The Network Infrastructure for E-Commerce

Course outline:

Introduction to information superhighway,
Components of the I-way,
Internet as network infrastructure, TCP/IP protocols suite, Intranet, Extranet etc
Software agents (static and dynamic),
Broadband technologies (xDSL, Wi-Fi, WAN).

Introduction to Information Superhighway (I-Way)

Electronic commerce needs a network infrastructure to transport the content (data) used for business purpose. Information superhighway is also known as interactive or multimedia superhighway. The information superhighway is a term coined by Vice President Albert Gore when giving a speech on January 11, 1994 describing the future of computers accessing and communicating over a world-wide network.

Basically, the term I-way describes a high-capacity (broadband), interactive (two-way) electronic pipeline to the home or office that is capable of simultaneously supporting a large number of electronic commerce applications and providing interactive connectivity between users and services and between users and other users. It is envisioned to provide very high speed access to information in all forms (text, graphics, audio, video) via a telephone or wireless connection.

Thus Information superhighway is the global information and communications network that includes the Internet and other networks and switching systems such as telephone networks, cable television networks, and satellite communication networks used for e-commerce and many more other purposes.

Components of the I-Way Three major components make up the I-way infrastructure, as shown in figure below: consumer access equipment, local on-ramps, and global information distribution networks.

Consumer access equipment is often ignored in discussions of the I-way but represents a critical category, the absence or slow progress of which is holding up other segments of the I-way. For instance, interactive TV is uncommon, not because of a lack of wiring, but because of a lack of affordable equipment on the customer's side for access and on the provider's side for distribution. This segment of the I-way includes hardware and software vendors, who provide physical devices such as routers and switches, access devices such as computers and set-top boxes, and software platforms such as browsers and operating systems.

Local or access rosds, or on-ramps, simplify linkages between businesses, schools, and homes to the communications backbone. This component is often called the "last mile" in the telecommunications industry. The providers of access ramps can be differentiated into four categories: telecom-based, cable TV—based, wireless-based, and computer-based on-line information services that include value-added networks (VANs).

Global information distribution networks represent the infrastructure crisscrossing countries and continents. Most of the infrastructure for the I-way already exists in the vast network of fiber optic strands, coaxial cables, radio waves, satellites, and copper wires spanning the globe.

Linking all the components of the I-way will require large capital investments in "open" systems (interoperable equipment that uses common standards) and installing gateways between various networks. A final requirement is switching hardware and software to move huge amounts of data effortlessly over such a complex network.

