Unit 9
The Internet

Introduction

The Internet is the most used network in the world. The Internet is a network of networks—a set of separate and distinct networks operated by various national and state government agencies, nonprofit organizations, and for-profit corporations.

Internet is a global communication system that links together thousands of individual networks. It allows exchange of information between two or more computers on a network. It has become mandatory for day-to-day activities, i.e. bills payment, online shopping, tutoring, working, communications etc.

Internet was evolved in 1969, under the project called **ARPANET (Advanced Research Projects Agency Network)** to connect computers at different universities and U.S. defense. Soon people from different backgrounds such as engineers, scientists, students and researchers started using the network for exchanging information and messages.

In 1990s the internet working of **ARPANET, NSFnet (National Science Foundation Network)** and other network resulted into Internet.

Components of Internet

1. **Computers and Devices:** The internet is accessed through various devices, including computers, Smartphone, tablets and IoT devices. These device connect to the internet via wired or wireless technologies.
2. **Network Infrastructure:** The internet comprises an intricate web of networks, including LAN, WAN and BN. These networks use various technologies like Ethernet, fiber optics and wireless connections to transmit data.
3. **Protocols and Standards:** The Internet operates on a set of protocols and standards such as TCP/IP. These protocols define how data is transmitted and received over the network ensuring seamless communication between devices and Networks.
4. **Internet Service Providers (ISP):** ISPs are companies that provide Internet access to individuals, businesses, and organizations. They offer different types of connections, including broadband, cable, fiber optics etc. to connect to the Internet.
5. **Web Servers and Websites:** Web servers host websites and web applications, making them accessible to users worldwide. Websites are accessed using web browsers like chrome, Safari, Edge etc.

How the Internet Works

Internet is a global communication system that connects various devices and sends a lot of information and media. It uses Internet Protocol (IP) and Transmission Control Protocol (TCP) based packet routing network. TCP and IP works together to ensure the data transmission across the internet is consistent and reliable, regardless of device or location.

Basic Architecture

The architecture of Internet is complex and distributed, allowing data to be transmitted globally between millions of interconnected devices.

The Internet is hierarchical in structure. At the top are the very large national **Internet Service Providers (ISPs),** such as AT&T and Sprint, which are responsible for large Internet networks. These **national ISPs,** called **tier 1 ISPs,** connect together and exchange data at **network access points (NAPs)** shown in figure below.

