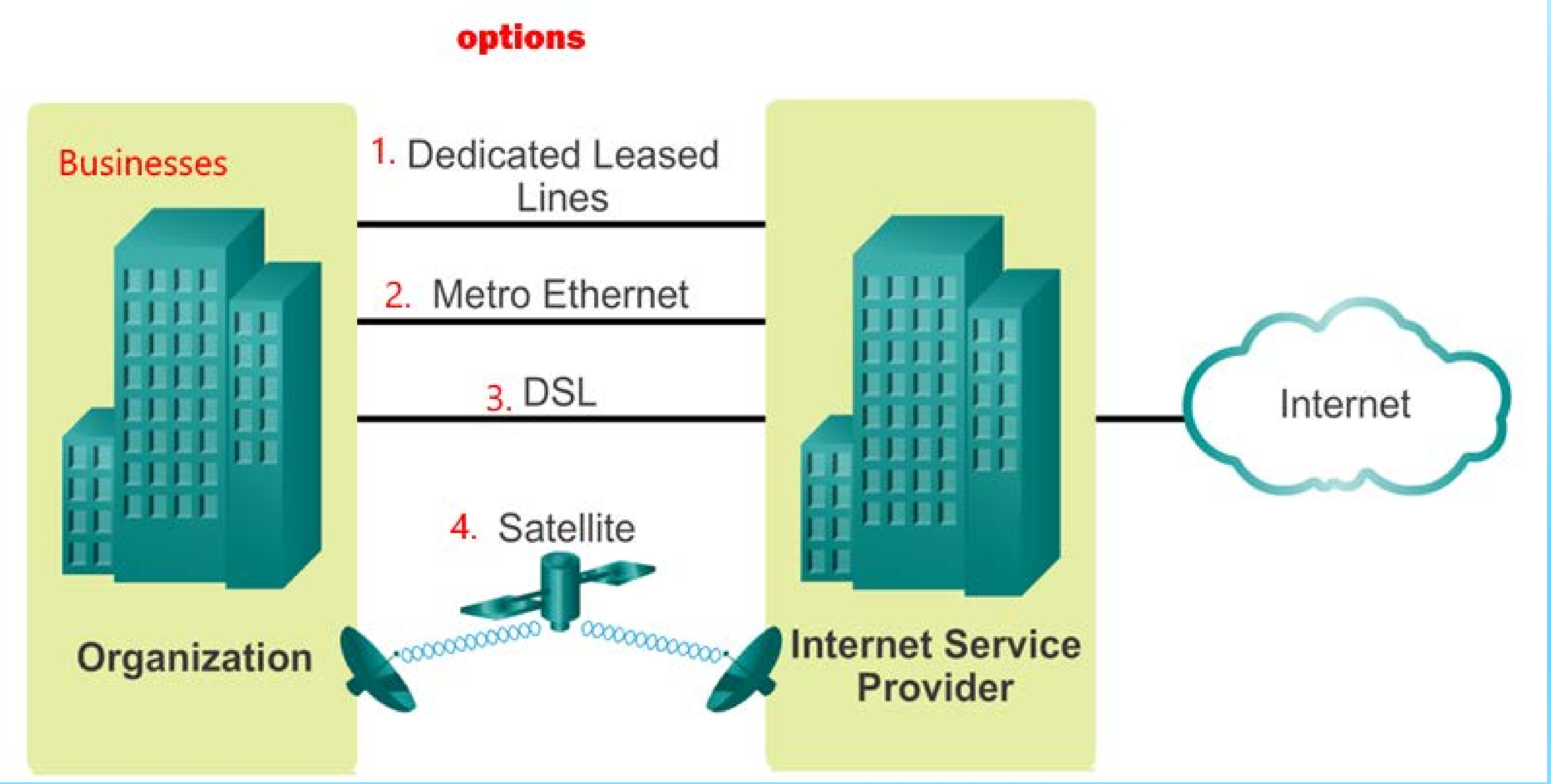


Connecting Users to the Internet



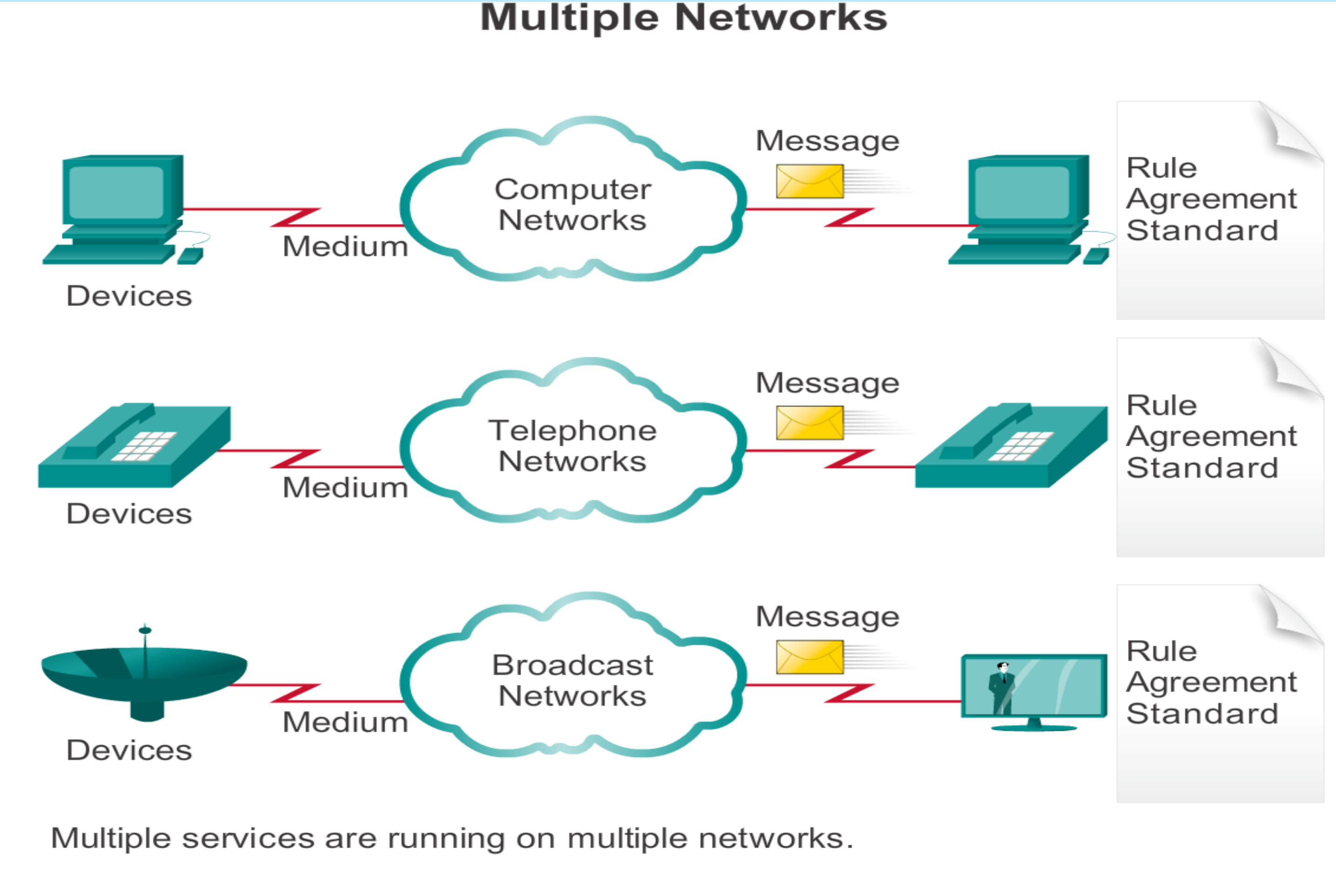
Connecting to the Internet

Connecting Businesses to the Internet



The Multiple Network

Computer networks, telephone networks and broadcast networks can operate on their own.

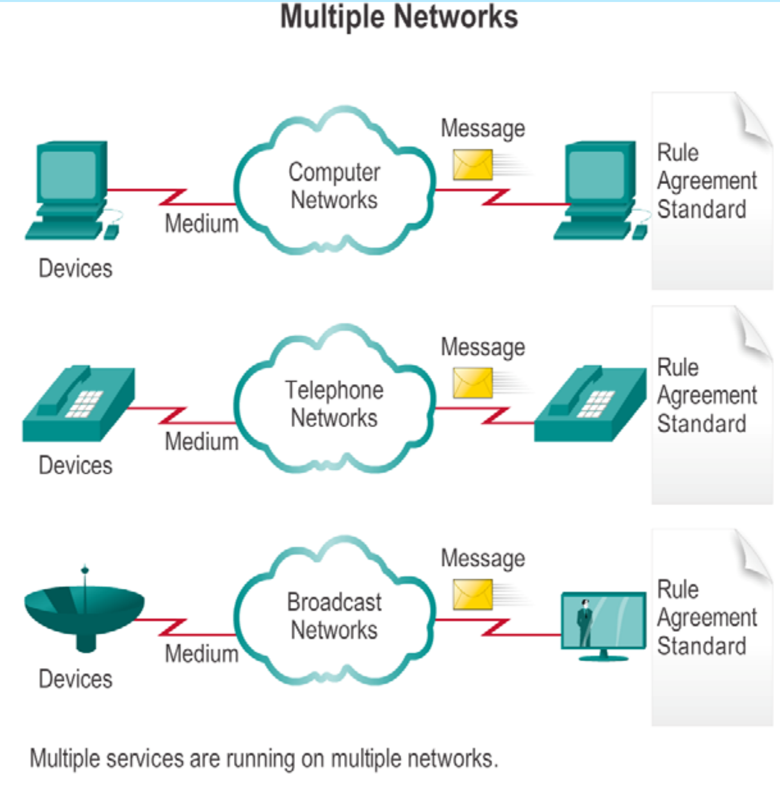


Multiple services are running on multiple networks.