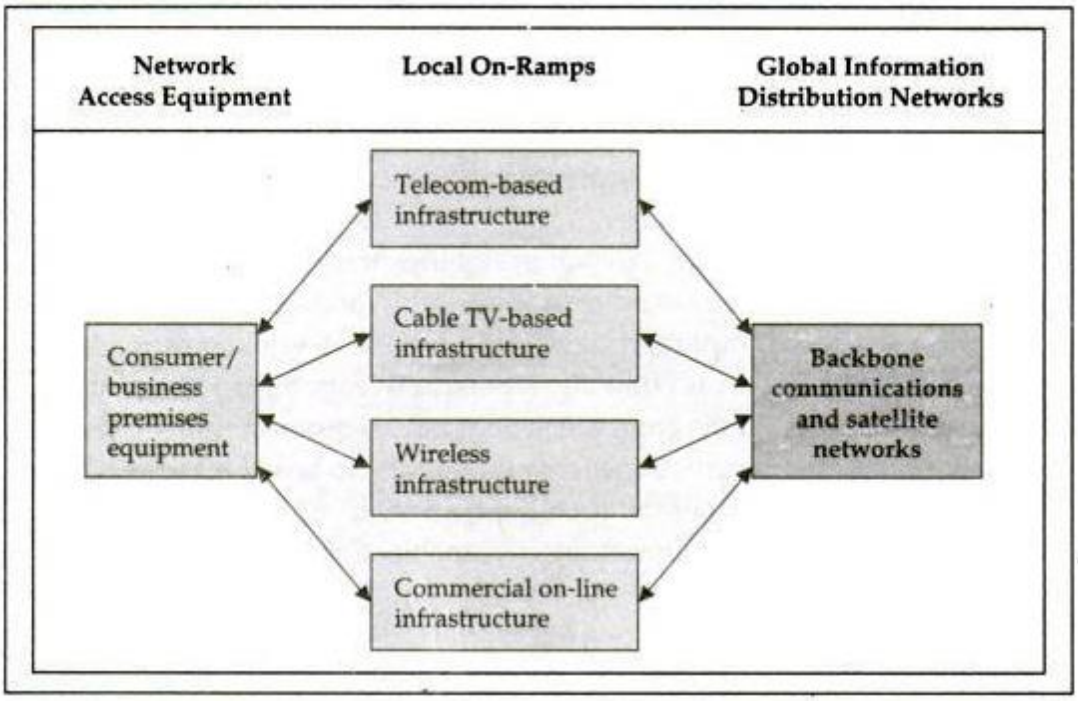


Fig: Components of the information superhighway infrastructure.

The three components of the information superhighway infrastructure can be summarized as:

1) Network access equipments:

   -represent the end users hardware and software which are often ignored

   For example computers, routers, hub, switches, browser, OS etc.

2) Local on-ramps:

   -simplifies linkages between users and the communication backbone.

   For example it cab be categories into:

   i. telecom-based
   ii. cable TV-based
   iii. wireless-based
   iv. computer-based

3) Global information distribution networks:

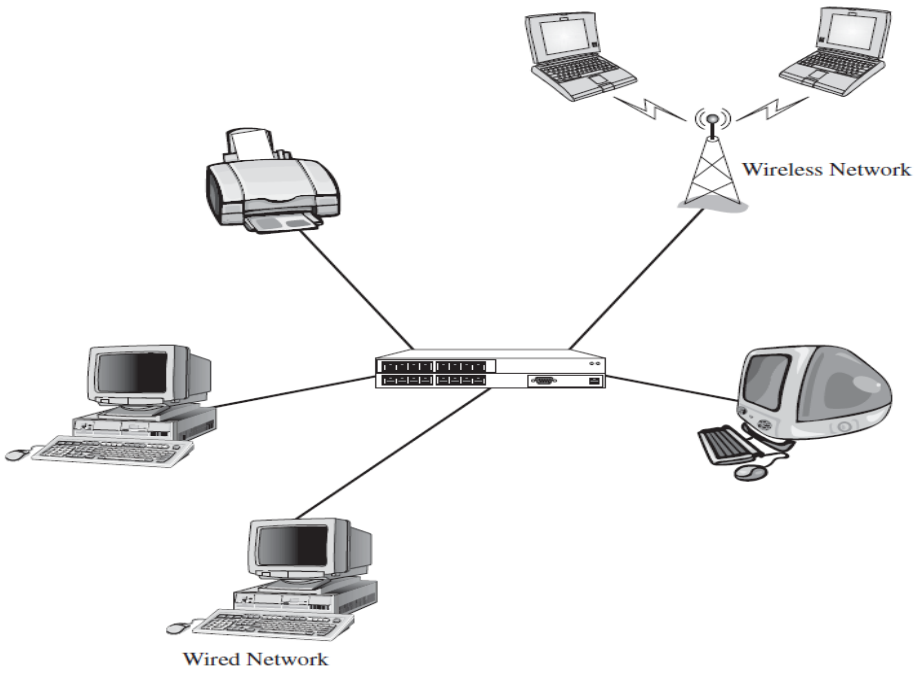
-communication infrastructure crossing the countries and continents. For example fiber optic strands, coaxial cables, radio waves, satellites, and copper wires.

Internet as a Network Infrastructure

Network Concept: In general, networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software. Networks are used to make work and communication more efficient. A network connects computers, but can also connect other devices such as shared printers, removable media drives, scanners, and other equipment.

Networks enable people to share resources, including printers, hard disks, and applications, which can greatly reduce the costs of providing these resources to each person in a company. Networks are built around this idea, connecting shared sources resources to their consumers. Several terms are used to describe these network devices, including hosts, nodes, workstations, peers, servers, and clients. Any device capable of communicating on the network is also referred to generically as a node.

