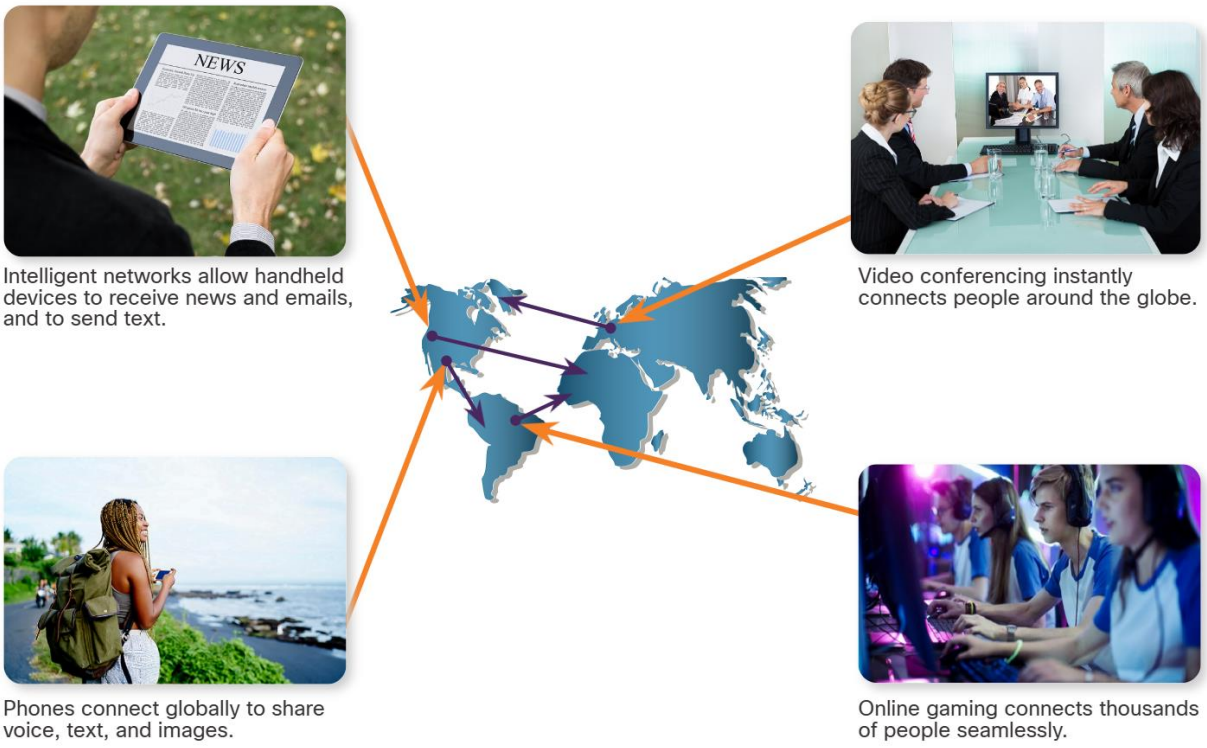
NETWORKING BASICS

Who Owns "The Internet"?

The internet is not owned by any individual or group. It is a worldwide collection of interconnected networks—often referred to as an internetwork or simply the internet—that cooperate to exchange information using common standards. This global network uses telephone wires, fiber-optic cables, wireless transmissions, and satellite links to allow users to share information in various forms, as illustrated in the figure.

Everything you access online is hosted somewhere on the global internet. Whether it's social media sites, multiplayer games, email services, or online courses, these destinations are part of local networks that communicate through the internet.

Consider all the interactions you have in a day that depend on being online.



Local networks

Local networks come in all sizes. They can range from simple networks consisting of two computers, to networks connecting hundreds of thousands of devices. Networks installed in small offices, or homes and home offices, are referred to as small office/home office (SOHO) networks. SOHO networks let you share resources such as printers, documents, pictures, and music, between a few local users.

In business, large networks can be used to advertise and sell products, order supplies, and communicate with customers. Communication over a network is usually more efficient and less expensive than traditional forms of communication, such as regular mail or long distance phone calls. Networks allow for rapid communication such as email and instant messaging, and provide consolidation and access to information stored on network servers.

Business and SOHO networks usually provide a shared connection to the internet. The internet is considered a "network of networks" because it is literally made up of thousands of local networks that are connected to each other.

- **Small Home Networks:** Small home networks connect a few computers to each other and to the internet.
- **Small Office and Home Office Networks:** The SOHO network allows computers in a home office or a remote office to connect to a corporate network, or access centralized, shared resources.
- **Medium to Large Networks:** Medium to large networks, such as those used by corporations and schools, can have many locations with hundreds or thousands of interconnected hosts.
- **World Wide Networks:** The internet is a network of networks that connects hundreds of millions of computers world-wide.

Mobile Devices

The internet connects more computing devices than just desktop and laptop computers. There are devices all around that you may interact with on a daily basis that are also connected to the internet. These include mobile devices, home devices, and a variety of other connected devices.

- **Smartphone:** Smartphones are able to connect to the internet from almost anywhere. Smartphones combine the functions of many different products together, such as a telephone, camera, GPS receiver, media player, and touch screen computer.
- **Tablet:** Tablets, like smartphones, also have the functionality of multiple devices. With the additional screen size, they are ideal for watching videos and reading magazines or books. With on-screen keyboards, users are able to do many of the things they used to do on their laptop computer, such as composing emails or browsing the web.

- **Smartwatch:** A smartwatch can connect to a smartphone to provide the user with alerts and messages. Additional functions, such as heart rate monitoring and counting steps, like a pedometer, can help people who are wearing the device to track their health.
- **Smart Glasses:** A wearable computer in the form of glasses, such as Google Glass, contains a tiny screen that displays information to the wearer in a similar fashion to the Head-Up Display (HUD) of a fighter pilot. A small touch pad on the side allows the user to navigate menus while still being able to see through the smart glasses.

Connected Home Devices

Many of the things in your home can also be connected to the internet so that they can be monitored and configured remotely.

- **Security System:** Many of the items in a home, such as security systems, lighting, and climate controls, can be monitored and configured remotely using a mobile device.
- **Appliances:** Household appliances such as refrigerators, ovens, and dishwashers can be connected to the internet. This allows the homeowner to power them on or off, monitor the status of the appliance, and also be alerted to preset conditions, such as when the temperature in the refrigerator rises above an acceptable level.
- **Smart TV:** A smart TV can be connected to the internet to access content without the need for TV service provider equipment. Also, a smart TV can allow a user to browse the web, compose email, or display video, audio, or photos stored on a computer.
- **Gaming Console:** Gaming consoles can connect to the internet to download games and play with friends online.

Other Connected Devices

There are also many connected devices found in the world outside your home that provide convenience and useful, or even vital, information.