The Converged Network

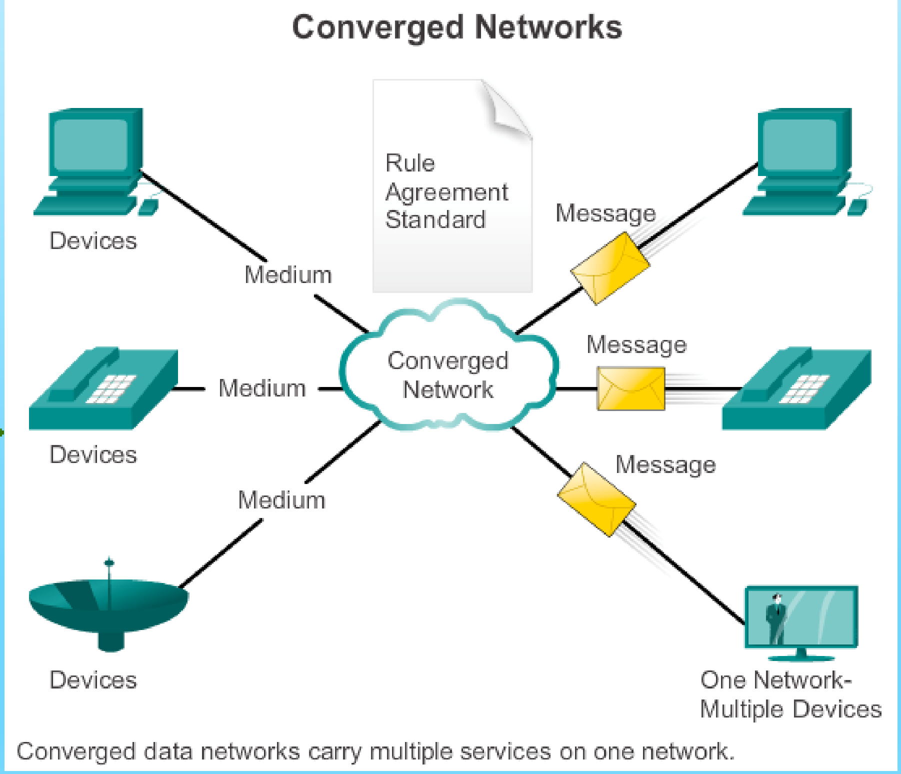
Multiple networks can be combined into converged networks.

Multiple Networks



Multiple services are running on multiple networks.

Converged Networks



Converged data networks carry multiple services on one network.

Reliable Network

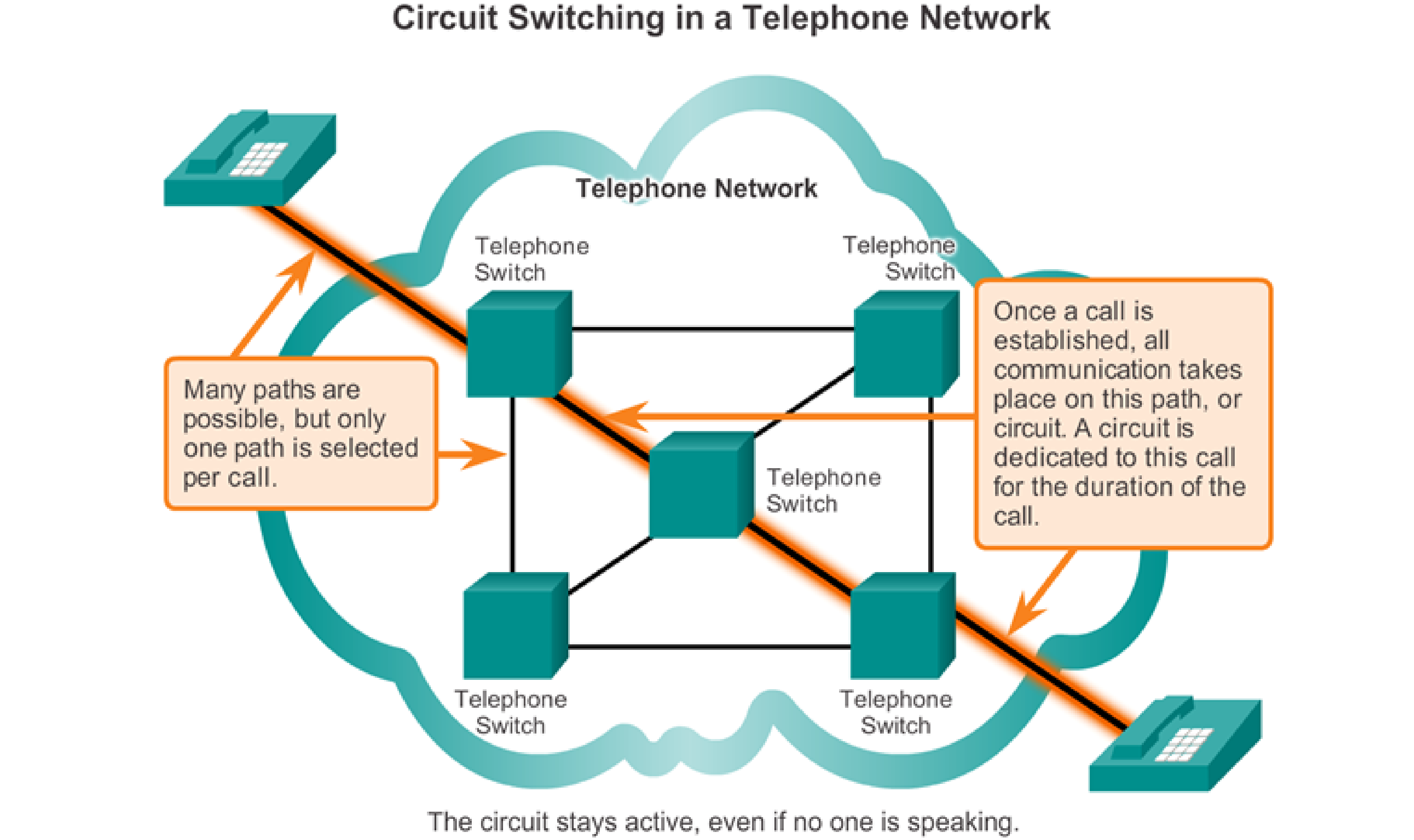
Supporting Network Architecture

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

- Fault Tolerance - Fault tolerance is the property that enables a system to continue operating properly in the event of the failure.
- Scalability – network able to expand as needed
- Quality of Service (QoS) - the overall performance of a telephony or computer network.
- Security – the ability of a system to protect against hacking and security threats.

Reliable Network

Fault Tolerance in Circuit Switched Network



Many paths are possible, but only one path is selected per call.

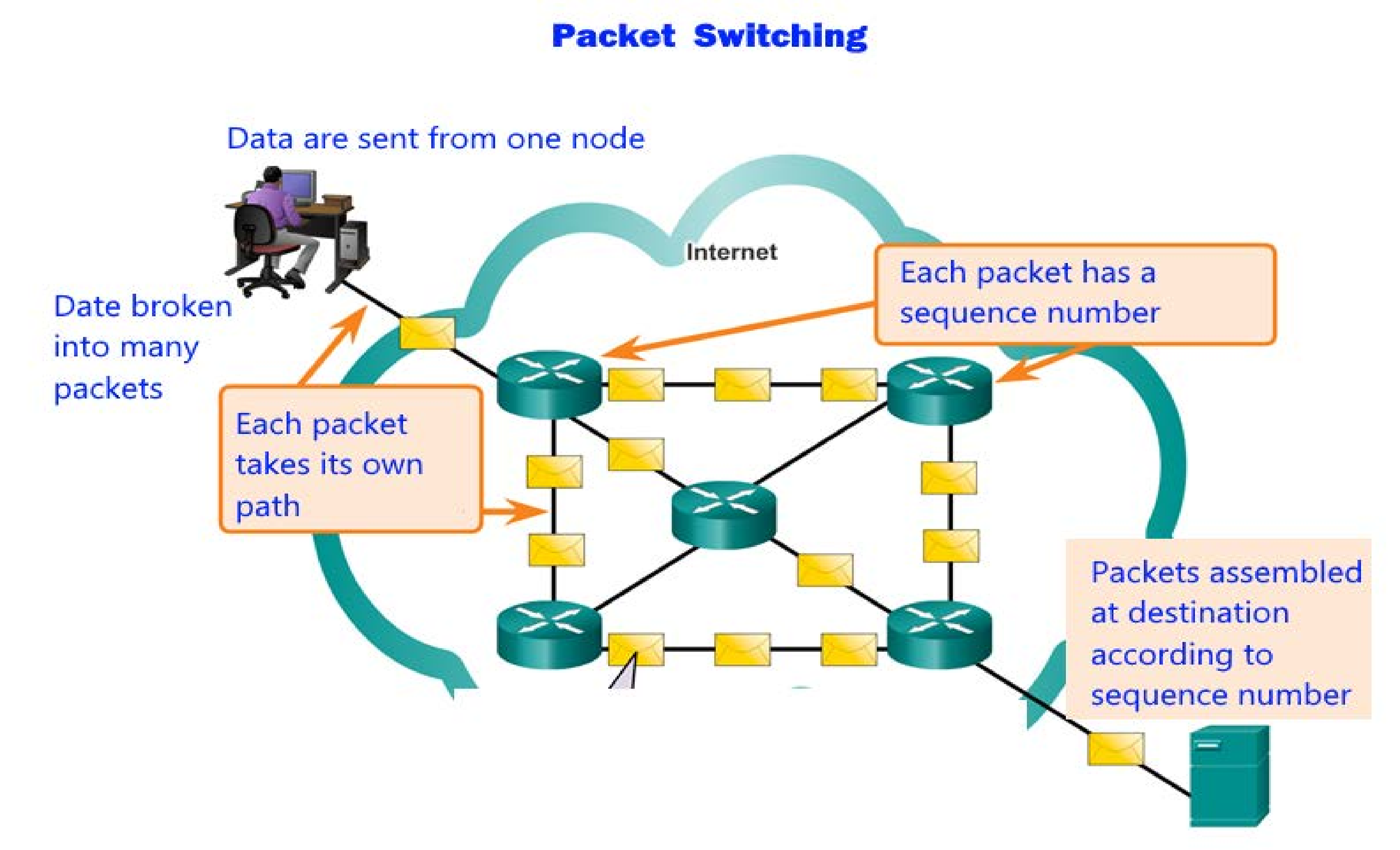
Once a call is established, all communication takes place on this path, or circuit. A circuit is dedicated to this call for the duration of the call.