A typical network like the one in figure below has three basic hardware components: one or more servers or host computers (including microcomputers and mainframes), clients (PCs), and a circuit or network system, which is the path over which they communicate.



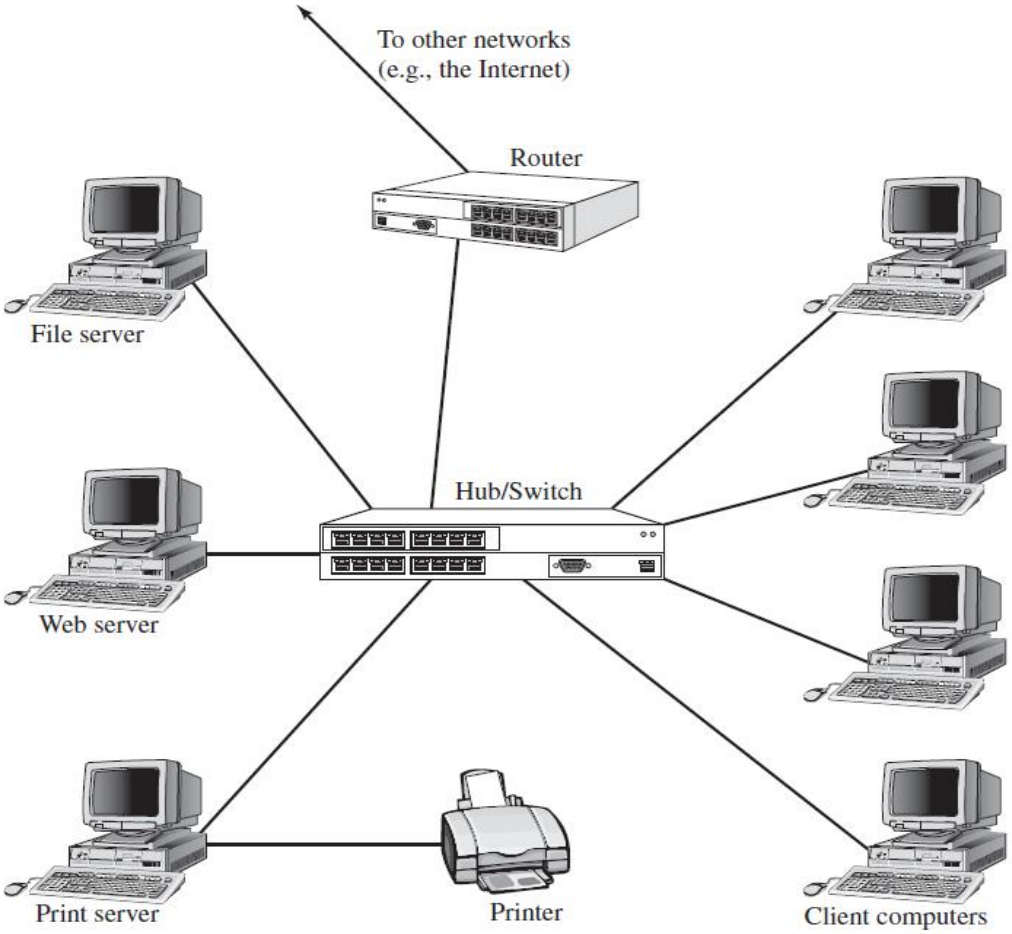
A typical network.

In addition, servers and clients also need special-purpose network software that enables them to communicate. The server stores data and software that the clients can access. You can have several servers working together over the network with client computers to support the business application. The client is the input–output hardware device at the user's end of a communication circuit. It provides users with access to the network, the data and software on the server, and other shared resources.

Strictly speaking, a network does not need a computer designated specifically as a server. Most modern client computers are designed to support the dual roles of both client and server, sharing resources to the network and, at the same time, accessing resources from the network. The circuit (cable plant or transmission media) is the pathway through which the data or information travels. Traditional wired networks typically use copper wire, although fiber-optic cable and wireless transmission hybrid systems are common. There are also devices in the circuit that perform special functions such as hubs, switches, routers, bridges, and gateways.