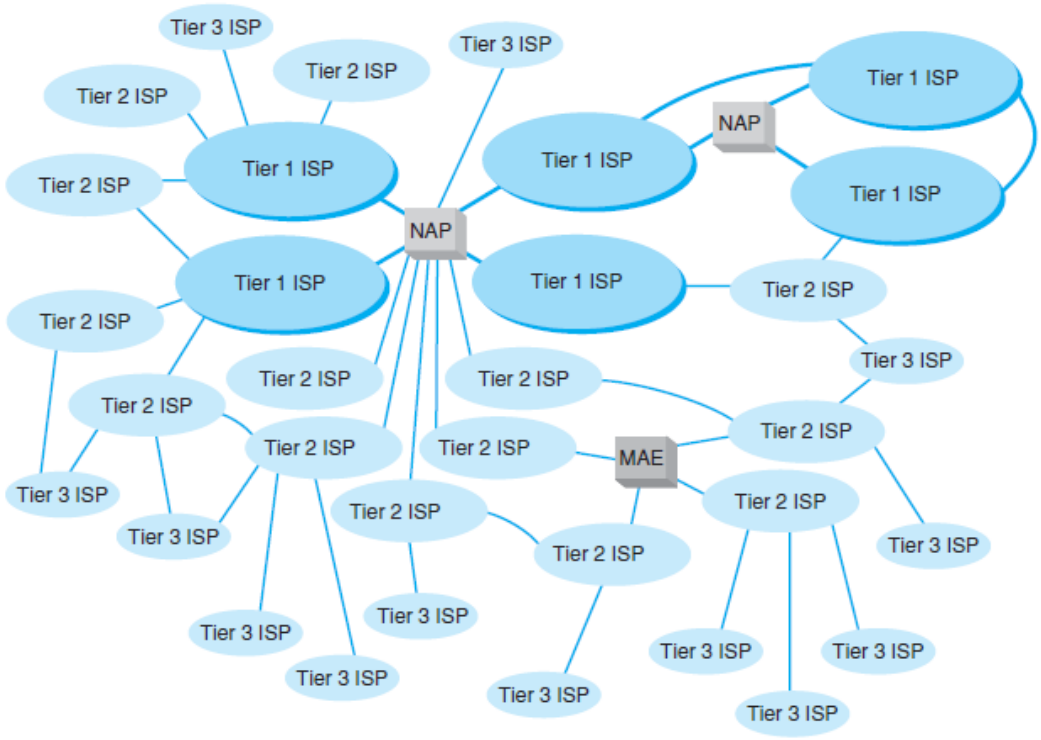

Fig: Basic Internet Architecture

In the early 1990s, when the Internet was still primarily run by the U.S. National Science Foundation (NSF), the NSF established four main NAPs in the United States to connect the major tier 1 ISPs. When the NSF stopped funding the Internet, the companies running these NAPs began charging the ISPs for connections, so today the NAPs in the United States are all not-for-profit organizations or commercial enterprises run by various common carriers such as AT&T and Sprint. As the Internet has grown, so too has the number of NAPs; today there are about a dozen NAPs in the United States with many more spread around the world.

Network access points were originally designed to connect only large tier 1 ISPs. These ISPs in turn provide services for their customers and also to **regional ISPs** (sometimes called **tier 2 ISPs**) such as Cogent Communications Comcast, or France Telcom. These tier 2 ISPs rely on the tier 1 ISPs to transmit their messages to ISPs in other countries. Tier 2 ISPs, in turn, provide services to their customers and to local ISPs (sometimes called **ISPs**) who sell Internet access to individuals. As the number of ISPs grew, a new form of NAP called a **metropolitan area exchange (MAE)** emerged. MAEs are smaller versions of NAPs and typically link a set of regional ISPs whose networks come together in major cities.

Because most NAPs, MAEs, and ISPs now are run by commercial firms, many of the early restrictions on who could connect to whom have been lifted. Most now openly solicit business from all tiers of ISPs and even large organizations. Regional and local
ISPs often will have several connections into other ISPs to provide backup connections in case one Internet connection fails. In this way, they are not dependent on just one higher-level ISP.

In general, ISPs at the same level do not charge one another for transferring messages they exchange. That is, a national tier 1 ISP does not charge another national tier 1 ISP to transmit its messages. This is called **peering.** Figure above shows several examples of peering. It is peering that makes the Internet work and has led to the belief that the Internet is free. This is true to some

extent, but higher-level ISPs normally charge lower-level ISPs to transmit their data (e.g., a tier 1 will charge a tier 2 and a tier 2 will charge a tier 3). And of course, any ISP will charge individuals like us for access!

Peering has risen to a new level in recent years with the arrival of **Internet Exchange Points (IXPs)**. An IXP, which is often run by a not-for-profit cooperative organization, permits any ISP (or large organization) to connect to its network. Some IXPs charge connection fees, others charge membership fees, and others don't charge at all. Once connected to the IXP, the ISP negotiates peering agreements with other ISPs who are members of the IXP, and then begins exchanging Internet traffic.

In Figure above each of the ISPs are **autonomous systems.** Each ISP is responsible for running its own interior routing protocols and for exchanging routing information via the **Border Gateway Protocol (BGP)** exterior routing protocol at NAPs, MAEs, IXPs, and any other connection points between individual ISPs.

Connecting to an ISP

Each of the ISPs is responsible for running its own network that forms part of the Internet. ISPs make money by charging customers to connect to their part of the Internet. Local ISPs charge individuals for broadband or dial-up access whereas national and regional ISPs (and sometimes local ISPs) charge larger organizations for higher-speed access.

Each ISP has one or more **points of presence (POP).** A POP is simply the place at which the ISP provides services to its customers. To connect into the Internet, a customer must establish a circuit from his or her location into the ISP POP. For individuals, this is often done using a DSL (Digital Subscriber Line) modem or cable modem (Figure below). This connects to the DSL multiplexer at the ISP and from there to a **remote-access server (RAS),** which checks to make sure the user is a valid customer. Once logged in, the user can begin sending TCP/IP packets from his or her computer to the POP. Figure below shows a POP using a switched backbone with a layer-2 switch.

