Introduction to Information Security

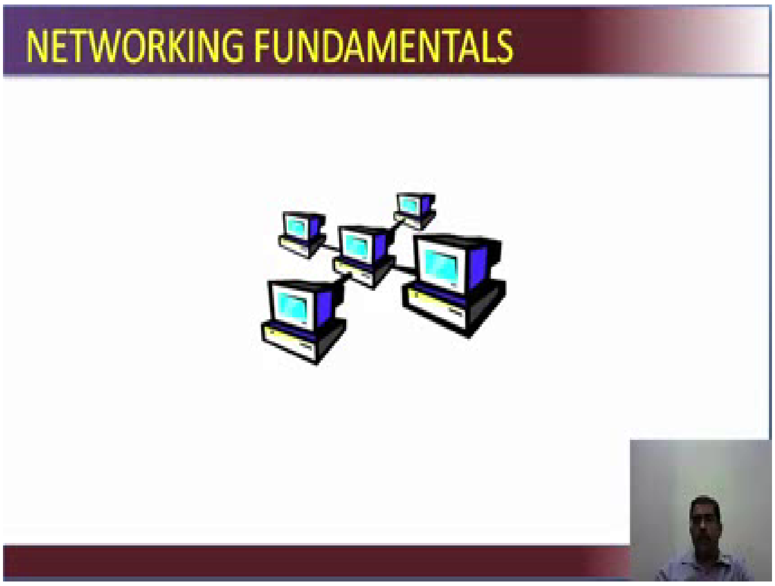
Prof. Dilip H. Ayyar

Department of Computer Science and Engineering

Indian Institute of Technology, Madras

Lecture – 43

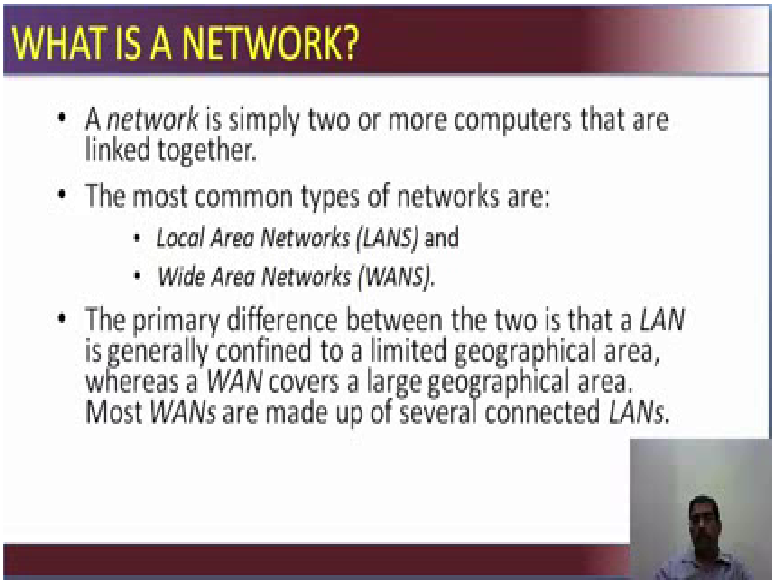
(Refer Slide Time: 00:11)



NETWORKING FUNDAMENTALS

After bit of cryptography, we will move on to fundamentals of networking. I suggest that you if you are not aware of the fundamentals of networking go to Google learn about ports, protocol, the kind of networks, you can study in depth of the security network, security networking aspects, also how routing works, what is the firewall we will go through all the fundamentals of these in this session, but I would suggest that you do deeper reading to have a strong foundation of what a network is.

(Refer Slide Time: 00:51)

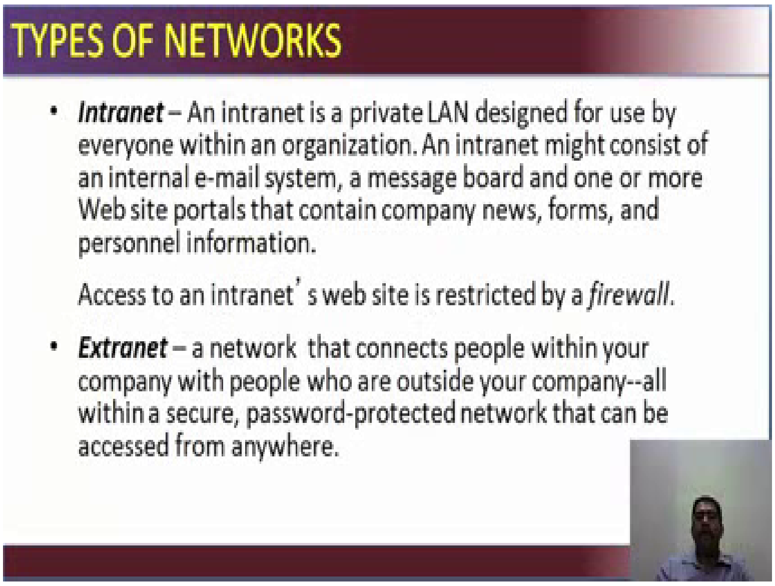


WHAT IS A NETWORK?

- A *network* is simply two or more computers that are linked together.
- The most common types of networks are:
  - *Local Area Networks (LANS)* and
  - *Wide Area Networks (WANS).*
- The primary difference between the two is that a *LAN* is generally confined to a limited geographical area, whereas a *WAN* covers a large geographical area. Most *WANs* are made up of several connected *LANs.*

So, what is a network, it is simply two or more computers connected together or link together using some form of communication media. The most common types of LAN and WAN; so most of you are would have heard about LAN and WAN. The primary difference between the two is the LAN is generally restricted to a limited area or limited geographical area; whereas, a WAN covers a large geographical area; most WANs are made up of several interconnected of several connected LANs.