Network Device Roles: Figure below shows a small network that has four client PCs and three

specialized server PCs connected by a hub or switch and cables that make up the circuit. In this network, messages move through the hub to and from the computers. All computers share the same circuit and take turns sending messages.



An example network.

Each computer, client, or server has a network adapter, or network interface card (NIC). In the case of a wireless network, the network adapter sends and receives radio frequency messages, not that different from a walkie-talkie or cell phone. The network adapter also determines the low level protocol used by the computer to communicate on the network. Network adapters running on one protocol cannot communicate with network adapters running on a different protocol.

In older networks, hubs are used as central points where the cables leading out to network PCs come together. A **hub** is simply a connection point that does not provide any sophisticated

control. In current networks, you are more likely to see a **switch** rather than a hub. From the outside, both look much the same, but a switch is a more sophisticated communication device that helps control and manage the data passing between the PCs.

Figure above also shows a **router**. The router enables computers on one network to communicate with computers on other networks, but at the same time provide a level of isolation between the networks. Routers are a key part of the Internet, which is, at its core, a massive set of interconnected networks. A **gateway** is used to connect dissimilar networks and devices. For example, a gateway can be used to connect PCs on a LAN to a mainframe computer.

Like routers, bridges connect a network to other networks. Bridges do not provide the same level of isolation as routers, but can be used in some situations where routers cannot be used. Another device, called a brouter, combines the functionality of a bridge and router in the same device.

Understanding Servers and Clients: Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request.

The basic difference between clients (which include peer servers) and servers is the software that they run. Clients, as you might guess, run a client operating system. Common client operating systems include Microsoft Windows XP, Windows Vista, and Windows 7.

Servers run what is called either a server operating system or network operating system. Either one enables the computer to act as a server, by running the software necessary for central security management. Server operating systems typically include a client interface. Familiar examples are Windows Server systems such as Windows 2003 Server and Windows Server 2008, as well as most Linux versions.

The Internet: The public Internet is a world-wide computer network, i.e., a network that interconnects millions of computing devices throughout the world. Most of these computing devices are traditional desktop PCs, Unix-based workstations, and so called "servers" that store

and transmit information such as WWW pages and e-mail messages. Increasingly, non-traditional computing devices such as Web TVs, mobile computers, pagers and toasters are being connected to the Internet. In the Internet jargon, all of these devices are called hosts or end systems. The Internet applications with which many of us are familiar, such as the WWW and e-mail, are network application programs that run on such end systems.

End systems, as well as most other "pieces" of the Internet, run protocols that control the sending and receiving of information within the Internet. TCP (the Transmission Control Protocol) and IP (the Internet Protocol) are two of the most important protocols in the Internet. The Internet's principle protocols are collectively known as TCP/IP protocols.

End systems are connected together by communication links. Links are made up of different types of physical media: coaxial cable, copper wire, fiber optics, and radio spectrum (wireless). Different links can transmit data at different rates. The link transmission rate is often called the link bandwidth, and is typically measured in bits/second.

Intranet and Extranet: An **intranet** is a private network that is setup and controlled by an organization to encourage interaction among its members, to improve efficiency and to share information, among other things. Information and resources that are shared on an intranet might include: organizational policies and procedures, announcements, information about new products, and confidential data of strategic value.

An intranet is a restricted-access network that works much like the Internet, but is isolated from it. As is the case with the Internet, an intranet is based on TCP/IP protocols. Therefore, a web page in an intranet may look and act just like any other webpage on the Internet, but access is restricted to authorized persons and devices. In some cases, access to an intranet is restricted by not connecting it to other networks, but in other cases a **firewall** is used to deny access to unauthorized entities.

The difference between an intranet and the Internet is defined in terms of accessibility, size and control. Unless content filters are being used or the government is censoring content, all the

Internet's content is accessible to everyone. On the other hand an intranet is owned and controlled by a single organization that decides which members are allowed access to certain parts of the intranet. In general, an intranet is usually very small and is restricted to the premises of a single organization.

