RELCOM inc.

CARRIER-BAND NETWORK Handbook

Table Of Contents

Introduction

This Handbook is a comprehensive guide to all of the facts that the user needs to know about the Carrier-Band network. The Handbook explains how the network operates, how to adapt it for different applications in the factory, how to install it, and how to keep it operational. The Handbook is intended for people who are not, and never want to be, networking experts but who need to know enough about the Carrier-Band network to automate their factory.

The basic specifications for the Carrier-Band network, as it is described in this Handbook, are taken from the IEEE Standard 802.4. Other specifications in the Handbook are based on working papers of the IEEE 802.4 committee and the standard's options selected by the MAP specification. Other specifications are derived from network product capabilities and general practices in the industry.

Chapter 1: Networks in the Factory

Local Area Networks, LANs, are used to provide data communications capability between various computer devices or **stations** in a building. There are many types of LANs, each one with its own characteristics and costs. Two types of networks have been selected for factory use because they are reliable and can support real-time data communication requirements that are needed in the factory. The two types of networks are broadband and carrier-band. Both of these networks are defined in the IEEE Standard 802.4.

Broadband

The **broadband** network uses cable-TV-type cabling and signaling. Broadband is intended for the factory **backbone.** That is, the whole factory is wired to use this broadband cable. The wiring is called "broadband" because many different types of signals can exist on the cable at the same time, in the same way that many channels of television signals can be on cable-TV wiring at the same time. A broadband LAN can use one set of channels on the cable at the same time that a different set of channels are used for other purposes, such as, point-to-point modem data, video, and even voice.

Carrier-Band

The **Carrier-band** network is much simpler than the broadband network. The Carrier-band network is intended to serve a smaller area within the factory-usually for some dedicated purpose, such as a manufacturing cell or the control of a particular process. The wiring for the carrier-band network is much simpler than that of the broadband network. The cable carries only one signal at a time. This type of signaling is called **baseband.**

A simplified representation of the two types of networks is shown in Figure 1-1. The broadband network is shown in the heavy lines. Note that the broadband network requires a **head end** to process the network signals. It also requires **amplifiers** to boost the signals as they travel over the cable. Many different types of computers or other devices can be connected to the broadband wiring, for example, computers communicating to terminals through modems, TV cameras sending pictures to TV monitors, etc. Any device that uses the network is called a **station.**

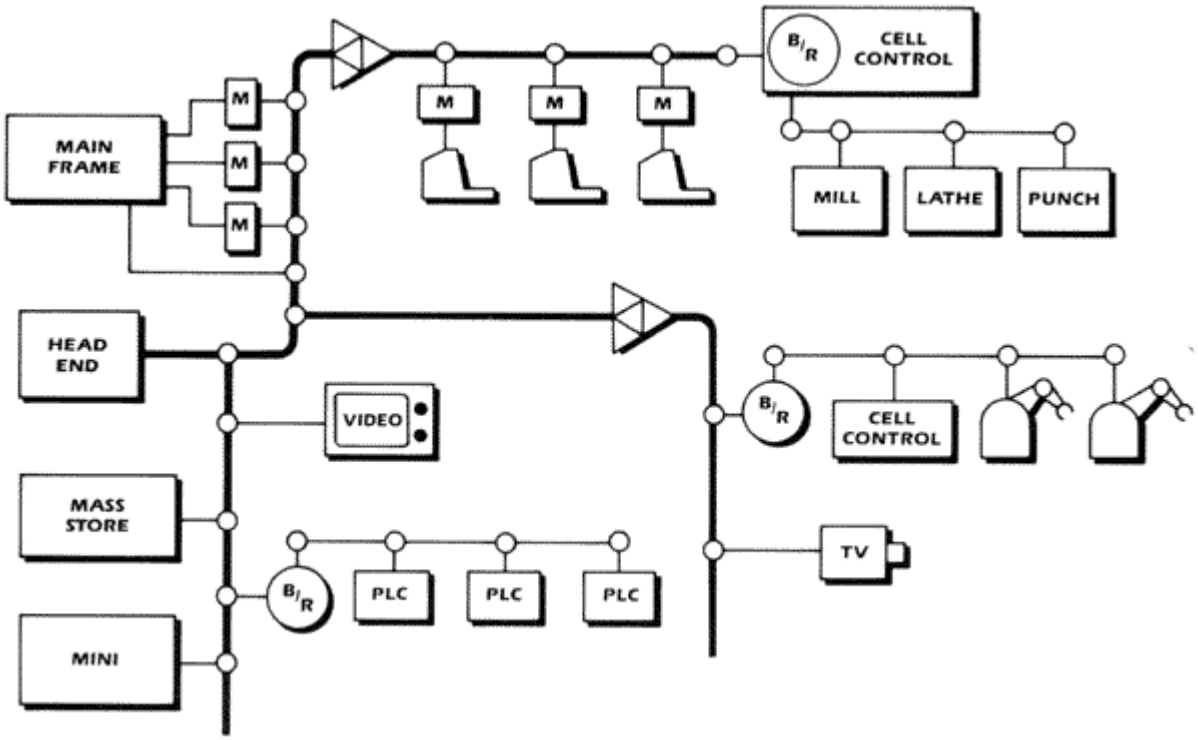

Figure 1-1. Broadband and Carrier-Band Networks

Carrier-band networks are shown by the lighter lines. The networks consist of simple wiring and a small number of computers or computer-controlled devices attached to the carrier-band cable. The carrier-band networks are intended for interconnecting devices in a manufacturing cell. For example, the network can interconnect a group of machine tools, a robot assembly operation, or an

operation run by programmable logic controllers. In many cases, the operation of the cell is controlled by a computer.

The carrier-band network can operate independently of the broadband network, or it can be interconnected to the broadband network. Stations on the broadband network can communicate with stations on the carrier-band network through devices known as **bridges** or **routers,** shown as circles in Figure 1-1. The difference between bridges and routers will be explained in Section 7. Bridges and routers can be separate stations, or they can be part of the cell controller computer

The remainder of the Handbook will examine the details of the carrier-band network.

Terms

Backbone: A network that interconnects other networks.

Baseband: A type of network wiring that supports only one signal at a time.

Bridge: A device that interconnects networks.

Broadband: A type of network wiring that can support many signals at the same time on different channels.

Carrier-band: A type of baseband network used in the factory.

Head-end: A common signal processing device in a broadband network.

LAN: Local Area Network, a data communications network for a limited area.

Router: A device that interconnects networks.

Station: A computer device on a local area network.

Chapter 2: Carrier-band Cable System

The carrier-band cable system is the part of the network that interconnects the stations and lets them send signals to each other. The cable system is the most visible part of the network. The other parts of the network are inside the stations

and attached to the cable. The cable system is made up of a number of component parts.

Cable-System Components

The cable system of the carrier-band network is shown in Figure 2-1. The main cable that carries the signals is called the **trunk** cable. Several types of cables can be used for the trunk. The benefits and drawbacks of each type will be discussed later.

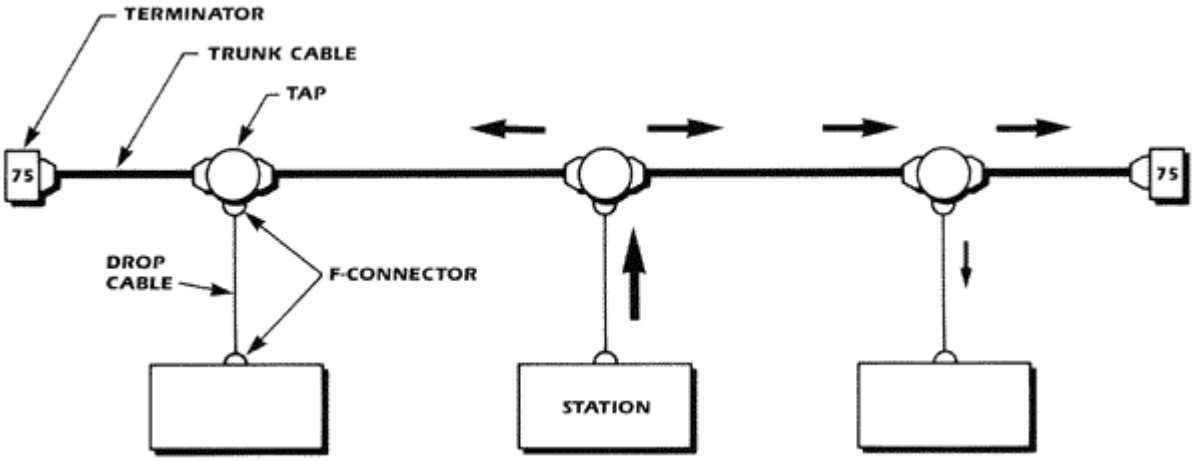

Figure 2-1. Cable-System Components

The carrier-band network uses the type of cable used for cable television, CATV. The cables are coaxial, with 75-ohm **characteristic impedance.** Characteristic impedance is the ratio of the signal voltage to the signal current that travels on the cable. It is similar to resistance, which is the ratio of voltage to current.

The trunk cable is **terminated** at each end with 75-ohm resistors that absorb the signals so that they do not reflect back and forth from the ends of the trunk cable.

Taps are used to get signals from the network stations onto the trunk cable and signals from the trunk cable to the network stations. The taps are **non-directional.** That is, the signal sent from a station splits equally at the tap and travels in both directions on the trunk cable, as shown at the middle station of Figure 2-1.

When a signal traveling on the trunk cable reaches a tap, a small portion of the signal is tapped off and sent to the network station, as shown in the right-hand station of Figure 2-1. Most of the signal continues traveling on the trunk cable until it reaches a terminator and is absorbed.

The cable that connects the tap to the station is called the **drop** cable. The drop cable is attached to the tap and to the network station by **F-connectors.** F-connectors are commonly used to connect television sets to TV antennas. For

factory automation applications, the F-connectors are made to be much more reliable than those found on TV sets. The connectors from the trunk cable to the taps are usually F-connectors, but other types of connectors can be used for special kinds of trunk cables.

Signal Characteristics

The type of signals used on the carrier-band network are shown in Figure 2-2. For a 5 Mbit/second network, the signals representing binary ones are one cycle of 5 MHz. The signals representing binary zeros are two cycles of 10 MHz. Each bit-cell is 0.2 microseconds long. There are also **non-data** symbols, which always come in pairs and take up two bit-cells. A non-data symbol pair is represented by 1 cycle of 10 MHz, followed by one cycle of 5 MHz, followed by one cycle of 10 MHz. The use of non-data symbols will be explained in Section 4.

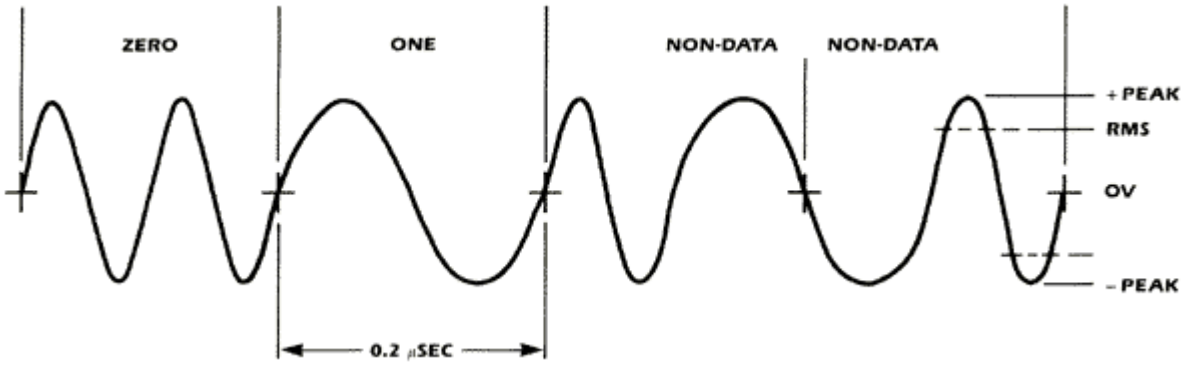

Figure 2-2. Carrier-Band Signal Characteristics

The type of signaling shown in Figure 2-2 is called **Frequency Shift Key, FSK.** Note that the frequency changes only on the zero voltage crossing. This type of FSK signaling is called **phase coherent.**

The strength or amplitude of the signal is measured in units called **dBmV** (**d**eci**B**ell, **m**illi**V**olt). These units make it simpler to talk about a very large range of signal amplitudes by using numbers that make it easy to compute signal strength. Suppose a signal has 1.4 volts or -1.4 volts at its maximum or minimum, as shown in Figure 2-2. Since the signal varies between the two values, its effective power value is only 1/1.4 of its maximum or 1 volt **rms.** One volt is 1000 times larger than 1 millivolt. It is easier to talk about the 1 volt signal if we calculate another value from it as a comparison to 1 millivolt using the following formula:

dBmV = 20 log (1 millivolt/signal voltage)

For 1 volt, the value in dBmV becomes 60. For 1/2 volt, the dBmV value is 54 or 6 dB down. For 2 volts, the dBmV value is 66 dBmV or 6 dB up. Table 2-1 shows the approximate values of signal strength in dBmV and in rms voltages. Working with signal values in dBmV makes it easier to calculate signal amplitudes by using addition and subtraction instead of multiplication of fractions.

dBmV	**rms voltage**
-18	0.13 mV
-12	0.25 mV
-6	0.5 mV
0	1 mV
6	2 mV
12	4 mV
18	8 mV
24	16 mV
30	32 mV
36	63 mV
42	126 mV
48	251 mV
54	501 mV
60	1000 mV
66	2000 mV

Table 2-1. dBmV to Voltage Conversion

Signal Attenuation

As a signal travels on a cable it is **attenuated**, that is, it gets smaller. Different types of cables have different attenuation values. These values are given in dB/100 feet or dB/100 meters at a given frequency. For the carrier-band network, the frequency of interest is 10 MHz. For example, if there is a 57 dBmV signal with an attenuation of 1.5 dB/100 meters on a 400 meter long trunk cable, then the signal at the other end will be:

$(100\text{-}57) - (4 \times 1.5) = 37$ dBmV

Signals traveling on the trunk cable are also attenuated by about 0.3 dB each time they pass through a tap.

