Notebook: CCNA Level 1

鲍煜坤

yukun.bao@telecom-paristech.fr
SJTU-ParisTech Elite Institute of Technology

March 12, 2017

Course Index

SHANGHAI JIAO TONG UNIVERSITY
TELECOM ParisTech

Introduction

The focus of this course is on learning the fundamentals of networking.We will do the following:

- Examine human versus network communication and see the parallels between them
- Be introduced to the two major models used to plan and implement networks: **OSI** and **TCP/IP**
- Gain an understanding of the ”layered” approach to networks
- Become familiar with the various network devices and network addressing schemes
- Discover the types of media used to carry data across the network
- Be able to build simple LANs, perform basic configurations for routers and switches, and implement IP addressing schemes.

Our studying is based on the following environment:

- System: **Ubuntu 16.04 LTS**
  installed on virtual machine ”Oracle VM VirtualBox”[1]
- Tools:
  - **Packet tracer 7.0** by Cisco Academy Community
  - **Wireshark** Network traffic analyzer
  - **XTerm** standard terminal emulator for the X window system
  - **Netkit-ng/UML** manipulation of virtual machines in User Mode Linux (UML) [2]
- Optional system image: **RES101-Ubuntu-2017**[3]
  It integrates all necessary tools and is accessible on the Google Drive [4].

Familiar with virtual machine commands

Here are the useful commands for manipulating virtual machines.

lstart: start the whole network, machine by machine
lstart PC1: only start PC1 in this network
lhalt [PC1]: stop gracefully the whole network, machine by machine
lcrash [PC1]: stop brutally or power off the whole network
visit: list all the machines running
lclean: delete all the temporary files

Attention: *lclean* is always appreciated after a *lcrash* or *lclean*.

Exercise on virtual machine

We are now going to do an exercise. Exercise files include ”*lab.conf*”(description of network), ”*PC1.startup*”(initialization of PC1) and ”*PC2.startup*”.

```
LAB_DESCRIPTION=”RES 101  Lab 1: Netkit Environment”
LAB_VERSION=1.0
LAB_AUTHOR=”L. Iannone (Based on C. Chaudet Labs)”
LAB_EMAIL=luigi.iannone@telecom-paristech.fr
LAB_WEB=http://www.telecom-paristech.fr/

PC1[0]=”Link”  //Connect the network card 0 to ”Link”
PC1[9]=tap,172.16.0.254,172.16.0.1
PC1[con0]=xterm  //xterm terminal appears right after PC1 starts

PC2[0]=”Link”
PC2[9]=tap,172.16.0.254,172.16.0.2
PC2[con0]=xterm
```

Listing 1: Virtual Machine lab.conf

[1] https://www.virtualbox.org
[2] https://netkit-ng.github.io
[3] User name: res101; Password: res101-2017
[4] https://drive.google.com/open?id=0Byh-un6Ly9NCWERmcXhJN2RlYVU

```
/sbin/ifconfig eth0 hw ether 00:00:00:01:00:aa
/sbin/ifconfig eth0 10.0.0.1 netmask 255.255.255.0 up
echo ”0” > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

chown root:root /root
chmod 700 /root/.ssh
chmod 755 /root
chmod 644 /root/.ssh/*
chmod 600 /root/.ssh/id_rsa
route del default gw 172.16.0.1
/etc/init.d/ssh start
```

Listing 2: Virtual Machine PC1.startup

```
/sbin/ifconfig eth0 hw ether 00:00:00:02:00:bb
/sbin/ifconfig eth0 10.0.0.2 netmask 255.255.255.0 up
echo ”0” > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

chown root:root /root
chmod 700 /root/.ssh
chmod 755 /root
chmod 644 /root/.ssh/*
chmod 600 /root/.ssh/id_rsa
route del default gw 172.16.0.1
/etc/init.d/ssh start
```

Listing 3: Virtual Machine PC2.startup

We can do many things on this network of two virtual machines. To start the network, first enter privileged mode by using *sudo -s*, then type *lstart* under the project directory.

