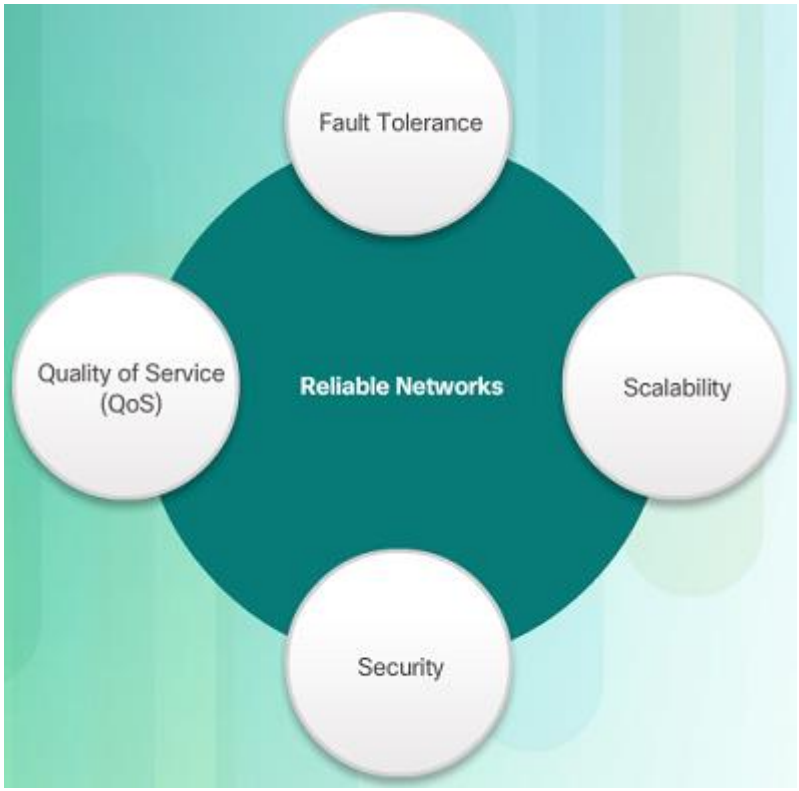
Module 2: Networking Today (part 2)

ARIS PULUMBARIT

1.6 Reliable Networks

Reliable Network

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

Reliable Network

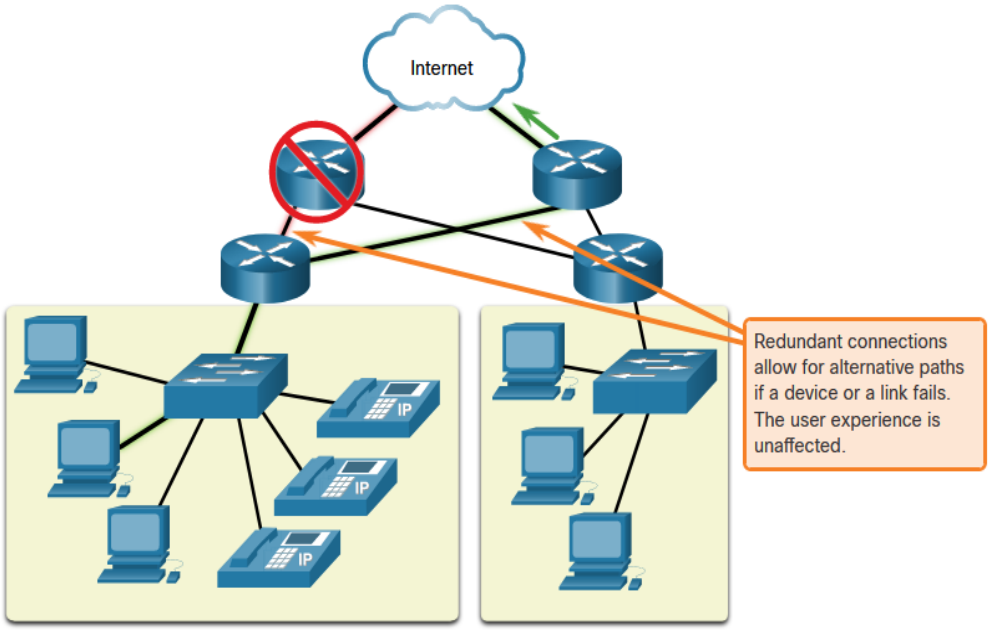
Fault Tolerance

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:

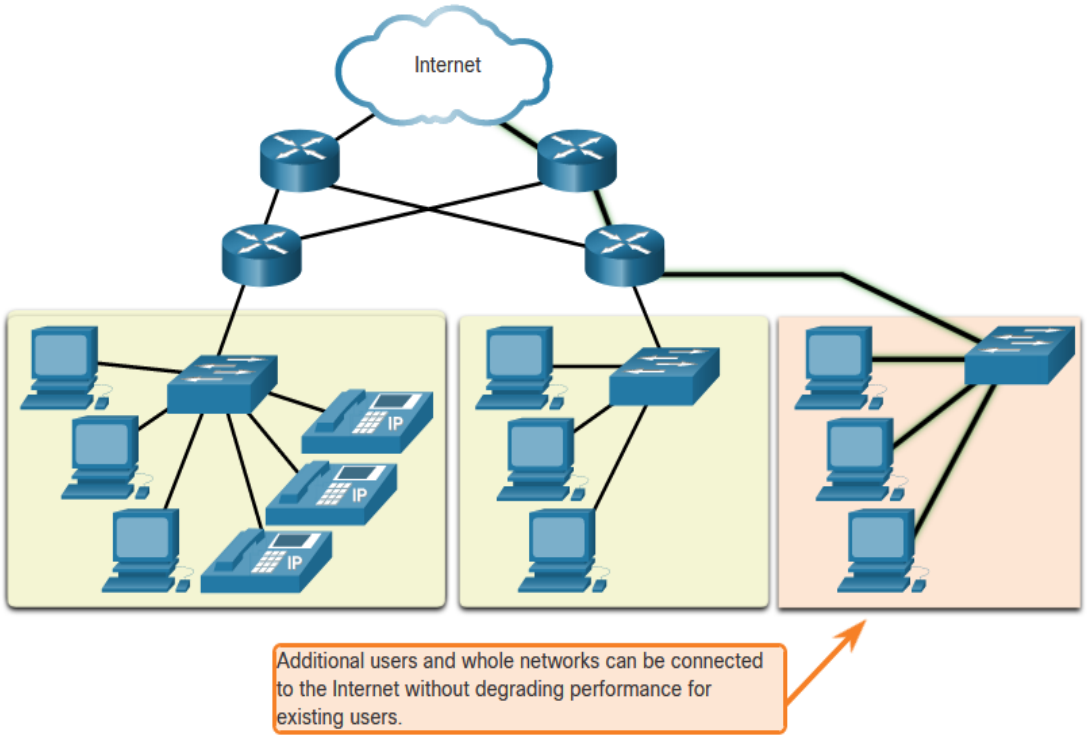
- Packet switching splits traffic into packets that are routed over a network.
- Each packet could theoretically take a different path to the destination.

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



Reliable Network

Scalability



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.