When a network station transmits, it sends out a signal of 63 to 66 dBmV through the drop cable to the tap. The tap attenuates the signal 20 dB and sends it in both directions on the trunk cable. For a 63 dBmV signal from a station, the signal on the trunk cable becomes:

$63 - 20 = 43$ dBmV

The amount of signal that is taken off the trunk by the tap and sent down the drop cable to the network station is 20 dB lower than the signal strength on the trunk cable at that point.

The total signal loss from a transmitting station to a receiving station is the sum of all the dB losses along the way, as shown in Figure 2-3. The smallest amount of signal that a station can reliably detect is 10 dBmV.

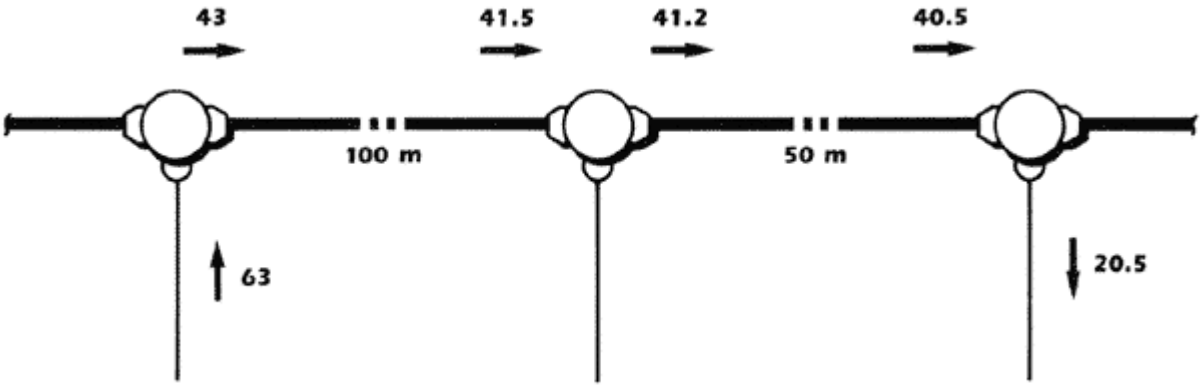

Figure 2-3. Signal Attenuation Example

Besides attenuation, there are a number of other signal characteristics that are important for the Carrier-band network.

Return Loss

Ideally, the cable and the taps should have a constant 75-ohm impedance. A constant characteristic impedance makes the signals travel smoothly over the cable system. In real cables and taps, however, it is not possible to maintain the 75-ohm impedance. If there is an impedance change in the cable or in the taps, some signal is reflected from that location. The reflection subtracts power from the signal and creates unwanted signals that travel in the reverse direction, as shown in Figure 2-4. These unwanted reflections essentially become noise.

The amount of reflection of a cable, a tap, or the whole wiring system is called **Return Loss.** The maximum amount of return loss allowable on the trunk cable and taps for reliable network operation is -22 dB. That is, for a signal on the trunk cable, less than 1/10 of the signal voltage can be reflected back by all the cable-system impedance mismatches. The more negative the return loss value, the better.

Figure 2-4 shows how return loss contributes to degrading a signal. At any given tap, the total signal is the sum of the main signal that is tapped off plus reflections that come from all the impedance discontinuities all along the cable.

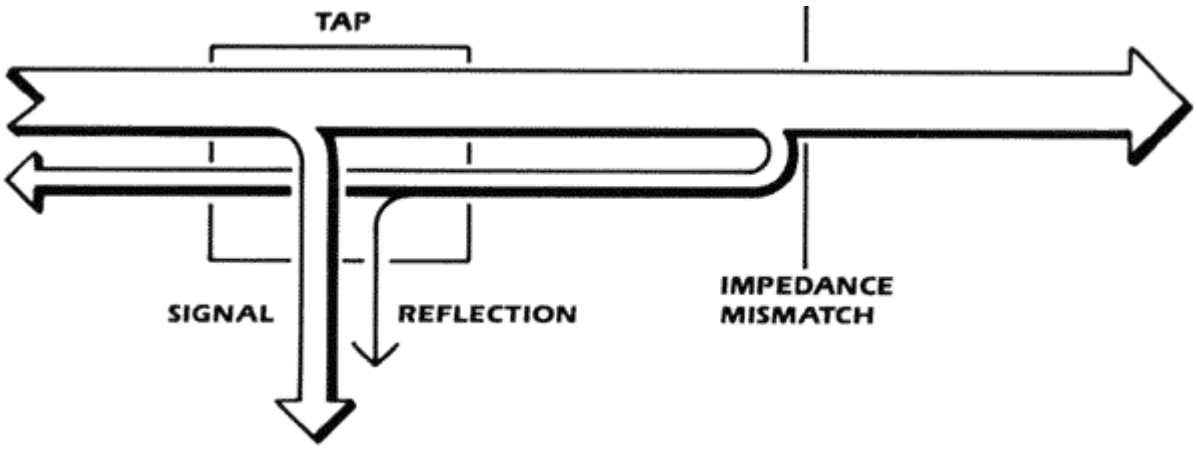

Figure 2-4. Return Loss

The trunk cable is not perfect. Because of manufacturing variations, or because the cable has been on a spool a long time, or for various other reasons, the characteristic impedance of the cable is not constant along its length. This change in characteristic impedance produces return loss. This return loss is called **structural return loss.** Good cable should have a structural return loss of more than -26 dB. The structural return loss should be measured while the cable is still on the spool and has not been installed.

Return loss also depends on how well the wiring is installed. If connectors are not properly tightened or the cable is crushed during installation, then the overall wiring system return loss will degrade.

The cable-system return loss can also increase with time as a result of various factors. Connectors can corrode, cable pulled too tightly around a corner can change impedance, rats can chew holes in the cable, or fork lifts can crush the cable.

The way to deal with these potential problems is to test the return loss when the wiring system is installed and during periodic maintenance of the network. This subject is covered in Section 9.

Tilt

On a cable, higher-frequency signals are attenuated more than lower-frequency ones. The difference in the amplitudes of the signals because of this type of attenuation is called **tilt.** The amount of tilt that can be tolerated in the entire length of the cable is 3.5 dB. To determine the maximum amount of cable that can be used in a network cable system, the attenuation at both 5 MHz and 10 MHz must be known. For example, if a particular cable has 1.2 dB attenuation at 5 MHz and 1.5 dB at 10 MHz for 100 meters of cable. then the maximum cable length can be:

Length × (1.5 – 1.2) = 3.5 dB

Length = 116 meters

Group Delay

Another characteristic of cables is that higher-frequency signals travel faster on cables than lower-frequency signals. Group delay means that ones and zeros (represented by the low- and high-frequency tones), which were sent within their own bit cells at the transmitter, arrive at the receiver with overlaps, as shown in Figure 2-5.

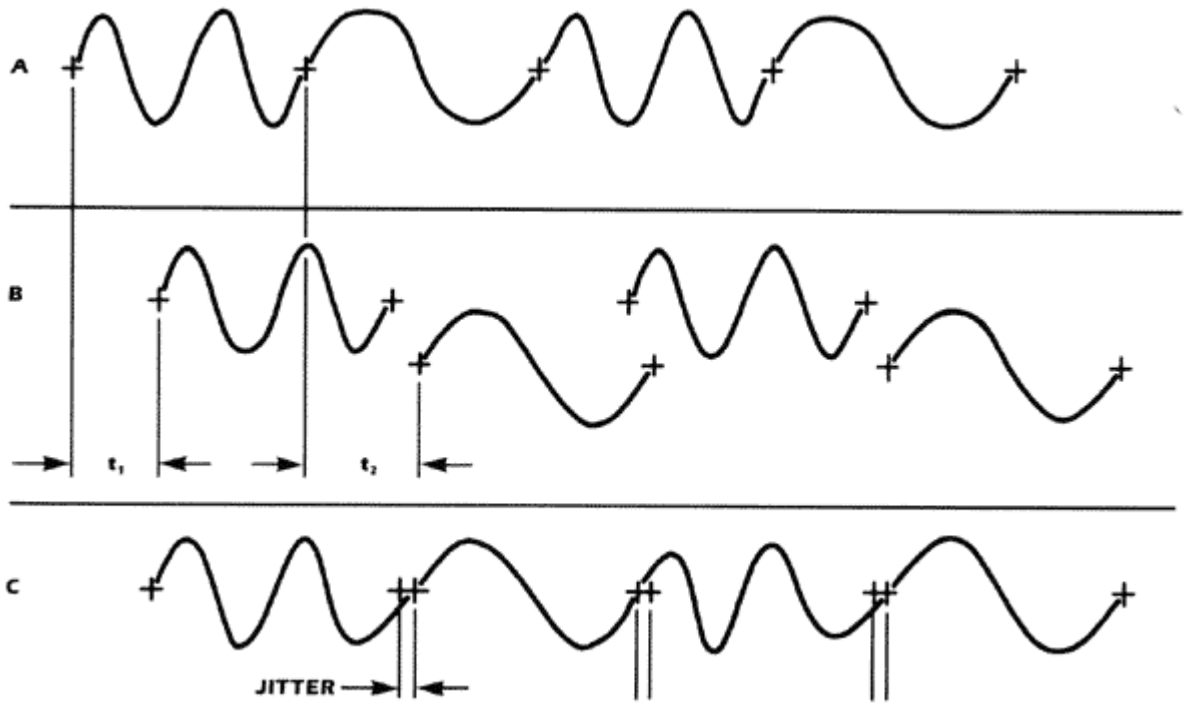

Figure 2-5. Group Delay

At the transmitter, all the signals are in their own time slots, as shown in A. If the signals in each time slot were to travel independently, they would arrive at the other end of the cable at different times, as shown in B. Note that t_2 is larger than t_1. If the signals are added together, as they are on the cable, the points where the signals cross zero volts are slightly shifted from where the crossing should be, as shown in C. This shift is called **Jitter.** Jitter makes the reception of signals difficult and can produce errors.

Noise

An operating factory often has a great deal of electrical noise, which can create problems on the network. **Noise** refers to the unwanted electrical signals induced into the cable by various sources. Noise is generated by welding equipment, electrical motors turning on and off, solenoids being activated, or any process that has an electric arc. Noise also comes from unsuspecting things, such as florescent lights and electric typewriters. The noise has various ways of getting on the cables. Cables that are poorly made or badly installed are more susceptible to noise. For reliable signal reception, the maximum amount of noise allowed is -10 dBmV

Another important cable characteristic is its ability to reject noise. One measure of cable quality is the **transfer Impedance,** which rates how well the cable can reject the effects of unwanted currents that get on its shield. The lower the value, the better the cable. A good cable will have a transfer impedance of less than 10 milliohm/meter in the I to 30 MHz range. Section 9 discusses good cable installation practices that keep the unwanted currents from getting onto the cable shield.

There are many methods of measuring transfer impedance so that just looking at a manufacturer's rating does not always tell the whole story. Also, a cable may have a good transfer impedance rating when it is first manufactured, but after the cable has been bent a few times, the transfer impedance degrades. A type of cable that exhibits good transfer impedance characteristics, even after bending, has four layers of outer shield: an aluminum foil shield covered by braided wire, covered by another layer of aluminum foil and covered by another layer of braided wire. This is called quad-shielded cable.

Cable Ratings

The effects of attenuation, tilt, and jitter place length limitations on the carrier-band network cabling system. The effect of these three factors varies for different types of cables. The maximum length each type of cable can be, while remaining within the IEEE Standard 802.4 specifications, is calculated by manufacturers. The maximum distance figure is an important parameter to look for when buying cable.

Cable attenuation is another important parameter. In the carrier-band network, the number of taps that can be put on the network is limited by the signal attenuation. The smaller the attenuation of the cable, the greater the amount of taps possible. This topic will be discussed in more detail in Section 8.