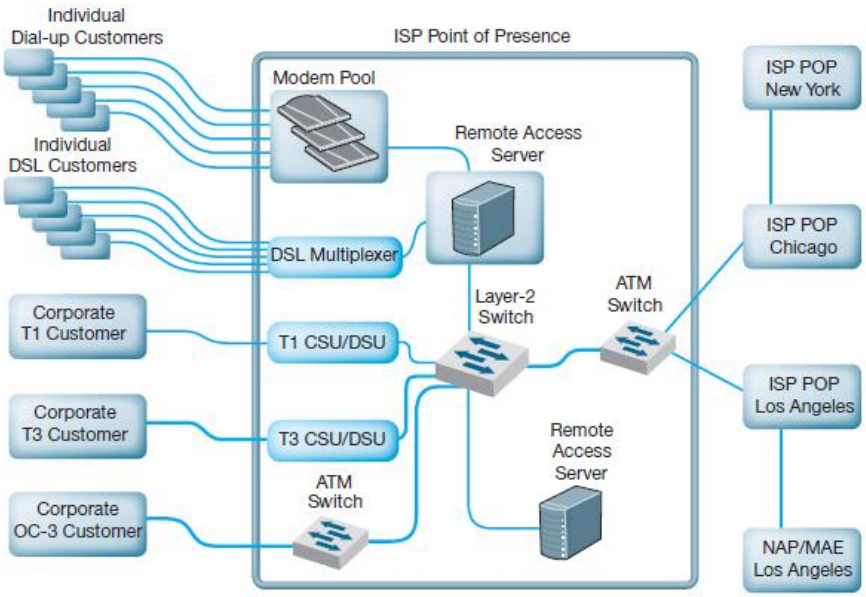

Fig: Inside an Internet service provider (ISP) point of presence (POP).
(ATM = asynchronous transfer mode; CSU = channel service unit; DSU = data service unit; MAE = metropolitan area exchange; NAP = network access point)

Figure above shows corporate customers with T1, T3, and OC-3 connections into the ISP POP. It is important to note that the customer must pay for both Internet access (paid to the ISP) and for the circuit connecting from their location to the POP (usually paid to the local exchange carrier [e.g., BellSouth, AT&T], but sometimes the ISP also can provide circuits). For a T1 connection, for example, a company might pay the local exchange carrier $400 per month to provide the T1 circuit from its offices to the ISP POP and *also* pay the ISP $300 per month to provide the Internet access.

As Figure above shows, the ISP POP is connected in turn to the other POPs in the ISP's network. Any messages destined for other customers of the same ISP would flow within the ISP's own network. In most cases, the majorities of messages entering the POP are sent outside of the ISP's network and thus must flow through the ISP's network to the nearest NAP/MAE/IXP and from there, into some other ISP's network.

Internet Access Technologies

There are many ways in which individuals and organizations can connect to an ISP. Most individuals use DSL or cable modem. As we discussed in the preceding section, many organizations lease T1 or T3 lines into their ISPs.

DSL and cable modem technologies are commonly called **broadband technologies** because they provide higher-speed communications than traditional modems. It is important to understand that Internet access technologies are used only to connect from one location to an ISP. Unlike the WAN technologies in the previous chapter, Internet access technologies cannot be used for general-purpose networking from any point to any point.

We discuss four principal Internet access technologies

1. **DSL (Digital Subscriber Line)**
2. **Cable Modem**
3. **Fiber to the home**
4. **WiMax**

Digital Subscriber Line

Digital subscriber line (DSL) is a family of point-to-point technologies designed to provide high-speed data transmission over traditional telephone lines. With this technology, user **voice** and **data** traffic go through this analog lines. DSL uses **high frequencies** for data transmission.

Architecture

DSL uses the existing local loop cable but places different equipment on the customer premises (i.e., the home or office) and in the telephone company end office. The equipment that is installed at the customer location is called the **Customer Premises Equipment (CPE).** Figure below shows one common type of DSL installation. The CPE in this case includes a **line splitter** that is used to separate the traditional voice telephone transmission from the data transmissions. The **line splitter** directs the telephone signals into the normal telephone system so that if the DSL equipment fails, voice communications are unaffected.

