Telephone Networks

A **telephone network** is a telecommunications network used for telephone calls between two or more parties.

There are a number of different types of telephone network:

- A fixed line network where the telephones must be directly wired into a single telephone exchange. This is known as the public switched telephone network or PSTN.
- A wireless network where the telephones are mobile and can move around anywhere within the coverage area.
- A private network where a closed group of telephones are connected primarily to each other and use a gateway to reach the outside world. This is usually used inside companies and call centers and is called a private branch exchange (PBX).

Basic Concepts

The most familiar component of a telephone network is the telephone set provided for each user. It is a relatively simple device which can exchange control signals with the network to help establish and release calls, and to send and receive a user’s speech signal.

Users are referred to as **subscribers**, because they subscribe to a service provided by the telephone company. Typically, many subscribers are attached to the same network, and each subscriber can contact every other subscriber. The system employs **switches** to facilitate connections between subscribers. The arrangement of switches and subscribers and the interconnections between them determines the structure of the network.

To better understand how the system works, we will begin by looking at a very simple network.

A Simple Network

Consider a small community of 100 families. The communication needs of this community can be served by one switch, to which every family (or subscriber) is directly connected (see Figure 10.1). The circuit which connects each subscriber (via a pair of wires) to the switch is called a **subscriber loop**. The switch itself is called a **local exchange** (local because the connection is direct).

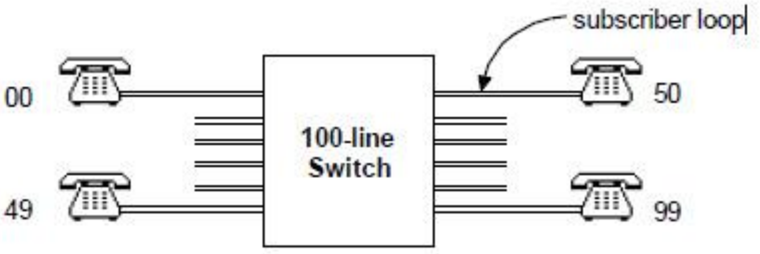


Figure 1. Single switch network.

A numbering scheme is used to uniquely identify each subscriber and to gather call-related information for billing purposes. In this case, a two-digit number would suffice (i.e., 00-99). When a subscriber dials the number of another subscriber, the switch follows a sequence of steps for establishing a communication path between the two subscribers. Provided the destination number is not engaged, a connection is guaranteed.

Now suppose that there is a similar community with its own local exchange, and that we wish to provide phone access between the two communities. To do this, the two exchanges are connected using a set of interexchange lines called **trunk lines** (see Figure 10.2). In practice, it is unlikely that all of the subscribers in one community would want to simultaneously contact subscribers in the other community. If we establish that at most say six subscribers are likely to call the other community, then six trunk lines will be sufficient.

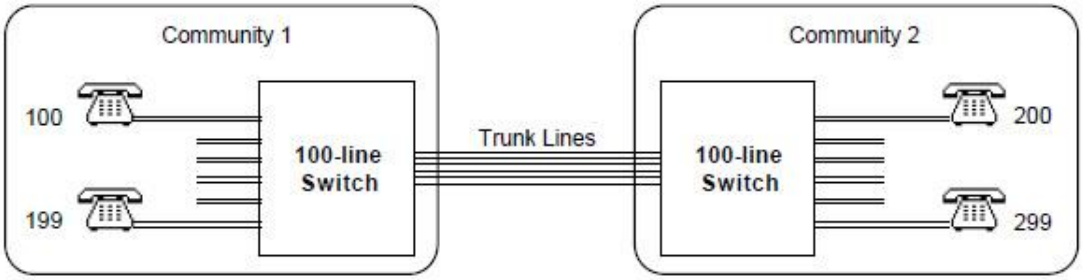


Figure 2. A network with two switches

The numbering scheme is expanded to take into account the above changes. Each subscriber is now allocated a three digit number. The first digit identifies the exchange (say 1 for the first community and 2 for the second community) and the next two digits identify a subscriber in that community as before. When a subscriber dials a number, the local exchange looks at the first digit of the number. If it matches its own number then it treats the remaining two digits as for a subscriber on the same exchange, and attempts to establish a direct connection between the two as before. If the first digit identifies the other exchange, then it uses one of the trunk lines to inform the other switch of the call and passes to it the two remaining digits. The two switches then cooperate to establish a call between the two subscribers. If more than six subscribers attempt to simultaneously call subscribers on the other exchange, the seventh call and beyond will be blocked due to insufficient trunk lines.