Structural return loss and transfer impedance are two important measures of cable quality

In summary the cable ratings to look for are: distance rating, attenuation, structural return loss and transfer impedance.

Cable Types

Flexible Cable

The most common type of cable used for the carrier-band trunk is known as "RG-11 type". This cable is flexible and is about 0.4" in diameter. RG-11 cable is easier to install than semi-rigid cable. Industrial-grade F-connectors are used to connect the cable to taps. The electrical characteristics of the RG-11 are not as good as the semi-rigid cable, therefore, the cable-system distance is limited to about 800 meters. However, this distance is adequate for most carrier-band network applications.

RG-11 type cable can also be armored. Armoring consists of an additional layer of corrugated aluminum and a tough plastic coating for the cable. The armoring has many benefits. It allows the cable to be easily installed without risk of damaging the signal-carrying inner cable. Armored cable can be directly buried without putting it into conduits. The cable can be directly hung between posts without using messenger wires for support. Armoring also protects the cable from moisture and damage. The greatest benefit of armoring is that it provides a great deal of protection from the electrical noise found in the factory. Figure 2-6 shows armored RG-11 type cable.

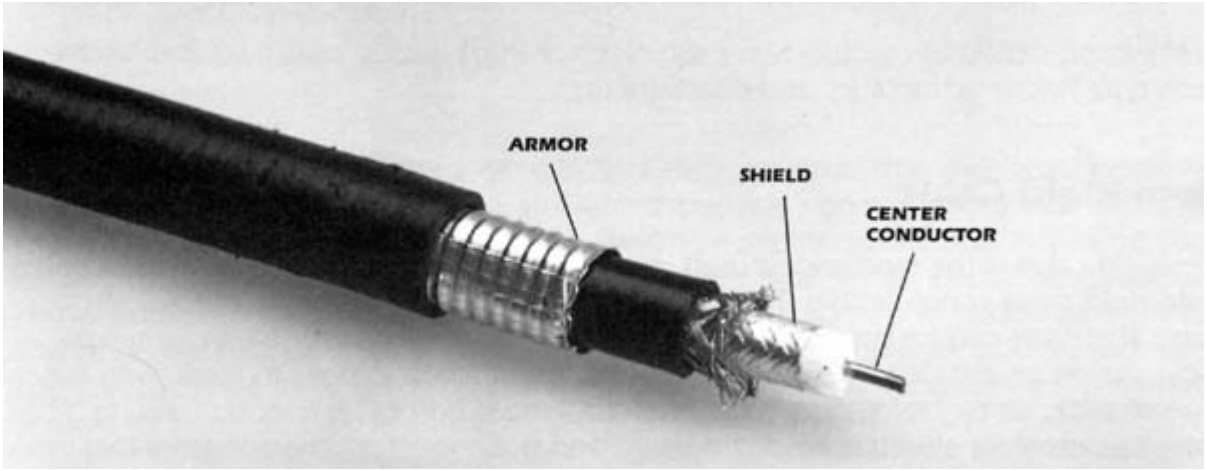

Figure 2-6. Armored RG-11 Cable

Drop Cable

The drop cable connects between the taps and the stations that use the network. The drop cable is flexible and can be either RG-11 type or RG-6 type. RG-6 cable is about 0.3" in diameter and is very flexible. These cables use F-connectors to attach to both the tap and the station. Drop cables are generally short and therefore noise and attenuation considerations are not as important as on the trunk cable. Although the drop cable usually does not need armoring, armoring is a good idea for systems that require reliability

Tap Characteristics

The discussion so far has considered only taps that have one drop cable connector, or **port,** per tap. There can be any number of ports on a tap, however. A two-port tap is a common type. Regardless of the number of ports, the following discussion applies to all taps

Taps are passive, that is, they do not require power to operate. Passive taps are not likely to fail and disrupt the network operation. Taps have a number of important characteristics:

Insertion Loss

A signal traveling on the trunk cable should only be attenuated a small amount by a tap. This attenuation is called **insertion loss.** The insertion loss of a good tap should be less then 0.15 dB for every drop cable port on the tap.

Trunk-to-Drop Attenuation

Drop cables receive only a small amount of the signal on the trunk cable. The amount of signal sent to the drop is 20 dB less than the signal on the trunk cable. Taking only a little signal power leaves most of the signal on the trunk cable. The trunk-to-drop attenuation also provides isolation between the trunk and the drop cables. If the drop cable is shorted or opened, there is little effect on the signals on the trunk cable.

Drop-to-Trunk Attenuation

The signal going from the drop cable to the trunk cable is also attenuated. This attenuation is not by design but is a fact of how electronics operates. Ideally, all the signals from the drop cable should be put on the trunk cable. If this were the case, the signal on the trunk cable would be 3 dB less then that on the drop because the signal power is split two ways. Taps attenuate the drop cable signal

by 20 dB. This means that most of the signal sent by a station is dissipated in the tap.

Drop-to-Drop Isolation

If a drop cable is shorted or is open, this should not affect the operation of the stations connected to the other drop ports of the same tap. This independent station operation is achieved if the attenuation between the drop ports on the same tap is greater than 20 dB.

Return Loss

Any tap on the trunk cable has some impedance mismatch, which disrupts the flow of the signal and produces reflections. Good taps produce very little reflection, -35 dB or less. The more negative the return loss number, the better the tap. The reflections that are caused by impedance mismatch at the drop ports are less critical. A -14 dB return loss is acceptable.

Ground Current Isolation

Taps can be made so that there is no DC current path between the trunk ports of the tap. This prevents currents from flowing on the trunk cable between parts of a building, which are at different ground potentials.

Surge Protection

Lightning strikes on the network cables or even nearby lightning strikes can induce large currents not only on the shield of the coaxial cable but also on the inner conductor. These large currents, on the order of 5000 Amps, can destroy the circuits in the tap and the station attached to the network. In places where lightning strikes are possible, the taps should have surge protectors built into them The surge protectors shunt the large currents to ground and protect the tap. The stations also have to have surge protectors built into them to protect the circuits inside them. If the network cable runs between buildings, surge protected taps should be used at the first tap where a cable comes into the building.

Mechanical Considerations

A number of mechanical factors have to be considered for the tap. The tap should be strong enough to take the pull of the trunk and the drop cables without breaking. It should be easy to mount and should be impervious to moisture and corrosives found in the factory The tap should provide a protrusion near the connector ports so that shrink tubing applied to the connectors will not slide off. Figure 2-7 shows a tap with F-connector fittings.

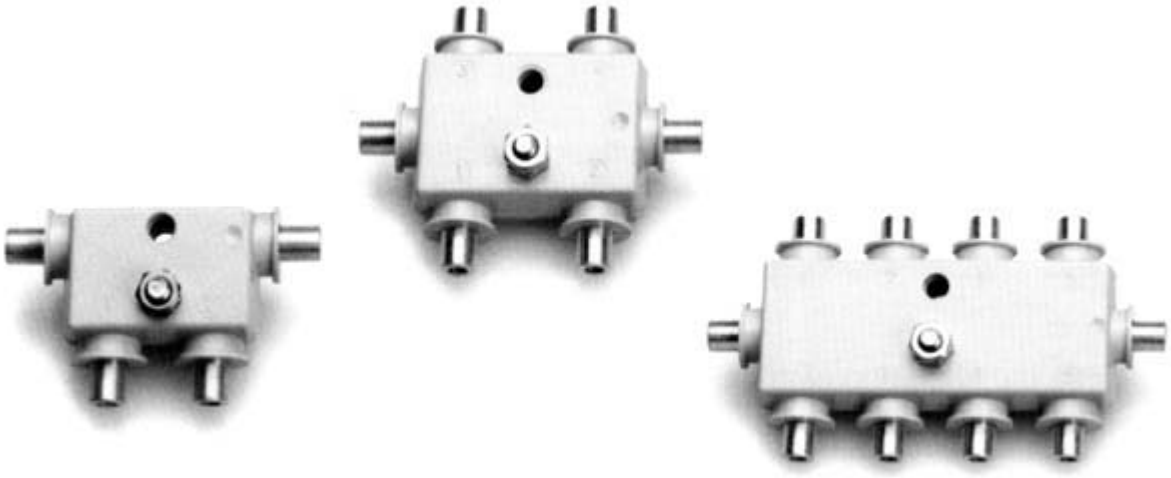

Figure 2-7. Taps

Early carrier-band taps were derived from the taps used in cable television industry and modified for carrier-band network use. These taps work moderately well but have a number of deficiencies. The mechanical connections inside the tap are questionable, especially under vibration. The aluminum body of the tap is subject to corrosion. Once the body of the tap is corroded, the circuits inside are not far behind. There is no explicit grounding mechanism provided by the tap so that ground currents are carried by the drop cables.

Newer taps have been designed specifically for the carrier-band network. These taps are made of a plastic material which totally encapsulates the circuits inside the tap and eliminates any corrosion. There are no mechanical connections inside the tap. A grounding stud is provided for carrying any ground current through a ground wire. Since the tap body is non-conductive, the tap can be mounted against metal building structures without the possibility of grounding the tap to the structure.

Terminating Taps

When a signal reaches the end of the trunk cable, it is absorbed by the terminator. The signal at the ends of the trunk cable is the weakest because it has been attenuated the most by the cable. Still, the signal on the end of the trunk cable is more than enough to be recognized by a station if it did not have to go through a 20 dB tap. What a shame to have to waste all this signal power in a terminator. Why not have more of the trunk cable signal go to the stations at the end of a cable?

This is exactly the purpose of a terminating tap. The terminating tap is the last tap at the end of a trunk cable. This tap terminates the signal on the trunk cable and it also sends a larger than usual amount of signal to the stations attached to the tap. The normal taps used in the carrier-band cable system attenuate signals by 20 dB. The terminating tap attenuates the signals to the drop ports by only 17

dB. Besides the convenience of not having to get special precision terminators for the ends of the trunk cable, the terminating tap allows more stations to be on the network and/or the trunk cable can be some 400 meters longer. (See Size Limitations in Section 8.)

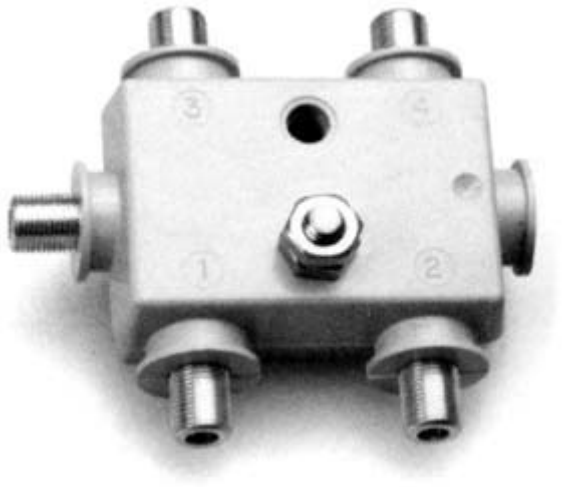

Figure 2-8. Terminating Tap

Connectors

F-connectors are used to connect the drop cable to the station and to attach cables to taps. F-connectors are the type of connector commonly used to attach antennas to TV sets. For this reason, there is a wide variety of connectors available with varying quality Most F-connectors are not suitable for industrial use. Consumer-grade connectors use the center conductor of the cable as the center pin of the connector. This wire makes a questionable contact and has a good chance of damaging the female contact of the mating connector. In order to define the characteristics of an F-connector suitable for industrial use, the Electronic Industries Association, EIA, has formulated the FD connector specification, Standard 550.

One of the most important parts of the FD standard is to specify a captive center conductor male pin for the F-connector. The size of the male pin and the corresponding female contact are well defined to insure good contact. The FD connector standard also specifies tin plating for the mating parts.

Tin is adequate for most applications. Some environments, however, mandate the use of gold plating. F-connectors are available with either kind of plating. Care should be taken to make sure that the mating connectors are either all tin or all gold. Mixing gold with tin can produce bad contacts at the mating surfaces.

The FD standard also lists a number of important mechanical and environmental characteristics. FD-type connectors should be used on the carrier-band network.

Another characteristic to look for in a connector is the amount of skill and the kinds of tools required to attach the connector to the cable. Most connector failures are a result of improper installation.

Figure 2-9. RG-11 and RG-6 cables with two types of quality F-connectors.

Terminators

In order to minimize the reflections on the cable system, everything must be terminated:

Precision 75 ohm terminators or terminating taps must be used at the ends of the trunk cable. The terminators commonly used in cable television are not adequate. They do not have a good center pin and do not absorb all of the signal.

If a drop port on a tap is not used, it must be terminated with 75 ohms. The drop port terminators do not have to be precise-the common cable television terminators are adequate.

If a drop cable attached to a tap is not attached to a station, it must be terminated with 75 ohms. The cable television terminators are adequate for this.