The line splitter also directs the data transmissions into a **DSL modem,** which is sometimes called a **DSL router**. This is both a modem and an FDM multiplexer. The DSL modem produces Ethernet 100Base-T packets so it can be connected directly into a computer or to a router and hub and can serve the needs of a small network. Most DSL companies targeting home users combine all of these devices (and a wireless access point) into one device so that consumers just

have to install one box, rather than separate **line splitters, modems, routers, switches and access points.**

Figure below also shows the architecture within the local carrier's end office (i.e., the telephone company office closest to the customer premises). The local loops from many customers enter and are connected to the **main distribution facility (MDF).** The MDF works like the CPE line splitter; it splits the voice traffic from the data traffic and directs the voice traffic to the voice telephone network and the data traffic to the **DSL Access Multiplexer (DSLAM).** The DSLAM demultiplexes the data streams and converts them into ATM data, which are then distributed to the ISPs. Some ISPs are collocated, in that they have their POPs physically in the telephone company end offices. Other ISPs have their POPs located elsewhere.

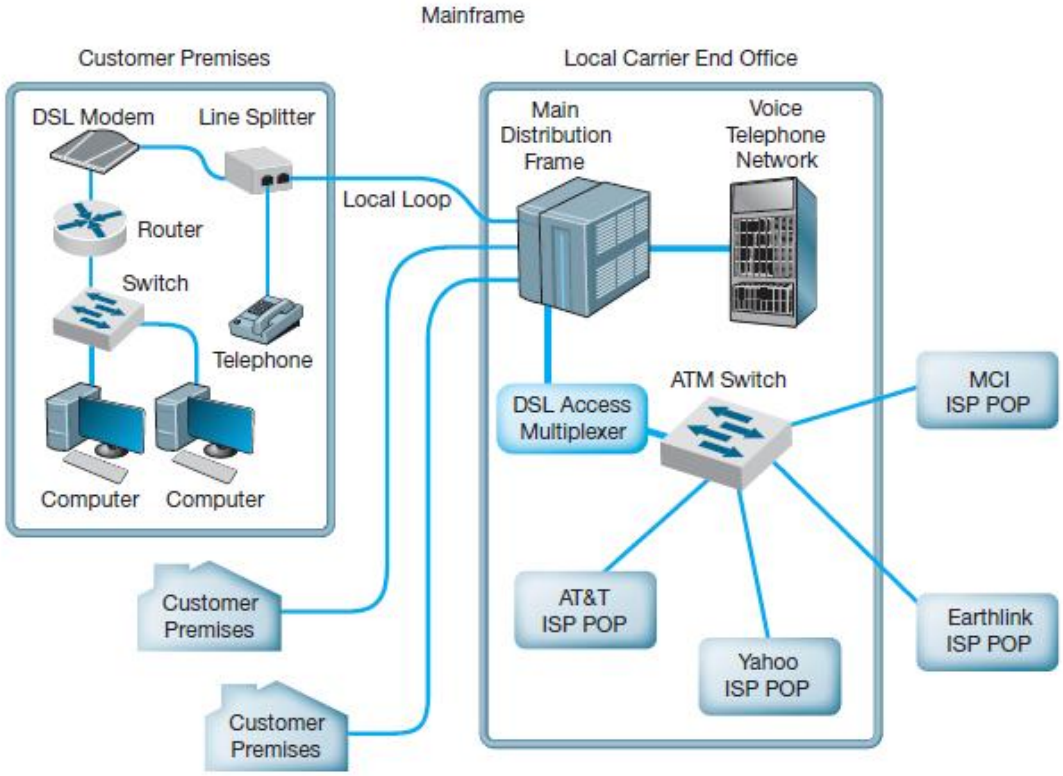

Fig: DSL Architecture
ATM = asynchronous transfer mode
ISP = Internet service provider, POP = point of presence

Types of DSL

There are many different types of DSL. The most common type today is **Asymmetric DSL (ADSL).** ADSL uses frequency division multiplexing to create three separate channels over the one local loop circuit. Some other types of DSL are:

1. Symmetric Digital Subscriber Line (SDSL)
2. Rate-Adaptive Digital Subscriber Line (RADSL)
3. High Bit-Rate Digital Subscriber Line (HDSL)
4. Very High Bit–rate Digital Subscriber Line (VDSL)
5. Very High Bit –rate Digital Subscriber Line 2 (VDSL2)

Advantages of DSL

1. **Availability:** DSL is availablswe in urban, suburban, and even in some rural areas. It utilizes existing telephone lines, making it accessible to large group of peoples.