1. Test connectivity from PC1 to PC2
   - type *ping* 10.0.0.2(IP address of PC2)
   - interrupt the connection by *Ctrl-C*
2. Connect to virtual PCs from the Ubuntu environment
   - in the PC1 window, type *passwd* to set a password for the root account
   - in a new terminal, type *sudo ssh* 172.16.0.1 to connect to PC1 (the password defined necessary)
3. Capture network traffic to or from a machine
   - keep ”ping” running
   - in the terminal with ”ssh” session, type *tcpdump -i eth0 -w /hostlab/TP1-PC1-eth0.pcap*
   - interrupt it by *Ctrl-C*
4. Share files between virtual PCs and the Ubuntu environment
   - run ”Wireshark” and open TP1-PC1-eth0.pcap
   - at the end of test, stop ”ssh” session, stop gracefully the whole network and clear all the temporary files.

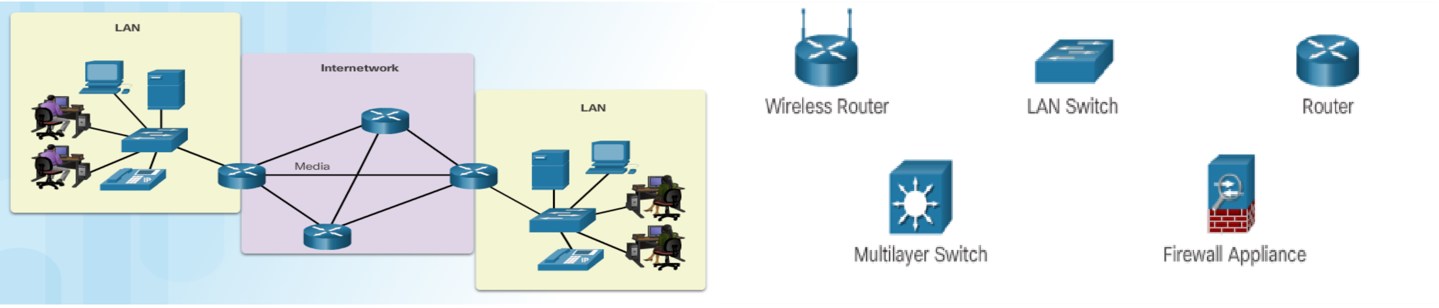
1 Explore the Network

1.1 LANs,WANs and the Internet

1.1.1 Network Components

The network infrastructure contains three categories of network components:

- **Devices**
  - **End devices**
    either the source or destination of a message transmitted over the network, identified by an address, such as laptop, PC, file/web/email server or client, etc.
  - **Intermediary network devices**
    connect the individual end devices to the network and connect multiple individual networks to form an internetwork, such as router or wireless router, LAN switch, multilayer switch, firewall appliance, etc.



(a) End devices

(b) Intermediary devices

Figure 1: Devices

- **Media**
  - **Metallic wires within cables** data is encoded into electrical impulses
  - **Fiber optic cable** data is encoded as pulses of light
  - **Wireless transmission** data is encoded using wavelengths from the electromagnetic spectrum

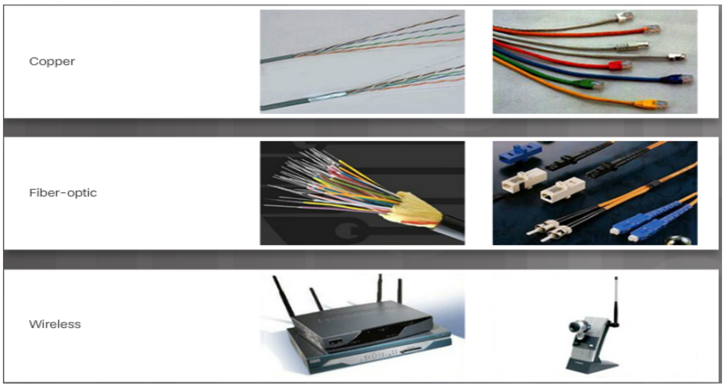


Figure 2: Media

- **Services**
  include many of the common network applications people use every day.

1.1.2 Network Representations

A **topology diagram** is used to visualize the organization and operation of a network.
Specialized terminology is used when discussing how each of these devices and media connect to each other.

- **Network Interface Card or LAN adapter (NIC)**
  provides the physical connection to the network at an end device.
- **Physical port**
  a connector or outlet on a networking device where the media is connected to an end device or another networking device.
- **Interface**
  specialized port on a networking device that connect to individual networks.