- **Smart Cars:** Many modern cars can connect to the internet to access maps, audio and video content, or information about a destination. They can even send a text message or email if there is an attempted theft or call for assistance in case of an accident. These cars can also connect to smartphones and tablets to display information about the different engine systems, provide maintenance alerts, or display the status of the security system.
- **RFID Tags:** Radio frequency identification (RFIDs) tags can be placed in or on objects to track them or monitor sensors for many conditions.
- **Sensors and Actuators:** Connected sensors can provide temperature, humidity, wind speed, barometric pressure, and soil moisture data. Actuators can then be automatically triggered based on current conditions. For example, a smart sensor can periodically send soil moisture data to a monitoring station. The monitoring station can then send a signal

to an actuator to begin watering. The sensor will continue to send soil moisture data allowing the monitoring station to determine when to deactivate the actuator.

- **Medical Devices:** Medical devices such as pacemakers, insulin pumps, and hospital monitors provide users or medical professionals with direct feedback or alerts when vital signs are at specific levels.

Data transmission

The following categories are used to classify types of personal data:

- **Volunteered data -** This is created and explicitly shared by individuals, such as social network profiles. This type of data might include video files, pictures, text, or audio files.
- **Observed data -** This is captured by recording the actions of individuals, such as location data when using cell phones.
- **Inferred data -** This is data such as a credit score, which is based on analysis of volunteered or observed data.

The term bit is an abbreviation of "binary digit" and represents the smallest piece of data. Each bit can only have one of two possible values, 0 or 1.

There are three common methods of signal transmission used in networks:

- **Electrical signals -** Transmission is achieved by representing data as electrical pulses on copper wire.
- **Optical signals -** Transmission is achieved by converting the electrical signals into light pulses.
- **Wireless signals -** Transmission is achieved by using infrared, microwave, or radio waves through the air.

Bandwidth

Bandwidth is the capacity of a medium to carry data. Digital bandwidth measures the amount of data that can flow from one place to another in a given amount of time. Bandwidth is typically measured in the number of bits that (theoretically) can be sent across the media in a second. Common bandwidth measurements are as follows:

- Thousands of bits per second (Kbps)
- Millions of bits per second (Mbps)
- Billions of bits per second (Gbps)

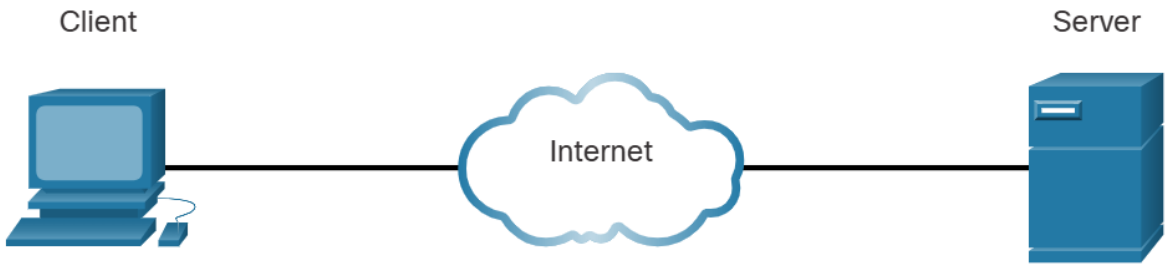
Throughput does not usually match the specified bandwidth. Many factors influence throughput including:

- The amount of data being sent and received over the connection
- The latency created by the number of network devices encountered between source and destination

Latency refers to the amount of time, including delays, for data to travel from one given point to another.

Client and Server Roles

All computers connected to a network that participate directly in network communication are classified as hosts. Hosts can send and receive messages on the network. In modern networks, computer hosts can act as a client, a server, or both, as shown in the figure. The software installed on the computer determines which role the computer plays.



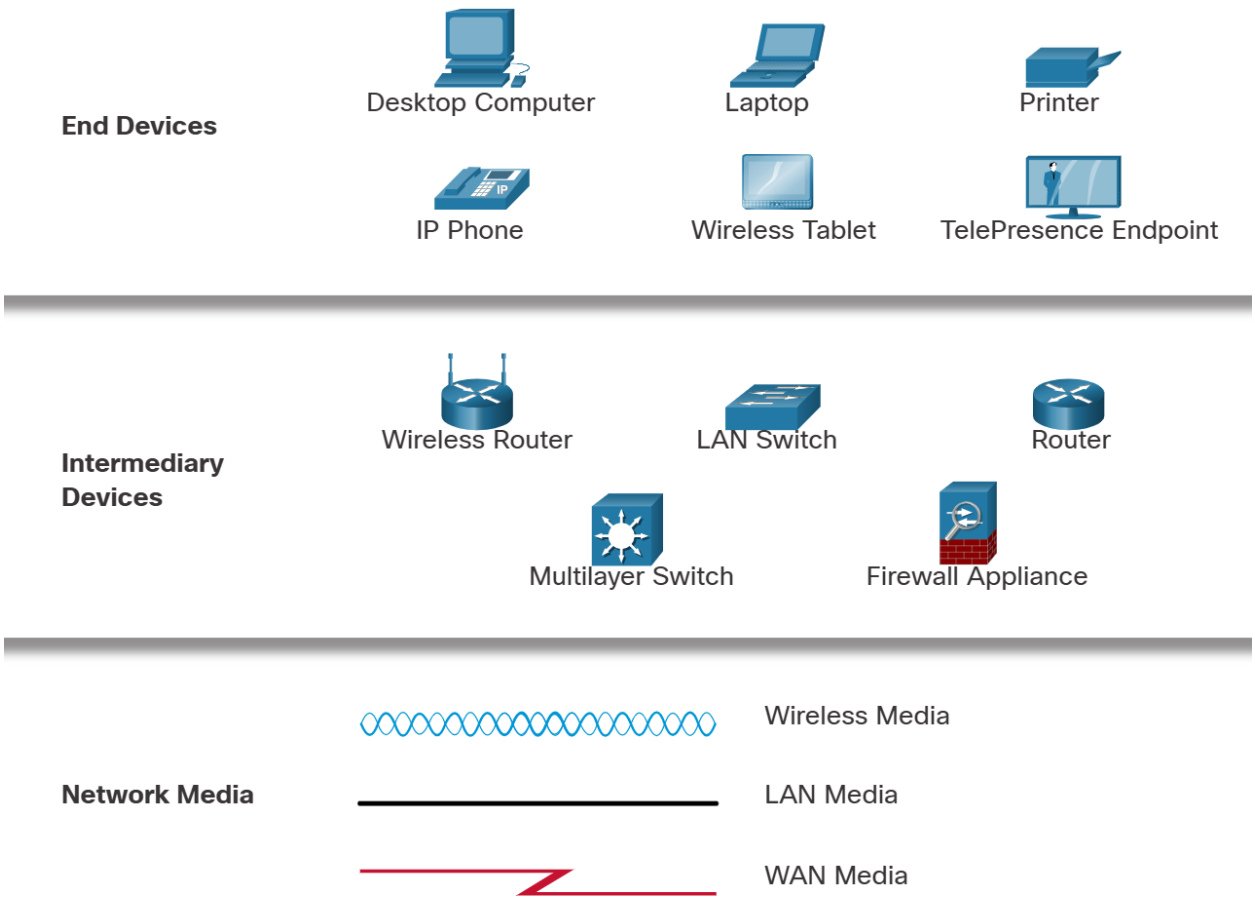
A **client** is a device or program that requests services or resources from another device, usually a **server**. For example, your laptop or smartphone acts as a client when it asks a web server for a website. A **server** is a device or program that provides services or resources to clients by responding to their requests. This client-server relationship is fundamental to how the internet and networks operate, where clients initiate communication to use services, and servers respond by delivering them.