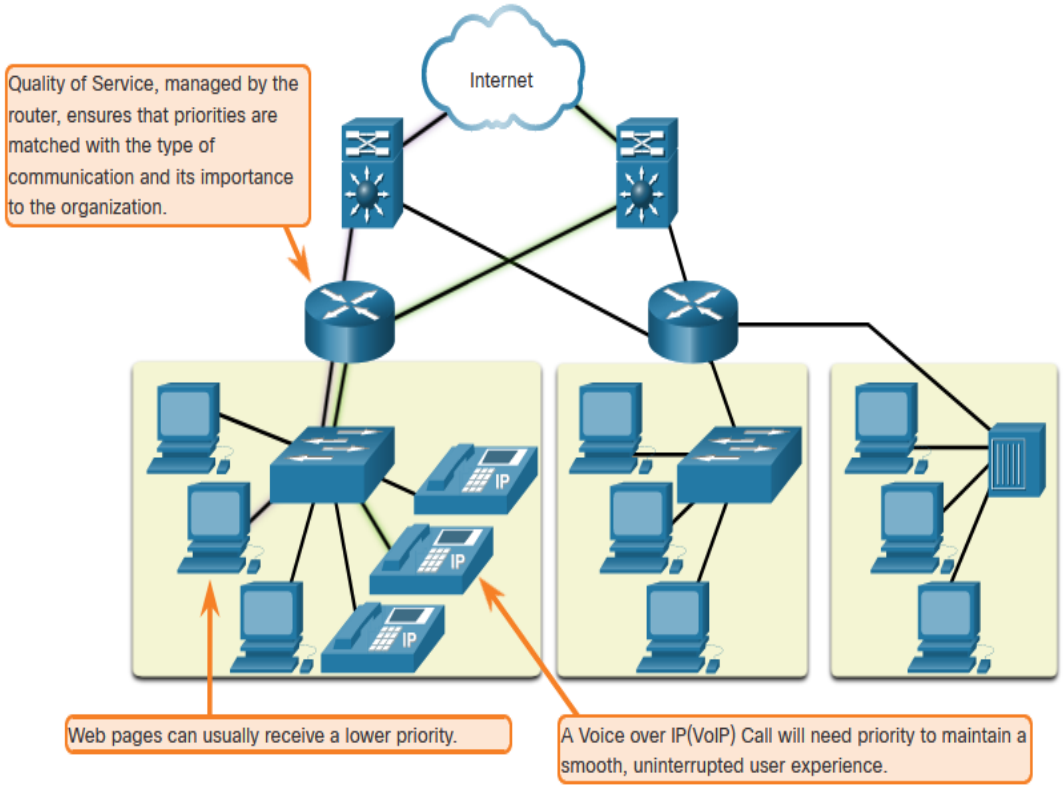
Reliable Network

Quality of Service

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

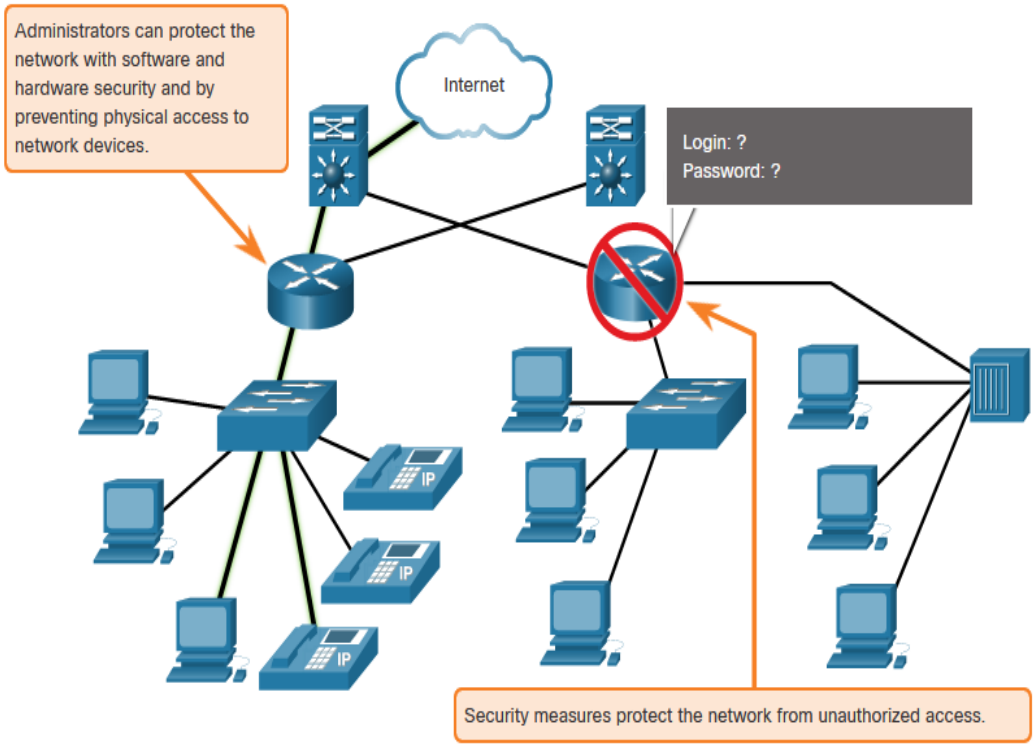
Have you ever watched a live video with constant breaks and pauses? This is caused when there is a higher demand for bandwidth than available – and QoS isn't configured.

- 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.