Figure 3: NIC

Note: Often, the terms "port" and "interface" are used interchangeably. The port on a router are referred to as "network interface".
There are two types of topology diagrams:

- **physical topology diagram**
  identify the physical location of intermediary devices and cable installation.
- **logical topology diagram**
  identify devices, ports, and addressing scheme.

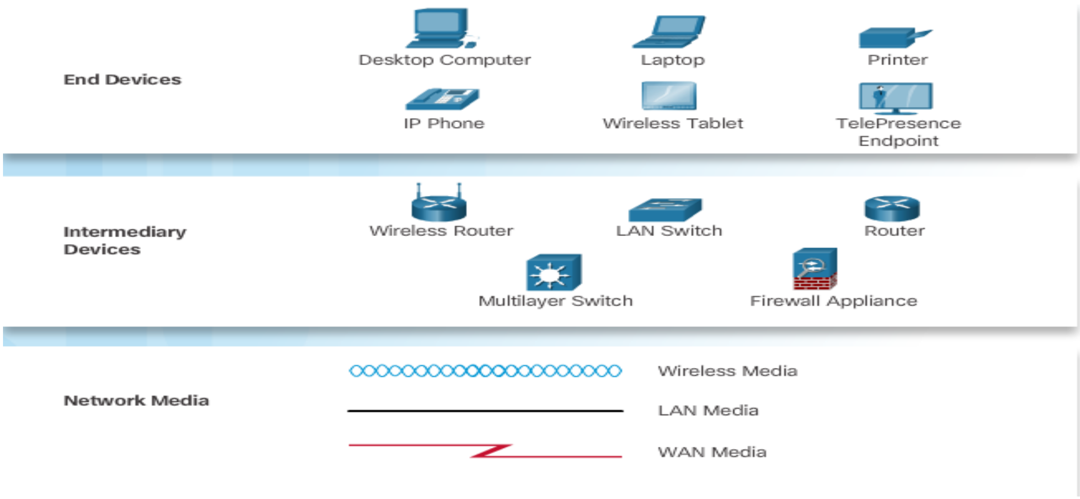
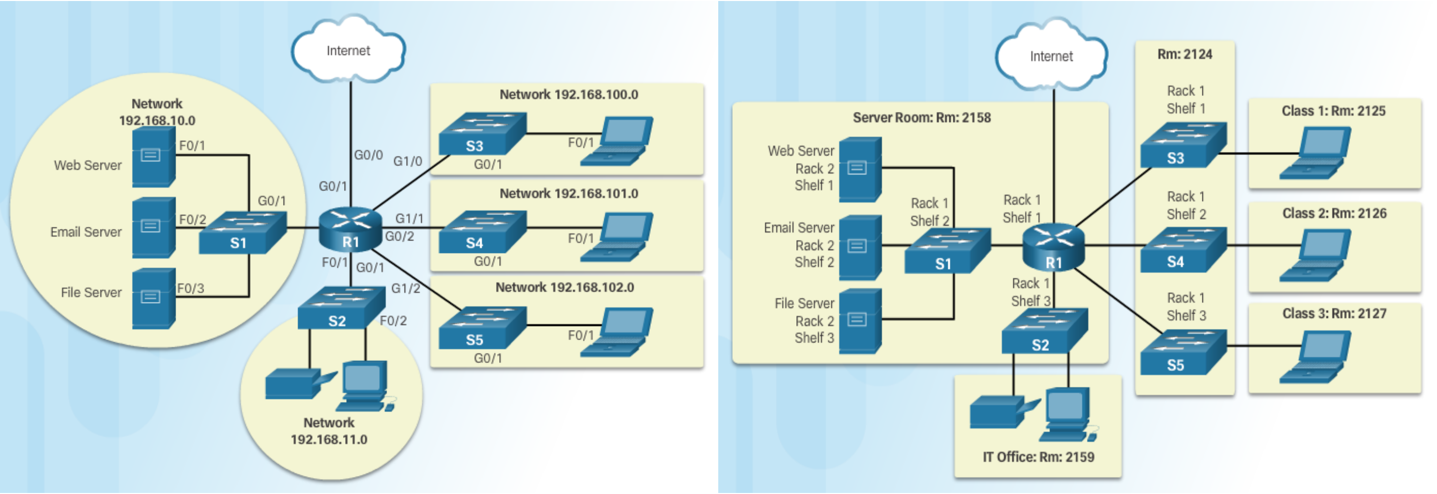