2. **Affordability:** DSL is affordable than high speed alternatives such as fiber-optic connections.
3. **Stability & Relaibility:** DSL connections are stable and reliable. User experience consistent speeds even during peak usages times.
4. **Low latency:** DSL have low latency making it suitable for online gaming, video conferencing and other real time applications.
5. **Security:** DSL connections are private and secured.
6. **No Interference from Weather:** Unlike satellites internet, DSL connections are not affected by weather conditions.

Disadvantages of DSL

1. **Distance Limitations:** DSL speed decreases significantly with distance from the telephone exchange. User closer to exchange experience higher speeds than those farther away.
2. **Speed Variability:** The speed of DSL connections can vary based on the quality and conditions of copper lines.
3. **Limited Upload limits:** DSL connections usually have slower upload speeds compared to download speeds.
4. **Competition with Newer Technologies:** DSL should compete with newer technologies like fiber optics and cable internet, which offer higher speeds and more reliable connections.
5. **Limited Support for Multiple Devices:** DSL might struggle to support multiple connected devices simultaneously, in houses with heavy internet usages.

Cable Modem

One alternative to DSL is the **cable modem,** a digital service offered by cable television companies. There are several competing standards, but the **Data over Cable Service Interface Specification (DOCSIS)** standard is the dominant one. DOCSIS is not a formal standard but is the one used by most vendors of **hybrid fiber coax (HFC)** networks i.e., cable networks that use both fiber-optic and coaxial cable. As with DSL, these technologies are changing rapidly.

Architecture

Cable modem architecture is very similar to DSL—with one very important difference. DSL is a point-to-point technology, whereas cable modems use *shared* multipoint circuits. With cable modems, each user must compete with other users for the available capacity.
Figure below shows the most common architecture for cable modems.

The cable TV circuit enters the customer premises through a cable splitter that separates the data transmissions from the TV transmissions and sends the TV signals to the TV network and the data signals to the cable modem. The cable modem (both a modem and frequency division multiplexer) translates from the cable data into Ethernet packets, which then are directed into a computer to a router and hub for distribution in a small network. As with DSL, cable modem companies usually combine all of these separate devices into one or two devices to make it easier for the home consumer to install.

The cable TV cable entering the customer premises is a standard coaxial cable. A typical segment of cable is shared by anywhere from 300 to 1,000 customers, depending on the cable company that installed the cable. This coax cable runs to a *fiber node,* which has an **optical-electrical (OE) converter** to convert between the coaxial cable on the customer side and fiber-

optic cable on the cable TV company side. Each fiber node serves as many as half a dozen separate coaxial cable runs.

The fiber nodes are in turn connected to the cable company **distribution hub** (sometimes called a *headend*) through two separate circuits: an **upstream circuit and a downstream circuit**.

The upstream circuit, containing data traffic from the customer, is connected into a **cable modem termination system (CMTS).** The CMTS contains a series of cable modems/multiplexers and converts the data from cable modem protocols into protocols needed for Internet traffic, before passing them to a router connected to an ISP POP.

The downstream circuit to the customer contains both ordinary video transmissions from the cable TV video network and data transmissions from the Internet. Downstream data traffic enters the distribution hub from the ISP POP and is routed through the CMTS, which produces the cable modem signals. This traffic is then sent to a *combiner,* which combines the Internet data traffic with the ordinary TV video traffic and sends it back to the fiber node for distribution.