In situations where stations are disconnected from the drop cable while the network is operating, some time may lapse before a terminator can be attached to the unused drop cable. In the meantime, the cable is unterminated. A single

unterminated drop cable will not materially affect the network's operation, but several unterminated cables might. To preclude this, self-terminators can be used. The way the self-terminations work is as follows:

The self-termination is attached to the station-end of a drop cable. When a station is not attached, the self-terminator terminates the drop cable. When a station is attached, the station itself becomes the terminator and the self-terminator disconnects itself. If the station is removed, the self-terminator again provides the needed termination.

Self-terminators are useful in situations where the people connecting and disconnecting stations on the network may not be knowledgeable enough to terminate unused drop cables.

Summary

The carrier-band cable system provides a means for stations to send signals to each other. It is a passive 75-ohm cable system because, unlike the broadband cable system, it does not require any head-end signal conditioning or amplifiers along the cable to boost the signals. The taps are non-directional and passive.

FSK phase coherent signaling is used. The transmitter signal amplitude is between 63 and 66 dBmV; the receiver requires 10 dBmV signals. The maximum noise at a station can be -10 dBmV. Signal tilt and group delay considerations limit the size of the network to about 800 meters. The trunk cable return loss can be up to -22 dB. Everything in the cable system must be terminated in 75 ohms.

Terms

Armor: Protective cladding over a cable.

Attenuation: Signals getting smaller as they travel on a cable.

Bus: A linear network topology.

Characteristic Impedance: The ratio of voltage to current of the signal on a cable.

dBmV: A measure of signal strength.

Drop Cable: The cable between the tap and the station.

Frequency Shift Key, Phase Coherent: The signaling method used on the carrier-band network.

Insertion Loss: The amount of signal lost while going through a tap on the trunk cable.

Jitter: The timing uncertainty of the signal crossing zero voltage.

Noise: Unwanted electrical signals on the cable.

Non-directional: Signal from drop cable splits equally in both directions on the trunk cable.

Port: A drop cable connector on a tap.

Return Loss: The amount of signal reflected from an impedance discontinuity**.**

Tap: A device for connecting the station to the trunk cable.

Chapter 3: Modems

All the cables, taps, and terminators used in the cable system to interconnect devices on a local area network are called the **medium.** The medium carries the signals between the stations on the network.

The part of the station that puts the signals onto the medium and receives signals from the medium is called a **modem,** shown in Figure 3-1. The modem has two tasks to perform:

1. Get ones and zeros that need to be sent from the station and transmit the corresponding signals onto the medium.

2. Receive signals from the medium and convert them to ones and zeros to be used at the station.

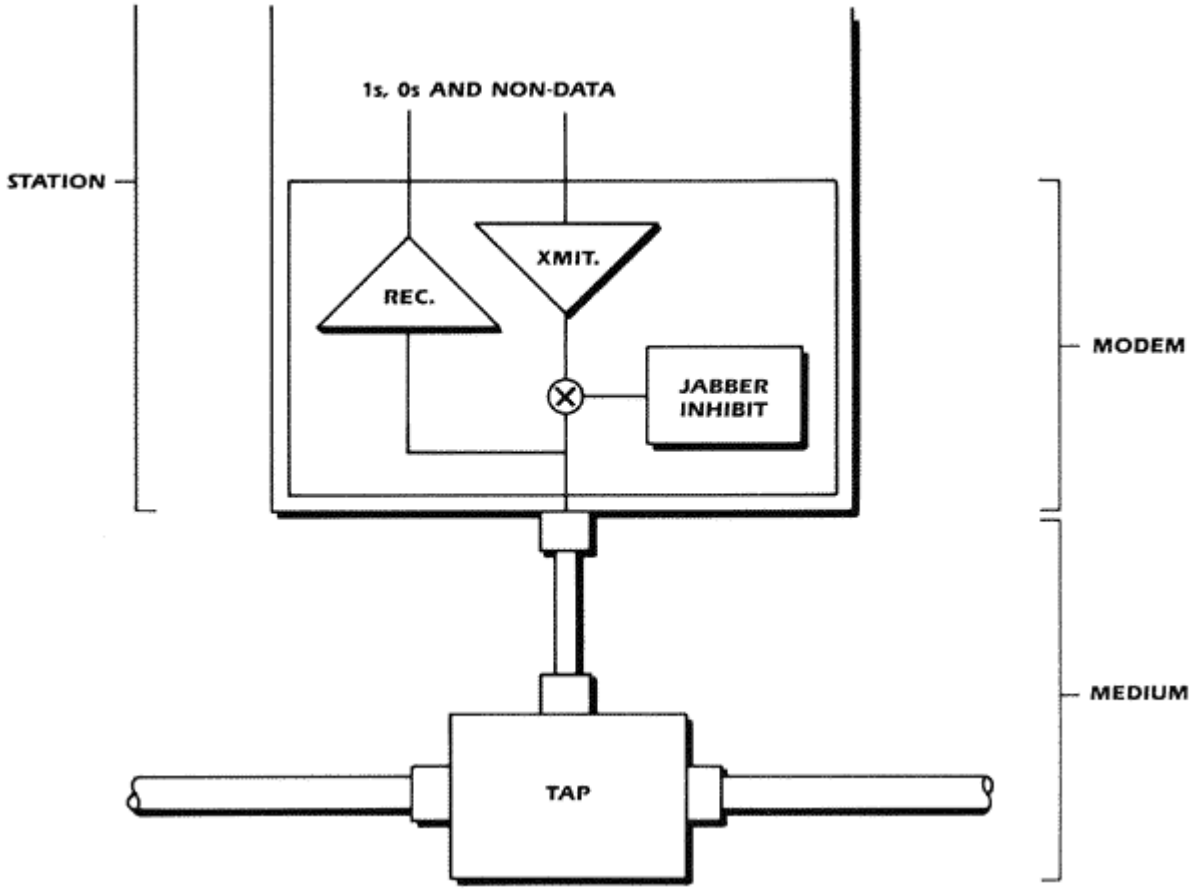

Figure 3-1. Medium and Modem

The modem can also send and receive non-data symbols, signals that are not ones or zeros but that have a special meaning. The use of the non-data symbols will be discussed in Section 4.

A feature called **Jabber Inhibit** permits the modem to detect if it is transmitting continuously. The modem shuts itself off after 1/2 second of continuous transmission. Jabber inhibit prevents a bad modem from bringing down the entire network.

The modem can take many forms. It can be a stand-alone box that connects some equipment to the medium, or it can be a board inside a station, or it can be a chip on a board. These different modem forms are shown in Figure 3-2.

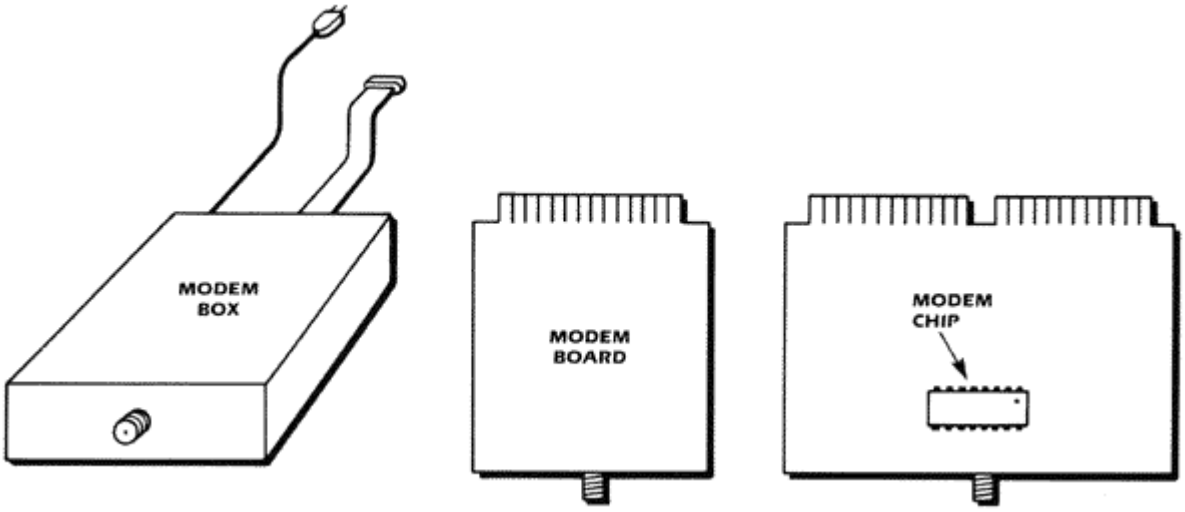

Figure 3-2. Various Forms of Modems

Generally the modem is not a separate box but is physically part of the station. Only the F-connector is exposed outside the station. The interface between the modem and the rest of the electronics in the station does not need to be exposed. This inside interface is called the **DTE-DCE Interface;** it is defined in the IEEE 802.4 Standard. This interface is also used on broadband and fiber optic modems. If a station is built so that the modem is removable from the station and uses the standard DTE-DCE interface, then it is possible to attach the station to different types of networks just by plugging in a different type of modem.

As the modem chips become available, they will be the preferred way to make modems. The modem chip reduces the cost and increases the reliability of the carrier-band modems. All that is needed with the modem chip is a crystal, a small transformer and a few resistors. It is possible to put the modem chip with the token bus control chip, described in Section 4, on the same board. The modem chips and the network control chips both have the DTE-DCE interface so that no additional circuits are needed to make the two work together.

The bit error rate specified in the carrier-band standard network states that no more than 1 bit will be received incorrectly for every billion bits sent if the noise at the receiver is less than -10 dBmV and the signal amplitude is more than 10 dBmV. This is a very good bit error rate and very appropriate for the automated factory. The function of the modem is to provide this level of performance.

Even though the modems are reliable and have excellent performance, it is possible for a modem to fail or the cable system to fail. In such cases, either a single station fails or, if the cable system is damaged, the whole network may fail. In some critical applications this is not acceptable. In these cases, two independent cable systems are installed to carry the same signals. Each station has a separate modem attached to each of the cable systems. This is called **Redundant Media.** If one cable system fails or if one modem fails, the whole network and each station on the network continue to operate.

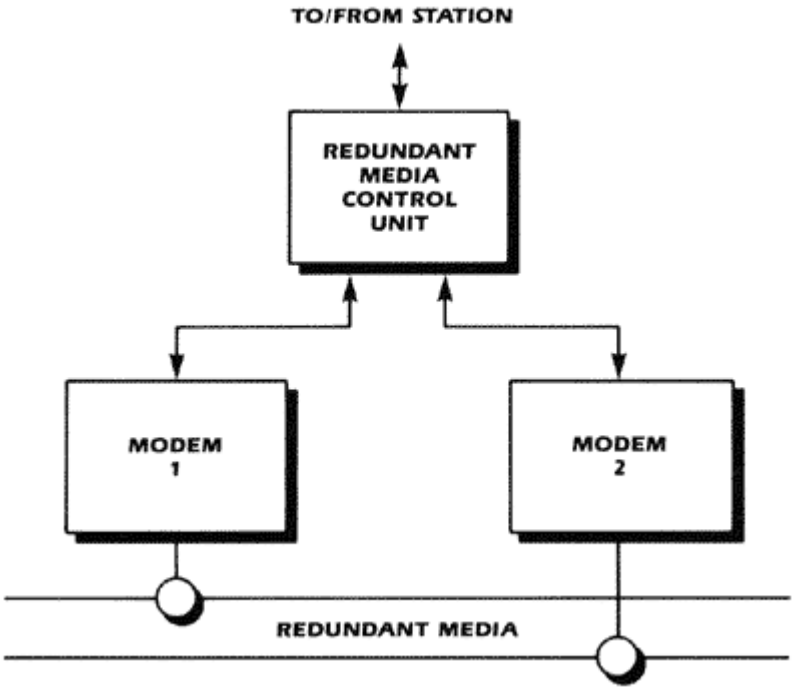

Figure 3-3. Redundant Media and Modems

When a station transmits, data are sent via both modems over both cable systems. When data are received, a redundant media control circuit selects which modem will be used based on which modem receives good data.

What has been described so far is an ability for one station to send data and for all the other stations to receive that data. In other words, the network wiring is shared by all the network devices. This is called a **broadcast medium.**

Terms

Bit Error Rate: The number of bits received in error divided by the total number of bits sent.

Broadcast Medium: The cable system that is shared by all stations; one station can transmit and all the others can receive signals.

DTE-OCE interface: The standard interface between a modem and the station.

Jabber Inhibit: Part of the modem that detects excessive transmission and inhibits it.

Medium: The entire cable system: wiring, taps, and terminators.

Modem: Part of the station that transmits and receives signals from the medium. (Also, an expression in American slang as in "gimme modem cookies".)

Redundant Media: Two or more cable systems carry the same signals.

Chapter 4: Token Bus Operation

On a local area network such as carrier-band, the cable system is shared by all the stations on the network. Any station can transmit; all stations can receive what is being transmitted. The shared cable is like a telephone party line. There are two questions that have to be answered for a shared cable:

1. Which station can transmit at what time? Two stations cannot transmit at the same time or the signals will be garbled.

2. For whom is the transmission intended? Every modem receives every transmission, but the transmission is intended for only one particular station.

