Mekelle University
EiT-M, School of Computing

Department of Computer Science

CoSc2061: Data Communications and Computer Networking

Chapter Two: Networking Hardware

1. Networking Hardware

Every network requires some hardware to make it work. Precisely what hardware is required depends on what type of network is being constructed. The following is summary of some of the more common networking hardware.

1.1 Cabling

The vast majority of networks today are connected by some sort of wiring or cabling that acts as a network transmission medium that carries signals between computers. Although many cable types are available to meet the varying needs and sizes of networks, from small to large, there are 3 primary cable types:

- Coaxial
- Twisted pair
- Fibre-optic

1.1.1 Coaxial cable

At one time, coaxial cable was the most widely used network cabling. There were a couple of reasons for coaxial cable's wide usage: it was relatively inexpensive, and it was light, flexible, and easy to work with.

In its simplest form, *coaxial cable* consists of a core of copper wire surrounded by insulation, a braided metal shielding, and an outer cover. Figure 1 shows the various components that make up a coaxial cable.

The *shielding* protects transmitted data by absorbing stray electronic signals, called *noise*, so that they do not get onto the cable and distort the data. The core of a coaxial cable carries the electronic signals that make up the data. This wire core can be either solid or stranded. If the core is solid, it is usually copper. Surrounding the core is an insulating layer that separates it from the wire mesh. The braided wire mesh acts as a ground and protects the core from electrical noise. Coaxial cable uses the BNC connector to connect to computers and other devices.

Coaxial cable is more resistant to interference and attenuation than twisted-pair cabling. The stranded, protective sleeve absorbs stray electronic signals so that they do not affect data being

sent over the inner copper cable. For this reason, coaxial cabling is a good choice for longer distances.

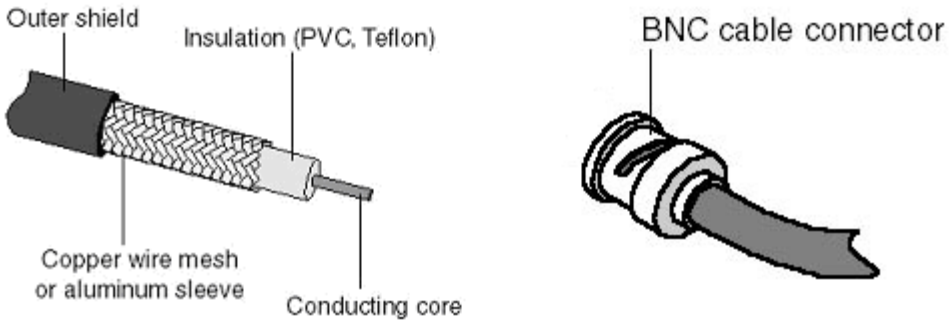

Figure 1 – The components of coaxial cable and the BNC connector

There are two types of coaxial cable: thinnet and thicknet. Thicknet cabling is thicker, and a better choice for longer distances, but is more expensive and more difficult to work with. Thinnet coaxial cable can carry a signal for a distance of up to approximately 185 meters before the signal starts to suffer from attenuation. Thicknet cable can carry a signal for 500 meters. Therefore, because of thicknet's ability to support data transfer over longer distances, it is sometimes used as a backbone to connect several smaller thinnet-based networks.

1.1.2 Twisted pair

In its simplest form, *twisted-pair cable* consists of two insulated strands of copper wire twisted around each other. Figure 2 shows the two types of twisted-pair cable: *unshielded twisted-pair (UTP)* and *shielded twisted-pair (STP)* cable.

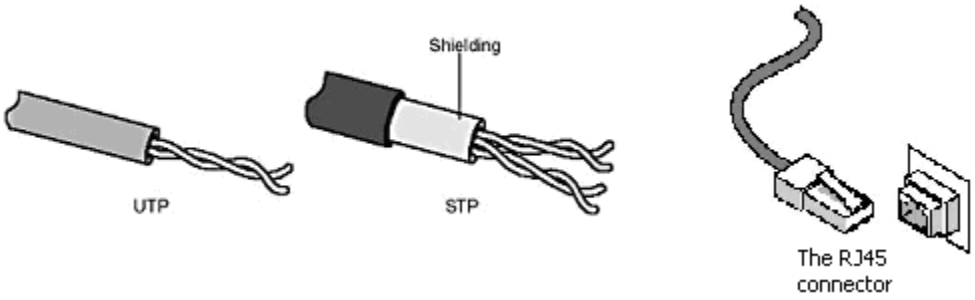

Figure 2 – Unshielded and shielded twisted pair cabling

UTP is the most popular type of twisted-pair cable and is fast becoming the most popular LAN cabling. It is cheap and easy to use. However, its performance over long distances is not as good as coaxial cable. The maximum cable length segment of UTP is 100 meters. There are a number of different types (or categories) of UTP cable, which differ in their specification and in the number of pairs of wire contained within the cable. Most telephone systems use UTP cable (with the RJ11 connector), and many LANs nowadays also use UTP (with the RJ45 connector). STP is higher quality than UTP, but more expensive and less popular.

1.1.3 Fibre-optic

In *fibre-optic cable*, optical fibres carry digital data signals in the form of modulated pulses of light. This is a relatively safe way to send data because, unlike copper-based cables that carry data in the form of electronic signals, no electrical impulses are carried over the fibre-optic cable. This means that fibre-optic cable cannot be tapped, and its data cannot be stolen.