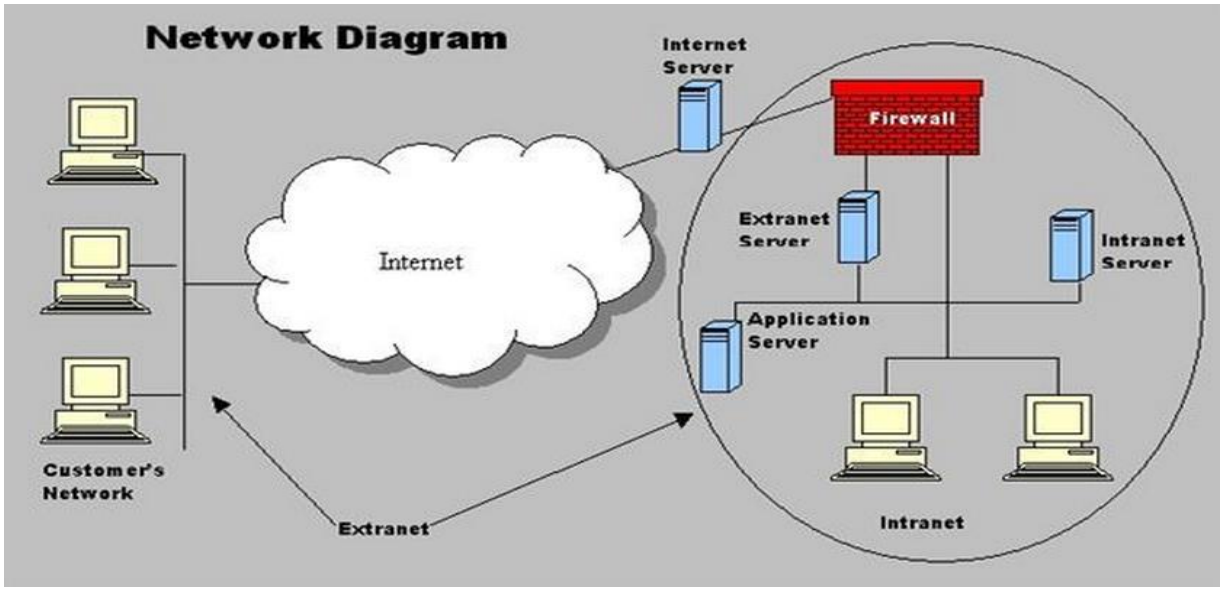


Fig: Relationship of Intranet and Extranet with Internet.

An **extranet** is an extended intranet. In addition to allowing access to members of an organization, an extranet uses firewalls, access profiles, and privacy protocols to allow access to users from outside the organization. In essence, an extranet is a private network that uses Internet protocols and public networks to securely share resources with customers, suppliers, vendors, partners, or other businesses.

Both intranets and extranets are owned, operated and controlled by one organization. However, the difference between intranets and extranets is defined in terms of who has access to the private network and the geographical reach of that network. Intranets allow only members of the organization to access the network, while an extranet allows persons from outside the organization (i.e. business partners and customers) to access the network. Usually, network access is managed through the administration of usernames and passwords, which are also used to determine which parts of the extranet a particular user can access.

Introduction to TCP/IP Protocol Suite

A computer communication protocol is a description of the rules computers must follow to communicate with each other. TCP/IP stands for Transmission Control Protocol/Internet Protocol, which is named after the primary protocols in the suite. It has become an industry standard protocol and, although it was originally designed for WANs, it is now widely used on LANs as well.

TCP/IP is a very robust protocol and can automatically recover from any communication link failures. It re-routes data packets if transmission lines are damaged or if a computer fails to respond, utilizing any available network path. A packet being sent from Network A to Network F may be sent via Network D (the quickest route). If this route becomes unavailable, the packet is routed using an alternate route (for example, A B C E F).

The TCP/IP Protocol Suite: The figure below shows a comparison of the OSI model and the TCP/IP protocol suite. The TCP/IP protocol maps to a four layer conceptual model: Application, Transport, Internet and Network Interface. This model is referred to as the Internet Protocol Suite or the ARPA model. As shown below, each layer in the Internet Protocol Suite corresponds to one or more layers of the OSI model.