Hierarchical network

Figure 10.4 Hierarchical networks illustrate the North American hierarchical network configuration. It is made up of five classes of exchanges. A class 1 exchange represents a regional center and has the highest order in the hierarchy. A class 5 exchange represents an end office (local exchange) and has the lowest order in the hierarchy. Solid lines represent main trunk lines between exchanges. Dashed lines represent **high usage trunk** lines and can be established between any two exchanges, regardless of their levels in the hierarchy. Should the high usage trunks reach their maximum capacity, additional traffic is overflowed to the main trunks, from which further overflow is permitted. Because of this, the latter is also referred to as the **final route**.

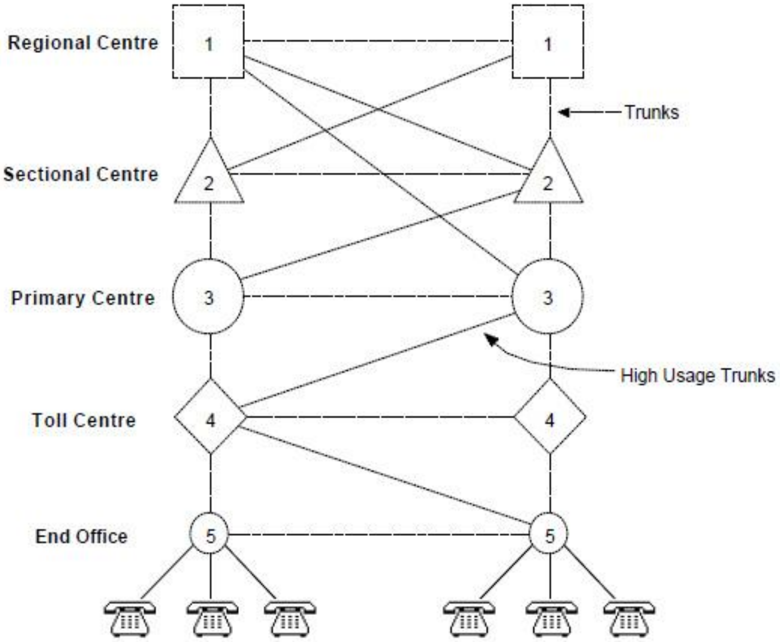


Figure 10.4 Hierarchical network

Switching Systems

Early telephone switches were **electromechanical**, many of which are still in use. They are so named because they use electromechanical relays to perform switching functions. The relays respond to the dial pulses from subscriber phones, and hence activate connections.

Existing electromechanical switches are of two types: step-by-step and crossbar. A **step-by-step switch** (also called Strowger after its inventor) uses step relays capable of assuming ten separate levels, to represent a decimal digit. For example, each of the two switches in **Figure 10.5** would consist of two banks of relays, arranged in a tree-like fashion. **Figure 10.5** illustrates how an incoming call to a subscriber whose number is 16 is connected.