Figure 4: Network Representation symbols



(a) Logical topology diagram

(b) Physical topology diagram

Figure 5: Topology Diagram

1.1.3 LANs and WANs

Typical network infrastructures include:

- **Local Area Network (LAN)** typically an enterprise, home, or small business network owned and managed by an individual or IT department.
- **Wide Area Network (WAN)** provides access to other networks over a wide geographical area, owned and managed by a telecommunication service provider, including Internet Service Provider (ISP).
- **Metropolitan Area Network (MAN)** larger than a LAN but smaller than a WAN (e.g., a city).
- **Wireless LAN (WLAN)** LAN wirelessly interconnecting end points.
- **Storage Area Network (SAN)** support file servers and provide data storage, retrieval and replication.

LANs provide high speed bandwidth to internal end devices and intermediary devices while WANs typically provide slower speed links between LANs.

1.1.4 The Internet, Intranets, and Extranets

The **Internet** is a worldwide collection of interconnected networks. There are organizations helping to maintain structure and standardization of Internet protocols and processes, including the Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Architecture Board (IAB), etc.
Note: The term "**internet**" describes multiple networks interconnected.

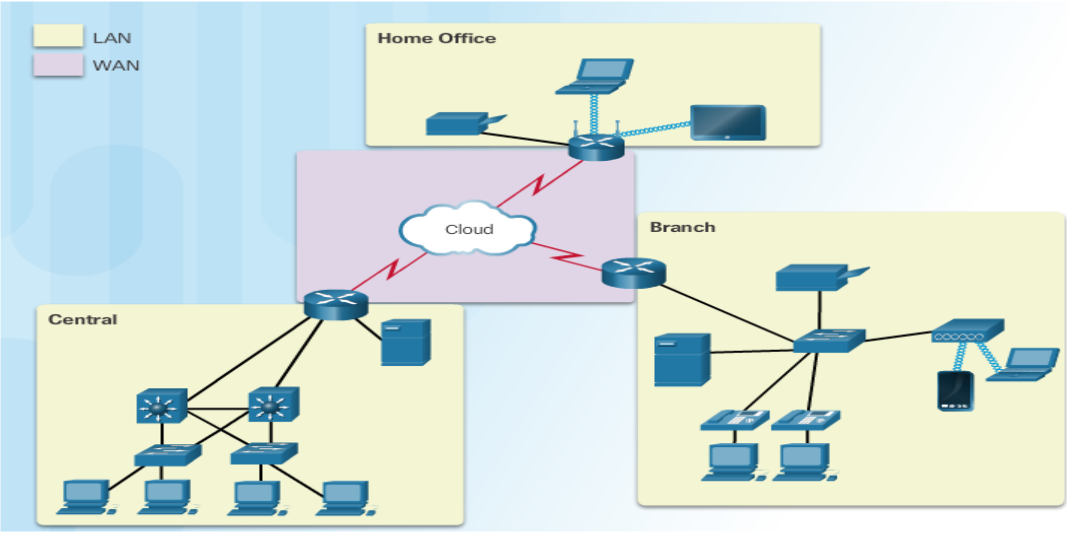
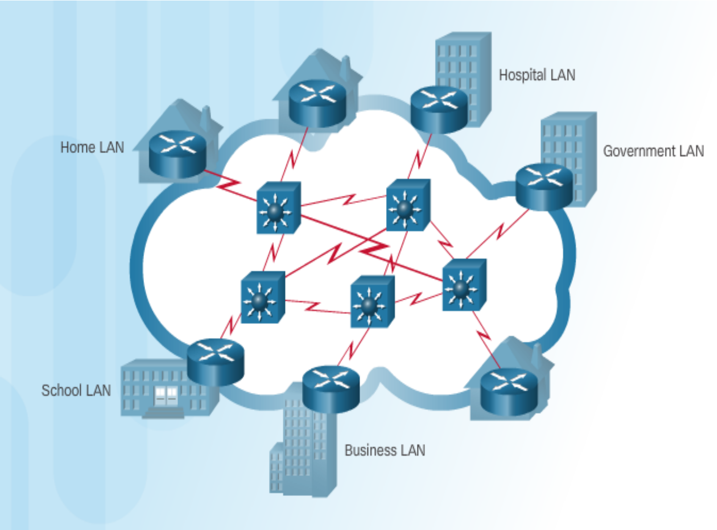


Figure 6: LANs and WANs

Intranet refers to a private connection of LANs and WANs that belongs to an organization, and is accessible only by the organization's members, employees, or others with authorization.
However, 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.