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

circuit switching aims at connecting two nodes for communication

Reliable Network

Packet-Switched Networks



Packet Switching

Data are sent from one node

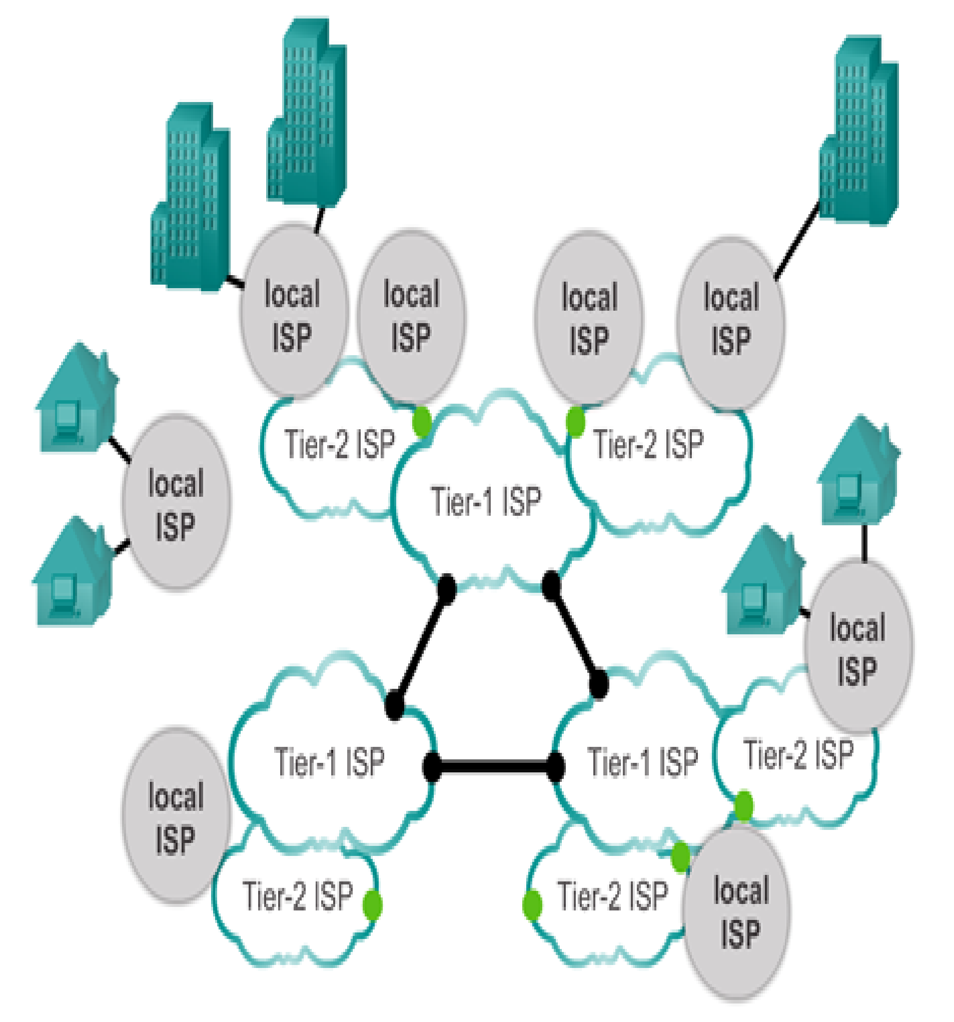
Date broken into many packets

Each packet takes its own path

Each packet has a sequence number

Packets assembled at destination according to sequence number

Scalable (Expandable) Networks



Tier 1 ISPs provide national and international services

Tier 2 ISPs are smaller and provide regional services; pay Tier 1 ISPs

Tier 3 ISPs provide services directly to users; pay Tier 2 ISPs
Also known as local ISPs

Reliable Network

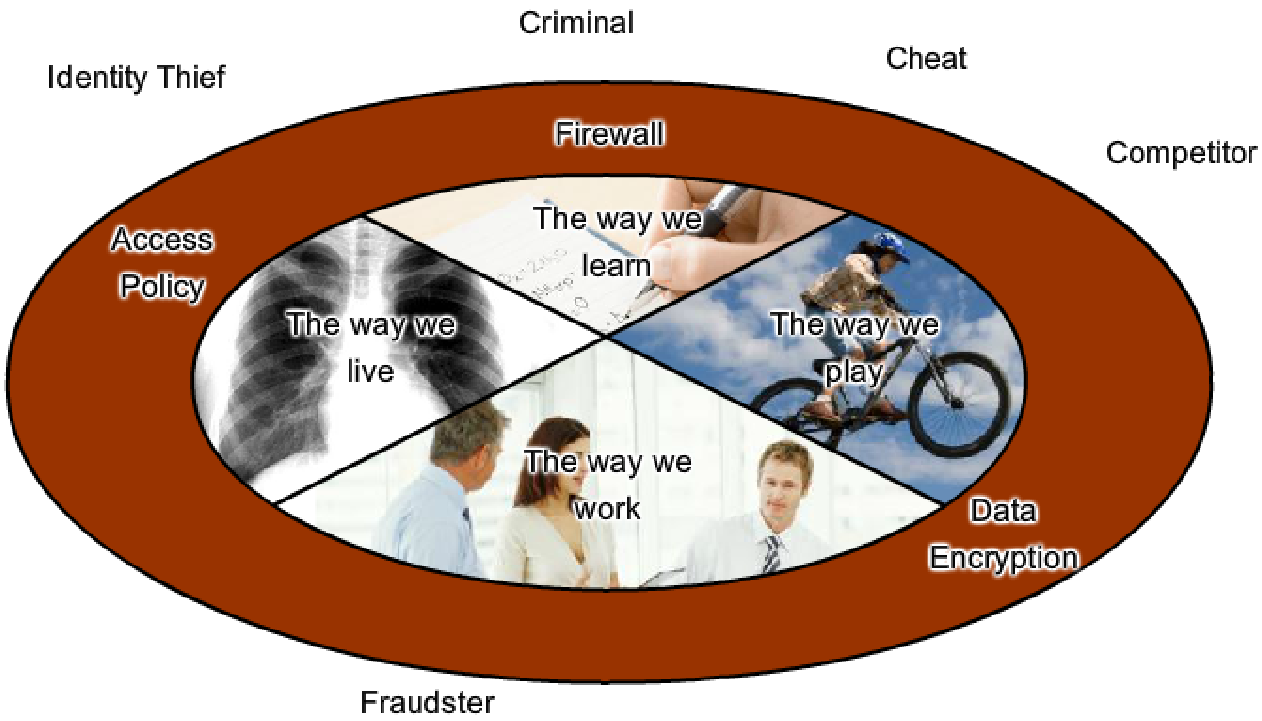
Providing QoS (Quality of Service)

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.

Reliable Network

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.

Network Trends

New trends

Some of the top trends include:

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

Network Trends

Bring Your Own Device (BYOD)

The concept of any device, to any content, in anyway is a major global trend. This trend is known as Bring Your Own Device (BYOD).

Online Collaboration - meetings

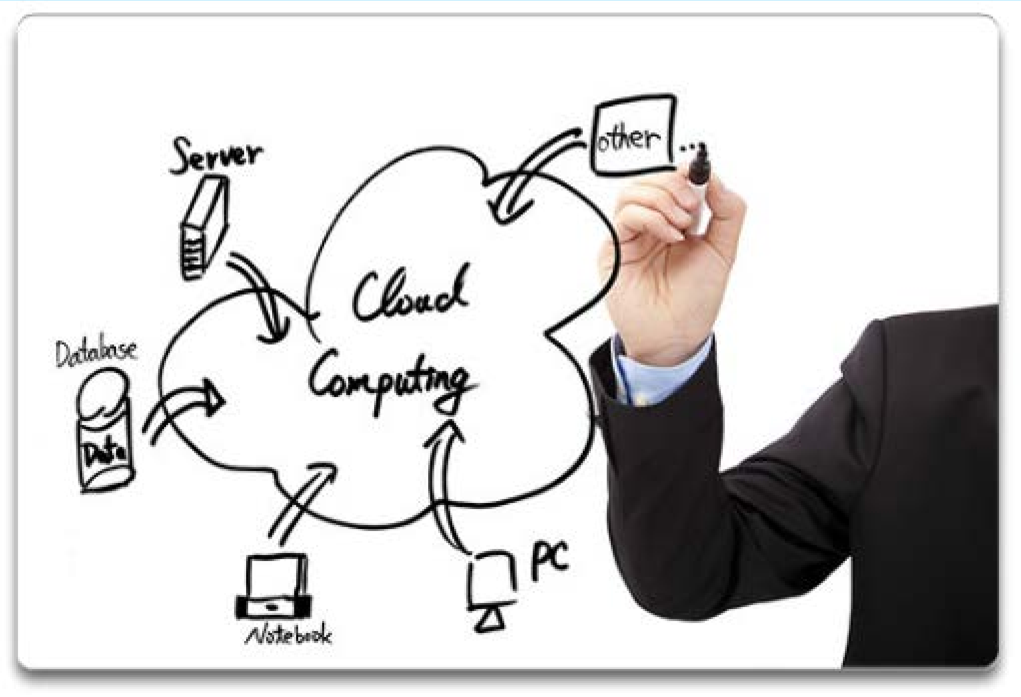
Collaboration
IP Communication
Mobile Applications
Telepresence
Messaging
Quarterly sales track for current fiscal year
Q1
Q2
Online Conferencing