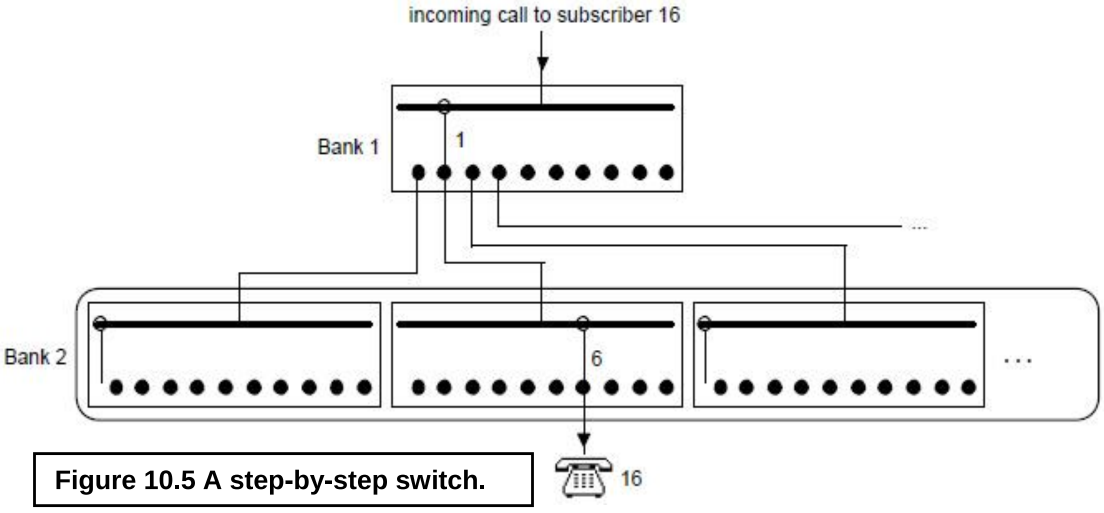
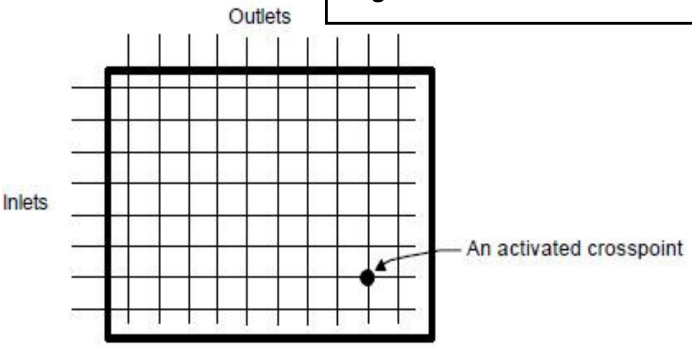


Figure 10.5 A step-by-step switch.

A **crossbar switch** consists of a matrix of crosspoints between rows of inlets and columns of outlets. Activating the relay of an inlet and the relay of an outlet causes the crosspoint at which they overlap to be activated and therefore result in a physical connection (see **Figure 10.6**).

Figure 10.6 A crossbar switch.



Modern switches are microprocessor controlled and use digital switching technology. They are generally referred to as **Stored Program Control** (SPC) switches. Unlike electromechanical switches which are inherently hardwired and therefore inflexible, SPC switches achieve significant flexibility by using programmable logic. Because there are no moving parts involved, connections can be established orders of magnitude faster. Furthermore, the functions of the switch can be reconfigured through software (even remotely). Software control has facilitated the introduction of many new service features which were previously beyond the scope of electromechanical switches

Transmission Characteristics

The basic transmission characteristics of a given medium are of primary importance. Those characteristics include bandwidth, or capacity, error performance, and distance between network elements. These three dimensions of a transmission system, in combination, dictate effective *throughput*, the amount of information that can be put through the system.

Bandwidth, in this context, refers to the raw amount of bandwidth the medium supports. *Error performance* refers to the number or percentage of errors which are introduced in the process of transmission. *Distance* refers to the minimum and maximum spatial separation between devices over a link, in the context of a complete, end-to-end circuit. Clearly, any given transmission system increases in attractiveness to the extent that available bandwidth is greater, introduced errors are fewer, and the maximum distance between various network elements (e.g., amplifiers, repeaters, and antennae) is greater.

It should be noted that bandwidth, error performance, and distance are tightly interrelated. In a twisted pair network, for example, more raw bandwidth requires higher transmission frequencies. Higher frequencies attenuate (lose power) more rapidly than do lower frequencies. This fact results in more errors in transmission, unless the amplifiers/repeaters are spaced more closely together. For instance, a physical four-wire, digital T1 circuit typically is provisioned over twisted pair, providing bandwidth of 1.544 Mbps with excellent error performance through the placement of regenerative repeaters spaced approximately every 6,000 ft. A somewhat better grade of twisted pair can be deployed in a Local Area Network (LAN) to support transmission rates of 100 Mbps between a workstation and a LAN hub or switch, with excellent error performance as long as the device separation is [le]100 meters (some manufacturers back away from support at 20 meters). In either case, certain measures must be taken to avoid high levels of ambient noise, the gauge of the conductors must be considered, etc. While this comparison is simplified, it clearly demonstrates the close and direct relationship between bandwidth, distance, and error performance.