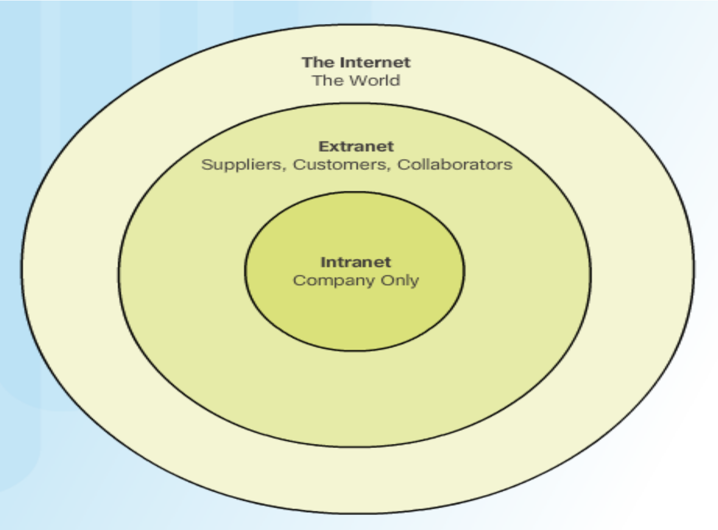


Figure 7: Internet: collection of interconnected networks

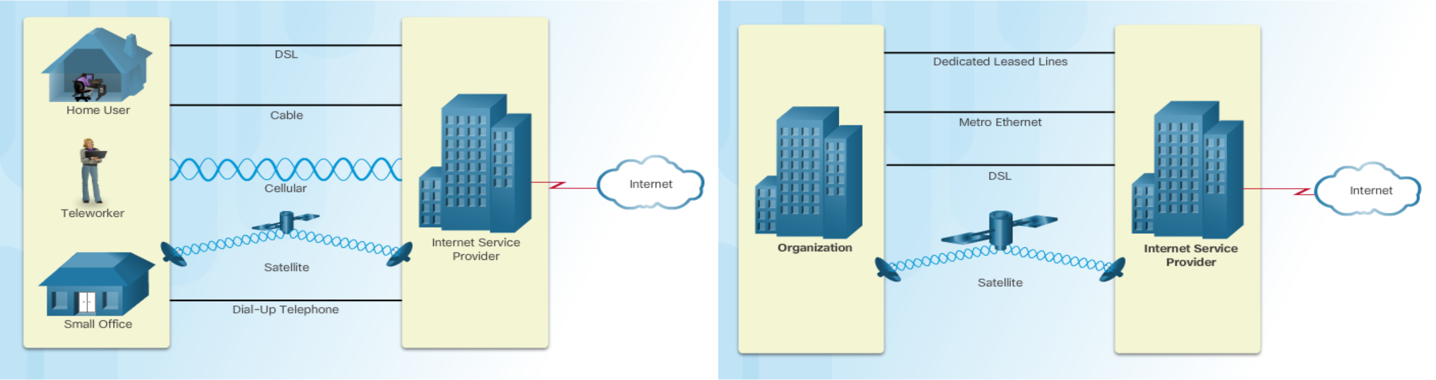
Figure 8: Internet Intranet and Extranet

1.1.5 Internet Connections

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

- Home and Small Office Internet Connections
  - **Cable** typically offered by cable television service providers or connected directly with fiber optic cables, providing a high bandwidth.
  - **Digital Subscriber Line (DSL)** runs over a telephone line. Popular choice is Asymmetrical Digital Subscriber Line (ADSL), where the download speed is faster than the upload speed.
  - **Cellular** uses a cell phone network to connect.
  - **Satellite** requires a clear line of sight to the satellite.
  - **Dial-up Telephone** an inexpensive option using any phone line and a modem, with a low bandwidth.
- Businesses Internet Connections

- **Dedicated Leased Line** reserved circuits within the service provider's network, geographically separated offices for private voice/data networking, expensive rented at a monthly or yearly rate.
- **Ethernet WAN** expend Ethernet technology into the WAN.
- **DSL** popular choice is Symmetric Digital Subscriber Line (SDSL), with equal upload and download speeds.
- **Satellite** when a wired solution is not available.