Shared-Media Protocols

To use a shared cable, all the stations must follow the same rules. These rules are called a **protocol.** For the modems described in Section 3, the protocol consists of the data rate and the way that ones and zeros are represented by the FSK signals on the cable. All the stations have to send data at the same rate and represent ones and zeros by the same kinds of signals; otherwise the stations cannot communicate. Another protocol determines which station is allowed to transmit, how much data that station can send at a time, and which station uses the data that is received by every station.

Frames

Because the cable is shared, no one station may transmit all the time. Instead, a station sends data in chunks called **frames.** A frame is a sequence of contiguous bits that can be up to 8214 bytes long. In data communications terminology, an 8-bit byte is called an **octet.**

Addresses

On a shared cable, when one station transmits a frame, all stations receive this transmission. However, the frame is intended for only one specific station, so there must be a way to identify each station. Therefore, a unique **address** is assigned to each station, like a number on a house. Each station knows its own address.

The transmitting station puts address information into the frame as part of the data in the frame. This information is like the house number in the address on an envelope. The part of the frame that has the address data is called the **address field.** The address field is 12 octets long. Six octets are used for the **destination address,** the address of the station for which the frame is intended; six octets are used for the **source address,** the address of the station transmitting.

All the stations on the network receive each frame. Each station examines the received frame to see if the destination address contains its address. If the address does not match, the frame is discarded; if the address matches, the frame is kept.

Media Access

When a cable system is shared, a protocol is needed to determine which station has the right to transmit, or to access the medium, at any given time. If two stations transmit at the same time, there is a **collision,** i.e., the data is garbled. A protocol is needed to eliminate collisions.

For factory applications, medium access protocol must allow the user to calculate, for any given network, how long it will be, in the worst collision case, before any given station has the right to transmit. If the network access time can be calculated, the network is called **deterministic.** Deterministic networks are needed to control real-time processes. The **token passing** network protocol for media access provides a way for stations to share the cable system in a way that avoids collisions and makes the network deterministic.

Token-Passing Protocol

On a token-passing network, only one station at a time has the right to transmit. That station possesses a **token.** When the token-holding station is through transmitting normal data, it sends a **token frame,** which is a short message to the next station to tell it that it now has the right to transmit. The token is passed from station to station on the network. Some stations that get the token will transmit normal data; stations that have no data to transmit will simply pass the token on to the next station. All stations participating in the token passing form a **logical ring** as is shown in Figure 4-1.

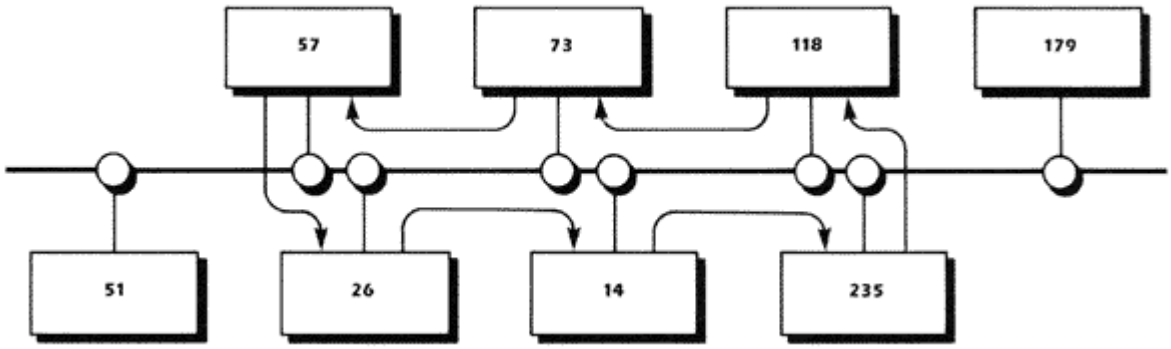

Figure 4-1. Token-Passing Logical Ring

Stations 235, 118, 73, 57, 26, 14,235... pass the token to each other in that order. The token is passed from a higher-addressed station to a lower one. The lowest-addressed station passes the token to the highest-addressed station. The time it takes for the token to be passed around the logical ring is called the **token rotation time.** For ease of explanation, the stations have been arranged in a circular placement on the cable. However, this need not be the case in a real network. Any station on the cable can have any address so long as it is unique. Stations 51 and 179 are not on the logical ring. They can receive frames but cannot send them. The basic token-passing protocol is simple, but there are a number of problems that have to be considered.

Problem 1: What if a station on the logical ring fails and cannot receive the token?

Solution: Each station knows not only the next station's address but also the previous token-holder's address. If a station tries to pass the token to its successor, but hears no subsequent activity on the medium, then it tries again. If again it hears no activity it sends out a **who__follows** frame asking for the successor of the failed station. The successor of the failed station then sends a **set__successor** frame identifying itself to the token holder. The station holding the token now knows a new successor and passes the token to it.

Problem 2: How does a new station get into the logical ring?

Solution: Periodically, a station holding the token will send out a **solicit__successor** frame asking if there are other stations that want to get in on the logical ring. The solicit-successor frame creates a **response window.** The response window is a period of time during which the token-holding station can accept an additional member of the logical ring. If another station does want to get into the logical ring, it sends back a **set__successor** frame and lets the token holder know that it is the next successor.

Problem 3: What if a number of stations want to get into the logical ring at the same time during a response window?

Solution: If a number of stations want to get into the logical ring during a response window, they will all send out the set-successor frame, there will be a collision, and the soliciting station will get a garbled message. The station holding the token senses the collision and sends out a **resolve__contention** frame. After this frame, the stations that want to get in on the logical ring **contend** for the privilege of getting into the logical ring in an orderly manner. Before describing how this contention proceeds, a characteristic of the network must be defined.

Slot time is the longest amount of time any station needs to wait for another station to respond. This delay is equal to the time it takes for a signal from the initiating station to propagate over the cable and be received by the addressed

station, for the addressed station to send out a response frame, and for the response frame signal to propagate back over the cable again. In any given network, the slot time must be calculated and put into each station as a network parameter.

Signals on the cable travel at about 82% of the velocity of light. This means that a meter of cable delays a signal about 4.1 nano-seconds. The typical delay of a single station's response is about 10 micro-seconds. A network with a 500 meter long cable system would have a slot time of:

$2 \times (500 \times 4.1 \times 10^{-9}) + 10 \times 10\text{-}6 = 14$ micro-seconds

Since the carrier-band network operates at 5 Mbits/second, each bit time is 0.2 microseconds and each octet time is 1.6 micro-seconds. The slot time in octets then becomes

14/1.6 = 8.75 octet times

Now back to contending for the logical ring.

During contention, all the stations that want to get into the logical ring listen for signals on the medium for 0, 1, 2, or 3 slot times. The amount of time a station waits is determined by taking the first pair of bits from its own address and determining the 0, 1, 2, or 3 slot times from that binary number. If a contending station hears no other station transmitting, then it sends a **set__successor** frame. This frame is one slot time long to the token holder. If a contending station hears anything during the time that it listens, that station eliminates itself from the contention. In this way, only one station gets into the logical ring every time the **resolve__contention** frame is sent.

If two stations have an identical first pair of bits in their addresses, then the stations will collide again. In this case, the procedure is repeated using the next pair of bits from the address. By the time all 48 bits of addresses are used, the contention is resolved, because eventually a pair of address bits for the two contending stations is different and only one station is admitted into the logical ring.

Problem 4: How does the logical ring get started initially? Or, what if a token gets lost?

Solution: If a station is connected to the medium and hears no signals, or if the station has been in the logical ring but now does not hear any activity on the medium, then the token is presumed to be lost. The station now sends out a frame that says it is claiming the token. This **claim__token** frame is 0, 2, 4, or 6 slot times long (based on pairs of bits from the station's address). If, after sending out the **claim__token** frame the station hears no bus activity, it knows it has

the token. If it hears activity, it assumes some other station has claimed the token.

This is a simplified explanation of how the token-passing protocol works. This protocol is implemented in semiconductor chips that work with the microprocessors in a network station. The people buying the factory automation equipment do not have to worry about the details of token-passing protocol built into the station.

The network manager has to know the concepts of token rotation time and slot time and how to calculate them, in order to set up the network correctly.

Priority

The data frames that are to be sent from a given station can be classified by their importance. The important frames can be given **priority** and sent first. Priority is an optional feature of any given station. Four classes of priority frames can be sent. Alarm and error messages could be assigned top priority. Real-time control messages could be the next priority file transfers the next, and periodic messages for time-of-day and other non-critical messages the last priority.

A token-holding station is allowed to send all the highest-priority frames it can within a time set by station management. When the time expires, then the token must be passed on.

For each of the lower-priority classes, a token rotation time is specified by the station management. If the actual token rotation time is less than the specified time, the station is allowed to send a priority message.

In a token bus system, the delay between when a frame is submitted for transmission and when it is actually sent can be calculated for a given system by knowing the number of stations, the size and frequency of frames that each station generates, and the priorities of the frames. When there is no load, the worst-case delay is the token rotation time. When the system is heavily loaded with the highest-priority messages, the delay is that of the token-passing time plus the time each station is allowed to send the first-priority messages.

Frame Structure

If a scope were used to look at signals on the cable, there would be a continuous stream of activity of various medium access control and data frames. as shown in Figure 4-2.

Figure 4-2. Token Bus Signal Activity

The short bursts of signal is the tokens being passed; the longer ones are the data frames. Figure 4-3 shows the structure of the data frame.

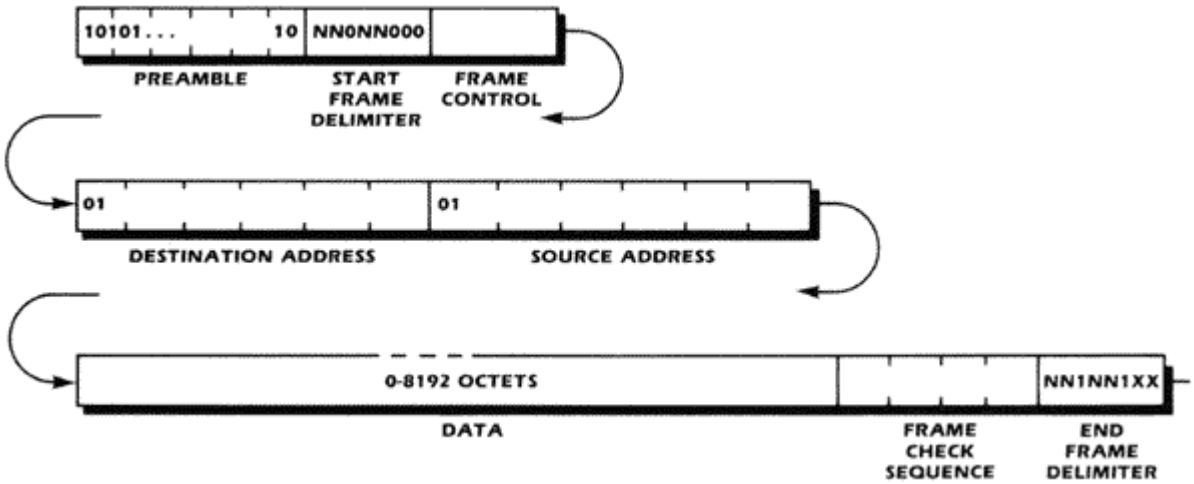

Figure 4-3. Frame Structure

Because the modem's receiving electronics need time to adapt to listen to the signal on the cable, each frame starts with a **preamble.** The preamble is like saying "pssst" to someone before starting to talk. It consists of six octets of alternating zeros and ones. Because the modem can lose some of these preamble bits, the station cannot simply depend on the number of preamble bits it received as an indication of where the real data starts. In order for the real data to be distinguished from the preamble, a **start delimiter** is used. The delimiter needs to be uniquely distinguished from the data that follow. For this reason, the start delimiter is made up of non-data symbols and zeros. Non-data symbols do not appear within the data portion of the frame.

One **frame control** octet is used to indicate the type of frame being sent (a token, a data frame, or a management frame), what the priority of the frame is, and other control information.

The frame must indicate which station on the shared medium it is intended for and which station it is sent from. This information is provided by the source and destination address fields. These addresses of physical stations on the medium are each 6 octets long.

Data follows the addresses. Data must be in integral octets up to 8191 in length.

The cable and the modem are susceptible to noise, which destroys the data being sent. To guard against frames with corrupted data, the **Frame Check**

Sequence, FCS, is used. As the data bits in the frame are transmitted, the transmitting station calculates the FCS code. The FCS is attached to the end of the frame. When the frame is received, the FCS is calculated again by the receiving station from the received bits including the sent FCS. If the result is not a particular bit pattern, then there must have been some bits that were destroyed in the transmission process. Frames that have bad frame check sequences are discarded.

For the FCS technique to work, the receiver of the frame must accurately know where the frame ends. For this reason, an **end delimiter** is needed. The end delimiter is made up of non-data symbols and ones. As in the start delimiter, the non-data symbols are necessary so that any data sent in the data portion of the frame will not be confused with the end delimiter.