Network Infrastructure

The path that a message takes from its source to destination can be as simple as a single cable connecting one computer to another, or as complex as a network that literally spans the globe. This network infrastructure is the platform that supports the network. It provides the stable and reliable channel over which our communications can occur.

The network infrastructure contains three categories of hardware components, as shown in the figure:

- End devices
- Intermediate devices
- Network media



Devices and media are the physical elements, or hardware, of the network. Hardware is often the visible components of the network platform such as a laptop, PC, switch, router, wireless access point, or the cabling used to connect the devices. Occasionally, some components may not be so visible. In the case of wireless media, messages are transmitted through the air using invisible radio frequencies or infrared waves.

Make a list of the network infrastructure components installed in your home network. Include the cables or wireless access points that provide your network connections.

End Devices

The network devices that people are most familiar with are called end devices, or hosts. These devices form the interface between users and the underlying communication network.

Some examples of end devices are as follows:

- Computers (workstations, laptops, file servers, web servers)
- Network printers
- Telephones and teleconferencing equipment

- Security cameras
- Mobile devices (such as smart phones, tablets, PDAs, and wireless debit/credit card readers and barcode scanners)

An end device (or host) is either the source or destination of a message transmitted over the network, as shown in the animation. In order to uniquely identify hosts, addresses are used. When a host initiates communication, it uses the address of the destination host to specify where the message should be sent.

Internet Service Provider (ISP)

An Internet Service Provider (ISP) provides the link between the home network and the internet. An ISP can be the local cable provider, a landline telephone service provider, the cellular network that provides your smartphone service, or an independent provider who leases bandwidth on the physical network infrastructure of another company.

Many ISPs also offer additional services to their contract subscribers, as shown in the figure. These services can include email accounts, network storage, and website hosting and automated backup or security services.

ISPs are critical to communications across the global internet. Each ISP connects to other ISPs to form a network of links that interconnect users all over the world. ISPs are connected in a hierarchical manner that ensures that internet traffic generally takes the shortest path from the source to the destination.

The internet backbone is like an information super highway that provides high-speed data links to connect the various service provider networks in major metropolitan areas around the world. The primary medium that connects the internet backbone is fiber-optic cable. This cable is typically installed underground to connect cities within continents. Fiber-optic cables also run under the sea to connect continents, countries, and cities.

Wireless Networks

- GPS **Global Positioning System:** The GPS uses satellites to transmit signals that cover the globe. The smartphone can receive these signals and calculate the phone's location to an accuracy of within 10 meters.
- **Wi-Fi:** Wi-Fi transmitters and receivers located within the smartphone enable the phone to connect to local networks and the internet. In order to receive and send data on a Wi-Fi network, the phone needs to be within the range of the signal from a wireless network access point. Wi-Fi networks are usually privately owned but often provide guest or public access hotspots. A hotspot is an area where Wi-Fi signals are available. Wi-Fi network connections on the phone are similar to the network connections on a laptop computer.
- **Bluetooth:** Bluetooth is a low-power, shorter range wireless technology that is intended to replace wired connectivity for accessories such as speakers, headphones, and microphones. Bluetooth can also be used to connect a smartwatch to a smartphone. Because Bluetooth technology can be used to transmit both data and voice, it can be used to create small local networks. Bluetooth is wireless technology that allows devices to communicate over short distances. Multiple devices can be connected at the same time with Bluetooth.
- **Near Field Communication (NFC):** Near Field Communication (NFC) is a wireless communication technology that enables data to be exchanged by devices that are in very close proximity to each other, usually less than a few centimeters. For example, NFC can be used to connect a Smartphone and a payment system. NFC uses electromagnetic fields to transmit data.

Mobile Devices and Wi-Fi

Mobile devices give us the freedom to work, learn, play, and communicate wherever we want. People using mobile devices do not need to be tied to a physical location to send and receive voice, video, and data communications. In addition, wireless facilities, such as internet cafes, are available in many countries. College campuses use wireless networks to allow students to sign up for classes, watch lectures, and submit assignments in areas where physical connections to the network are unavailable. With mobile devices becoming more powerful, many tasks that needed to be performed on large computers connected to physical networks can now be completed using mobile devices on wireless networks.

Almost all mobile devices are capable of connecting to Wi-Fi networks. It is advisable to connect to Wi-Fi networks when possible because data used over Wi-Fi does not count against the cellular data plan. Also, because Wi-Fi radios use less power than cellular radios, connecting to Wi-Fi networks conserves battery power. Like other Wi-Fi-enabled devices, it is important to use

security when connecting to Wi-Fi networks. These precautions should be taken to protect Wi-Fi communications on mobile devices:

- Never send login or password information using unencrypted text (plaintext).
- Use a VPN connection when possible if you are sending sensitive data.
- Enable security on home networks.
- Use WPA2 or higher encryption for security.

Network Mode

The 802.11 protocol can provide increased throughput based on the wireless network environment. If all wireless devices connect with the same 802.11 standard, maximum speeds can be obtained for that standard. If the access point is configured to accept only one 802.11 standard, devices that do not use that standard cannot connect to the access point.

A mixed mode wireless network environment can include devices that use any of the existing Wi-Fi standards. This environment provides easy access for older devices that need a wireless connection but do not support the latest standards.

When building a wireless network, it is important that the wireless components connect to the appropriate WLAN. This is done using the SSID.

The SSID is a case-sensitive, alphanumeric string that contains up to 32 characters. It is sent in the header of all frames transmitted over the WLAN. The SSID is used to tell wireless devices, called wireless stations (STAs), which WLAN they belong to and with which other devices they can communicate.

We use the SSID to identify a specific wireless network. It is essentially the name of the network. Wireless routers usually broadcast their configured SSIDs by default. The SSID broadcast allows other devices and wireless clients to automatically discover the name of the wireless network. When the SSID broadcast is disabled, you must manually enter the SSID on wireless devices.