(Refer Slide Time: 01:26)



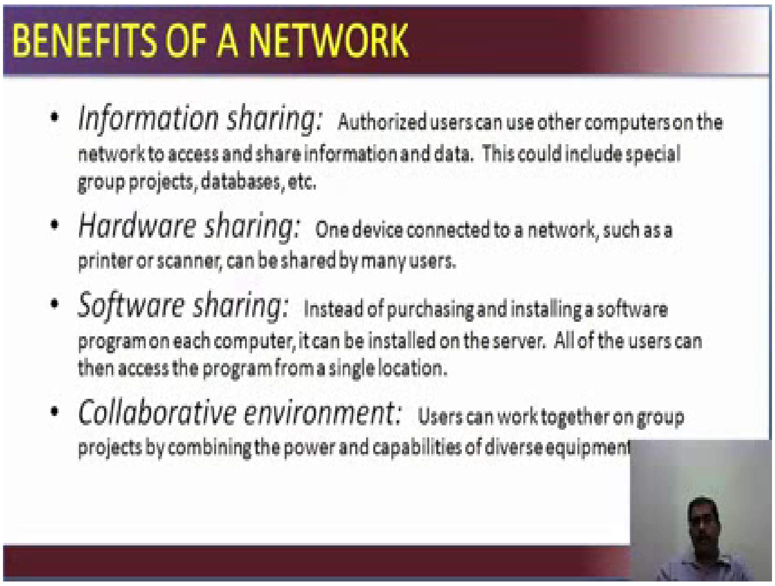
TYPES OF NETWORKS

- ***Intranet*** – An intranet is a private LAN designed for use by everyone within an organization. An intranet might consist of an internal e-mail system, a message board and one or more Web site portals that contain company news, forms, and personnel information.

  Access to an intranet' s web site is restricted by a *firewall.*
- ***Extranet*** – a network that connects people within your company with people who are outside your company--all within a secure, password-protected network that can be accessed from anywhere.

Then you have intranet and extranet; intranet is a private LAN designed for use by everyone within an organisation. An intranet may consist of an internal e- mail system, a file server, a message board, a print server and one or two web site portals which have information about the company, news, company news, forms, HR system and access to intranets web site is generally restricted by the use of firewall. Extranet is a network that connects people within your organisation with people who are outside your organisation, like your vendors, consultants, auditors all within a secure password protected network that can be accessed from anywhere.

(Refer Slide Time: 02:19)



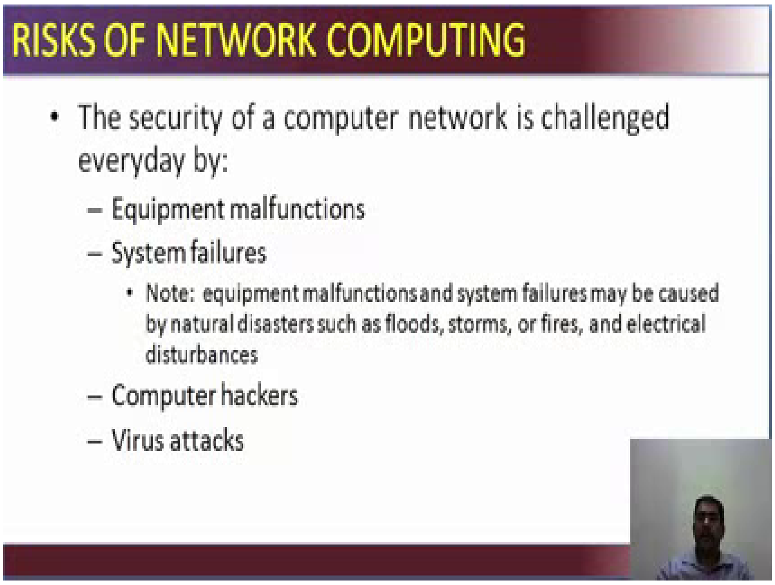
BENEFITS OF A NETWORK

- *Information sharing:* Authorized users can use other computers on the network to access and share information and data. This could include special group projects, databases, etc.
- *Hardware sharing:* One device connected to a network, such as a printer or scanner, can be shared by many users.
- *Software sharing:* Instead of purchasing and installing a software program on each computer, it can be installed on the server. All of the users can then access the program from a single location.
- *Collaborative environment:* Users can work together on group projects by combining the power and capabilities of diverse equipment

What are the benefits of a network of having a network. One is information sharing authorised users can use computers on the network to access and share information and data. This could include special group projects databases etcetera. So, you take a example of accounting package, tally is used where several people or several peoples in the accounts departments can access, update the accounts details, share the account details. Then hardware sharing - one device is connected to a network such as a printer or scanner can be shared by many users, so one device which is connected to a network. So, it can be a scanner, it can be a printer, it can be any other, it can be a SAN, storage area network, it is connected on the network and it can be shared by different users. Take the example of file server file server is connected on the network people can collaborate share files with each other.

Then software sharing - instead of purchasing and installing a software program on each computer, it can be installed on the server itself; all of the users can then access the program from a single location. So, it is similar to the example or it is same as having tally installed where all the accounts need to be cared and viewed. It can be a Microsoft office suite or you can say other softwares which required or which is required by different users within the organisation. Then collaborative environment - users can work together on group projects by combining the power and capabilities of different diverse equipments.

(Refer Slide Time: 04:08)

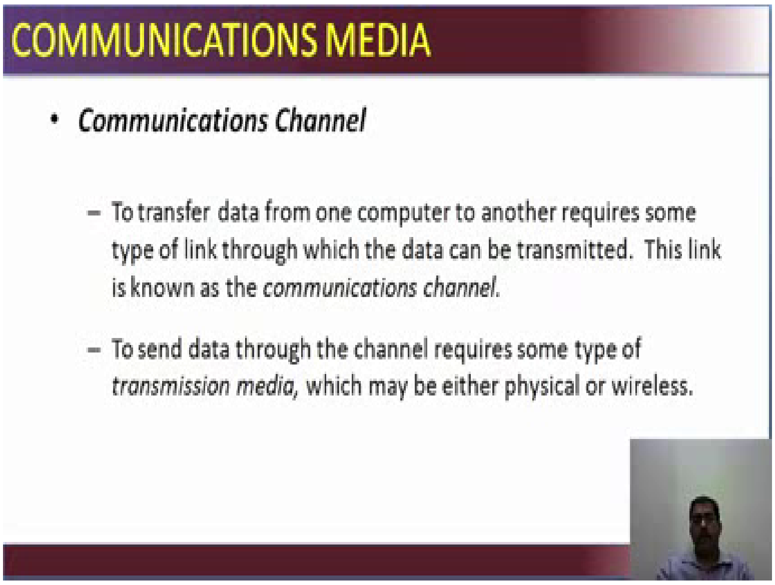


RISKS OF NETWORK COMPUTING

- The security of a computer network is challenged everyday by:
  - Equipment malfunctions
  - System failures
    - Note: equipment malfunctions and system failures may be caused by natural disasters such as floods, storms, or fires, and electrical disturbances
  - Computer hackers
  - Virus attacks