(a) Home and Small Office

(b) Businesses

Figure 9: Internet Connection Technology

1.2 Network Environments

Today, separate networks are converging. Converged networks delivers data, voice, and video between different types of devices over the same network infrastructure, using the same set of rules, agreements, and implementation standards.

1.2.1 Reliable Network

There are four basic characteristics that the network architecture[5] needs to address in order to meet user expectations:

- **Fault tolerant**
  keyword: redundancy, packet-switched network
- **Scalability**
  keyword: standards, protocols
- **Quality of Service (QoS)**
  keyword: congestion, network bandwidth, priority queue policy
- **Security**
  - network infrastructure security[6]
  - information security[7]

  keyword: confidentiality, integrity, availability

Fault tolerant limits the impact of a failure and allows quick recovery when such a failure occurs. The solution is **redundancy** by implementing a **packet-switched network**. Redundant connections allow for alternative paths if a device or a link fails. A single message, is broken into multiple message blocks, called packets. Each packet has the necessary addressing information of the source and destination of the message. The routers within the network switch the packets. All the packets in a single message could take very different paths to the destination. This is quite different from circuit-switched network traditionally used for voice communications where a dedicated circuit is established between the source and destination before the users may communicate.

A scalable network can **expand quickly** to support new users and applications without impacting the performance of the service being delivered to existing users, because the designers follow accepted **standards and protocols**.

[5] technologies that support the infrastructure and the programmed services, rules or protocols.

[6] the physical securing of devices, and preventing unauthorized access to the management software that resides on them.

[7] protecting the information within the packets and the information stored on network attached devices.

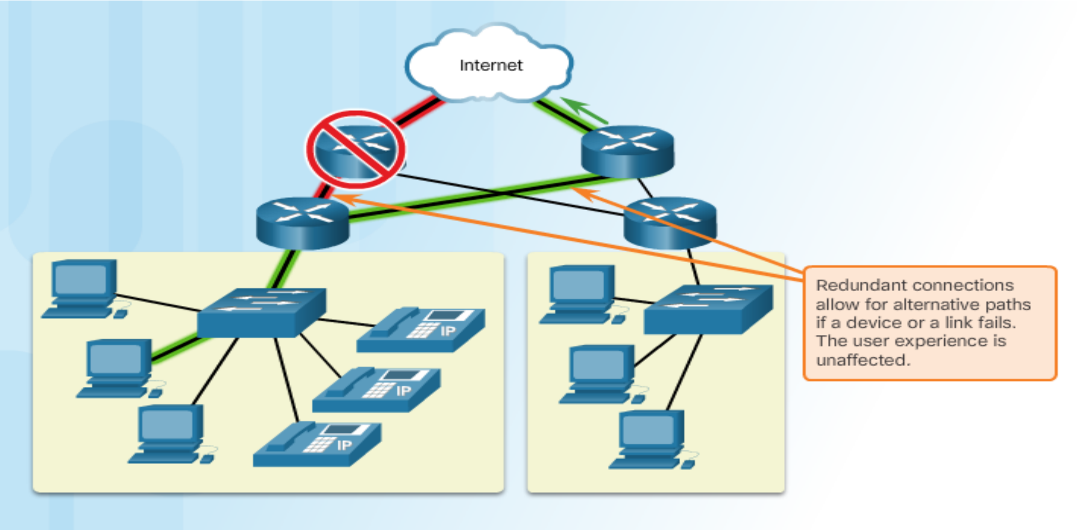

Internet
IP
IP
IP
Redundant connections allow for alternative paths if a device or a link fails. The user experience is unaffected.