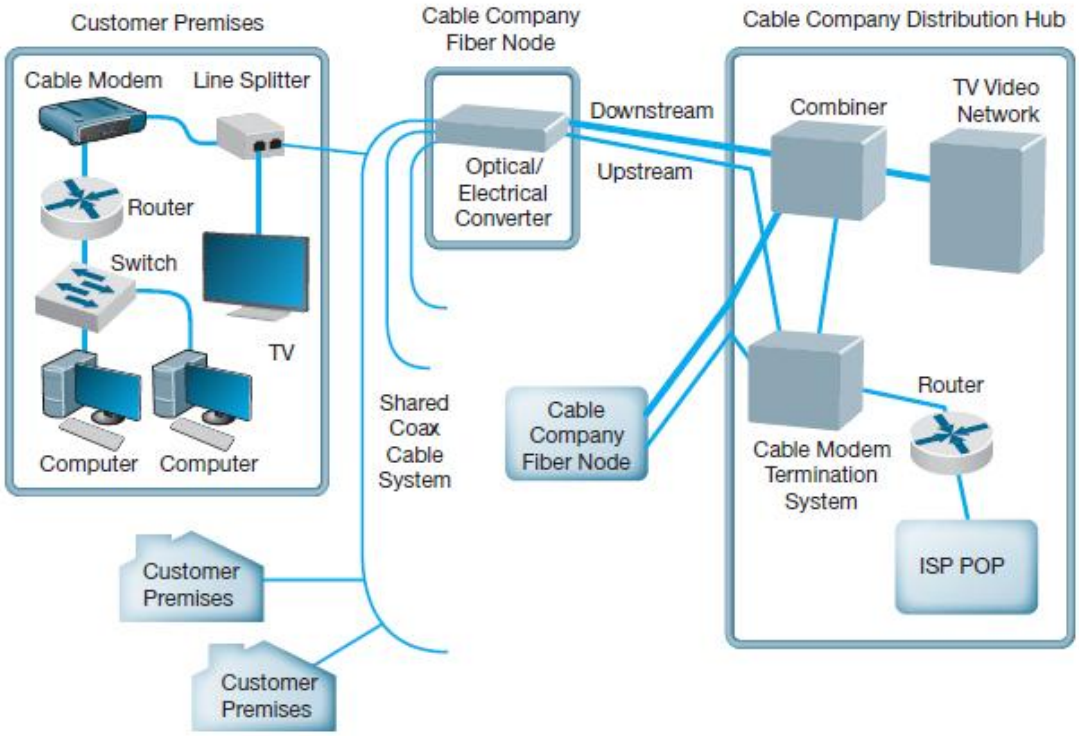

Fig: Cable Modem Architecture

Advantages

1. **High Speeds:** Cable Internet provide high-speed internet access, compared to traditional DSL connections.
2. **Widespread Availability:** Cable Internet is widely available particularly in urban and suburban areas.
3. **Bundled Services:** Cable providers provide bundled package that include Internet, cable TV and even phone services.
4. **Reliable Connection:** Cable Internet connections are generally stable and reliable.
5. **Shared Infrastructure:** Cable Internet uses the same infrastructure as cable television. If there is cable TV services , setting up cable Internet is convenient.

Disadvantages

1. **Shared Bandwidth:** the major drawback of cable Internet is shared bandwidth among multiple users in the neighborhood which can slow during peak usage time.
2. **Limited Upload Speed:** Cable Internet provides slower upload speeds compared to download speed. The limitation can affect activities like online gaming, video conferencing which require stable upload connections.
3. **Vulnerable to Interference:** Cable Internet signals can be affected by electromagnetic interference which creates problems such as signal degradation.
4. **Reliability during Outages:** During power outages, Cable Internet service might also be affected unless there is a backup power source.
5. **Pricing and Bundling:** Bundling can save money. However some users might find that cable internet bundled with other services can lead to complex pricing structures.
6. **Limited availability in Rural Areas:** Being widely available in urban and suburban regions, cable Internet is not as accessible in rural areas. Remote locations might lack the necessary infrastructure for cable Internet connections.
7. **Decent Upload speed:** While not as fast as download speeds, cable Internet usually provides acceptable upload speeds for activities like uploading files and video conferencing.

Fiber to the Home

Fiber to the home (FTTH) is exactly what it sounds like: running fiber-optic cable into the home. The traditional set of hundreds of copper telephone lines that run from the telephone company switch office is replaced by one fiber-optic cable that is run past each house or office in the neighborhood. Data are transmitted down the signal fiber cable using wavelength division multiplexing (WDM), providing hundreds or thousands of separate channels. Fiber Optic cable offers better data speeds compared to copper cables.