But then with great power comes it great responsibility also. In the words of Stanley whose is the creator of superman, I am sorry Spiderman. The risk of network computing is the security of a computer network is challenged everyday by equipment malfunctions, the server may be stop working. The printing may stop working, they can be system failures, they can be hard disk failure, it can be caused by a natural disasters, it can be because of not connecting the equipment to uninterrupted power supply. It can be the because of computer hackers, it can also be the because of the virus or malware attacks. So, any of the reason can be a cause for network downtime. So, bigger a network the more protection mechanism we have to put to safeguard from different kinds attacks, different kinds of failures.

(Refer Slide Time: 05:17)

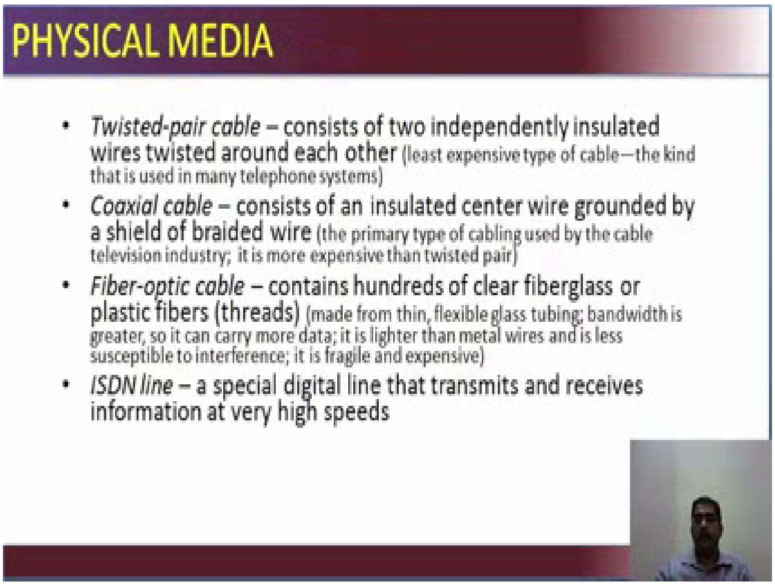


COMMUNICATIONS MEDIA

- *Communications Channel*
  - To transfer data from one computer to another requires some type of link through which the data can be transmitted. This link is known as the *communications channel.*
  - To send data through the channel requires some type of *transmission media,* which may be either physical or wireless.

Then we will move on the communication media or communication channel is to transfer data from one computer to another, which requires some type of link through which the data can be transferred, this link is known as the communications channel. Your RJ45 cables are communication channel; your RJ11 which is a telephone cable is a communication channel. So, to send data through the channel requires some type of transmission media. So, your media itself with cable itself media, the channel is within the media you transmit data, you transmit voice, you transmit video, and this media can be a physical or wireless.

(Refer Slide Time: 06:01)

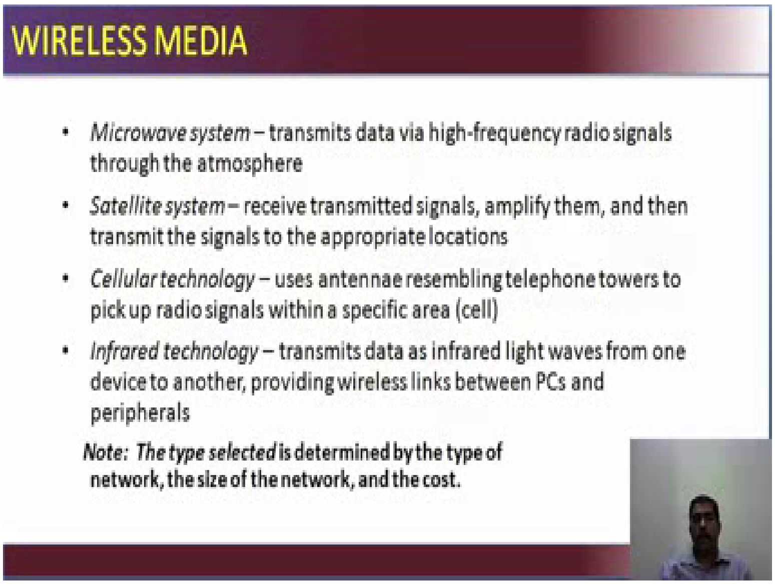


PHYSICAL MEDIA

- *Twisted-pair cable* – consists of two independently insulated wires twisted around each other (least expensive type of cable—the kind that is used in many telephone systems)
- *Coaxial cable* – consists of an insulated center wire grounded by a shield of braided wire (the primary type of cabling used by the cable television industry; it is more expensive than twisted pair)
- *Fiber-optic cable* – contains hundreds of clear fiberglass or plastic fibers (threads) (made from thin, flexible glass tubing; bandwidth is greater, so it can carry more data; it is lighter than metal wires and is less susceptible to interference; it is fragile and expensive)
- *ISDN line* – a special digital line that transmits and receives information at very high speeds

Look at physical media, there are different kinds here, coaxial cable, twisted pair, fibre optics, ISDN lines. The twisted-pair cable consists of two independently insulated wires twisted around each other; this is the least expensive kind of cable, the kind that is used in many telephone systems. So, I mentioned RJ11, RJ11 is the cable which is used to connecting telephone instruments or the telephone line that comes into your building. Then coaxial cable is consists of an insulated centre wire grounded by a shield of braided wire; this is your cable that the cable connects a setup box or which is directly used to connect with a television, but this is a little more expensive than the twisted pair. Then you have fibre optic cable, which consists of hundreds of clear fibreglass or plastic fibres or threads, which is the latest or which is the media which is used more frequently nowadays, where the data transmission is much more faster. Then there is a kind called UTP which is unshielded twisted pair which is used in your ethernetcables. Then there is ISDN line which is a special kind of digital line that transmits and receives information at very high speeds. So the ISDN lines are also more expensive.