Reliable Network

Network Security



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

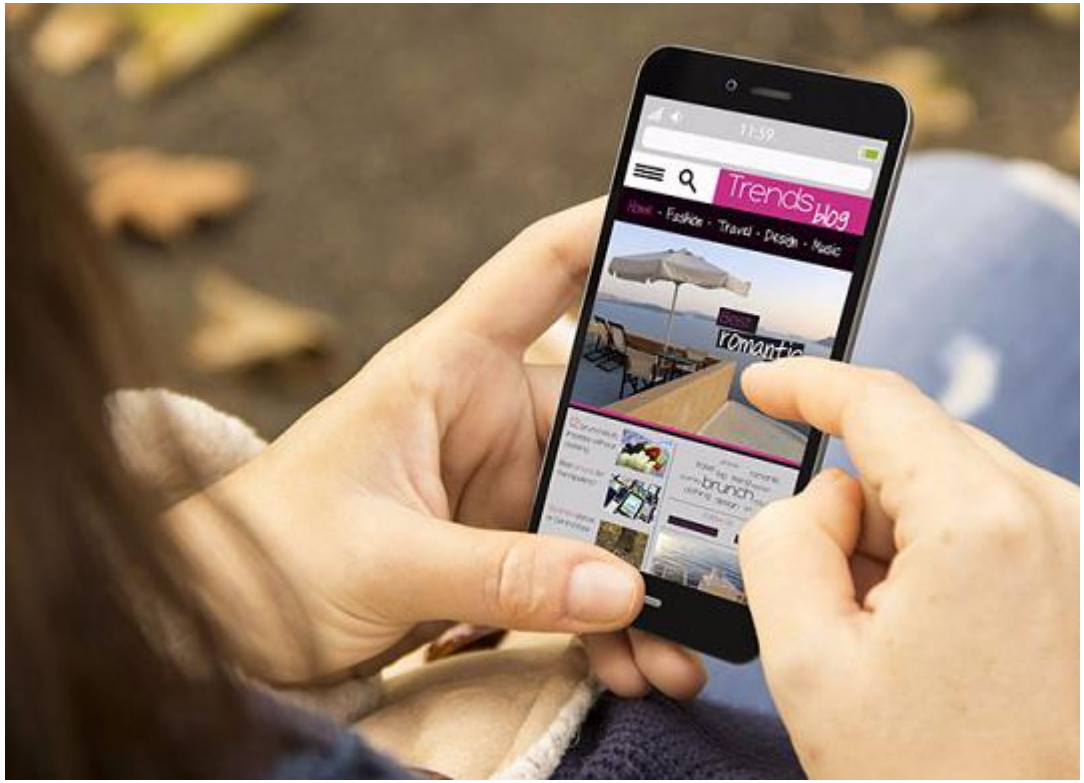
Recent Trends

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.