Disabling SSID broadcasting can make it more difficult for legitimate clients to find the wireless network. However, simply turning off the SSID broadcast is not sufficient to prevent unauthorized clients from connecting to the wireless network. All wireless networks should use the strongest available encryption to restrict unauthorized access.

Network design

Network Architecture

Have you ever been busy working online, only to have “the internet go down”? As you know by now, the internet did not go down; you just lost your connection to it. It is very frustrating. With so many people in the world relying on network access to work and learn, it is imperative that

networks are reliable. In this context, reliability means more than your connection to the internet. This topic focuses on the four aspects of network reliability.

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. For networks to function efficiently and grow in this type of environment, the network must be built upon standard network architecture.

Networks also support a wide range of applications and services. They must operate over many different types of cables and devices, which make up the physical infrastructure. The term network architecture, in this context, refers to the technologies that support the infrastructure and the programmed services and rules, or protocols, that move data across the network.

As networks evolve, we have learned that there are four basic characteristics that network architects must address to meet user expectations:

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

Fault Tolerance

Fault Tolerance is the ability of a network to **continue operating properly even when one or more of its components fail**.

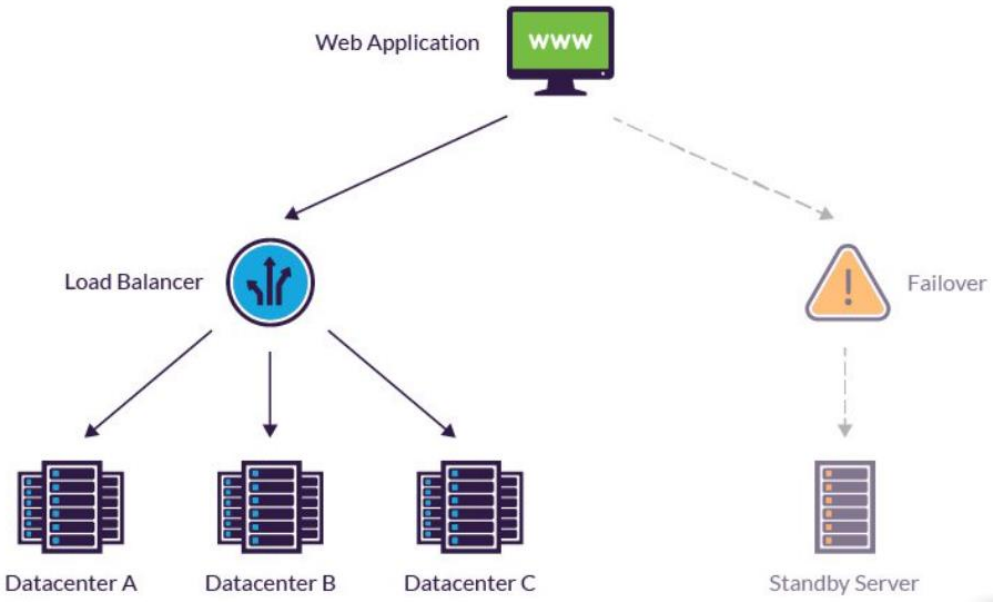
Key Points:

- It ensures that there is **no single point of failure** in the network.
- Fault-tolerant networks use **redundancy** — for example, backup links, devices, or power sources — to keep services running.
- If a component like a switch, router, or cable fails, the network **automatically reroutes traffic** through another path.

Example:

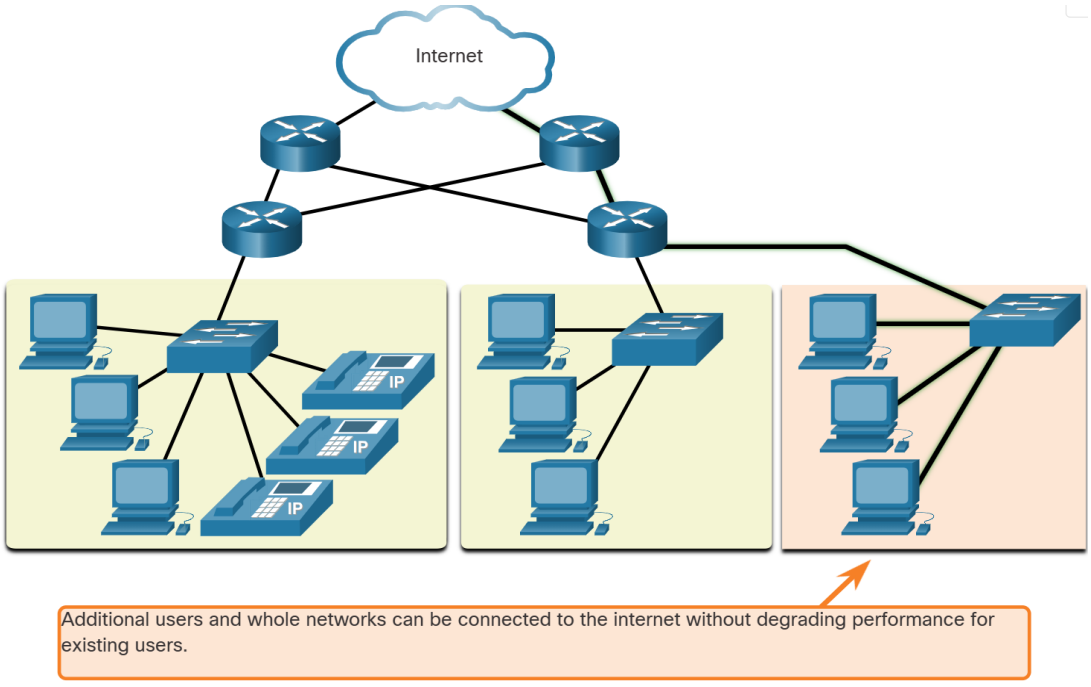
If your home internet router fails but you have a mobile hotspot as backup, your devices can still access the internet — that's a simple form of fault tolerance.

In large networks (like those of banks, hospitals, or cloud services), fault tolerance is critical to prevent downtime and ensure reliability.



Scalability

A scalable network expands quickly to support new users and applications. It does this without degrading the performance of services that are being accessed by existing users. The figure shows how a new network is easily added to an existing network. These networks are scalable because the designers follow accepted standards and protocols. This lets software and hardware vendors focus on improving products and services without having to design a new set of rules for operating within the network.