Local Loop

In telephony, the **local loop** (also referred to as a **subscriber line**) is the physical link or circuit that connects from the demarcation point of the customer premises to the edge of the carrier or telecommunications service provider's network. At the edge of the carrier access network in a traditional PSTN (Public Switched Telephone Network) scenario, the local loop terminates in a circuit switch housed in an ILEC (Incumbent Local Exchange Carrier) CO (Central Office).

Traditionally, the local loop was wireline in nature from customer to central office, specifically in the form of an electrical circuit (i.e. loop) provisioned as a single twisted pair in support of voice communications. Where the number of local loops was restricted, different customers could share the same loop, known as a party line. Modern implementations may include a digital loop carrier system segment or fiber optic transmission system known as fiber-in-the-loop. The local loop may terminate at a circuit switch owned by a CLEC (Competitive Local Exchange Carrier) and housed in a point of presence (POP), which typically is either an ILEC CO or a "carrier hotel". A local loop may be provisioned to support data communications applications, or combined voice and data:

- analog voice and signaling used in traditional POTS
- Integrated Services Digital Network (ISDN)
- variants of Digital Subscriber Line (DSL)

Many owners of local loops are public utilities that hold a natural monopoly. To prevent the owner from using this natural monopoly to monopolize other fields of trade, some jurisdictions require utilities to unbundle the local loop, that is, make the local loop available to their competitors.

The term "local loop" is sometimes used for any "last mile" connection to the customer, regardless of technology or intended purpose. Hence the phrase "wireless local loop". Local loop connections in this sense include:

- Electric power line local loop: PLT or PLC
- Optical local loop: Fiber Optics services such as FiOS
- Satellite local loop: communications satellite and cosmos Internet connections of satellite television (DVB-S)
- Cable local loop: Cablemodem
- Wireless local loop (WLL): LMDS, WiMAX, GPRS, HSDPA, DECT

Signaling

Signaling refers to the exchange of control information between the components of a network (telephones, switches, etc.) in order to establish, manage, and disconnect calls. Four different types of signaling are used by telephone networks:

- **Supervisory**. This type of signaling provides the necessary control and status signals to establish calls, release calls, and make other service features possible.

It includes the informing of exchanges about subscriber loop on-hook/off-hook conditions, and providing information about the status of calls.

- **Address**. This type of signaling conveys addressing information (subscriber number, area code, access code) between network components.
- **Network Management**. This type of signaling supports the management of network resources. It includes the handling of congestion and component failure situations, and the gathering and reporting of useful status information such as traffic conditions and operating anomalies.
- **Audio-Visual**. This type of signaling informs the calling subscriber about the status of a call, and alerts the called subscriber about a waiting call.

Two categories of signaling are discussed below: subscriber signaling and interexchange signaling.

Subscriber Signaling

Subscriber signaling refers to the signals exchanged between a subscriber and a local exchange via the subscriber's loop. The sequence diagram in Figure 10.7 illustrates (a simplified version of) the signals exchanged for successfully establishing a call between two subscribers.

This process works as follows. We assume that initially both subscribers have their phones on-hook. The calling subscriber sends an off-hook signal to the local exchange by lifting the receiver. The switch responds by activating an