Network Interface: The network interface layer is the equivalent of the OSI physical and data link layers as it defines the host's connection to the network. This layer comprises the hardware and software involved in the interchange of frames between computers. The technologies used can be LAN- based (e.g. Ethernet) or WAN-based (e.g. ISDN).

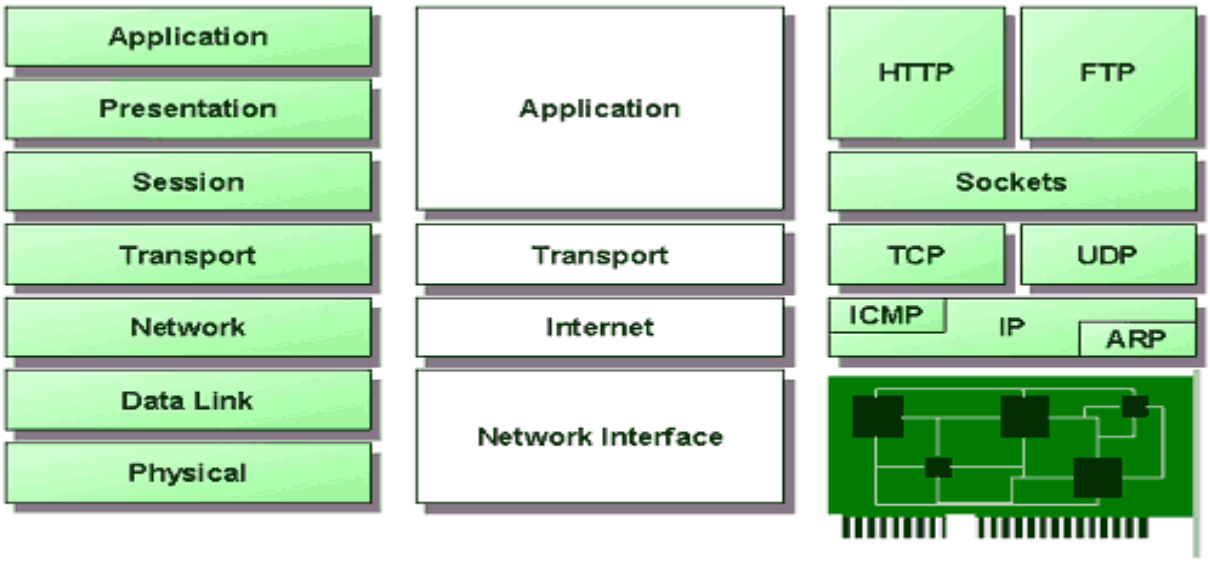
Internet Layer: The network layer uses a number of protocols to ensure the delivery of packets. These are described below:

> **IP (Internet Protocol) --** IP is the protocol responsible for addressing and routing packets (on the basis of routing algorithms) between networks. It ensures they reach the correct destination network.

ARP -- The Address Resolution Protocol (ARP) is responsible for obtaining hardware addresses and matching them to their IP address when the destination computer is on the same network.

ICMP -- The Internet Control Management Protocol (ICMP) is used to report errors and send messages about the delivery of a packet. It can also be used to test TCP/IP networks. Two examples of ICMP messages include:

- Destination unreachable - used when a router cannot locate the destination
- Time exceeded - used when the Time To Live (TTL) of a packet reaches zero



OSI and TCP/IP

Transport Layer: The transport layer provides communication between the source and destination computers, and breaks application layer information into packets. TCP/IP provides two methods of data delivery:

- Connection-orientated delivery using TCP

- Connectionless delivery using UDP

Application Layer: This is the layer at which many TCP/IP services (high level protocols) can be run (such as, FTP, HTTP and SMTP).

Introduction to Broadband Technology

Broadband is defined as a high bandwidth connection to the Internet. Broadband is easier and faster to use than the traditional telephone and modem as information can be sent and downloaded much quicker. It involves large volumes of information being carried at high speeds to your PC. This allows websites, text, graphics, music and videos to be experienced in real time. Broadband, therefore, has many features that can be taken advantage of in the home or office:

- The connection to the Internet is always on, allowing for constant Internet access and no need to dial up.
- The phone line is unaffected; this means that you can make telephone calls whilst the Internet is on.
- Websites, music and videos can be downloaded at a fast rate.
- You can receive uninterrupted real time services, such as Internet radio, streaming video and voice-over-ip, phone calls.