(Refer Slide Time: 07:37)



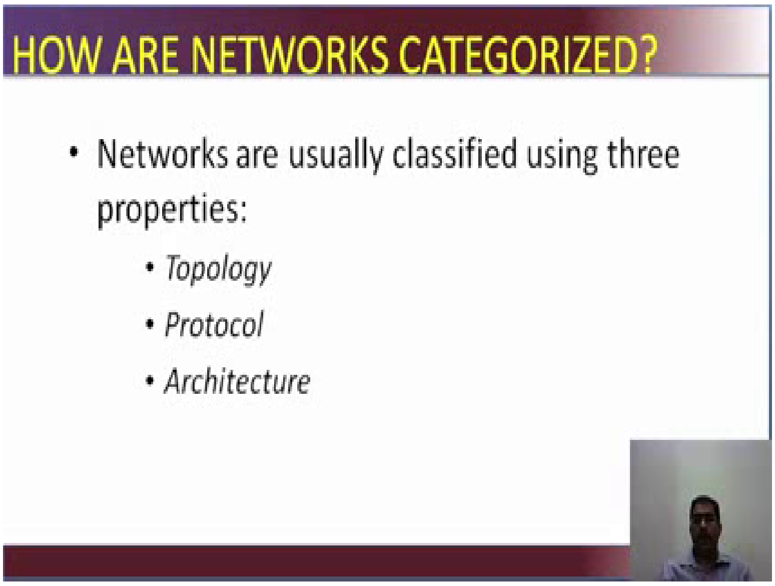
WIRELESS MEDIA

- *Microwave system* – transmits data via high-frequency radio signals through the atmosphere
- *Satellite system* – receive transmitted signals, amplify them, and then transmit the signals to the appropriate locations
- *Cellular technology* – uses antennae resembling telephone towers to pick up radio signals within a specific area (cell)
- *Infrared technology* – transmits data as infrared light waves from one device to another, providing wireless links between PCs and peripherals

Note: *The type selected* is determined by the type of network, the size of the network, and the cost.

There are wireless media also like a microwave system; it transmits data via high frequency radio signals through the atmosphere, through the air. Then the satellite system which receive transmitted signals, amplify them and then retransmit the signals to the appropriate locations. Cellular technology just the one's we use in the mobile phone; it uses an antennae resembling telephone towers to pick up radio signals within a specific area or a cell, let say it is called a cell tower. Infrared technology which transmits data as infrared light waves from one device to another, providing wireless links between PCs and peripherals. Again what a point we know here is the type selected is determined by the type of network, the size of the network and the cost that the company is ready to put in.

(Refer Slide Time: 08:34)

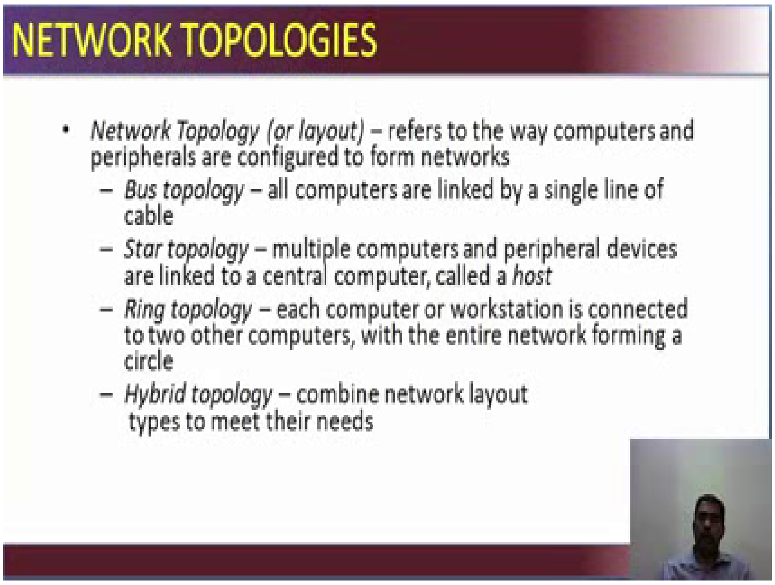


HOW ARE NETWORKS CATEGORIZED?

- Networks are usually classified using three properties:
  - *Topology*
  - *Protocol*
  - *Architecture*

How are the networks categorized, they are classified using three properties, based on the topology, based on the protocols and based on the architecture.

(Refer Slide Time: 08:48)

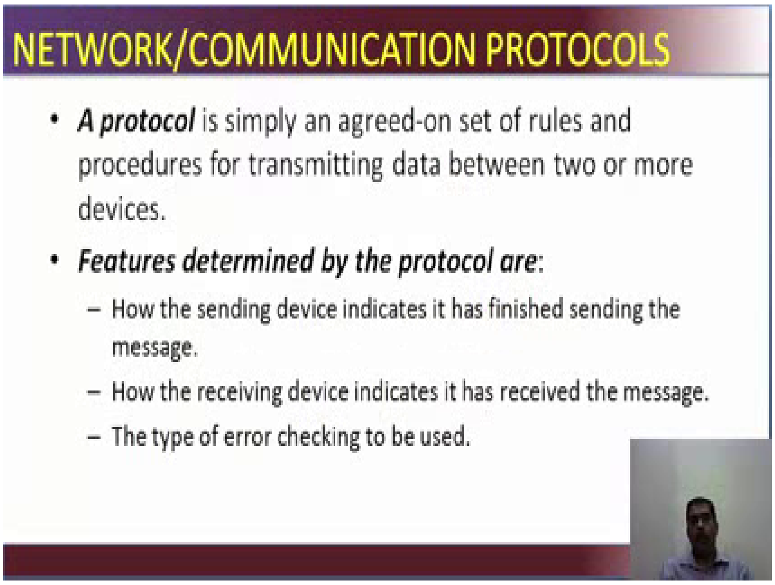


NETWORK TOPOLOGIES

- *Network Topology (or layout)* – refers to the way computers and peripherals are configured to form networks
  - *Bus topology* – all computers are linked by a single line of cable
  - *Star topology* – multiple computers and peripheral devices are linked to a central computer, called a *host*
  - *Ring topology* – each computer or workstation is connected to two other computers, with the entire network forming a circle
  - *Hybrid topology* – combine network layout types to meet their needs