Network Trends

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



Network Trends

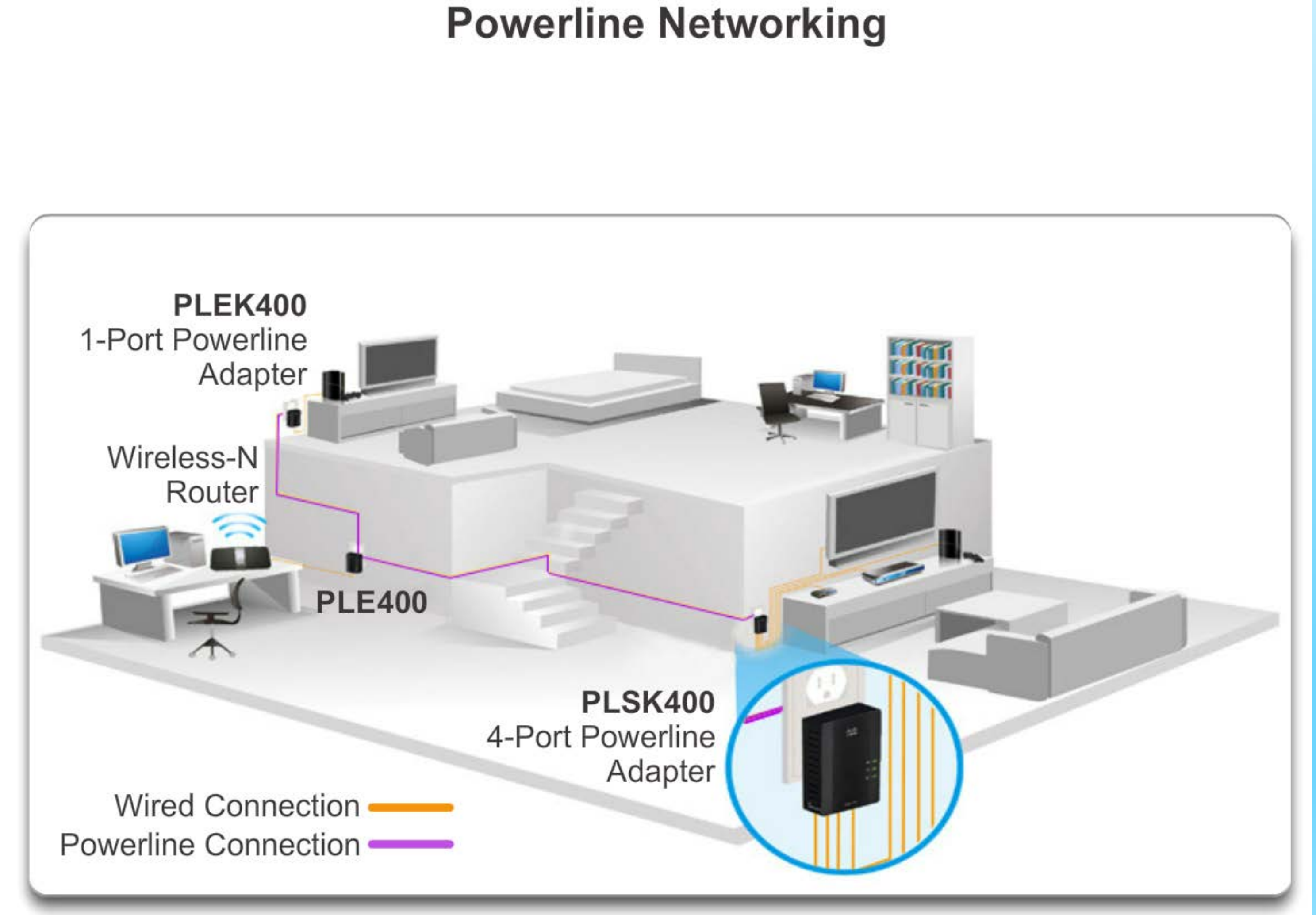
Data Centers

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

- Redundant data communications connections
- High-speed virtual servers
- Redundant storage systems
- Redundant or backup power supplies
- Environmental controls (e.g., air conditioning, fire suppression)
- Security devices

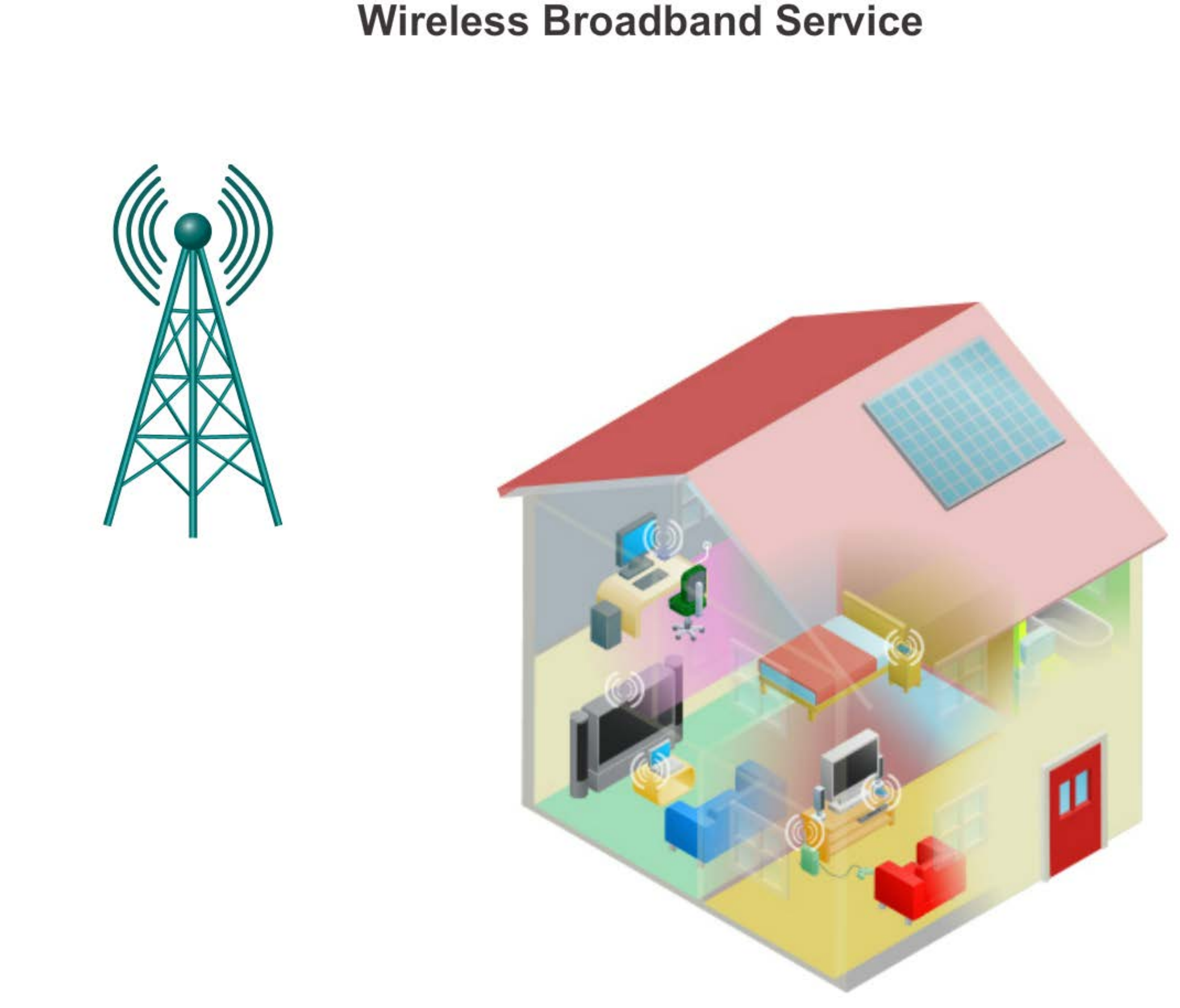
Networking Technologies for the Home

Powerline Networking



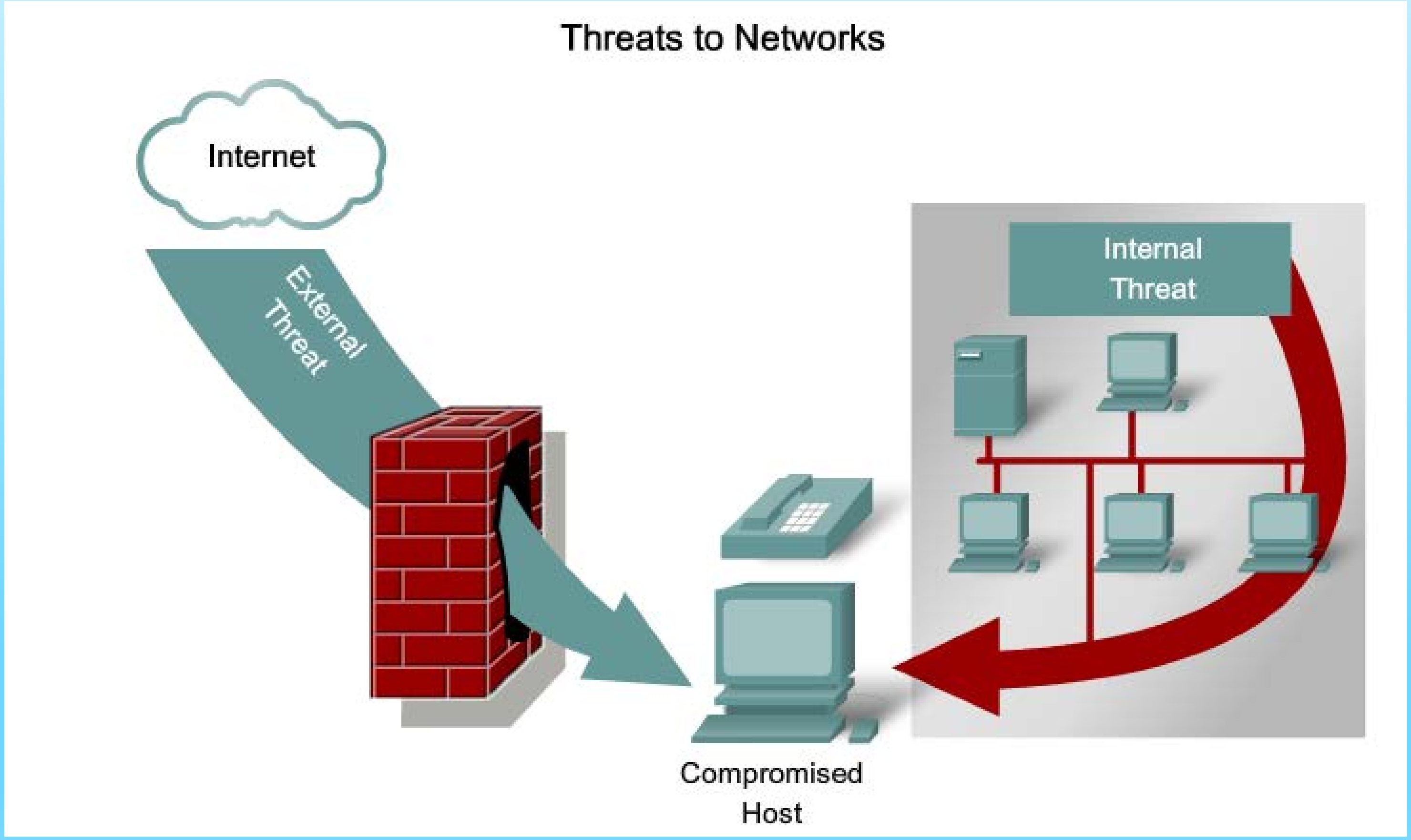
Networking Technologies for the Home

Wireless Broadband



Future of Networking

Network Security



Security Threats

The most common external threats to networks include:

- 1. Viruses, worms, and Trojan horses – softwares that replicate themselves
- 2. Spyware and adware
- 3. Zero-day attacks/Zero-hour attacks
  A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack.