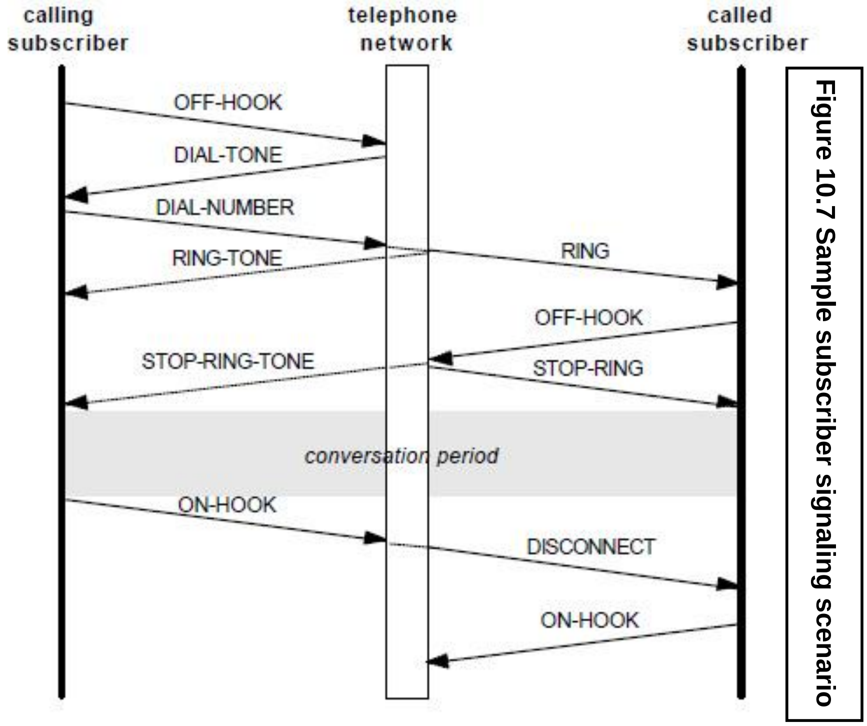


Figure 10.7 Sample subscriber signaling scenario

audible dial tone over the subscriber loop, informing the subscriber that a number may be dialed now. The subscriber dials the other party’s number, and each dialed digit is signaled to the local exchange. This number is used as an address to route the call through the network and finally arrives at the local exchange of the called party. This local exchange applies a ringing signal to the called subscriber’s loop. At the same time, a confirmation is sent back to the calling subscriber’s local exchange, which in turn applies a ring tone to the calling subscriber’s local loop. This serves as an audible feedback that the number is dialed. When the called subscriber lifts the receiver, an off-hook signal is sent back to its local exchange. This causes the local exchange to stop the ringing, and is propagated back to the calling subscriber’s exchange which in turn stops the ring tone. The network connects the two parties and they may engage in a conversation. Either subscriber can terminate the call by pressing the hook switch. This sends an on-hook signal to the local exchange, which in turn terminates the call and informs the other subscriber accordingly.

Interexchange Signaling

Interexchange signaling refers to the signals exchanged between two or more network exchanges in order to handle calls. The sequence diagram in Figur 10.**Error! Bookmark not defined.** illustrates (a simplified version of) the signals exchanged between two local exchanges via the trunk lines which may involve zero or more tandem exchanges. The scenario is the same as that of Figure 10.**Error! Bookmark not defined.**, except that here we are looking inside the network. This process works as follows. After the calling subscriber has dialed the number of the called subscriber and this address has been provided to the calling exchange, the latter conveys a connect signal to the local exchange of the called subscriber via the network. The called exchange *winks* in response to this by sending an off-hook followed by an on-hook signal, confirming that it is ready to receive the address.

Once the address is communicated to called exchange, it starts ringing the ca subscriber and at the same time sends a tone to the calling subscriber’s phone.

This feedback confirms to the cal subscriber that the called subscriber’s phoı ringing. When the called subscriber answ this is signaled back to the calling excha and the ring tone is terminated to confirm the call has been answered. The two pa can now engage in a conversation. As soo either subscriber hangs up the phone, disconnect signal is communicated by its local exchange to the local exchange of the other party and the call is terminated.

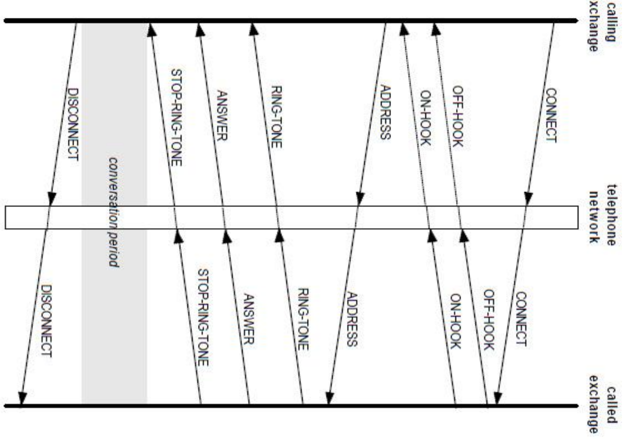


Figure 10.8 Sample interexchange signaling scenario.

Modem

A **modem** (modulator-demodulator) is a device that modulates an analog carrier signal to encode digital information, and also demodulates such a carrier signal to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used over any means of transmitting analog signals, from driven diodes to radio.