Network Trends

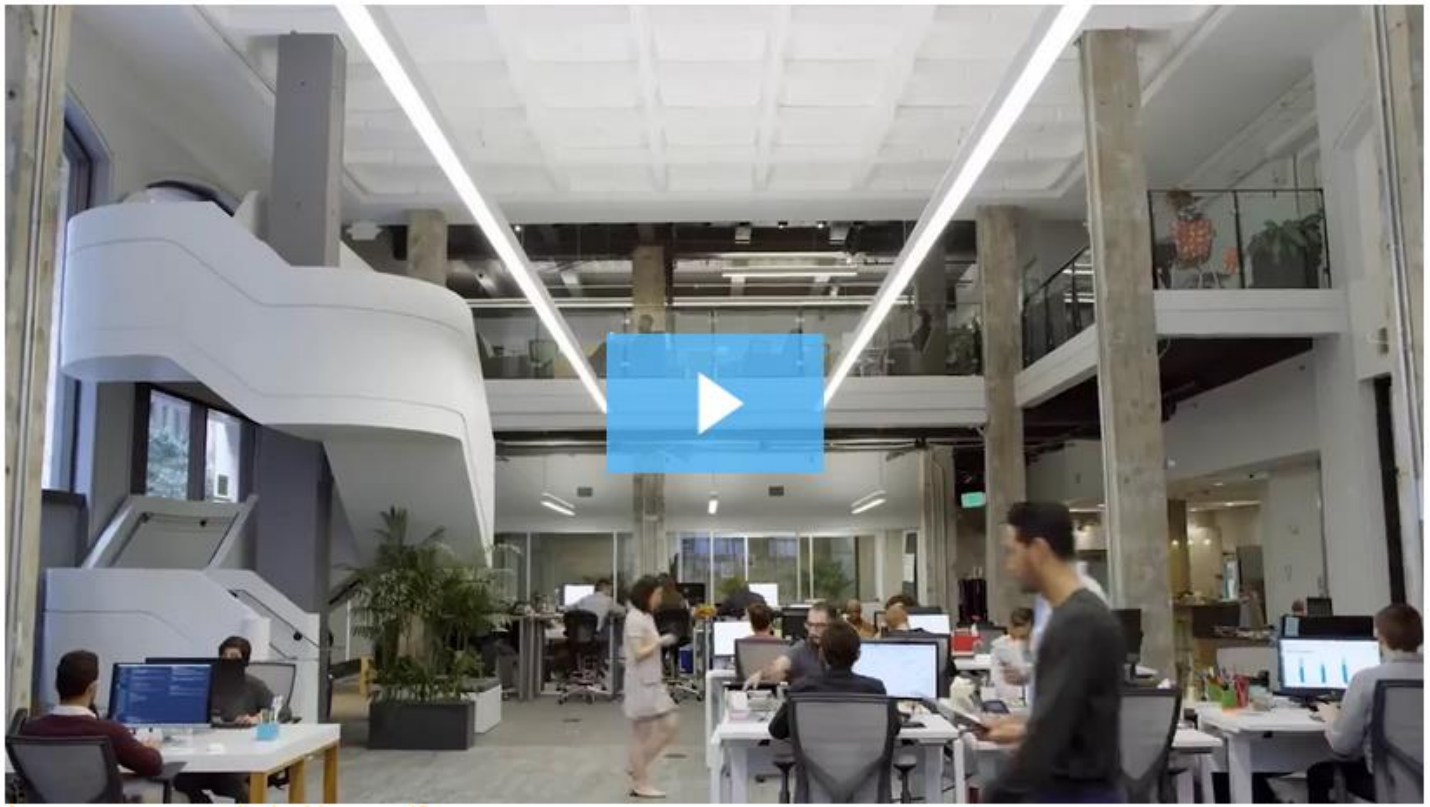
Online Collaboration

- 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.

Video – Cisco WebEx for Huddles



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.

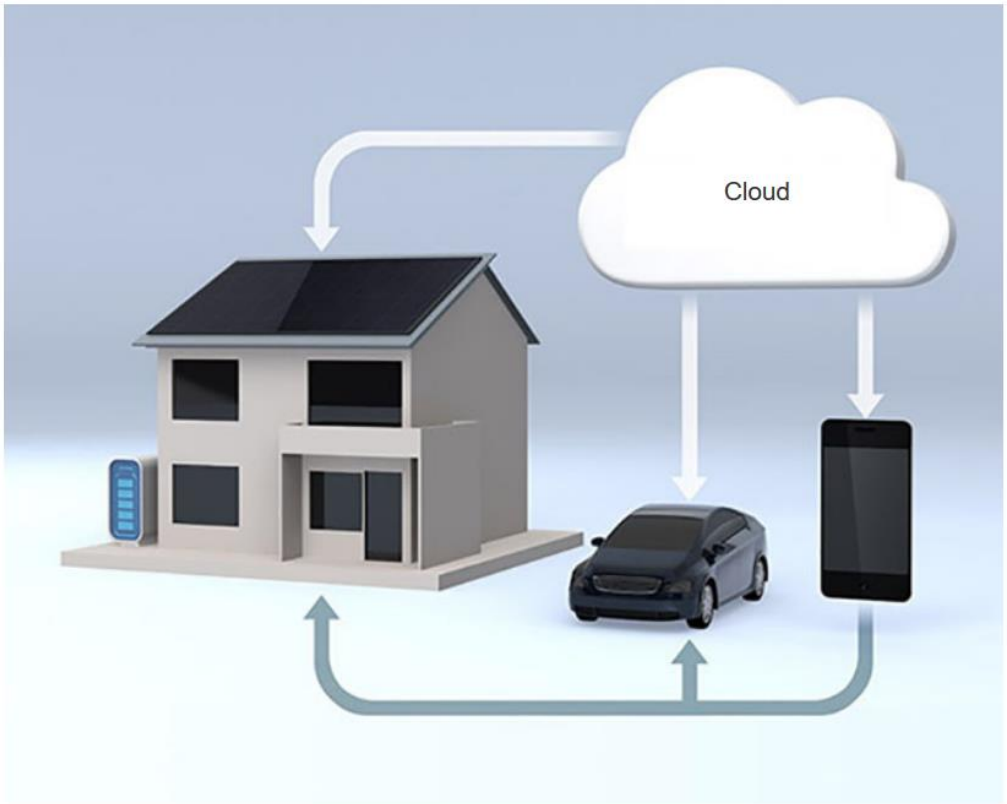
- Smaller companies that can't afford their own data centers, lease server and storage services from larger data center organizations in the Cloud.