Network Security

Security Threats

The most common external threats to networks include:

- 4. Hacker attacks
- 5. Denial of service (DoS) attacks - an attempt to make a machine or network resource unavailable to its intended users
- 6. Data interception and theft
- 7. Identity theft

Network Security

Security Solutions

Network security components often include:

- Antivirus and anti-spyware
- Firewall filtering - a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.
- Dedicated firewall systems
- Access control lists (ACL) - a list of access control entries that identify a trustee and specifies the access rights allowed, denied, or audited for that trustee.

Network Security

Security Solutions

Network security components often include:

- Intrusion prevention systems (IPS) - a network security/threat prevention technology that detects and prevents vulnerability exploits.
- Virtual Private Networks (VPNs) - extends a private network across a public network or internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

END OF CHAPTER 1

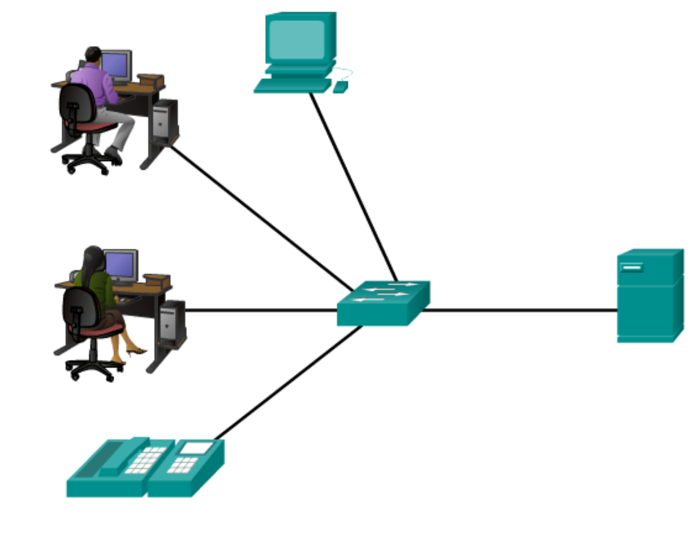
CHAPTER 1 B REVIEW

21 Questions

1. What does LAN stand for?

1. What does LAN stand for?

Ans : Local Area Network



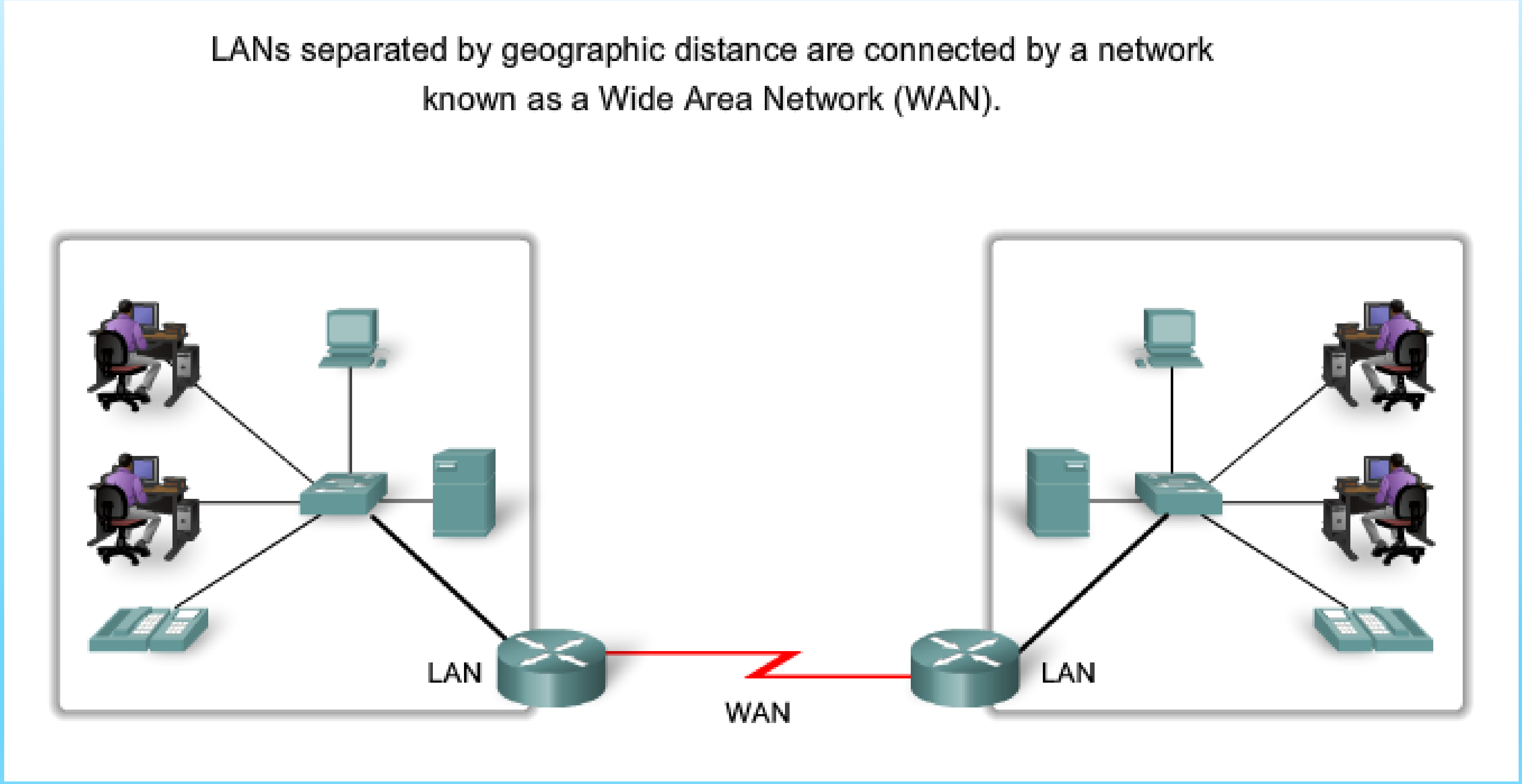
A network serving a home, building, or campus is considered a LAN.

2. What does WAN stand for?

Wide Area Network

3. How are LANs and WANs related?

3. How are LANs and WANs related?



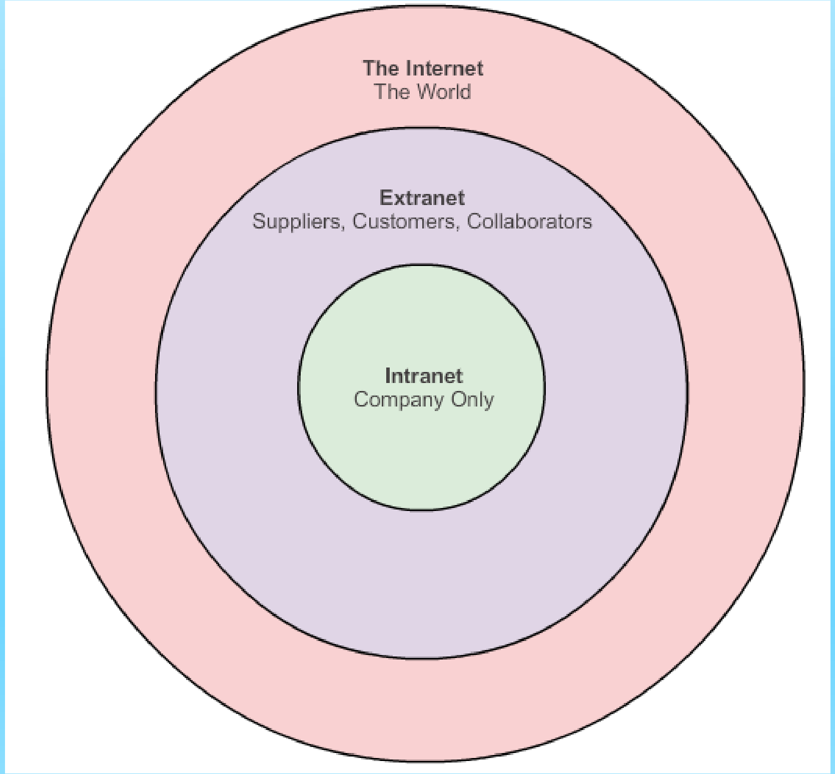
LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN).

4. What is the difference between Intranet, Extranet and Internet?

4. What is the difference between Intranet, Extranet and Internet?

Intranet can only be accessed by authorized users who are employees in an organization.