MAC Services

When the carrier-band modem was discussed in Section 3, it was easy to identify that part of the station; the modem was a box, a board, or a chip. The part of the station that has just been described is not as easy to identify. Some of the protocol is performed by a semiconductor chip; other parts are performed by software running in a microprocessor in the station. Conceptually, we can think of a "box" within the network station that performs these protocol tasks, as shown in Figure 4-4.

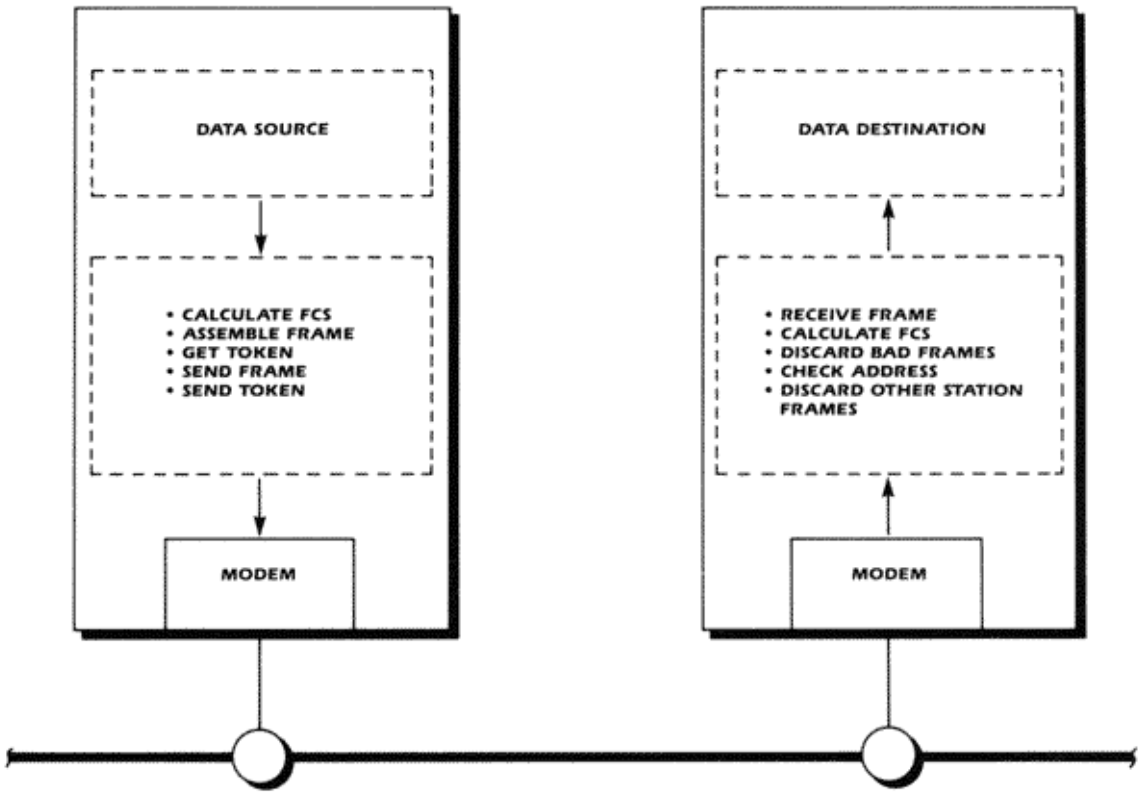

Figure 4-4. MAC Functions

In a transmitting station, the "box" gets a data block from a data source to send and then waits to get a token to gain access rights to the shared cable. If the priority is right, the "box" then sends a frame with a preamble, a start delimiter, an address field a control field, the data itself, the frame check sequences, and then the end delimiter.

In a receiving station, the "box" recognizes addresses and examines the FCS to see if good data has been received. The "box" discards corrupted frames and passes only good data blocks to a data destination "box" in the receiving station.

All together, this part of the network station is called the **Medium Access Control** or **MAC.** MAC performs a **service** for other "boxes" in the station, and it utilizes the service provided by the modem.

What has been described so far, the cable system, the modem, and the MAC token bus protocol, is directly related to the carrier-band network. Other protocols are needed to provide communication between two stations on the carrier-band network. These protocols deal with how reliable data transmission is achieved even when some of the frames are lost to noise. The protocols also deal with how the flow of data between a sending station and receiving station is regulated, and many, many other issues. These higher protocols, which are the same for the factory broadband network and even other types of networks, will be discussed in Sections 5 and 6.

Terms

Address: An identification of a station.

Collision: The result of two or more stations transmitting simultaneously and getting the signals garbled.

Contention: The process by which multiple stations attempt to get into the logical ring during the same response window.

Deterministic: A network in which the time between when a station needs to transmit and when it is permitted to, so it can be calculated.

Destination Address: The address of the station for which a frame is intended.

End Delimiter: An octet that defines the end of a frame.

Frame: A group of contiguous bits.

Frame Check Sequence, FCS: A code that is used to determine whether a frame was received correctly.

Frame Control: An octet in a frame that identifies the type of the frame.

Logical Ring: A group of stations that pass the token to each other.

Medium Access Control, MAC: The part of a station that performs the protocols needed for sharing the cable.

Octet: An 8-bit byte.

Preamble: The initial signal of a frame to get the modem ready to receive.

Priority: Ability to give transmission preference to more important frames.

Protocol: Rules that all stations must follow in order to communicate.

Response Window: Time during which a new station is admitted into the logical ring.

Service: A group of tasks that one part of a station performs for another part of the station.

Slot Time: The worst-case time between when a station sends a frame and the time when it can get a response.

Source Address: The address of the station sending a frame.

Start Frame Delimiter: An octet that defines the start of real data in a frame.

Token: The right to transmit.

Token Passing: A deterministic protocol for gaining access to a shared cable.

Token Rotation Time: The time it takes for a token to be passed around the logical ring.

Chapter 5: Logical Link Protocol

So far, the discussion has been about network topics that are hardware related: cables, taps, modems, and medium access semiconductor chips. Now a protocol will be examined that is implemented in computer software.

Protocols can be described by the **service** they provide. The modem provides the service of sending and receiving ones, zeros, and non-data symbols. The modem service is used by the Medium Access Control, or MAC, protocol. The MAC protocol provides the service of sending frames. The next protocol, the **Logical Link Control, LLC,** uses the service of the MAC and provides a reliable way of sending frames.

Each of the protocols can be thought of as a department within a company. Each department receives services from a department below and gives services to a user department above, as shown in Figure 5-1. User A in one station is sending data to User B in another station using the LLC services.

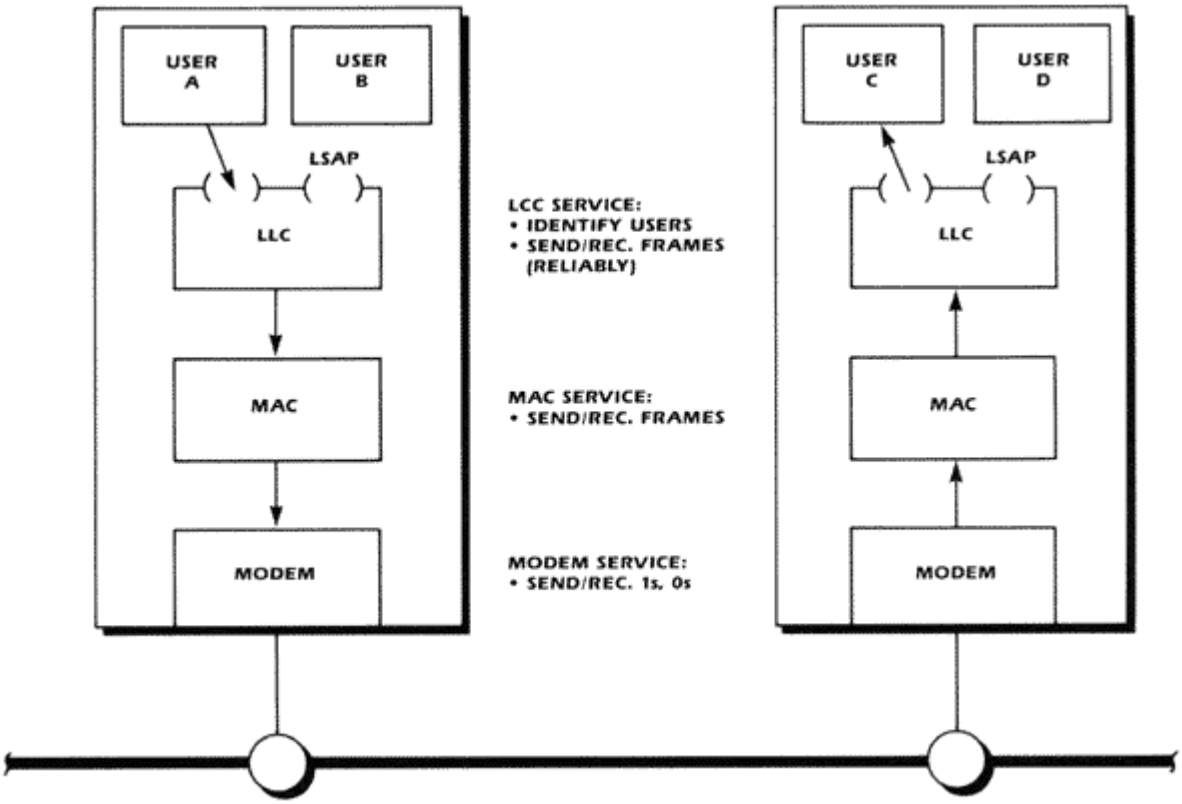

Figure 5-1. Protocols and Services

LLC can provide services to a number of users in higher "departments". Within a station, there may be several protocols or computer programs that are the users of the LLC services. The LLC users are identified by the **Link Service Access Points,** or **LSAPs** in a frame being sent.

If you were to walk into the LLC Department and ask, "Who do you work for?" the "people" there would answer:

"We in the LLC department work for the departments on the other side of the doors identified by the LSAPs. They give us frames to ship and we ship them; or if we get some frames from the network, we give them to the appropriate department above."

Another way to think of the LSAPs is to consider them as a component of the address. The source or destination address in a frame is similar to the street number of a building; the LSAP is similar to the department name within the building.

Figure 5-2 shows where the LSAP fields are located in the frame. The portion of the frame that was simply labeled "data" as far as the MAC layer was concerned is not all used for data. Part of the frame is used by the LLC. The LSAPs are two octets, the **Destination Service Access Point, DSAP,** that identifies the

destination user and the **Source Service Access Point, SSAP,** that identifies the source user, as shown in Figure 5-2. Most of the time, the codes in both these fields are the same because the protocols that use the LLC services need to be the same in order to work with each other. Specific LSAP codes have been assigned to identify specific standard higher-layer protocols.

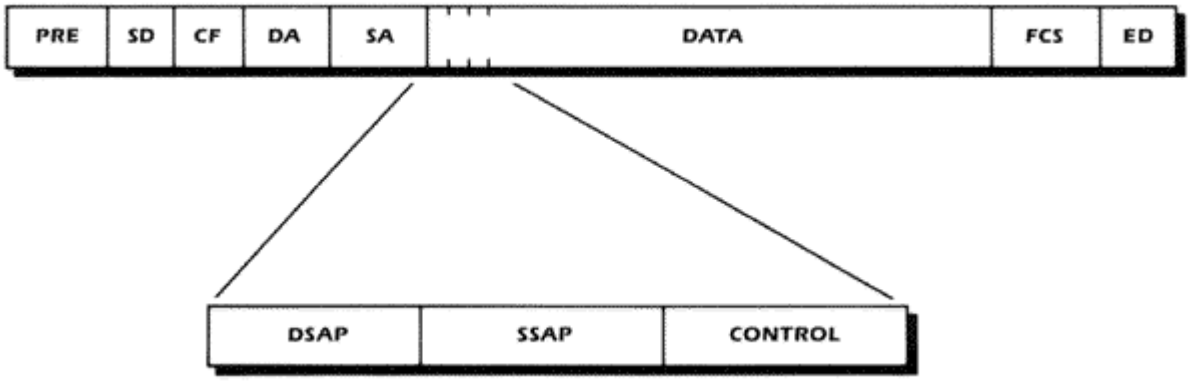

Figure 5-2. LLC Fields

Two LSAP codes of particular interest to the carrier-band network are:

01110010 Manufacturing Messaging Service Protocol, EIA Standard RS-511.

01111111 The ISO inter-network protocol.

These protocols will be discussed in Sections 6 and 7, respectively

The third octet, the **Control** field, is used for identifying the type of service that the LLC protocol is to perform and the control data associated with that service.

There are three types of LLC services defined in the IEEE 802.2 standard. Only Type 1 and Type 3 are relevant for the carrier-band network.