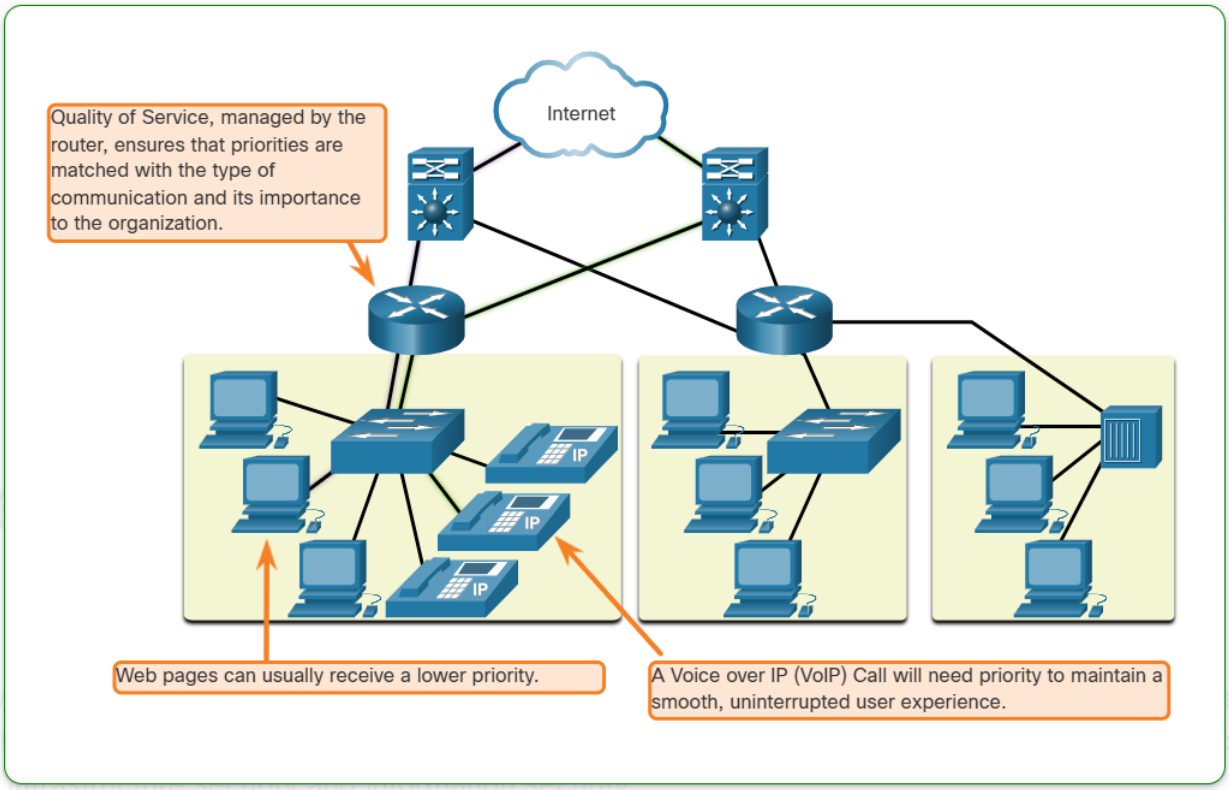


Quality of Service (QoS)

Quality of Service (QoS) is an increasing requirement of networks today. New applications available to users over networks, such as voice and live video transmissions, create higher expectations for the quality of the delivered services. Have you ever tried to watch a video with constant breaks and pauses? 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.

Congestion occurs when the demand for bandwidth exceeds the amount available. Network bandwidth is measured in the number of bits that can be transmitted in a single second, or bits per second (bps). When simultaneous communications are attempted across the network, the demand for network bandwidth can exceed its availability, creating network congestion.

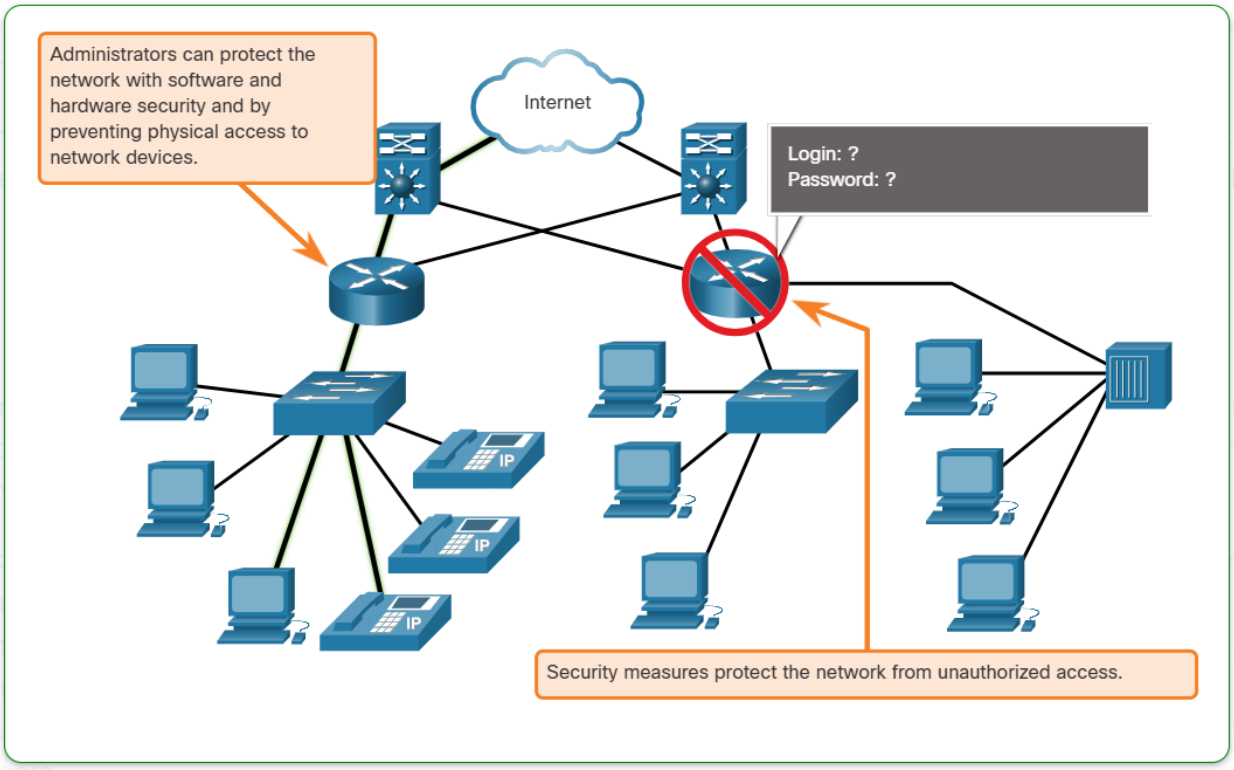
When the volume of traffic is greater than what can be transported across the network, devices will hold the packets in memory until resources become available to transmit them. In the figure, one user is requesting a web page, and another is on a phone call. With a QoS policy in place, the router can manage the flow of data and voice traffic, giving priority to voice communications if the network experiences congestion. The focus of QoS is to prioritize time-sensitive traffic. The type of traffic, not the content of the traffic, is what is important.