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.

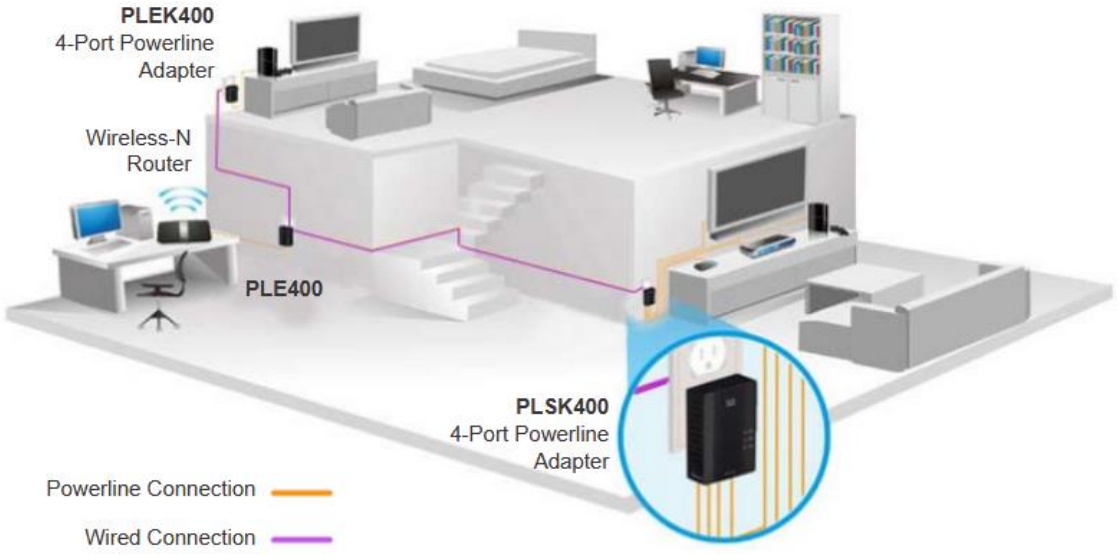
Technology Trends in the Home



- 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



- 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

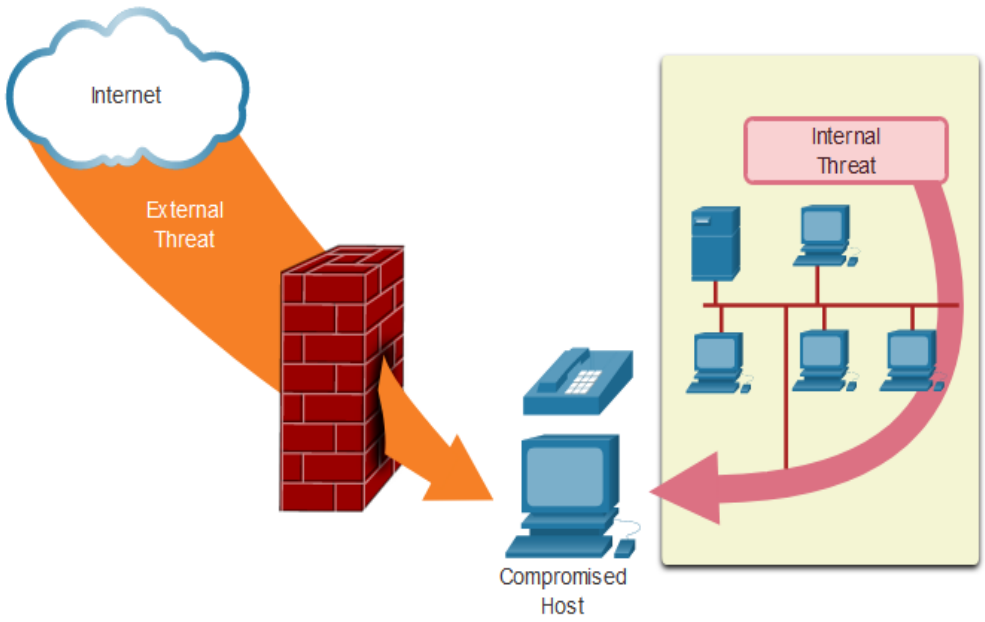
In addition to DSL and cable, wireless is another option used to connect homes and small businesses to the internet.