Type 1 Service

The **Type 1 service** is called **unacknowledged.** The Unacknowledged LLC service does nothing more than MAC does. The data submitted to LLC is simply sent and no further action is taken by the LLC to assure that the data is correctly received by the other station. Most of the time the data is delivered correctly because the carrier-band network is inherently reliable. Sometimes, however, the data is corrupted by noise on the medium. In that case, the FCS is not correct and the data frame is discarded by the receiving stations. In addition, if the receiving station is overloaded and has no memory buffers to accommodate the incoming data, again the data is lost. If the Type 1 service is used, the concern for reliable data delivery is something for higher protocols to worry about. For some applications, Type 1 service is all that is needed.

Type 3 Service

LLC can also provide a reliable frame-delivery service. When Type 3 LLC service is used, the source and destination LLCs cooperate to make sure the frames are delivered correctly Whenever a frame of data is received by the destination LLC and the destination LLC user is willing to deal with the frame (memory buffers are available), then an **Acknowledgment, ACK,** frame is sent by the destination LLC to the source LLC. The Type 3 service is also called **Acknowledged Connectionless.**

Figure 5-3 shows a frame being submitted to LLC, being sent (1) and being delivered to the destination LLC client. The destination LLC then sends an acknowledgment (2) to the source LLC, and a confirmation is given to the source LLC service user that the frame has been delivered. In Figure 5-3, the services under the LLCs, the MAC, and the modem are not shown but are simply assumed to be there.

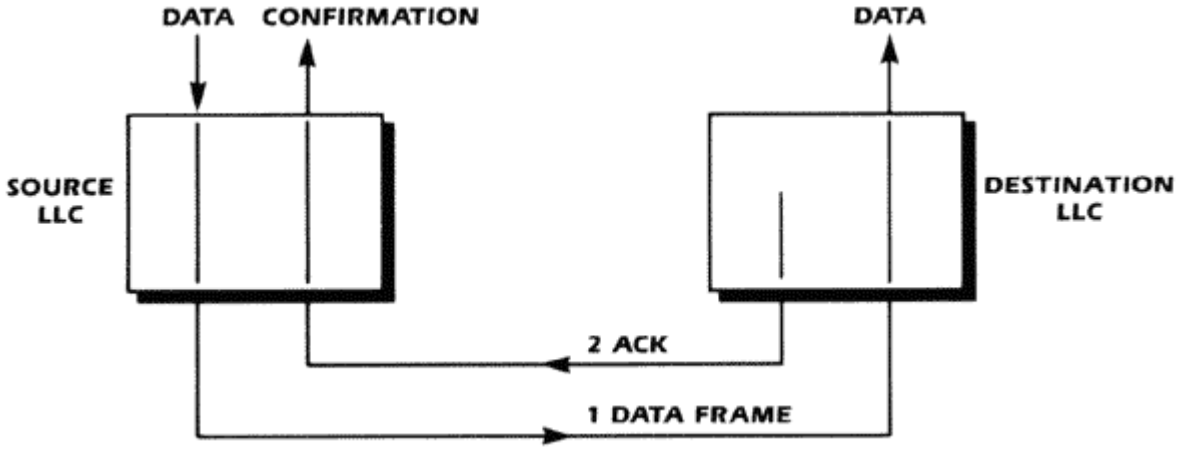

Figure 5-3. Acknowledged Connectionless LLC Service

The source LLC keeps a copy of the data frame that it has sent until it gets an ACK. If the source LLC does not receive an acknowledgment within a given period of time, it sends, or **Retransmits,** the frame again. Figure 5-4 shows the retransmission.

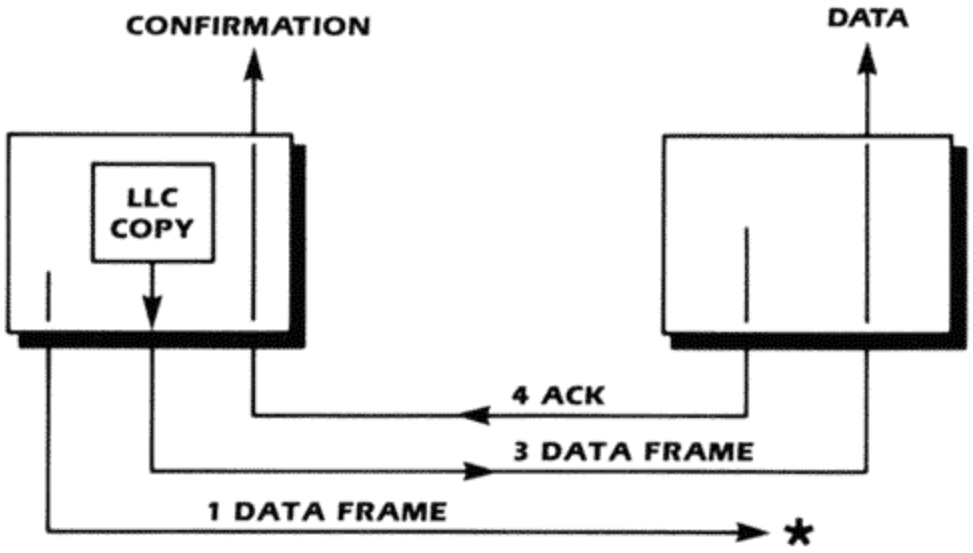

Figure 5-4. Retransmission

When a frame had been sent but was lost (1), the source LLC times out and retransmits the frame again (3). The destination LLC then acknowledges the frame (4).

The waiting time for acknowledgment is controlled by a **retransmission timer.** The retransmission is repeated until the frame gets acknowledged or the source LLC gives up. The station being addressed may have failed, so there is no point in trying to send to it indefinitely The number of times the source LLC will retry is controlled by the **retry counter.**

The retransmission timer and the retry counter are two parameters that can be set by the network manager.

A possibility exists that the ACK itself may get destroyed in transmission, as shown by the asterisk in Figure 5-5.

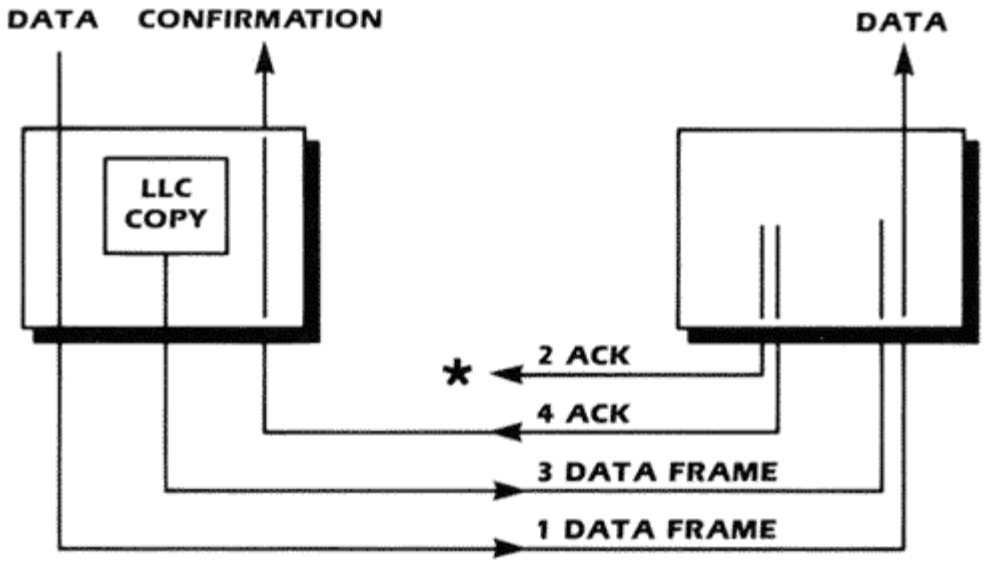

Figure 5-5. Duplicate Frames

When sending an ACK or the requested data, the responding station does not get the token. The responding LLC gets an implicit temporary right to transmit. The LLC Type 3 service works closely with its MAC protocol to get temporary transmission rights. With this service, not all stations on the carrier-band network need to be in the logical ring and get the token in order to transmit on the network. Simple devices can be sent data or be polled by the station that is holding the token

Diagnostic Aids

The LLC Type 3 protocol has the capability to indicate its operation to its users. One such indication is the ACK that tells the user that the frame has been successfully delivered. There are other indications. If, for example, it is not possible for a destination LLC to give a data frame to its client, it will notify the source LLC of that condition by means of a **Status Field,** which is part of the ACK frame, and the source LLC will notify its user. This condition can happen if the wrong LSAP is sent and the receiving LLC does not have anyone to give the data to. In case of problems, diagnostic messages are very useful for determining why the network is not operating as expected.

The status frames can also be used to control the rate at which data is sent between stations. If the destination LLC user runs out of buffer space for frames, it can notify the source LLC user to slow down the sending. This is called **Flow Control.**

Another diagnostic capability of the LLC protocol is the **Loopback.** If a station receives a data frame with a control field that requests a loopback, the receiving station returns the same data frame to the sending station.

In this way a network management station can interrogate each station on the network and find out if the modem, the MAC, and the LLC protocol in the remote station are working. The loopback can be used only with stations that are in or can get into the logical ring. For stations that do not have the token-holding capability but are only simple responders, the response itself is an indication that the station is functioning.

Summary of LLC

The Logical Link Control protocol provides the ability to interconnect two LLC users in two network stations. The LLC provides a means of identifying the users of the LLC service with LSAPs. The stations are interconnected physically with the cable system; the users of the LLC services are connected to each other logically through the LSAPs. This is why the protocol is called Logical Link Control. The LLC Type 1 service is unreliable because the LLC user does not get a confirmation that a frame was received. The Type 3 service is reliable because the LLC user gets a confirmation that the destination has received a frame.

Terms

Acknowledgment, ACK: A response frame that indicates that a data frame has been received correctly.

Acknowledged Connectionless: The Type 3 LLC service where frame delivery is guaranteed and the sending user is notified of the success of the transmission.

Control Field: A field, which identifies the type of service, the LLC protocol performs.

Destination Service Access Point, DSAP: The identification of the destination user of the LLC.

Duplicate Frame: A frame received twice because an acknowledgment frame was lost.

Flow Control: The ability of the destination LLC user to send a status frame to the source LLC user indicating that it is out of buffer space.

Link Service Access Point, LSAP: A field within the frame that identifies the users of the LLC service.

Logical Link Control, LLC: The protocol responsible for identifying users of the network and the provision of reliable frame delivery.

Loopback: The ability of one station to send data to another station with the request that the same data be returned.

Reply Service: A service where one station can ask another for data.

Retransmission: The repeated sending of a frame if an ACK is not received by the source LLC.

Retransmission Time: The amount of time that a source LLC waits for an ACK before it retransmits a frame again.

Retry Count: The number of times that a source LLC will try to send a frame before it gives up.

Sequence Number: A number in each data frame that is used to identify duplicate frames.

Service: Some task that one protocol performs for another protocol or for a program.

Source Service Access Point, SSAP: The identification of the source user of the LLC.

Status Field: Part of the ACK frame sent by the destination LLC to the source LLC used to indicate reception of data or other status.

Type 1 Service: Sending of frames without expecting acknowledgment (also called "send and pray").

Type 3 Service: Sending of frames and expecting acknowledgment or retransmitting the frame again.

Unacknowledged: Type 1 service where frames are sent but not necessarily received correctly.

Chapter 6: Network Interconnection

Some stations on the carrier-band network may need to communicate with other stations in the factory that are on different networks. For example, the cell controller may need to get instructions from a production scheduling computer and send the results of some operation to an accounting computer. For this communication to take place, it is necessary for the carrier-band network to be interconnected with other networks. Networks can be interconnected in a number of ways.

Repeater

The size of the carrier-band network is limited by the cable characteristics. If the size of the network needs to be bigger, a device called a **repeater** can be used. A repeater joins two cable segments. Any signal on one cable segment is received by the repeater, put into digital form (that is, turned into ones, zeros, or non-data symbols) and transmitted as signals on the other cable segment, as shown in Figure 6-1.

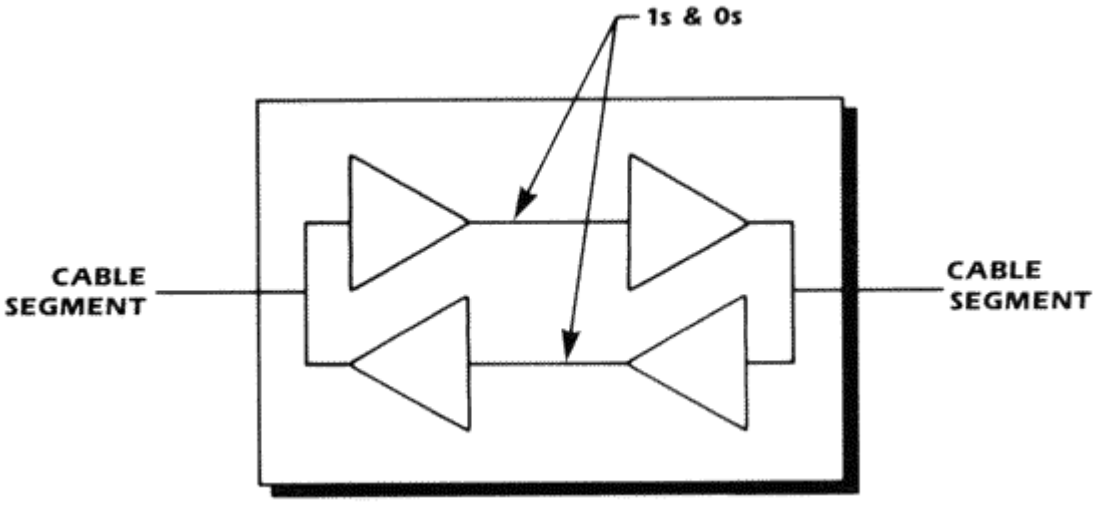

Figure 6-1. Repeater

A repeater does more than just amplify signals; it regenerates the data symbols and then converts them back into signals. The repeater can be thought of as a pair of back-to-back modems.