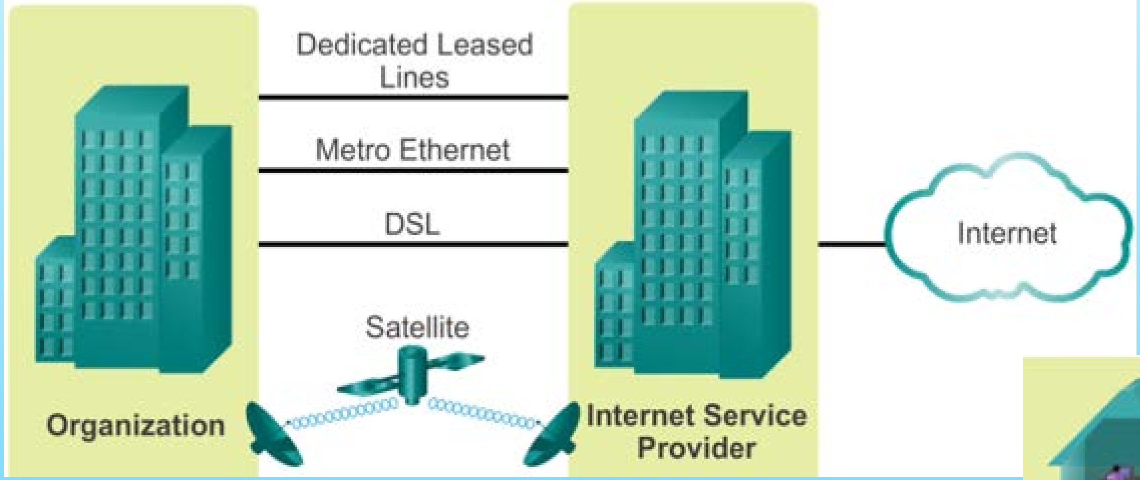
Extranet can only be accessed by authorized users, including employees and non-employees of an organization.

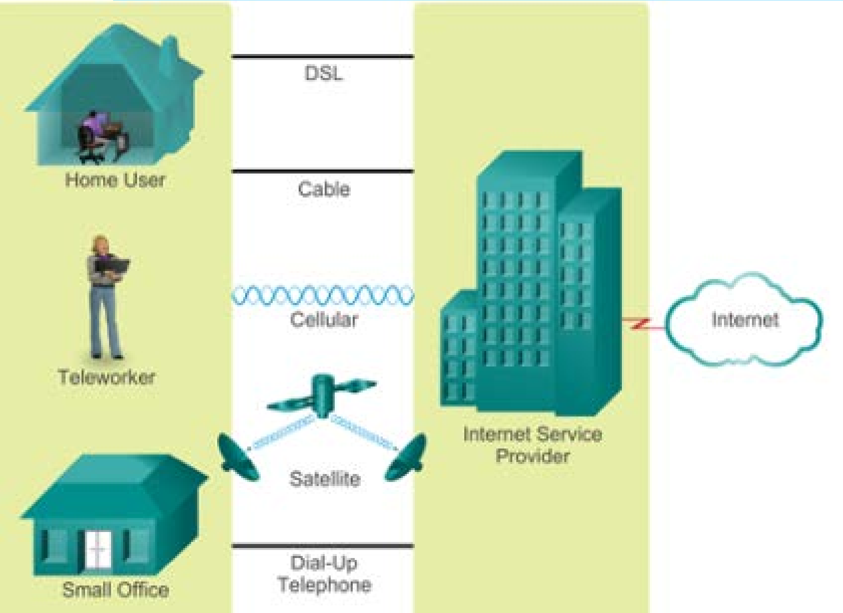


5. How do people in a country get access to the Internet?

5. How do people in a country get access to the Internet?

They can only do so via Internet Service Providers.





6. What are the 3 networks used over the Internet?

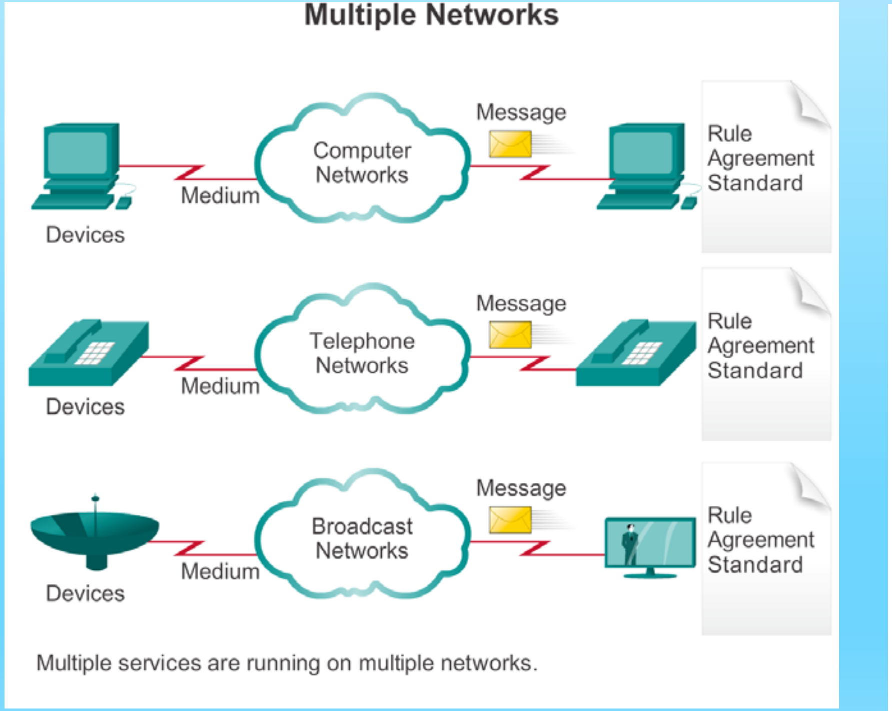
6. What are the 3 networks used over the Internet?

Computer network
Telephone network
broadcast network

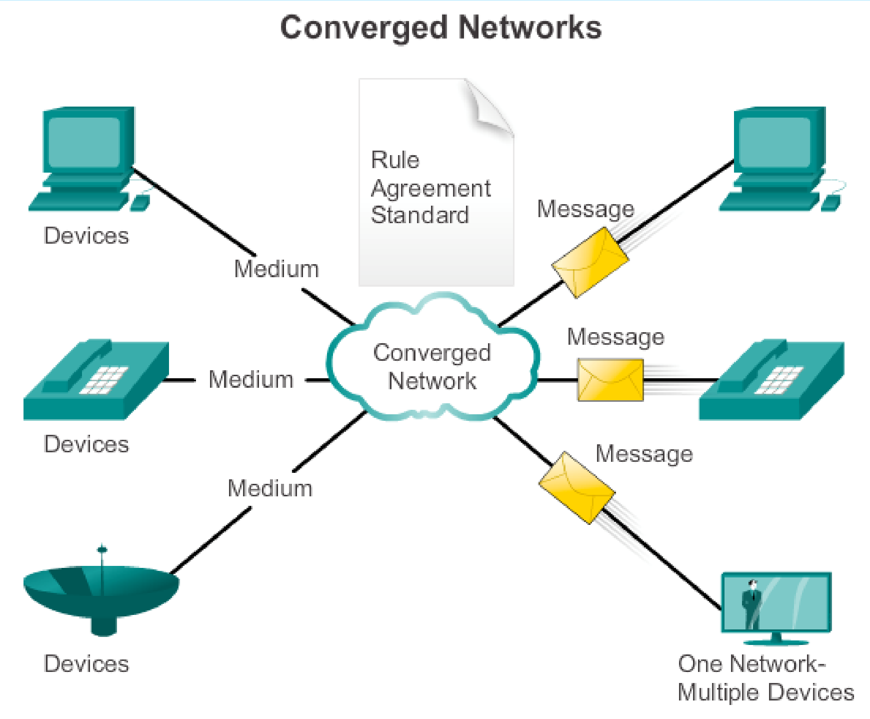
7. What is the difference between Multiple Networks and Converged Network?

7. What is the difference between Multiple Networks and Converged Networks?

Multiple Networks – each network operates on its own.
Converged Networks – all networks are run as one system.



Multiple services are running on multiple networks.



Converged data networks carry multiple services on one network.

8. What are the four characteristics of underlying network architectures?

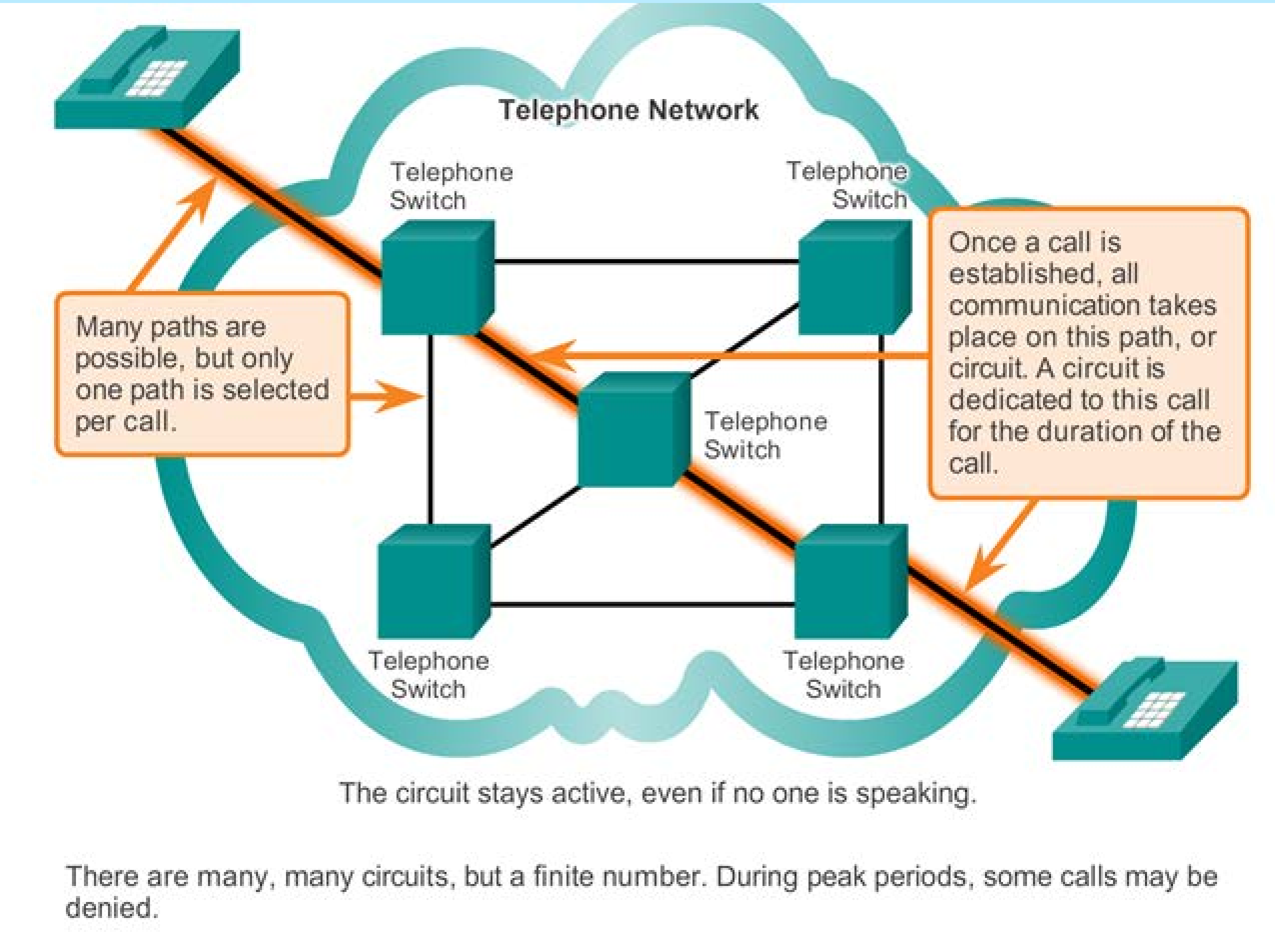
8. What are the four characteristics of underlying network architectures?