We will look at all of these. Topology is nothing but a layout which refers to the way computers and peripherals are configured to form the networks. There are different kinds of topologies of network. The older one are the bus topology where in all the computers are linked by a single line of cable. The problem with this was if where is the loose connection or if a one computer fails then all the other computer also used to fails. Then there was ring topology - the second one, where each computer or workstation is connected to two other computers with the entire network forming a circle. Here also then was a problem. Then came the star topology which is widely used now where multiple computers and peripheral devices are linked to a central computer called a host, so it is like a server and clients. Then you have the hybrid topology where with combine network layout types of meet their needs of the organisation.

(Refer Slide Time: 09:49)

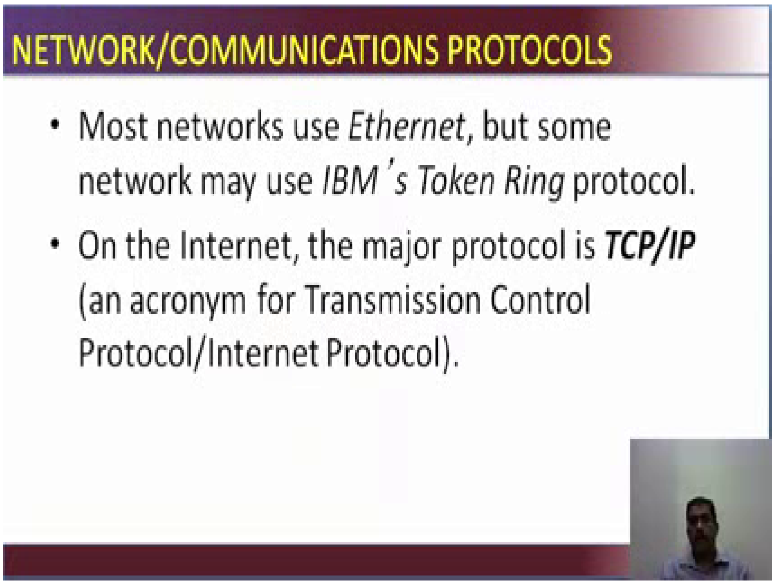


NETWORK/COMMUNICATION PROTOCOLS

- ***A protocol*** is simply an agreed-on set of rules and procedures for transmitting data between two or more devices.
- ***Features determined by the protocol are***:
  - How the sending device indicates it has finished sending the message.
  - How the receiving device indicates it has received the message.
  - The type of error checking to be used.

What is a protocol, a protocol is simply an agreed set of rules and procedures for transmitting data between two or more devices. In simple terms, the rule of communication is called a protocol. What a computer can do to communicate is determined by what a protocol is. Now what are the features determined by the protocol, how the sending device indicated it has finished sending the message, how the receiving device indicate that it has received the message, and what is the type of error checking that has been done. Again this is what these are the basics of what are the protocol is or the definition of protocol. You can Google it and find more or have in depth information about what protocol is and how they communicate, what are the different kinds of protocol, what are the common protocols we will of course go through in the coming slides.

(Refer Slide Time: 10:53)

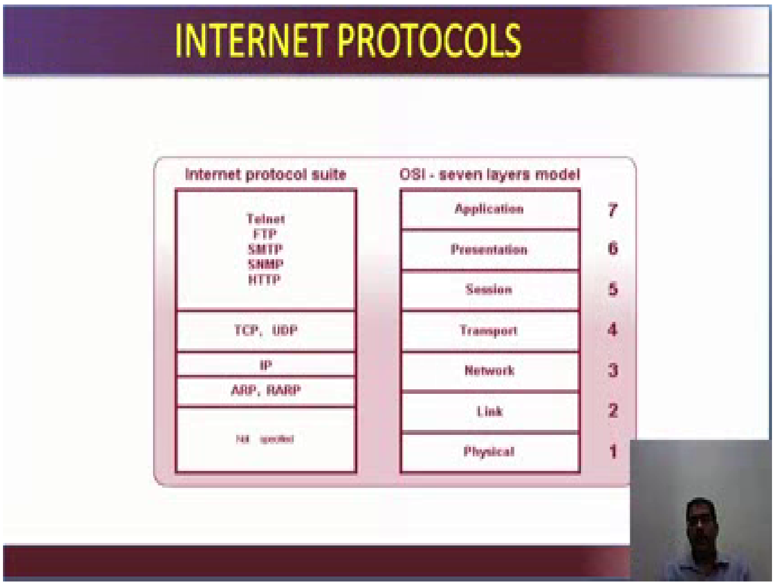


NETWORK/COMMUNICATIONS PROTOCOLS

- Most networks use *Ethernet*, but some network may use *IBM's Token Ring* protocol.
- On the Internet, the major protocol is ***TCP/IP*** (an acronym for Transmission Control Protocol/Internet Protocol).

Most of the computers use Ethernet, but some network one may use IBMs token ring protocol. When you see the internet, the major protocol is TCP IP - transmission control protocol internet protocol. An acronym is transmission control protocol, internet protocol for TCP I P.