Figure 10: Reliable Network: Fault tolerant

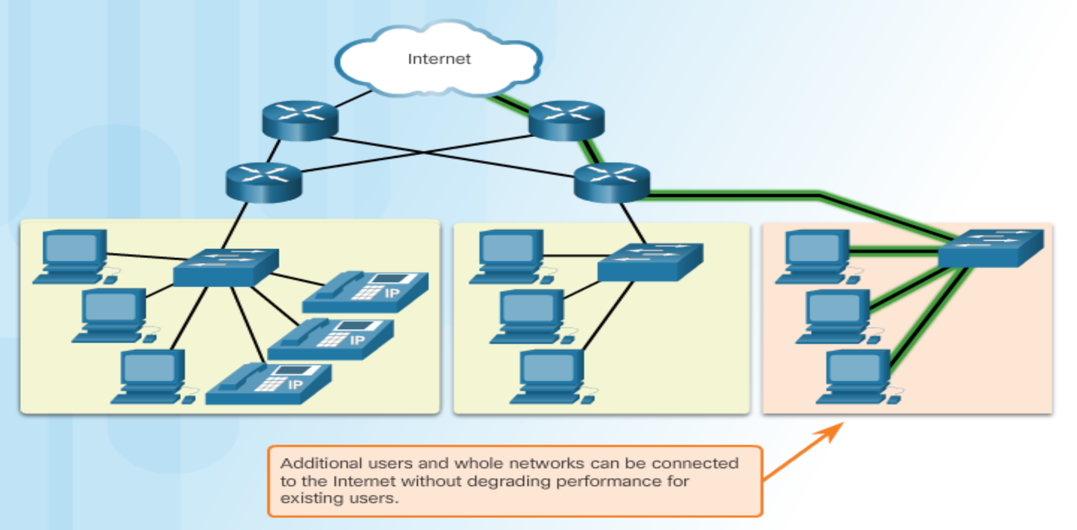

Internet
IP
IP
IP
Additional users and whole networks can be connected to the Internet without degrading performance for existing users.

Figure 11: Reliable Network: Scalability

QoS is a primary mechanism for managing congestion and ensuring reliable delivery of content to all users. **Congestion** occurs when the demand for bandwidth exceeds the amount available. **Network bandwidth** is measured in *bits per second*(bps), the number of bits that can be transmitted in a single second. **Priority queue policy** is implemented by routers if the network experiences congestion.

As for network security, there are three primary requirements. Firstly, **confidentiality**, only the intended and authorized recipients can access and read data. Secondly, **integrity**, the information has not been altered in transmission. Thirdly, **availability**, timely and reliable access to data services for authorized users.

1.2.2 Network Trends

fdasf

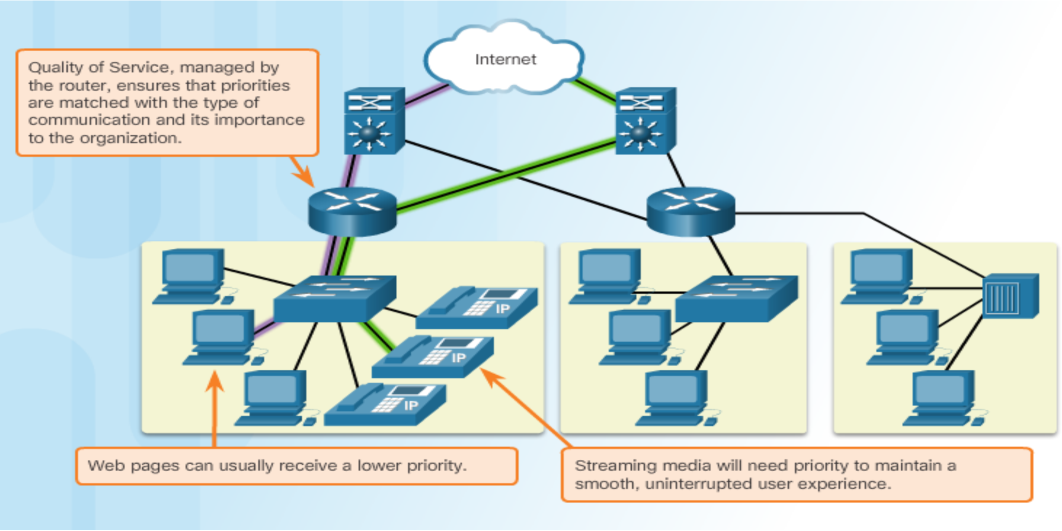

Quality of Service, managed by the router, ensures that priorities are matched with the type of communication and its importance to the organization.
Internet
IP
Web pages can usually receive a lower priority.
Streaming media will need priority to maintain a smooth, uninterrupted user experience.