Architecture

FTTH architecture is very similar to DSL and cable modem. At each subscriber location, an **optical unit network (ONU)** (also called an **Optical Network Terminal ONT)** acts like a DSL modem or cable modem and converts the signals in the optical network into an Ethernet format. The ONU acts as an Ethernet switch and can also include a router. FTTH is a dedicated point-to-point service like DSL, not a shared multipoint service like cable modem. Providers of fiber to the home can use either active optical networking or passive optical networking to connect the ONU in the customer's home. Active networking means that the optical devices require electrical power and works in much the same way as traditional electronic switches and routers. Passive optical networking devices require no electrical current and thus are quicker and easier to install and maintain than traditional electrical-based device, but because they are passive, the optical signal fades quickly, giving a maximum range of about 10 miles.

Advantages of Fiber to the Home FTTH

1. **Incredibly high speeds: FTTH** offers some of the fastest internet speeds available, with symmetrical upload and download speeds that can range from hundreds of Mbps to 1 Gbps or even more.
2. **Low Latency:** Fiber Optic connection have lower latency, making them ideal for real-time applications, online gaming and video conferencing.
3. **Reliable Performance:** Fiber optics are less susceptible to interference, signal degradation and electromagnetic noise, ensuring a stable and reliable internet connections.

4. **Higher Bandwidth:** FTTH provides significantly higher bandwidth compared to other internet technologies, allowing for the concurrent use of multiple devices without comprising speed or quality.
5. **Security:** Fiber optic signals do not radiate electromagnetic signals, making it difficult for hackers to intercept data.
6. **Scalability: FTTH** networks are highly scalable and can support future technologies and higher speeds without the need for significant infrastructure upgrades.

Disadvantages

1. **Initial Cost and Deployment Challenges:** Deploying FTTH infrastructure involves high initial costs, including the installation of fiber optic cables and network equipments.
2. **Limited Availability: FTTH** is not widely available as other internet technology such as cable or DSL.
3. **Dependency or External Factors: FTTH** infrastructure may be affected by external factors such as construction work, natural disasters or physical damages to cables.
4. **Dependency on Power Supply: FTTH** network equipment including **Optical network Terminals (ONTs)** requires power source. During power outages, user might lose internet connectivity.
5. **Fiber Fragility:** Fiber Optic cables are delicate and can be damaged easily, requiring careful handling and protection during installation and maintenance.

WiMax

WiMAX (Worldwide Interoperability for Microwave Access) is the commercial name for a set of standards developed by the *IEEE 802.16* standards group. WiMax is family of technologies that is much like the 802.11 Wi-Fi family. It reuses many of the Wi-Fi components and was designed to connect easily into Ethernet LANs. WiMax can be used as a fixed wireless technology to connect a house or an office into the Internet, but its future lies in its ability to connect mobile laptops and smart phones into the Internet.

WiMax technology is often used in areas where it might be challenging to lay traditional wired infrastructure, offering an alternative solution for broadband connectivity.

WiMax is relatively old technology. However many experts envision a future where both Wi-Fi and WiMax coexist. Laptops and smartphones will connect to Wi-Fi networks in home and office location where Wi-Fi is available. If Wi-Fi is not available the the laptop and smartphones will connect to WiMax networks. But yet WiMax is still not common.

Architecture

Although WiMax can be used in fixed locations to provide Internet access to homes and offices, we will focus on mobile use as this is likely to be the most common use. Mobile WiMax works in much the same way as Wi-Fi. The laptop or smart phone has a **WIMAX Network Interface Card (NIC**) and uses it to establish a connection to a **WiMax Access Point (AP**). Many devices use the same AP so WiMax is a shared multipoint service in which all computers must take turns transmitting. Media access control is controlled access, using a version of the 802.11 point coordination function (PCF).

Types of WiMax

There are several types of WiMax available, with new versions under development. The most common type of mobile wireless provides speeds of 40 Mbps, shared among all users of the same AP. Some providers have versions that run at 70 Mbps. New versions under development promise speeds of 300 Mbps.

Advantages

1. **Wide Coverage Area:** WiMax can cover area up to 50KM making it suitable for providing broadband access in rural areas.
2. **High Data Rates:** It offers data rate upto 75mbps which is higher than other wireless technologies.
3. **Scalability:** WiMax can easily be scaled to support large number of users and devices.
4. **Cost- effective:** WiMax is cost-effective solution for providing broadband access in areas where it is not economically feasible to deploy wired infrastructure.