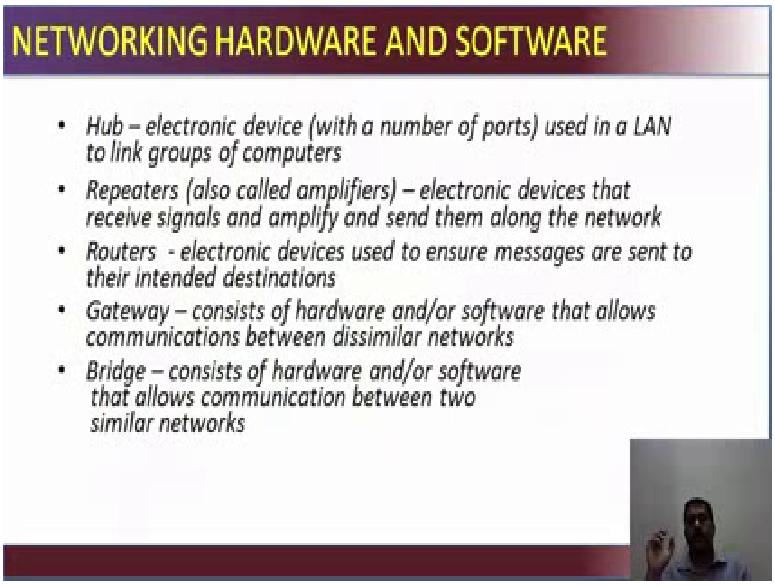
(Refer Slide Time: 11:14)



INTERNET PROTOCOLS

There are different kinds of protocol protocols internet protocols. You have if you see the OSI layer, which is a seven layer model, which starts from the physical and goes on to application. Here in your internet protocol shows several of the protocol sit be different layer of the internet protocol suite and some of the examples are given file transfer protocol FTP. The first one is telnet; the second one is file transfer protocol, simple network transfer protocol, the message transfer protocol, hypertext transfer protocol. If you notice all these are called protocols. TCP - transmission control protocol, UDP - user data card protocol; IP is internet protocol; ARP is address resolution protocol which is used for converting IP address to hardware addresses ARP, RARP does the reverse. So, there are different kinds of protocol used in different purposes. Now HTTP is used of browsing, SNMP is for monitoring device, SNTP is sending your mails, messages; FTP is a file transfer. Telnet is use to connect a router, firewall, server, different kinds of devices. ARP is an function where the IP address is converted to MAC address so that the computer can understand.

(Refer Slide Time: 12:55)

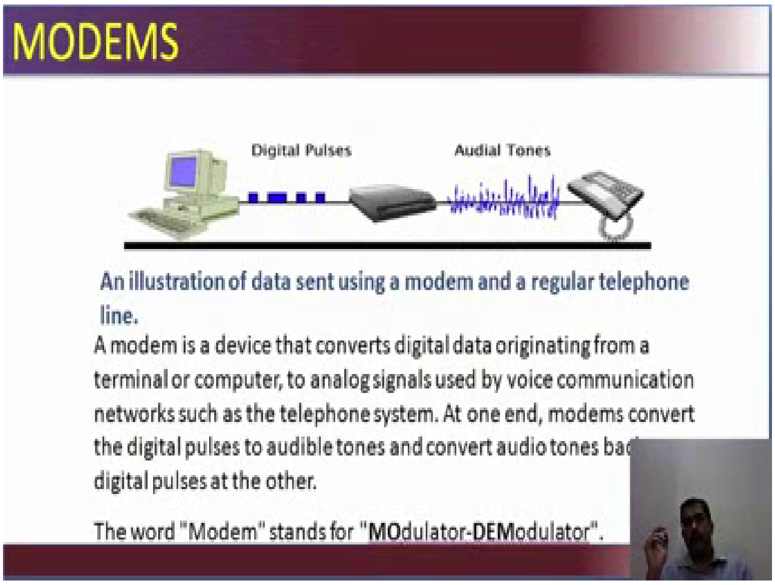


NETWORKING HARDWARE AND SOFTWARE

- *Hub – electronic device (with a number of ports) used in a LAN to link groups of computers*
- *Repeaters (also called amplifiers) – electronic devices that receive signals and amplify and send them along the network*
- *Routers - electronic devices used to ensure messages are sent to their intended destinations*
- *Gateway – consists of hardware and/or software that allows communications between dissimilar networks*
- *Bridge – consists of hardware and/or software that allows communication between two similar networks*

There are several devices used in Tel networking. Hub is an electronic device with a number of ports which is used in a LAN to link groups of computers. Repeaters they also called amplifiers, it is a whole implementation because networks were limited to a certain distance, because of the topology and the media used. Then routers are the devices used to ensure the messages are sent to their intended destinations. Gateways are the hardware and or software that allows communications between dissimilar networks. Bridges are hardware or and or software that allows communication between two similar networks.

(Refer Slide Time: 13:46)



MODEMS

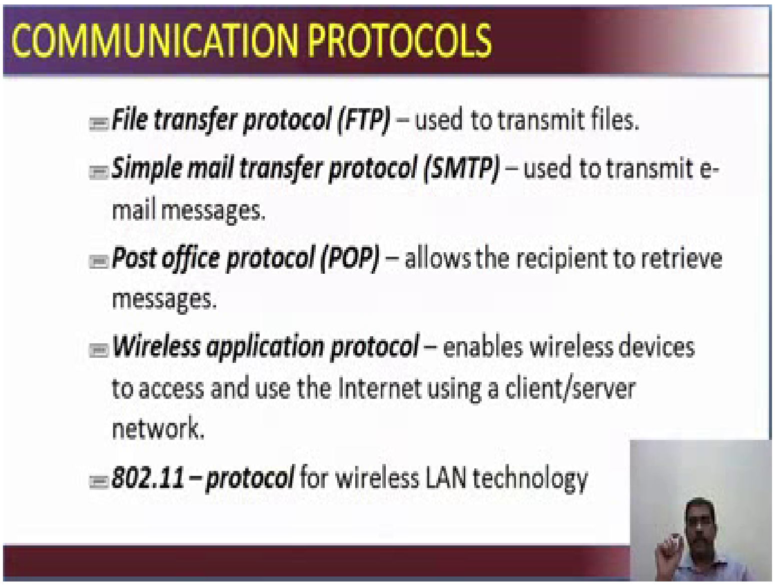
An illustration of data sent using a modem and a regular telephone line.

A modem is a device that converts digital data originating from a terminal or computer, to analog signals used by voice communication networks such as the telephone system. At one end, modems convert the digital pulses to audible tones and convert audio tones bac digital pulses at the other.

The word "Modem" stands for "MOdulator-DEModulator".