- 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

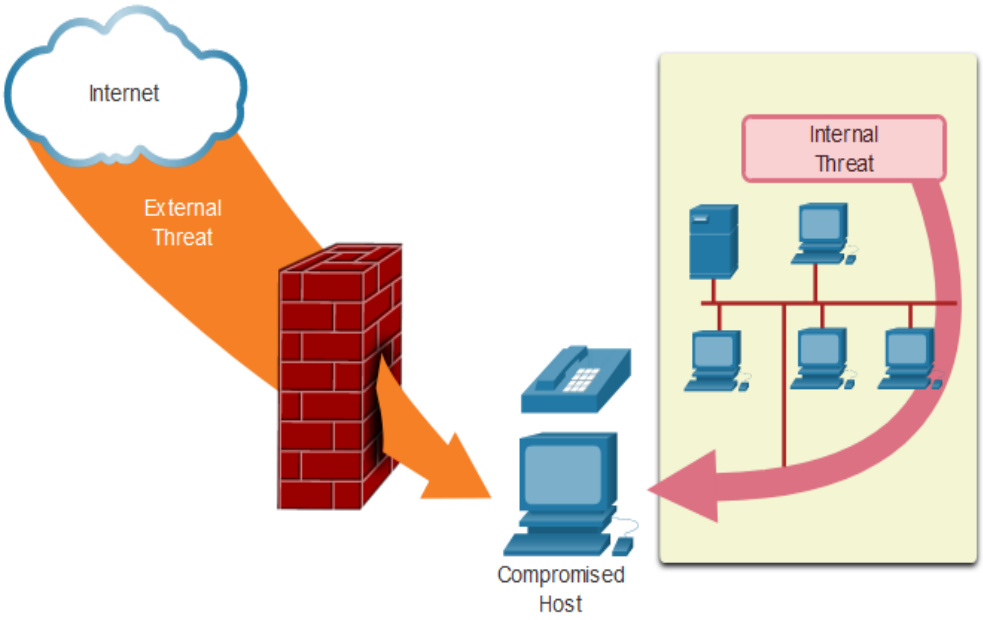
Network Security

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.)



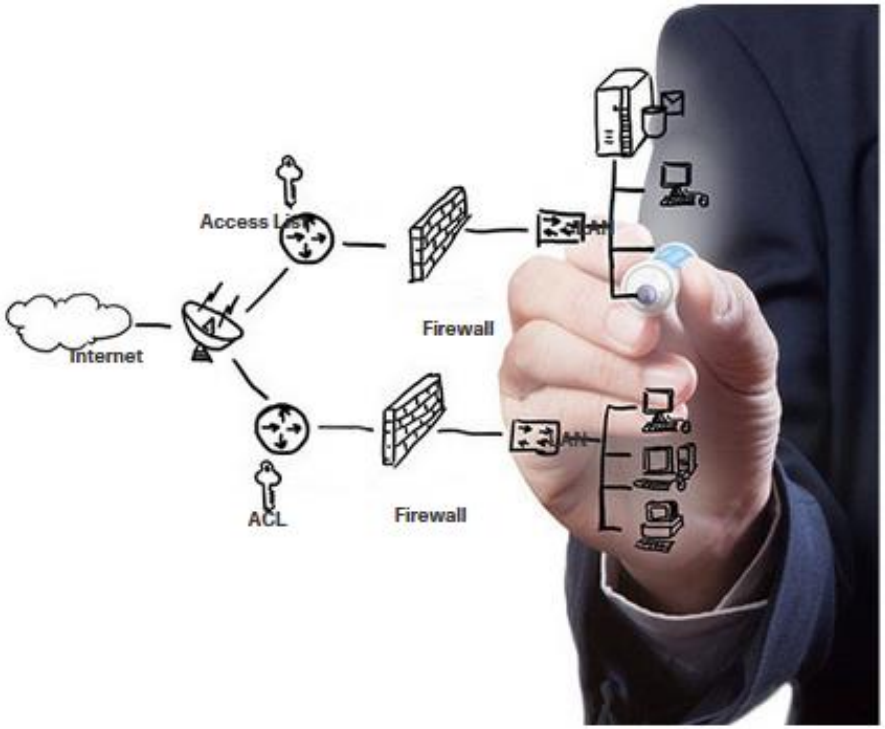
External Threats:

- 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

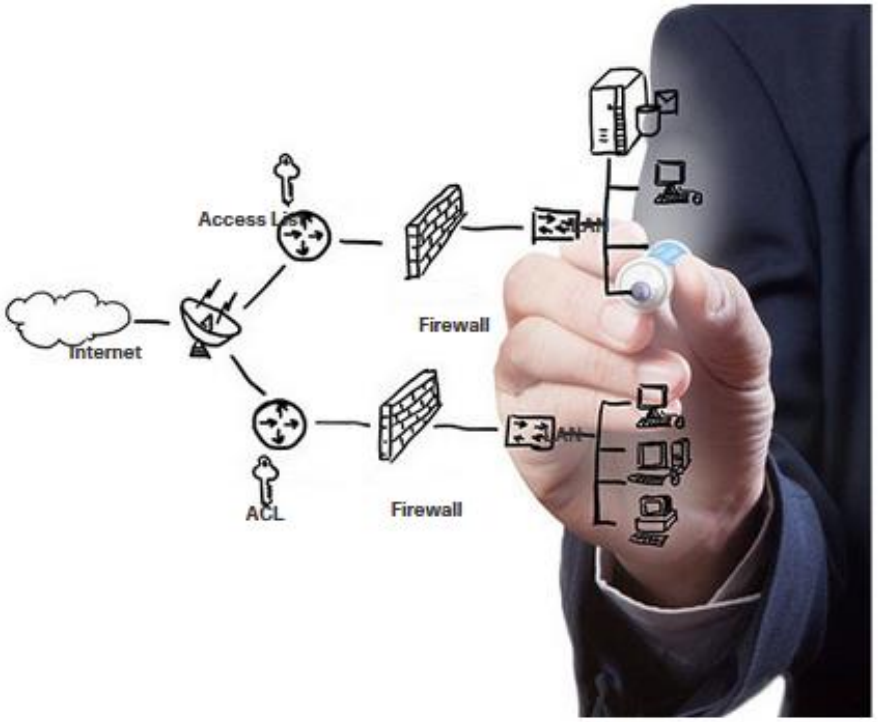


Security must be implemented in multiple layers using more than one security solution.

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:

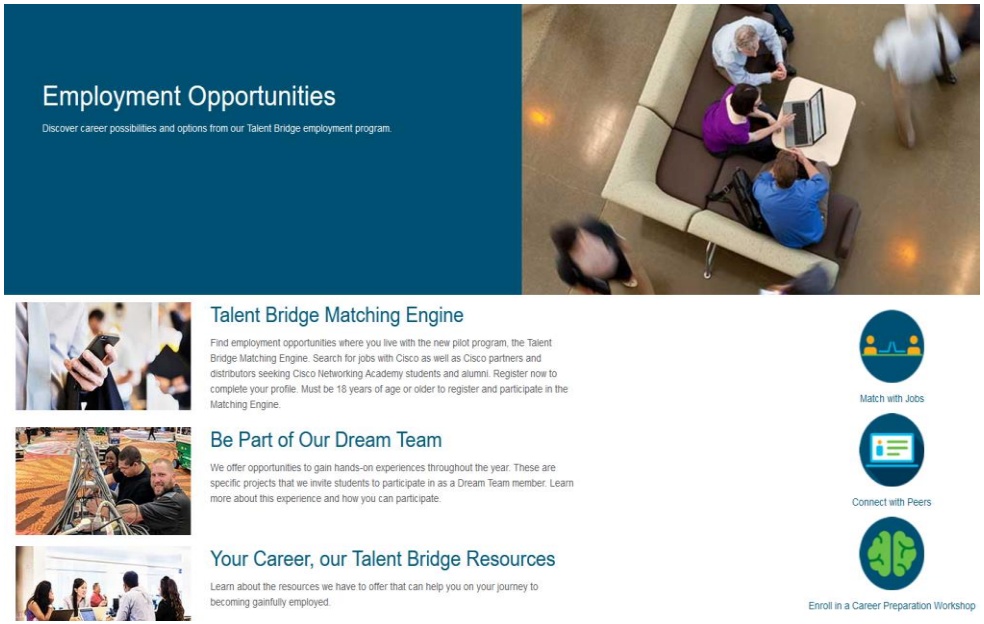
- IP foundation and security topics
- Wireless, virtualization, automation, and network programmability.

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



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.

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

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.

Module Practice and Quiz

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.

Thank You