Network Security

The network infrastructure, services, and the data contained on network-attached devices are crucial personal and business assets. Network administrators must address two types of network security concerns: network infrastructure security and information security.

Securing the network infrastructure includes physically securing devices that provide network connectivity and preventing unauthorized access to the management software that resides on them, as shown in the figure.



Network administrators must also protect the information contained within the packets being transmitted over the network, and the information stored on network attached devices. In order to achieve the goals of network security, there are three primary requirements.

- **Confidentiality** - Data confidentiality means that only the intended and authorized recipients can access and read data.
- **Integrity** - Data integrity assures users that the information has not been altered in transmission, from origin to destination.
- **Availability** - Data availability assures users of timely and reliable access to data services for authorized users.

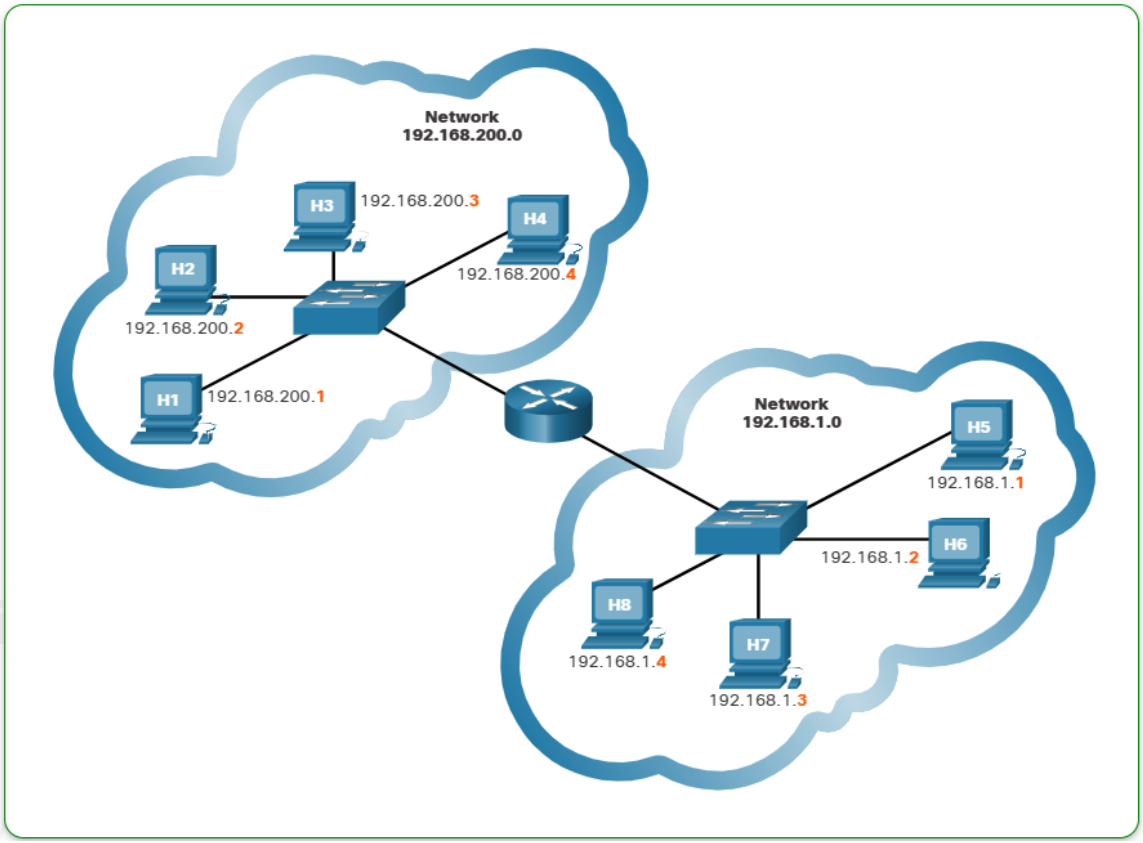
Hierarchical Network Design

A person's name usually does not change. A person's address on the other hand, relates to where the person lives and can change. On a host, the MAC address does not change; it is physically assigned to the host NIC and is known as the physical address. The physical address remains the same regardless of where the host is placed on the network.

The IP address is similar to the address of a person. It is known as a logical address because it is assigned logically based on where the host is located. The IP address, or network address, is assigned to each host by a network administrator based on the local network.

IP addresses contain two parts. One part identifies the network portion. The network portion of the IP address will be the same for all hosts connected to the same local network. The second part of the IP address identifies the individual host on that network. Within the same local network, the host portion of the IP address is unique to each host, as shown in the figure.

Both the physical MAC and logical IP addresses are required for a computer to communicate on a hierarchical network, just like both the name and address of a person are required to send a letter.



Cloud and virtualization

The terms “cloud computing” and “virtualization” are often used interchangeably; however, they mean different things. Virtualization is the foundation of cloud computing. Without it, cloud computing, as it is most-widely implemented, would not be possible.

Over a decade ago, VMware developed a virtualizing technology that enabled a host OS to support one or more client OSs. Most virtualization technologies are now based on this technology. The transformation of dedicated servers to virtualized servers has been embraced and is rapidly being implemented in data center and enterprise networks.

Virtualization means creating a virtual rather than physical version of something, such as a computer. An example would be running a "Linux computer" on your Windows PC, which you will do later in the lab.

To fully appreciate virtualization, it is first necessary to understand some of the history of server technology. Historically, enterprise servers consisted of a server OS, such as Windows Server or Linux Server, installed on specific hardware, as shown in the figure. All server RAM, processing power, and hard drive space were dedicated to the service provided (e.g., web, email services, etc.).

“The major problem with this configuration is that when a component fails, the service that is provided by this server becomes unavailable. This is known as a single point of failure. Another problem was that dedicated servers were underused. Dedicated servers often sat idle for long periods of time, waiting until there was a need to deliver the specific service they provide. These servers wasted energy and took up more space than was warranted by the amount of service provided. This is known as server sprawl.”

Three main service of cloud computing.

1. **SaaS (Software as a Service)**

    - **What it is:** Ready-to-use software delivered over the internet.
    - **Example:** Gmail, Microsoft 365, Zoom.
    - **User Role:** Just use the app — no need to install, manage, or update it.

2. **PaaS (Platform as a Service)**

    - **What it is:** A platform for developers to build, test, and deploy applications.
    - **Example:** Google App Engine, Heroku.
    - **User Role:** You manage your app and data, while the provider handles servers, OS, and runtime.

3. **IaaS (Infrastructure as a Service)**

    - **What it is:** Virtualized computing resources over the internet — like virtual machines, storage, and networking.
    - **Example:** Amazon EC2, Microsoft Azure VMs.
    - **User Role:** You manage everything from the OS up; provider manages the physical hardware.