Disadvantages

1. **Limited Mobility: WiMax** is designed for fixed or nomadic (semi- fixed) use, not for mobile use.
2. **Interference: WiMax** operates at same frequency range as other wireless technology, which can lead to interference.
3. **Security Concerns: WiMax** uses shared spectrum, which can make it vulnerable to security threats such as jamming.
4. **Limited device availability: WiMax** devices are not as widely available as devices for other technologies, such as WiFi.
5. **Limited penetration: WiMax** signal has trouble penetrating through walls, buildings and other obstacles.

The Future of the Internet

The future of internet is a fascinating and rapidly evoving landscape, shaped by emerging technologies, changing user behaviors and global connectivity. Some key trends development that define future of Internet are:

1. **5G and Beyond**
2. **Internet of Things**
3. **AI and Machine Learning**
4. **Blockchain and Decentralization**
5. **Augmented Reality (AR) and Virtual Reality (VR)**
6. **Sustainable Internet**

Internet Governance

Because the Internet is a network of networks, no one organization operates the Internet. The closest thing the Internet has to an owner is the **Internet Society (ISOC)** (www.isoc.org). ISOC is an open-membership professional society with more than 175 organizational and 8,000 individual members in over 100 countries, including corporations, government agencies, and foundations that have created the Internet and its technologies.

Because membership in ISOC is open, anyone, including students, is welcome to join and vote on key issues facing the Internet. The ISOC mission is to ensure "the open development, evolution and use of the Internet for the benefit of all people throughout the world."

It works in three general areas: **public policy, education, and standards**.

In terms of public policy, ISOC participates in the national and international debates on important issues such as censorship, copyright, privacy, and universal access.

ISOC delivers training and education programs targeted at improving the Internet infrastructure in developing nations.

The most important ISOC activity lies in the development and maintenance of Internet standards.

ISOC works through four interrelated standards bodies: **Internet Engineering Task Force (IETF), Internet Engineering Steering Group (IESG), Internet Architecture Board (IAB), and Internet Research Task Force (IRTF).**

The **Internet Engineering Task Force (IETF)** (www.ietf.org) is a large, open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Closely related to the IETF is the **Internet Engineering Steering Group (IESG).** The IESG is responsible for technical management of IETF activities and the Internet standards process. It administers the process according to the rules and procedures that have been ratified by the ISOC trustees. The IESG is directly responsible for the actions associated with entry into and movement along the Internet "standards track," including final approval of specifications as Internet standards.

The **Internet Architecture Board (IAB)** provides strategic architectural oversight. The IAB attempts to develop conclusions on strategic issues (e.g., top-level domain names, use of international character sets) that can be passed on as guidance to the IESG or turned into published statements or simply passed directly to the relevant IETF working group.

The **Internet Research Task Force (IRTF)** operates much like the IETF through small research groups focused on specific issues. Whereas IETF working groups focus on current issues, IRTF research groups work on long-term issues related to Internet protocols, applications, architecture, and technology.

Building the Future

The Internet is changing. New applications and access technologies are being developed at lightning pace. But these innovations do not change the fundamental structure of the Internet. It has evolved more slowly because the core technologies (TCP/IP) are harder to change gradually; it is difficult to change one part of the Internet without changing the attached parts.

Many organizations in many different countries are working on dozens of different projects in an attempt to design new technologies for the next version of the Internet.

The two primary American projects working on the future Internet got started at about the same time in 1996. The U.S. National Science Foundation provided $100 million to start the **Next Generation Internet (NGI)** program, and 34 universities got together to start what turned into the **University Corporation for Advanced Internet Development (UCAID),** which developed the **Abilene network,** commonly called **Internet2.** In 1997, the Canadian government established the **Advanced Research and Development Network Operations Center (ARDNOC),** which developed **CA*net,** the Canadian project on the future Internet.

Besides providing very high-speed Internet connections, these networks are intended to experiment with new protocols that one day may end up on the future Internet.

For example, most of these networks run IPv6 as the primary network layer protocol, rather than IPv4. Most are also working on new ways to provide quality of service (QoS) and multicasting. Internet2 is also working on developing new applications for a high-speed Internet, such as tele-immersion and videoconferencing.