Then you have modulators demodulators which are also called modems. The basic purpose of a modem is to convert the digital pulse to analogue pulse and transmit over the wire. So this is a simple example of how the modem works. A modem is a device that converts a digital data originating from a terminal to analog signal used by voice communication networks such as the telephone this. At one end modems convert the digital pulses to audible tonnes, and convert the audio tones back to digital pulses at the other end. So, the word modem stands for modulator demodulator.

(Refer Slide Time: 14:32)

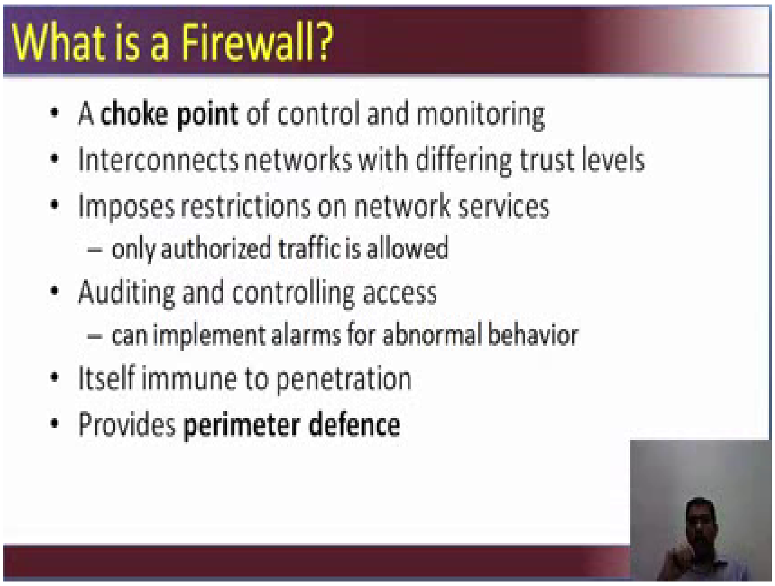


COMMUNICATION PROTOCOLS

- ***File transfer protocol (FTP)*** – used to transmit files.
- ***Simple mail transfer protocol (SMTP)*** – used to transmit e-mail messages.
- ***Post office protocol (POP)*** – allows the recipient to retrieve messages.
- ***Wireless application protocol*** – enables wireless devices to access and use the Internet using a client/server network.
- ***802.11 – protocol*** for wireless LAN technology

We have seen some of the protocol in the internet protocol group. FTP stands for file transfer protocol for uploading, downloading files. SMPT is simple mail transfer protocol used for transmitting email messages; POP is again use of mails which allows the recipient to retrieve messages on the server. Wireless application protocol enables wireless devices to access the network using a client server architecture, and 802.11 is the protocol for wireless LAN technology.

(Refer Slide Time: 15:10)

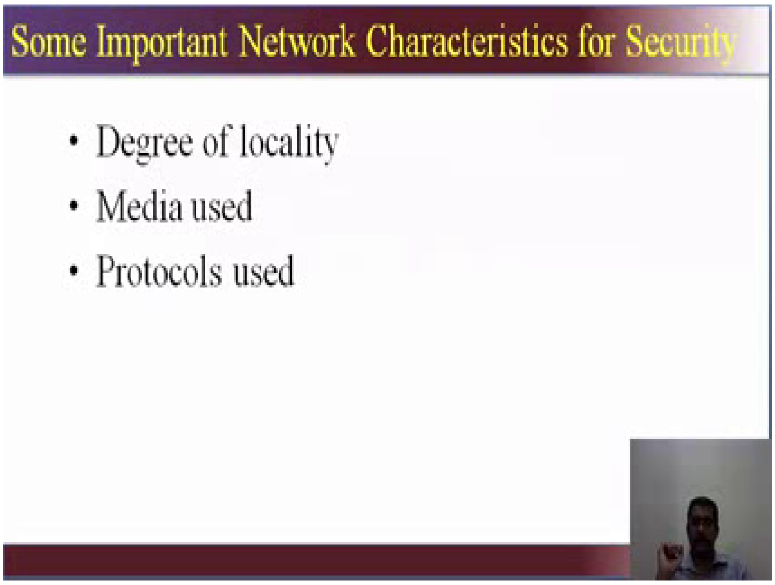


What is a Firewall?

- A **choke point** of control and monitoring
- Interconnects networks with differing trust levels
- Imposes restrictions on network services
  - only authorized traffic is allowed
- Auditing and controlling access
  - can implement alarms for abnormal behavior
- Itself immune to penetration
- Provides **perimeter defence**

So, all the basic details we are covering. So, now, let see what is a firewall, firewall is a choke point or something that controls the ingress and eggress to and from the network. It is also used for monitoring, it interconnects networks with differing trust levels meaning I allow services of only HTTP to network a, but I allow is services of FTP and HTTP and SSH to network b. So, this imposes restrictions on network services; that means, only authorized traffic or only the allowed what is supposed to come in, what is configured to come in only will come in. Then it also has capability of auditing and controlling the access to the network. It can also implement alarms for abnormal behaviour. So, now a days you have something called UTM device uniform threat management which consist of your firewall, your router, your IDR, your IP address your IP address email gateways, all these put together in one box. So, it itself immune to penetration and it provides perimeter defence. So, basically it provides defence at the edge of a network or the place, where your network exits your internal network and goes to an external network.

(Refer Slide Time: 16:39)

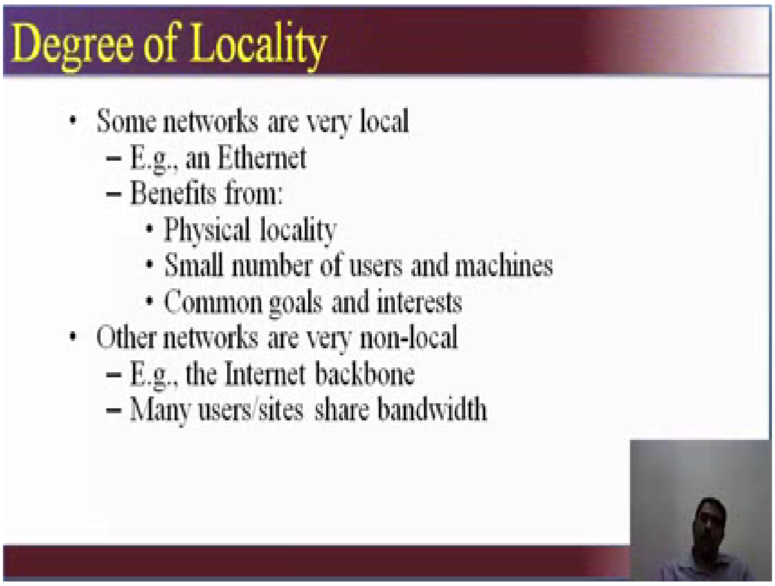


Some Important Network Characteristics for Security

- Degree of locality
- Media used
- Protocols used

When you take security consideration, what are the important characteristics of a network that is a degree of locality, media used and the protocol used.