*"In short: **SaaS** = Use it, **PaaS** = Build on it and **IaaS** = Control it"*

Types of Clouds

There are four primary cloud models:

- **Public clouds** - Cloud-based applications and services offered in a public cloud are made available to the general population. Services may be free or are offered on a pay-per-use model, such as paying for online storage. The public cloud uses the internet to provide services.
- **Private clouds** - Cloud-based applications and services offered in a private cloud are intended for a specific organization or entity, such as the government. A private cloud can be set up using the private network of an organization, though this can be expensive to build and maintain. A private cloud can also be managed by an outside organization with strict access security.
- **Hybrid clouds** - A hybrid cloud is made up of two or more clouds (example: part private, part public), where each part remains a separate object, but both are connected using a single architecture. Individuals on a hybrid cloud would be able to have degrees of access to various services based on user access rights.
- **Community clouds** - A community cloud is created for exclusive use by a specific community. The differences between public clouds and community clouds are the functional needs that have been customized for the community. For example, healthcare organizations must remain compliant with policies and laws (e.g., HIPAA) that require special authentication and confidentiality.

Advantages of Virtualization

One major advantage of virtualization is overall reduced cost:

- **Less equipment is required** - Virtualization enables server consolidation, which requires fewer physical devices and lowers maintenance costs.
- **Less energy is consumed** - Consolidating servers lowers the monthly power and cooling costs.
- **Less space is required** - Server consolidation reduces the amount of required floor space.

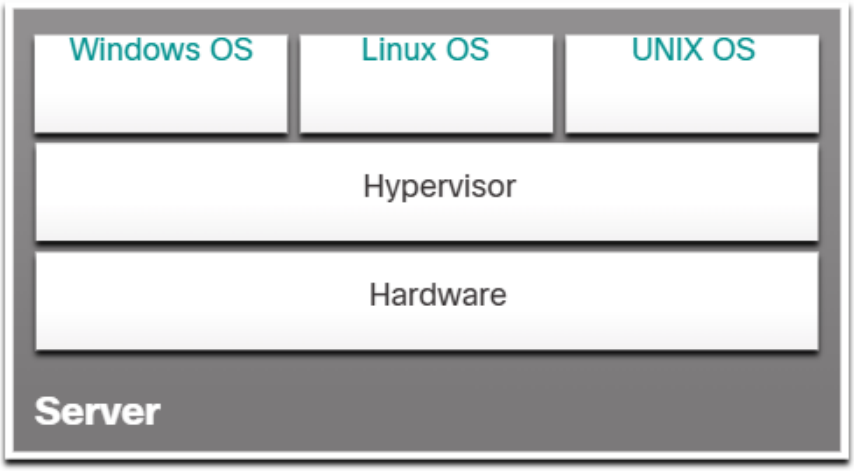
These are additional benefits of virtualization:

- **Easier prototyping** - Self-contained labs, operating on isolated networks, can be rapidly created for testing and prototyping network deployments.
- **Faster server provisioning** - Creating a virtual server is far faster than provisioning a physical server.
- **Increased server uptime** - Most server virtualization platforms now offer advanced redundant fault tolerance features.
- **Improved disaster recovery** - Most enterprise server virtualization platforms have software that can help test and automate failover before a disaster happens.
- **Legacy support** - Virtualization can extend the life of OSs and applications providing more time for organizations to migrate to newer solutions.

Hypervisor

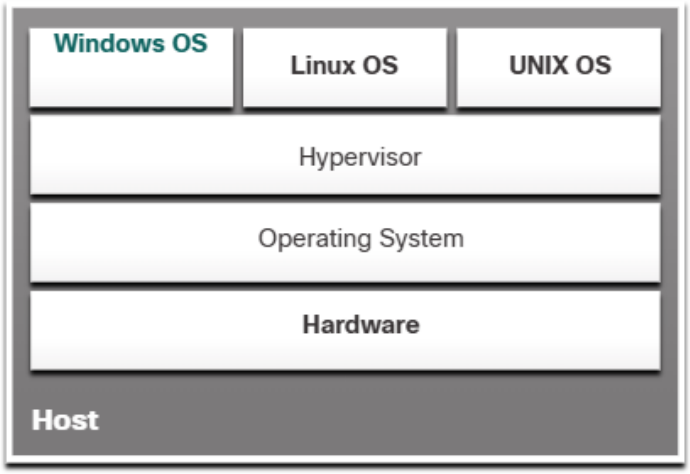
The hypervisor is a program, firmware, or hardware that adds an abstraction layer on top of the physical hardware. The abstraction layer is used to create virtual machines which have access to all the hardware of the physical machine such as CPUs, memory, disk controllers, and NICs. Each of these virtual machines runs a complete and separate operating system. With virtualization, it is not uncommon for 100 physical servers to be consolidated as virtual machines on top of 10 physical servers that are using hypervisors.

- **Type 1 Hypervisor - "Bare Metal" Approach:** Type 1 hypervisors are also called the "bare metal" approach because the hypervisor is installed directly on the hardware. Type 1 hypervisors are usually used on enterprise servers and data center networking devices. Type 1 hypervisors are also called the "bare metal" approach because the hypervisor is installed directly on the hardware. Type 1 hypervisors are usually used on enterprise servers and data center networking devices. With Type 1 hypervisors, the hypervisor is installed directly on the server or networking hardware. Then, instances of an OS are installed on the hypervisor, as shown in the figure. Type 1 hypervisors have direct access to the hardware resources; therefore, they are more efficient than hosted architectures. Type 1 hypervisors improve scalability, performance, and robustness.



- **Type 2 Hypervisor - "Hosted" Approach:** A Type 2 hypervisor is software that creates and runs VM instances. The computer, on which a hypervisor is supporting one or more VMs, is a host machine. Type 2 hypervisors are also called hosted hypervisors. This is because the hypervisor is installed on top of the existing OS, such as macOS, Windows, or Linux. Then, one or more additional OS instances are installed on top of the hypervisor, as shown in the figure. A big advantage of Type 2 hypervisors is that management console software is not required.

  Note: It is important to make sure that the host machine is robust enough to install and run the VMs, so that it does not run out of resources.



Lab - Install Linux in a Virtual Machine and Explore the GUI

Objectives

Part 1: Prepare a Computer for Virtualization

Part 2: Install a Linux OS on the Virtual Machine

Part 3: Explore the GUI

Background / Scenario

Computing power and resources have increased tremendously over the last 10 years. A benefit of multi-core processors and large amounts of RAM is the ability to install multiple operating systems through the use of virtualization on a computer.

With virtualization, one or more virtual computers can operate inside one physical computer. Virtual computers that run within physical computers are called virtual machines. Virtual machines are often called guests, and physical computers are often called hosts. Anyone with a modern computer and operating system can run virtual machines.

In this lab, you will install a Linux OS in a virtual machine using a desktop virtualization application, such as VirtualBox. After completing the installation, you will explore the GUI

interface. You will also explore the command line interface using this virtual machine in a lab later in this course.