In general, broadband refers to telecommunication in which a wide band of frequencies is available to transmit information. Because a wide band of frequencies is available, information can be multiplexed and sent on many different frequencies or channels within the band concurrently, allowing more information to be transmitted in a given amount of time (much as more lanes on a highway allow more cars to travel on it at the same time).

Various definers of broadband have assigned a minimum data rate to the term. Here are a few:

- Newton's Telecom Dictionary: "...greater than a voice grade line of 3 KHz...some say [it should be at least] 20 KHz."
- Jupiter Communications: at least 256 Kbps.
- IBM Dictionary of Computing: A broadband channel is "6 MHz wide."

Types of Broadband Connections: Broadband includes several high-speed transmission technologies such as:

1) Digital Subscriber Line (DSL)
2) Cable Modem
3) Fiber
4) Wireless
5) Satellite
6) Broadband over Powerlines (BPL)

The broadband technology you choose will depend on a number of factors. These may include whether you are located in an urban or rural area, how broadband Internet access is packaged with other services (such as voice telephone and home entertainment), price, and availability.

Digital Subscriber Line (DSL) DSL is a wireline transmission technology that transmits data faster over traditional copper telephone lines already installed to homes and businesses. DSL-based broadband provides transmission speeds ranging from several hundred Kbps to millions of bits per second (Mbps). The availability and speed of your DSL service may depend on the distance from your home or business to the closest telephone company facility.
The following are types of DSL transmission technologies:

- **Asymmetrical Digital Subscriber Line (ADSL)** – Used primarily by residential customers, such as Internet surfers, who receive a lot of data but do not send much. ADSL typically provides faster speed in the downstream direction than the upstream direction.
- **Symmetrical Digital Subscriber Line (SDSL)** – Used typically by businesses for services such as video conferencing, which need significant bandwidth both upstream and downstream.

Faster forms of DSL typically available to businesses include:

- High data rate Digital Subscriber Line (HDSL); and
- Very High data rate Digital Subscriber Line (VDSL).

Cable Modem Cable modem service enables cable operators to provide broadband using the same coaxial cables that deliver pictures and sound to your TV set. Most cable modems are external devices that have two connections: one to the cable wall outlet, the other to a computer. They provide transmission speeds of 1.5 Mbps or more.
Subscribers can access their cable modem service by simply turning on their computers, without dialing-up an ISP. You can still watch cable TV while using it. Transmission speeds vary depending on the type of cable modem, cable network, and traffic load. Speeds are comparable to DSL.

Fiber Fiber optic technology converts electrical signals carrying data to light and sends the light through transparent glass fibers about the diameter of a human hair. Fiber transmits data at speeds far exceeding current DSL or cable modem speeds, typically by tens or even hundreds of Mbps.

The actual speed you experience will vary depending on a variety of factors, such as how close to your computer the service provider brings the fiber and how the service provider configures the service, including the amount of bandwidth used. The same fiber providing your broadband can also simultaneously deliver voice (VoIP) and video services, including video-on-demand.

Wireless Wireless broadband connects a home or business to the Internet using a radio link between the customer's location and the service provider's facility. Wireless broadband can be mobile or fixed.

Wireless technologies using longer-range directional equipment provide broadband service in remote or sparsely populated areas where DSL or cable modem service would be costly to provide. Speeds are generally comparable to DSL and cable modem. An external antenna is usually required.

Satellite Just as satellites orbiting the earth provide necessary links for telephone and television service, they can also provide links for broadband. Satellite broadband is another form of wireless broadband, and is also useful for serving remote or sparsely populated areas.