(Refer Slide Time: 16:54)

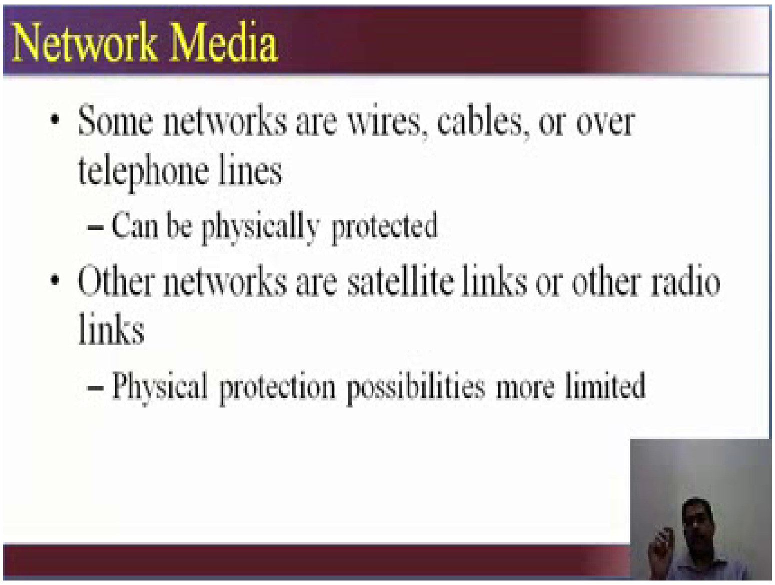


Degree of Locality

- Some networks are very local
  - E.g., an Ethernet
  - Benefits from:
    - Physical locality
    - Small number of users and machines
    - Common goals and interests
- Other networks are very non-local
  - E.g., the Internet backbone
  - Many users/sites share bandwidth

Let see the the three; degree of locality means some networks are very local, meaning it is confine to a specific physical area, and there only a small number users and machines are there, which have a common goals and interest. All our windows system all views specific software controlling the business and all websites within the same office premises so that is a degree of locality. And there are other networks which are very non local, example the internet backbone, which consist of several servers hosted in different geographical area within the world; many users access it, many users from different area different countries accesses, they share bandwidth. So, degree of locality becomes what kind of network is used. If you see a e-commerce site, there are several millions of subscribers who will coming for let say for a book or subscribing the service on the network, these subscribers may be some may be from India, some may be from Russia, some may be from US. So, share the bandwidth to access in file share the bandwidth in the sense to different parts they come in, but the resources they are accessing is the same. So, the degree of locality determines the type of network which are used.

(Refer Slide Time: 18:24)

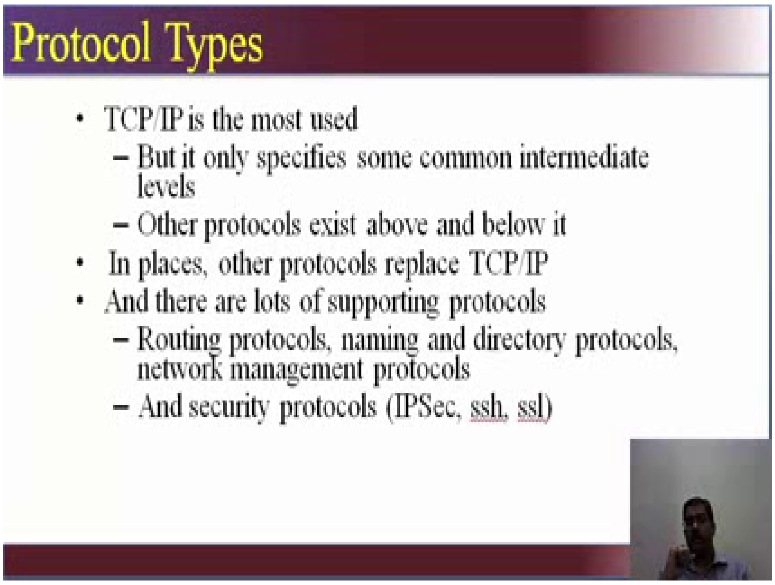


Network Media

- Some networks are wires, cables, or over telephone lines
  - Can be physically protected
- Other networks are satellite links or other radio links
  - Physical protection possibilities more limited

We have spoken little bit of media. Some networks are wires, cables or over telephone lines, they can be physically protected. When we talk about media, when it comes to wire, when it comes to cables or when it comes to telephone lines within the organisation domains it can be physically protected, it can be made tamper proof. But then the wireless technology, we are saying 4 or 5 like your satellite links or other radio links it is difficult to provide physical protections for these devices, you may be able to protect device itself, but not the data they have to sending out and receiving in.

(Refer Slide Time: 19:05)



Protocol Types

- TCP/IP is the most used
  - But it only specifies some common intermediate levels
  - Other protocols exist above and below it
- In places, other protocols replace TCP/IP
- And there are lots of supporting protocols
  - Routing protocols, naming and directory protocols, network management protocols
  - And security protocols (IPSec, ssh, ssl)

Then the protocol types TCP IP is the most used, but it only specifies some common intermediate levels, other protocols also exist above and below it TCP. in some places other protocols are replace TCP IP, and then there are lots of supporting protocols they are routing protocols, naming protocols, directory protocols, network management protocols then you have security protocols which is IP Sec ssh ssl. To understand the basic TCP the three ways handshake how it establishes a communication domain to server we will look at in the coming slide.