Required Resources

- Computer with a minimum of 2 GB of RAM and 10 GB of free disk space
- High-speed Internet access to download Oracle VirtualBox and Linux OS image, such as Ubuntu Desktop

Instructions

Part 1: Prepare a Computer for Virtualization

In Part 1, you will download and install desktop virtualization software and a Linux OS image. Your instructor may provide you with a Linux OS image.

Step 1: Download and install VirtualBox.

VMware Player and Oracle VirtualBox are two virtualization programs that you can download and install to support the OS image file. In this lab, you will use the VirtualBox application.

a. Navigate to https://www.virtualbox.org/. Click the download link on this page.

b. Choose and download the appropriate installation file based on your operating system.

c. After the VirtualBox installation file is downloaded, run the installer and accept the default installation settings.

Step 2: Download a Linux Image.

a. Navigate to the Ubuntu website at http://www.ubuntu.com. Click the Download link on this page to download and save an Ubuntu Desktop image.

Step 3: Create a New Virtual Machine.

a. Click **Start** and search for **Virtualbox**. Click **Oracle VM VirtualBox** to open the manager. When the manager opens, click **New** to start the Ubuntu installation.

b. In the **Name and operating system** screen, type **Ubuntu** in the **Name** field. For the **Type** field, select **Linux**. In the **Version** field, select the corresponding downloaded version. Click **Next** to continue.

c. In the **Memory size** screen, increase the amount of RAM as long as the amount of RAM for the virtual machine is in the green area. Going beyond the green area would adversely affect the performance of the host. Click **Next** to continue.

d. In the **Hard disk** screen, click **Create** to create a virtual hard disk now.

e. In the **Hard disk file type** screen, use the default file type settings of **VDI (VirtualBox Disk Image)**. Click **Next** to continue.

f. In the **Storage on physical hard disk** screen, use the default storage settings of **dynamically allocated**. Click **Next** to continue.

g. In the **File location and size** screen, you can adjust the hard drive and change the name and location of the virtual hard drive. Click **Create** to use the default settings.

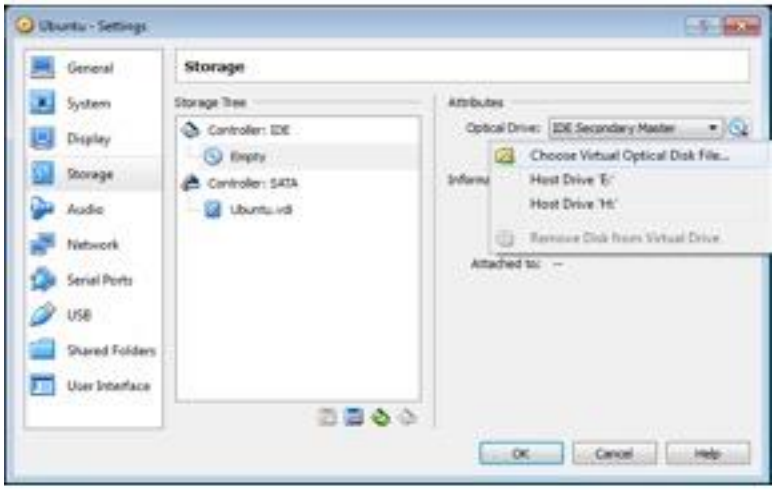
h. When the hard drive creation is done, the new virtual machine is listed in the **Oracle VM VirtualBox Manager** window. Select **Ubuntu** and click **Start** in the top menu.

Part 2: Install Ubuntu on the virtual machine

Step 1: Mount the Image.

a. In the **Oracle VM Virtualbox Manager** window. Right-click **Ubuntu** and select **Settings**. In the **Ubuntu – Settings** window, click **Storage** in the left pane. Click **Empty** in the middle pane. In the right pane, click the CD symbol and select the file location of the Ubuntu image. Click **OK** to continue.

b. In the **Oracle VM VirtualBox Manager** window, click **Start** in the top menu.



Step 2: Install the OS.

a. In the **Welcome** screen, you are prompted to try or install Ubuntu. The try option does not install the OS, it runs the OS straight from the image. In this lab, you will install the Ubuntu OS in this virtual machine. Click **Install Ubuntu**.

b. Follow the on-screen instructions and provide the necessary information when prompted.

Note: If you are not connected to the Internet, you can continue to install and enable the network later.

c. Because this Ubuntu installation is in a virtual machine, it is safe to erase the disk and install Ubuntu without affecting the host computer. Select **Erase disk and install Ubuntu**. Otherwise installing Ubuntu on a physical computer would erase all data on the disk and replace the existing operating system with Ubuntu. Click **Install Now** to start the installation.

d. Click **Continue** to erase the disk and install Ubuntu.

e. In the **Who are you?** screen, provide your name and choose a password. You can use the username generated or enter a different username. Enter your desired username and password. If desired, you can change the other settings. Click **Continue**.

f. The Ubuntu OS is now installing in the virtual machine. This will take several minutes. When the **Installation is complete** message displays, return to the **Oracle VM Virtualbox Manager** window. Right-click **Ubuntu** and select **Settings**. In the **Ubuntu – Settings** window, click **Storage** in the left pane. Click the mounted Ubuntu image in the middle pane. In the right pane, click the CD symbol and click **Remove Disk from Virtual Drive**. Click **OK** to continue.

g. In the Ubuntu VM, click **Restart Now**.

Part 3: Explore the GUI

In this part, you will install the VirtualBox guest additions and explore the Ubuntu GUI.

Step 1: Install Guest Additions.

a. Log on to your Ubuntu virtual machine using the user credentials created in the previous part.

b. Your Ubuntu Desktop window may be smaller than expected. This is especially true on high-resolution displays. Click **Device > Insert Guest Additions CD image…** to install the Guest Additions. This allows more functions, such as changing the screen resolution in the virtual machine.

c. Click **Run** to install the additions. When prompted for a password, use the same password that you used to log on. Click **Authenticate** to continue.

d. If the computer was not connected to the Internet during the installation, click **Devices > Network Settings** in the Oracle VirtualBox menu. Enable network adapters and configure the proper setting for network connections as necessary. Click **OK**.

e. When the installation of the additions is done, restart the virtual machine again. Click the menu in the upper-right corner and click **Shut down**. Click **Restart** to restart Ubuntu.

Step 2: Open a web browser.

a. Log on to Ubuntu again. After you are logged on again, you can resize the virtual machine window.

b. Open a web browser. Depending on the Linux distribution, you may need to search for a web browser or there is a link to a web browser already on the Desktop.

c. Locate a terminal emulator to access the command line interface. You will be using a terminal emulator in later labs.

d. Explore the installed Linux distribution and locate a few applications that you may use.