The most familiar example is a voice-band modem that turns the digital data of a personal computer into modulated electrical signals in the voice-frequency range of a telephone channel. These signals can be transmitted over telephone lines and demodulated by another modem at the receiver side to recover the digital data.

Modems are generally classified by the amount of data they can send in a given time unit, normally measured in bits per second (bit/s, or bps). They can also be classified by the symbol rate measured in baud, the number of times the modem changes its signal state per second. For example, the ITU V.21 standard used audio frequency-shift keying, aka tones, to carry 300 bit/s using 300 baud, whereas the original ITU V.22 standard allowed 1,200 bit/s with 600 baud using phase-shift keying.

Modem Types

- Asynchronous - The common modem used today. Each byte is placed between a stop and a start bit. Each modem must operate with the same start and stop bit sequence, operate at the same baud rate and have the same parity settings for the data checking in order to communicate correctly. Define parity checking.
- Synchronous - Synchronous modems can be faster than asynchronous. They depend on timing to communicate. Data is transmitted in frames with synchronization bits which are used to be sure the timing of the transmission and reception of data is accurate. Synchronous modems are normally used on dedicated leased lines. Synchronous modems are one of binary synchronous communications protocol (bisync), high level data link control (HDLC), or synchronous data link control (SLDC). Three methods can be used to control synchronization:
  - Additional clock signal
  - Guaranteed state change - Clocking is part of the data signal.
  - Oversampling - The reciever samples the signal much faster than the data is sent. The extra samples can be used to be sure the clock is synchronized.
- Digital Modems - These are used with ISDN services and are not actually modems, although they are called modems. They can provide connection speeds of 128Kbps.

Error Detection and correction

In information theory and coding theory with applications in computer science and telecommunication, **error detection and correction** or **error control** are techniques that enable reliable delivery of digital data over unreliable communication channels. Many communication channels are subject to channel noise, and thus errors may be introduced during transmission from the source to a receiver. Error detection techniques allow detecting such errors, while error correction enables reconstruction of the original data.

The general definitions of the terms are as follows:

- ***Error detection*** is the detection of errors caused by noise or other impairments during transmission from the transmitter to the receiver.
- ***Error correction*** is the detection of errors and reconstruction of the original, error-free data.

Error correction may generally be realized in two different ways:

- ***Automatic repeat request (ARQ)*** (sometimes also referred to as *backward error correction*): This is an error control technique whereby an error detection scheme is combined with requests for retransmission of erroneous data. Every block of data received is checked using the error detection code used, and if the check fails, retransmission of the data is requested – this may be done repeatedly, until the data can be verified.
- ***Forward error correction (FEC)*****:** The sender encodes the data using an *error-correcting code (ECC)* prior to transmission. The additional information (redundancy) added by the code is used by the receiver to recover the original data. In general, the reconstructed data is what is deemed the "most likely" original data.

ARQ and FEC may be combined, such that minor errors are corrected without retransmission, and major errors are corrected via a request for retransmission: this is called *hybrid automatic repeat-request (HARQ).*

The general idea for achieving error detection and correction is to add some redundancy (i.e., some extra data) to a message, which receivers can use to check consistency of the delivered message, and to recover data determined to be erroneous. Error-detection and correction schemes can be either systematic or non-systematic: In a systematic scheme, the transmitter sends the original data, and attaches a fixed number of *check bits* (or *parity data*), which are derived from the data bits by some deterministic algorithm. If only error detection is required, a receiver can simply apply the same algorithm to the received data bits and compare its output with the received check bits; if the values do not match, an error has occurred at some point during the transmission. In a system that uses a non-systematic code, the original message is transformed into an encoded message that has at least as many bits as the original message.

Error detection is most commonly realized using a suitable hash function (or checksum algorithm). A hash function adds a fixed-length *tag* to a message, which enables receivers to verify the delivered message by recomputing the tag and comparing it with the one provided.

There exists a vast variety of different hash function designs. However, some are of particularly widespread use because of either their simplicity or their suitability for detecting certain kinds of errors (e.g., the cyclic redundancy check's performance in detecting burst errors).