- Fault Tolerance - the property that enables a system to continue operating properly in the event of the failure of (or one or more faults within) some of its components.
- Scalability – network able to expand as needed
- Quality of Service (QoS) - the overall performance of a telephony or computer network, particularly the performance seen by the users of the network.
- Security – the ability of a system to protect against hacking and security threats.

9. What is Fault Tolerance in Circuit Switched Network

9. What is Fault Tolerance in Circuit Switched Network

If the number of calls exceed the limit, additional calls will may not get through.



Many paths are possible, but only one path is selected per call.

Once a call is established, all communication takes place on this path, or circuit. A circuit is dedicated to this call for the duration of the call.

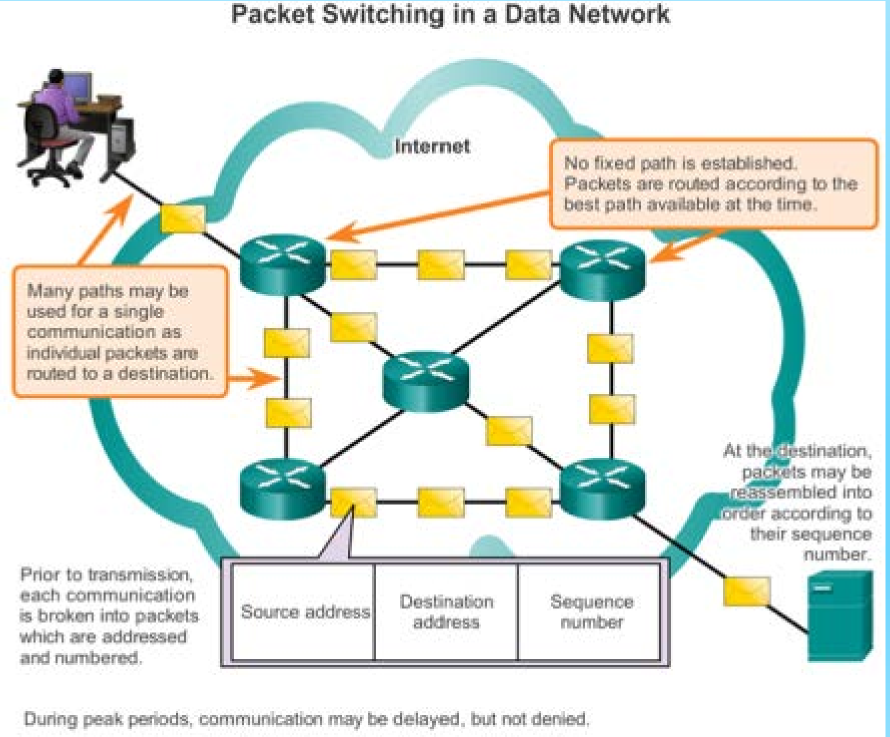
The circuit stays active, even if no one is speaking.

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

10. What is fault tolerance in Packet-Switched Networks

10. What is fault tolerance in Packet-Switched Networks

When traffic is high, communication may be delayed, but will not be denied.



Packet Switching in a Data Network

No fixed path is established. Packets are routed according to the best path available at the time.

Many paths may be used for a single communication as individual packets are routed to a destination.

At the destination, packets may be reassembled into order according to their sequence number.

Prior to transmission, each communication is broken into packets which are addressed and numbered.

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

11. What are Scalable Networks

11. What are Scalable Networks

Scalable networks are networks that can be expanded.

12. What does providing QoS (Quality of Service) mean?

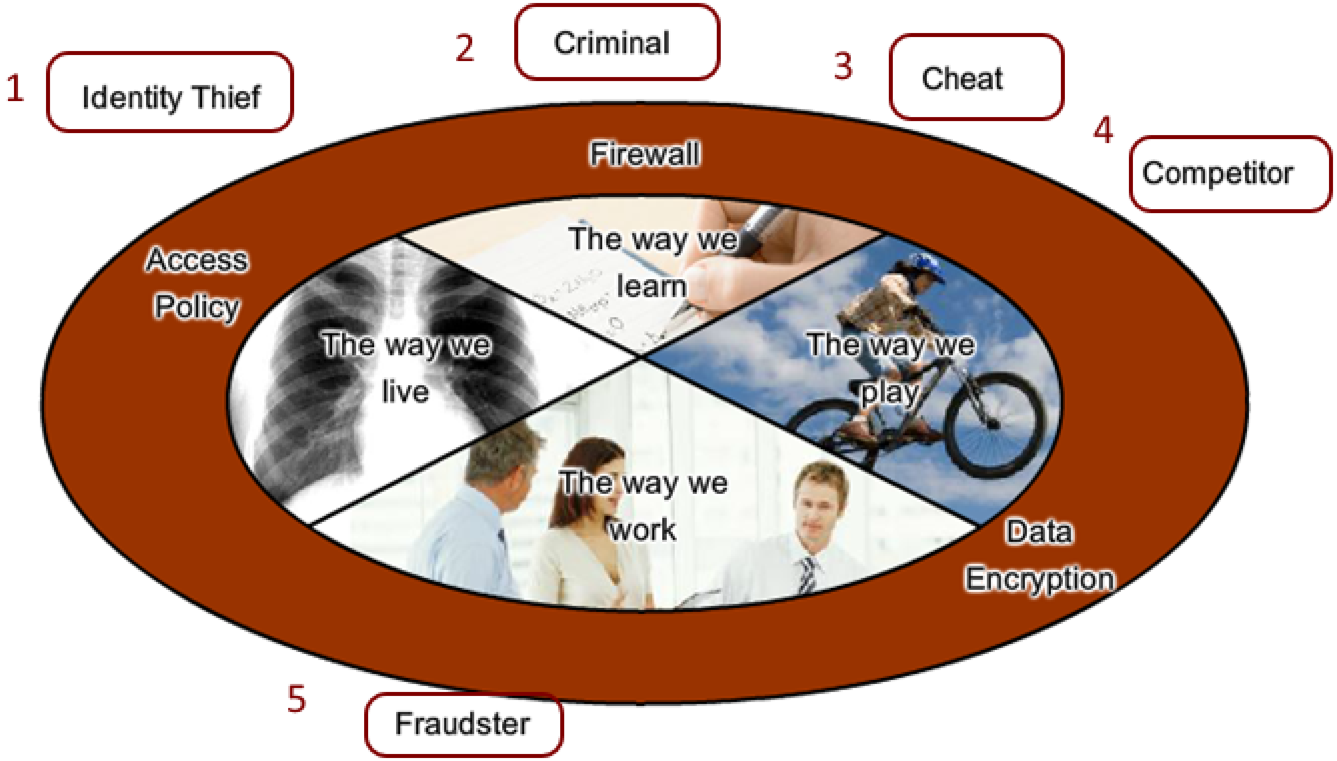
12. What does providing QoS (Quality of Service) mean?

It means providing priority decisions for an organization.

- 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.

13. Who must networks be protected from?

13. Who must networks be protected from?



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

14. What are 4 new network trends?

14. What are 4 new network trends?

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

Network Trends

Online Collaboration

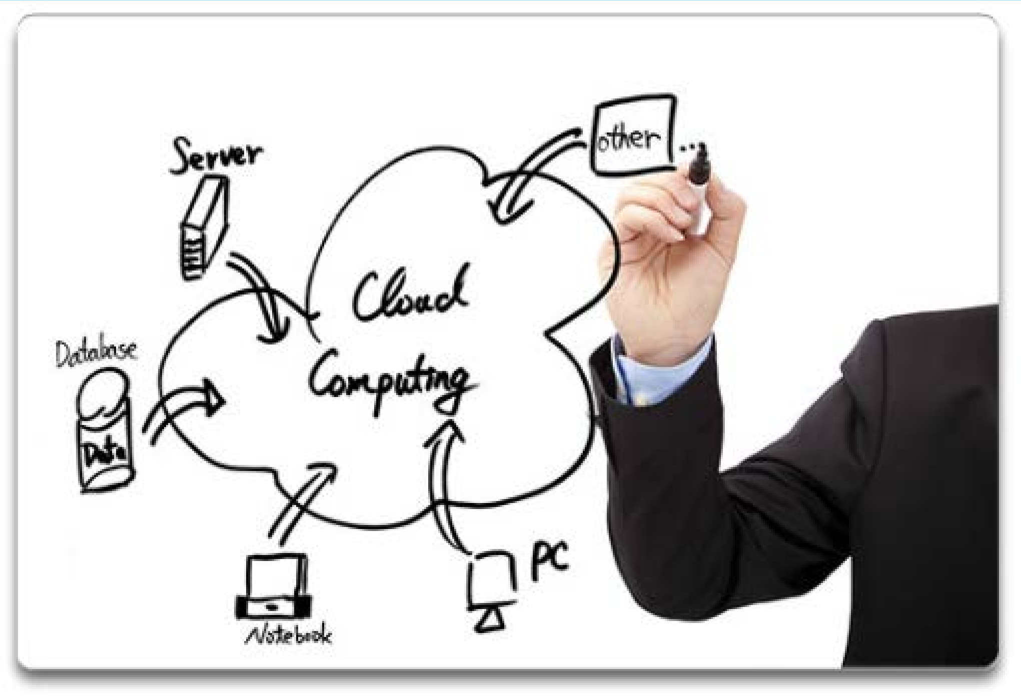
Collaboration
IP Communication
Mobile Applications
Telepresence
Messaging
Quarterly sales track for current fiscal year
Q1
Q2
Online Conferencing