Figure 12: Reliable Network: Quality of Service (QoS)

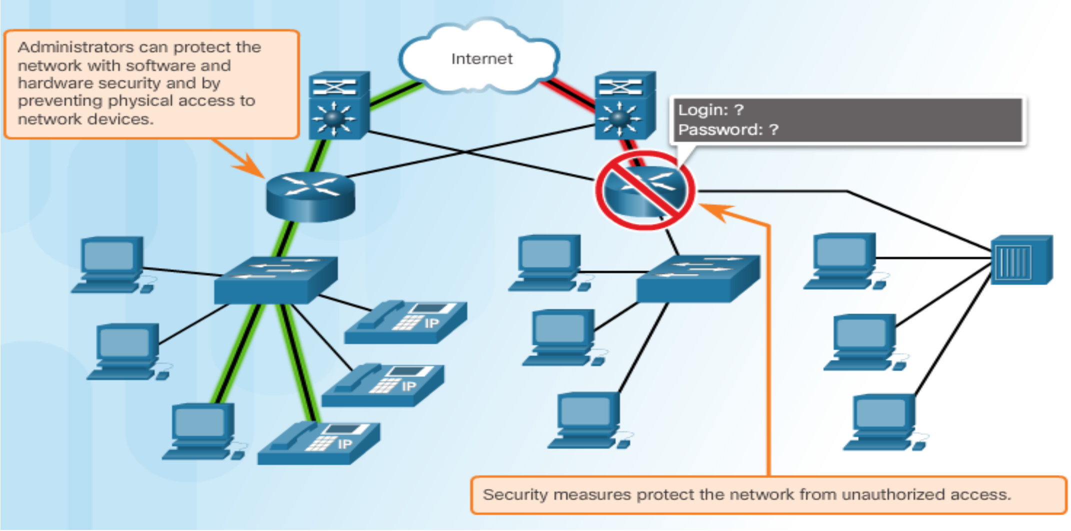

Administrators can protect the network with software and hardware security and by preventing physical access to network devices.
Internet
Login: ?
Password: ?
IP
Security measures protect the network from unauthorized access.

Figure 13: Reliable Network: Security

2 Configure a Network Operating System

3 Network Protocols and Communications

4 Network Access

5 Ethernet

6 Network Layer

7 IP Addressing

8 Subnetting IP Networks

9 Transport Layer

10 Application Layer

11 Build a Small Network

Acronyms

ADSL Asymmetrical Digital Subscriber Line. 6

DSL Digital Subscriber Line. 6

ISP Internet Service Provider. 5

LAN Local Area Network. 5

MAN Metropolitan Area Network. 5

NIC Network Interface Card or LAN adapter. 4

QoS Quality of Service. 7, 8, 12

SAN Storage Area Network. 5

SDSL Symmetric Digital Subscriber Line. 7

UML User Mode Linux. 2

WAN Wide Area Network. 5

WLAN Wireless LAN. 5

Terms

availability timely and reliable access to data services for authorized users. 8

confidentiality only the intended and authorized recipients can access and read data. 8

congestion the demand for bandwidth of simultaneous communications exceeds the amount available. 7

integrity the information has not been altered in transmission. 8

interface specialized port on a networking device that connect to individual networks. 4

logical topology diagram identify devices, ports, and addressing scheme. 4

network bandwidth the number of bits that can be transmitted in a single second, measured in bps. 7

network interface the port on a router. 4

packet-switched network packet switching splits traffic into packets that are routed over a shared network. 7

physical topology diagram identify the physical location of intermediary devices and cable installation. 4

physical port a connector or outlet on a networking device where the media is connected to an end device or another networking device. 4

redundancy having multiple paths to a destination. 7

Commands

lclean delete all the temporary files. 2

lcrash stop brutally or power off the whole network. 2

lhalt stop gracefully the whole network. 2

lstart start the whole network. 2

passwd set a password for the root account. 3

ping ping [IP destination], test the accessibility through an IP network. 3

sudo ssh sudo ssh [IP destination], connect to a machine in the IP network. 3

sudo -s enter privileged mode. 3

visit list all the machines running. 2

List of Figures