Error correction

Automatic repeat request

Automatic Repeat request (ARQ) is an error control method for data transmission that makes use of error-detection codes, acknowledgment and/or negative acknowledgment messages, and timeouts to achieve reliable data transmission. An *acknowledgment* is a message sent by the receiver to indicate that it has correctly received a data frame.

Error-correcting code

An error-correcting code (ECC) or forward error correction (FEC) code is a system of adding redundant data, or *parity data*, to a message, such that it can be recovered by a receiver even when a number of errors (up to the capability of the code being used) were introduced, either during the process of transmission, or on storage. Since the receiver does not have to ask the sender for retransmission of the data, a back-channel is not required in forward error correction, and it is therefore suitable for simplex communication such as broadcasting.

Encryption

In cryptography, **encryption** is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is **encrypted** information (in cryptography, referred to as ciphertext). In many contexts, the word **encryption** also implicitly refers to the reverse process, **decryption** (e.g. “software for encryption” can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted).

Encryption has long been used by militaries and governments to facilitate secret communication. Encryption is now commonly used in protecting information within many kinds of civilian systems. For example, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage.[1] Encryption can be used to protect data "at rest", such as files on computers and storage devices (e.g. USB flash drives). In recent years there have been numerous reports of confidential data such as customers' personal records being exposed through loss or theft of laptops or backup drives. Encrypting such files at rest helps protect them should physical security measures fail. Digital rights management systems which prevent unauthorized use or reproduction of copyrighted material and protect software against reverse engineering (see also copy protection) are another somewhat different example of using encryption on data at rest.

Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. There have been numerous reports of data in transit being intercepted in recent years. Encrypting data in transit also helps to secure it as it is often difficult to physically secure all access to networks.

Protocol

Network protocols define a language of rules and conventions for communication between network devices.

It is a formal description of digital message formats and the rules for exchanging those messages in or between computing systems and in telecommunications. Protocols may include signaling, authentication and error detection and correction capabilities. A protocol describes the syntax, semantics, and synchronization of communication and may be implemented in hardware or software, or both.

In the field of computer networking, different types of network protocols are used to carry on the wired the wireless networking smoothly. Basically network protocol is defined as the bundle of rules and regulations of computer networking which are require setting up the communicational process between different multiple computers present or attached with the network is called as the network protocol. Network protocol is an essential component of the computer networking because without the protocols we cannot carry the communicational functions over the network. Network protocols also play an important role the field of computer networking because they are able to provide the different types of paths to do the access to the network, also deals the topologies of the network and can also take part in enhancing the speed of data transmission during the communicational process.

The most common network protocols are:

- Ethernet
- Local Talk
- Token Ring
- FDDI
- ATM
- Arcnet

Ethernet

Ethernet is a family of frame-based computer networking technologies for local area networks (LANs). The name came from the physical concept of the ether. It defines a number of wiring and signaling standards for the Physical Layer of the OSI networking model as well as a common addressing format and Media Access Control at the Data Link Layer.

Ethernet is standardized as IEEE 802.3. The combination of the twisted pair versions of Ethernet for connecting end systems to the network, along with the fiber optic versions for site backbones, is the most widespread wired LAN technology. It has been used from around 1980[1] to the present, largely replacing competing LAN standards such as token ring, FDDI, and ARCNET.

ARCNET

ARCNET (also CamelCased as ARCnet, an acronym from Attached Resource Computer NETwork) is a local area network (*LAN*) protocol, similar in purpose to Ethernet or Token Ring. ARCNET was the first widely available networking system for microcomputers and became popular in the 1980s for office automation tasks. It has since gained a following in the embedded systems market, where certain features of the protocol are especially useful.

To mediate access to the bus, ARCNET, like Token Ring, uses a token passing scheme, rather than the carrier sense multiple access approach of Ethernet. When peers are inactive, a single "token" message is passed around the network from machine to machine, and no peer is allowed to use the bus unless it has the token. If a particular peer wishes to send a message, it waits to receive the token, sends its message, and then passes the token on to the next station. Because ARCNET is implemented as a distributed star, the token cannot be passed machine to machine around a ring. Instead, each node is assigned an 8 bit address (usually via DIP switches), and when a new node joins the network a "reconfig" occurs, wherein each node learns the address of the node immediately above it. The token is then passed directly from one node to the next.