15. What are some potential benefits of Cloud Computing

15. What are some potential benefits of 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



16. What are Data Centers

16. What are Data Centers

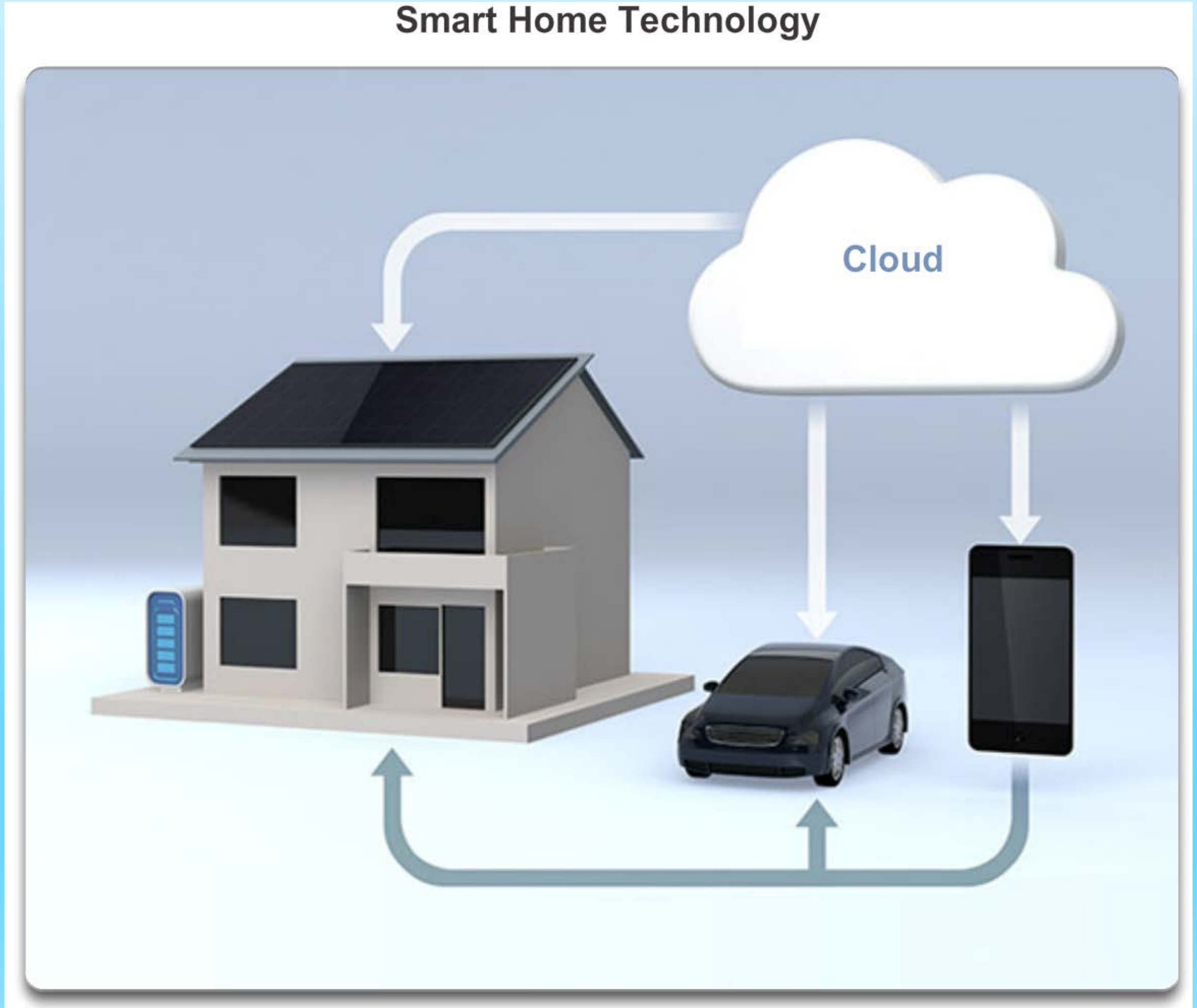
A data center is a facility used to house computer systems and associated components.

17. What devices are found at Data Centers?

17. What devices are found at Data Centers?

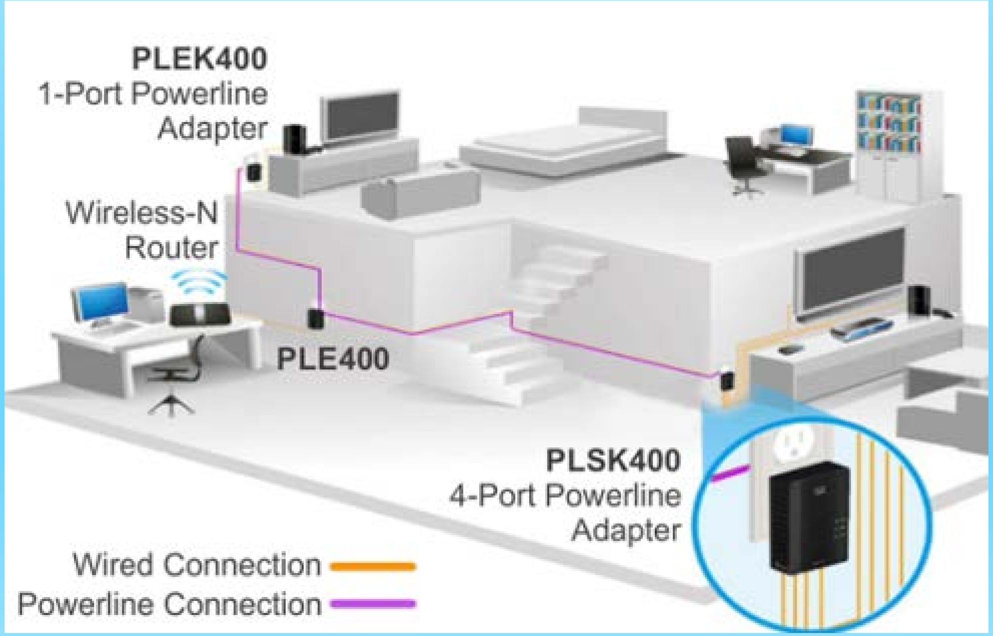
- Redundant data communications connections
- High-speed virtual servers
- Redundant storage systems
- Redundant or backup power supplies
- Environmental control devices (e.g., air conditioning, fire suppression)
- Security devices

18. What are 2 trends in home technology?



18. What are 2 trends in home technology?

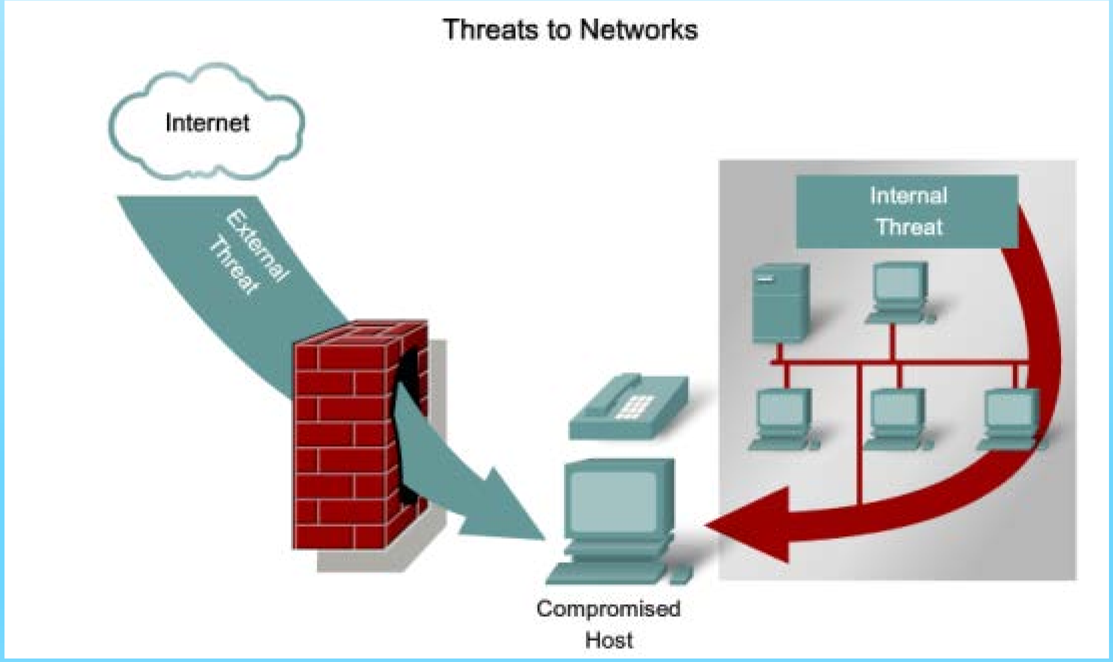
- Power Line Networking
- Wireless Broadband



19. What are the 2 categories of Network Security threats?

19. What are the 2 categories of Network Security threats?

Internal threats (employees in organisation)
and external threats (people outside organisation)



20. Name 7 external Security Threats

20. Name 7 external Security Threats

- 1. Viruses, worms, and Trojan horses – softwares that replicate themselves
- 2. Spyware and adware
- 3. Zero-day attacks/Zero-hour attacks
- . Hacker attacks
- 5. Denial of service (DoS) attacks - an attempt to make a machine or network resource unavailable to its intended users
- 6. Data interception and theft
- 7. Identity theft

21. What are Security Solutions available for use against threats?

21. What are Security Solutions available for use against threats?

Network security solutions include:

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