Downstream and upstream speeds for satellite broadband depend on several factors, including the provider and service package purchased, the consumer's line of sight to the orbiting satellite, and the weather. Typically a consumer can expect to receive (download) at a speed of about 500 Kbps and send (upload) at a speed of about 80 Kbps. These speeds may be slower than DSL and cable modem, but they are about 10 times faster than the download speed with dial-up Internet access. Service can be disrupted in extreme weather conditions.

Software Agents

E-commerce is changing the way business is being done in the Information Age. The **software agents** act on behalf of their human users/organizations to perform information gathering tasks, such as locating and accessing information from various sources, filtering unwanted information, and providing decision support.

Example of Information Overload: *The information overload can be illustrated with the example of Sun Microsystems which reports that employees receive on an average over 100 e-mail messages a day. For Sun, that is a million and a quarter messages a day. The content of the Web grows by an estimated 170.000 pages daily. Also, surveys of data warehouse projects reveal that a number of the larger retail and telecommunications companies have multiple terabyte databases.*

A software agent can be defined as one that acts or exerts power. It can be an autonomous, (preferably) intelligent, collaborative, adaptive, computational entity. Software agents have synonyms including knowbots (i.e. knowledge-based robots), softbots (software robots).

A major advantage of employing software agents with intranet, the Internet, and extranet applications is that they are able to assist in locating and filtering all the data. They save time by making decisions about what is relevant to the user. They are able to sort through the network and the various databases effortlessly and with unswerving attention to detail to extract the best data.

To date, the list of tasks to which commercially available agents and research prototypes have been applied includes advising, alerting, broadcasting, browsing, critiquing, distributing, enlisting, empowering, explaining, filtering, guiding, identifying, matching, monitoring,

navigating, negotiating, organizing, presenting, querying, reminding, reporting, retrieving, scheduling, searching, securing, soliciting, sorting, storing, suggesting, summarizing, teaching, translating, and watching.

On the whole, the software agents make the networked world less forbidding, save time by reducing the effort required to locate and retrieve data, and improve productivity by offloading a variety of tedious and mindless tasks.

A Typology of Agents (Classification): The agents may be classified by their mobility, i.e. by their ability to move around some networks. They can thus be called **static** or **(dynamic)** mobile agents.

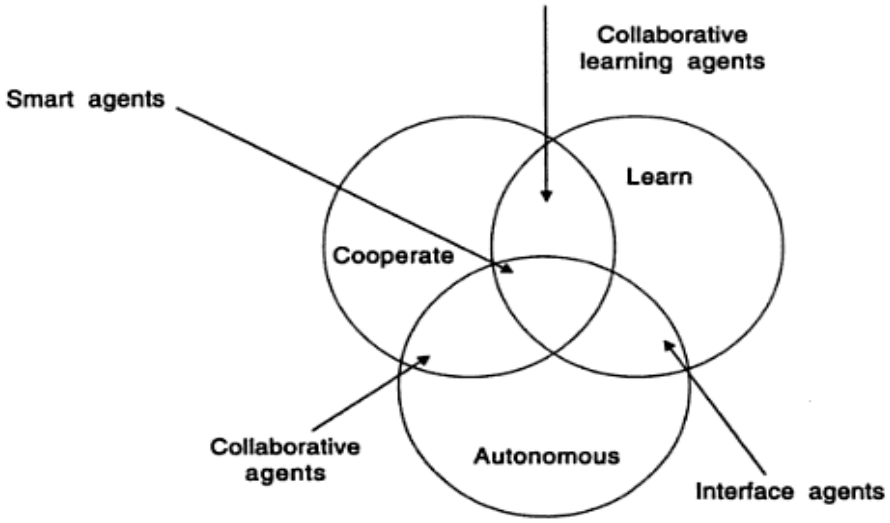


Fig. 3.9 A partial view of agent typology.

The static and dynamic agents may be classified along several attributes. Some of the attributes are: **autonomy, learning and cooperation** as shown in figure above. **Autonomy** refers to the principle that agents can operate on their own without any need for human guidance, even though this would sometimes be invaluable. In order to **cooperate**, agents need to possess a social ability. i.e. the ability to interact with other agents and possibly humans via some communication language. Lastly, for agent systems to be only smart, they would have to **learn** as they react and/or interact with their external environment.