Fibre-optic cable is good for very high-speed, high-capacity data transmission because of the purity of the signal and lack of signal attenuation.

An optical fibre consists of an extremely thin cylinder of glass, called the *core*, surrounded by a concentric layer of glass, known as the *cladding*. The fibres are sometimes made of plastic. Plastic is easier to install, but cannot carry the light pulses for as long a distance as glass.

Because each glass strand passes signals in only one direction, a cable includes two strands in separate jackets. One strand transmits and one receives. A reinforcing layer of plastic surrounds each glass strand, and Kevlar fibres provide strength. See Figure 3 for an illustration of fibre-optic cable. The Kevlar fibres in the fibre-optic connector are placed between the two cables. Just as their counterparts (twisted-pair and coaxial) are, fibre-optic cables are encased in a plastic coating for protection.

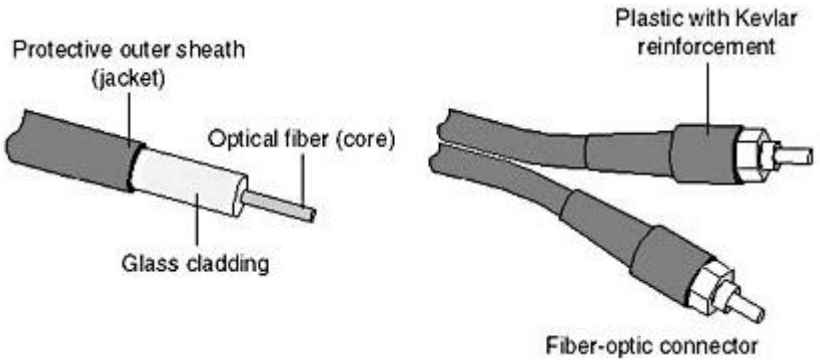

Figure 3 – The composition of a fibre-optic cable

1.2 Networking hardware devices

1.2.1 Network interface card

The Network Interface Card (NIC), also known as a *network adaptor*, acts as the interface between the computer and the physical network connection. In most networks, every computer must have a network interface card to be able to connect to the network. NICs are usually specific to a particular type of cabling – for example, a NIC may have either an RJ45 connector or a BNC connector – although it is possible to get *combo cards*, which include more than one type of connector.

1.2.2 Transceivers

A transceiver is a networking device that converts from one cabling technology to another. For example, a transceiver may act as an interface between a network based on coaxial cable and one using fibre-optic cable.

1.2.3 Repeater

In a bus topology, signal loss can occur if the *segments* are too long. A repeater is a device that connects two network segments and broadcasts data between them. It amplifies the signal, thereby extending the usable length of the bus.

1.2.4 Hub

One network component that has become standard equipment in networks is the hub. A hub acts as the central component in a star topology, and typically contains 4, 8, 16 or even more different *ports* for connecting to computers or other hubs. It is similar in operation to a repeater, except that it broadcasts data received by any of the ports to all other ports on the hub. Hubs can be active, passive or hybrid.

Most hubs are *active*; that is, they regenerate and retransmit signals in the same way as a repeater does. Because hubs usually have eight to twelve ports for network computers to connect to, they are sometimes called *multiport repeaters*. Active hubs require electrical power to run. Some types of hubs are passive. They act as connection points and do not amplify or regenerate the signal; the signal passes through the hub. *Passive hubs* do not require electrical power to run. Advanced hubs that will accommodate several different types of cables are called *hybrid hubs*.

1.2.5 Bridges, switches and routers

For large networks it is often necessary to partition it into smaller groups of nodes to help isolate traffic and improve performance. A *bridge* is a device that acts as an interface between two sets of nodes. For example, if a company's network has been partitioned into two *subnets*, for the sales department and administration department respectively, a bridge will be placed between the two networks. If a computer on the sales subnet sends data to another computer on the sales subnet, the bridge will not pass on the data to the administration subnet. However, if the same computer sends data to a computer on the administration subnet, it will be forwarded by the bridge. Because not all data is passed onto the other subnet, network traffic is reduced.

A *switch* is similar to a bridge, except that it has multiple ports. A switch can also be seen as a more intelligent hub – whereas a hub passes on all data to every port, a switch will only pass data on to the port that it is intended for.

A *router* is also used for connecting networks together. However, unlike a bridge, a router can be used to connect networks that use different network technologies. Routers are very commonly found in the hardware infrastructure that forms the basis of the Internet.

1.3. Wireless networking

Although most networks use physical connections between the network components, recently wireless networking has been increasing in popularity. Wireless networks can use infrared light, line-of-sight lasers, or radio waves to transmit data between nodes without the need for physical cabling. They eliminate the need to install physical cabling and offer a lot of flexibility for users using the network. However, they are currently more expensive and slower than cable-based networks. As costs drop and performance increases, wireless networks are sure to be increasingly popular in the future.

There are two main types of hardware associated with wireless communication in computing: *Bluetooth* and *802.11*. Bluetooth only allows very short-range transmission (typically less than 10m) and is intended primarily for cable-free peripherals, such as mouses and keyboards. 802.11, or *wireless Ethernet*, is the standard for wireless networking of computers, and will be discussed in more detail in **Network Architecture.**