The repeater is not a station because it does not have an address. Stations on the network do not have to know that a repeater is on the trunk cable or work any differently; a repeater is transparent to them. A repeater simply joins two cable segments.

Bridge

A bridge is a smart repeater that knows whether stations are located on one or the other cable segment. Instead of taking all frames from one cable segment and sending them on to the other segment, a bridge examines the destination address of the frame. If the destination station and the source station are on different segments, the bridge repeats the frame. If the source and destination stations are on the same segment, the bridge discards the frame as shown in Figure 6-2.

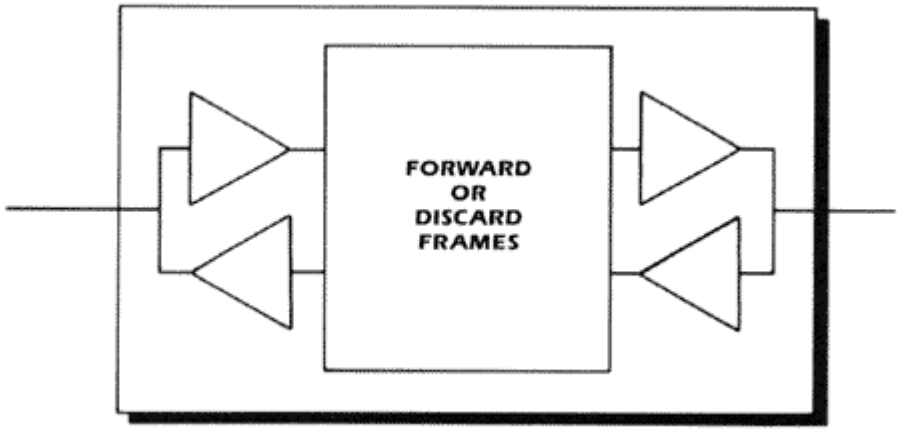

Figure 6-2. Bridge Operation

In order for the bridge to work, the addresses of the stations on the interconnected segments have to be unique. Bridges can be configured by network management to know where each station in the network is located, or the bridge can learn the location of the stations itself. When the learning bridge begins operation, it acts like a repeater and passes all frames from one segment to the other. Each time the bridge receives a frame, it notes the source address and the segment the frame came from. As time goes by the bridge develops the knowledge of the location of all the stations that transmit on the two segments. The learning bridge cannot learn the locations of the non-transmitting stations. Bridges are also different from repeaters in that the token frames are not repeated across the bridge. Each cable segment has its own token. A bridge participates in the token passing on both of the cable segments. For this reason, a bridge has to have an address on each cable segment.

A bridge can be used between two carrier-band network cable segments, or it can be used between a carrier-band and a broadband token network. There is a restriction: the two networks connected by the bridge, must be unique. Also, the frame sizes on each network must be the same. The bridge has no capability to take a, say 8000-octet frame that is possible in the token bus network and put this frame on a network that has a 1500-octet frame limit.

Bridges are useful because they can be used to interconnect networks that have related but independent applications. Bridges separate the data traffic in each network from the other so that the token rotation time and the amount of data traffic on each network are kept at lower levels. The stations that need to communicate across the bridge do so transparently, without having to know that a bridge exists.

Router

In situations where two different networks are to be interconnected, a **router** is used. Routers overcome the limitations of the bridge. The addresses of the stations on the interconnected networks do not have to be unique; the addresses on each network can be independently administered. Routers can also take care of the different frame sizes used on the two networks by segmenting large frames into smaller ones and reassembling small frames into larger ones.

There is a price to pay for these features, however. Routers and the stations that use them have to use another protocol called the ISO Network protocol. This protocol is identified by the LSAP discussed in Section 5. Frames from a station on one network that need to be sent to a station on another network have to be explicitly addressed and sent to the router with directions on how to forward the frame to its ultimate destination. This requires that networks, not just stations on a network, be uniquely identified with a network address.

Most of the stations on carrier-band networks do not use the services of a router. Only the cell controller or other sophisticated devices may have this capability. This will be discussed later in "Enhanced Performance Architecture and Mini-MAP".

Gateway

When two networks are very different in the kinds of data communications or applications protocols that they use, then a **gateway** is needed. A gateway not only interconnects the networks, but also translates between the two types of protocols. Depending on the complexity of the translation, the gateway can be an expensive device and may severely restrict the flow of data between the two networks.

Enhanced Performance Architecture and Mini-MAP

Now that the differences between repeaters, bridges, routers, and gateways have been discussed, the architecture of the carrier-band network can be examined more closely

Most of the stations on a carrier-band network are not expected to communicate with stations on other networks. In these cases, the stations have no need to use routers or gateways. These stations are likely to use the Manufacturing Message Service, MMS, directly with the LLC Type 3 protocol without the need for any other data communications protocols. In specific factories, such as a semiconductor processing plant, special application protocols may be developed, much like MMS, that are suited for the specialized applications. The stations that use an application protocol directly with the LLC protocol are referred to as **Mini-MAP**. As compared to full MAP stations that use more powerful protocols to communicate world-wide, Mini-MAP stations are quite simple and relatively inexpensive in their data communications capabilities. Mini-MAP stations are intended for real-time application.

In some situations, a station on the carrier-band network needs to communicate with other stations on other networks. This would be a requirement for a cell controller. Files of information that tell the cell what to make may need to be down-loaded to the controller from some computer within the factory. Production data may need to be uploaded from the cell controller to some other computer in the factory or even to some financial computer at the company headquarters. For this communication, a comprehensive set of data communications protocols must be used. These are the Network, Transport, Session, Presentation and FTAM (File Transfer, Access and Management) protocols. They are not discussed in this Handbook.

On the other hand, when the cell controller is not engaged in long-distance communications, it has to work in real-time with the mini-MAP stations on the carrier-band network and utilize the minimal protocols. The stations that have both the full and mini-MAP capability are called Enhanced Performance Architecture, EPA. The structure of an EPA and a mini-MAP station are shown in Figure 6-3.

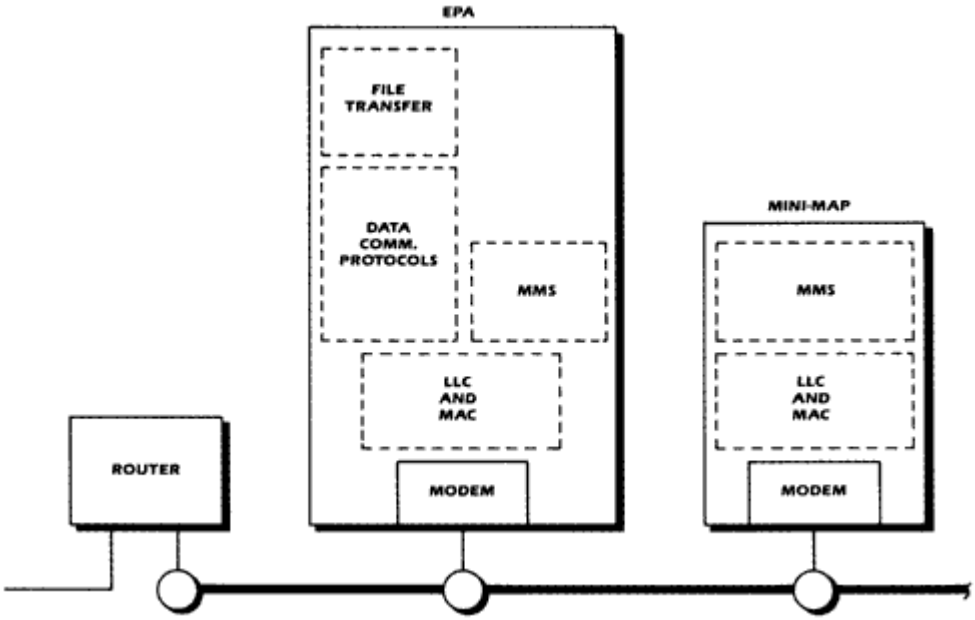

Figure 6-3. EPA and Mini-MAP Stations

Terms

Bridge: A device used to transparently interconnect two similar networks and to separate the data traffic between them.

Enhanced Performance Architecture: A station that incorporates both the mini-MAP capabilities and the general data communications protocols.

Gateway: A station use to interconnect two different types of networks and to translate application protocols.

Mini-MAP: A station whose application protocol works directly with the Logical Link Control protocol and that communicates only with stations on its own network.

Repeater: A device used to extend the distance of the cable by interconnecting two cable segments and regenerating the signals between them.

Router: A station between two similar or dissimilar networks used to route data through possibly many interconnected networks.

Chapter 7: Network Planning and Design

Because the carrier-band network is normally used for a small area within a factory, it usually has only a few stations. Although planning for a small network is relatively simple, it still is instructive to go through the planning process and describe one way that planning can be done. Regardless of the size of the network, it is easier to modify or expand the network at a later time when the network's configuration and capabilities are documented.

Every network is unique in that it has particular requirements. The procedures suggested here should be viewed only as a checklist of items to be considered, and not as hard-and-fast rules.

Three steps need to be taken: requirements determination, analysis, and detailed design.

Requirements

The first thing to do is determine what the network is to do. Start out by listing all the stations that need to be connected to the network. Consider a bridge or a router as a single station, even though many stations on other networks may be connected through it. Also, list all devices that might be attached to the network in the future.

List the amount of data per second, the frames, and the octets in the frames that each station will send, and identify which stations are to receive the data. Don't forget that each frame has 22 octets of protocol data besides the Manufacturing Message Service data.

To visualize the network activity, make a matrix. List each station on both axes of the matrix. The stations in the vertical list are transmitting; the ones in the horizontal are receiving. Enter the data traffic in the intersections. A sample matrix is shown in Figure 7-1.

FROM: \ TO:	CONT.	TM1	TM2	BR.	A	B	C	
CONT.		6 32	4 32	1 4000	30 120	30 200	30 380	101 25,320
TM1	4 32			5 320				9 1,728
TM2	6 32			8 32				14 448
BR.	2 4000	5 132	3 150					10 9,110
A	30 60					1 50	1 50	32 1,900
B	30 70				1 50		1 50	32 2,200
C	30 80				1 50	1 50		32 2,500
	102 14,620	11 852	7 578	14 5,856	32 3,700	32 6,100	32 11,500	230 43,206 TOTAL

Figure 7-1. A Data Traffic Matrix

In the sample matrix, the number of frames per second is listed first in each intersection and the length of the frames is listed below. The amount of data is the product of the two. Note that the stations do not send data to themselves and that some stations may not have anything to do with some other stations.

Add all the rows to determine traffic out of each device. Add all columns to get the traffic going into each device. The sum of all the data traffic from all the sources should equal the sum of all the data traffic from the destinations. In the example of Figure 7-1, the network carries 230 frames and 43,206 octets every second.

The matrix can be used to get a quick look at the data traffic on the network. The major data sources or destinations can be readily identified, and the overall network traffic can be estimated.

Next, get a plan of the area where the network is to be used, and identify the approximate locations of all the stations.

At this point, there is an approximation of how much data the network has to carry and how large the network is going to be.

Analysis

Before a cable system can be designed that will interconnect all the identified devices, it is necessary to know what the networks limitations are.

Size Limitations

The carrier-band network is limited in both the area it can cover and the number of stations it can interconnect by the cable-system characteristics discussed in Section 2. For any given type of cable, the cable vendor should provide three important parameters of the trunk cable:

- the maximum length of the cable over which the cable is within the IEEE 802.4 specification,
- the cable attenuation, and
- the noise-immunity figure of the cable.

As an example, consider a particular cable that has a distance rating of 500 meters. This limitation may be due to the tilt of the cable or to group delay-characteristics rather than signal attenuation. The reason for the limitation is not important; the only parameter that matters is the distance rating. In effect, the rating means that the 500-meter-long cable can connect at least two stations and work within the specifications in the IEEE Standard 802.4.

Assume that the taps have a 20-dB trunk-to-drop attenuation and a 20-dB drop-to-trunk attenuation. A transmitting station at one end of the cable can send a signal as small as +63 dBmV. The receiving station at the other end of the cable needs at least + 10 dBmV of signal. Therefore, the maximum amount of signal attenuation by the trunk cable and the taps is:

63 - 20 - 20 - 10 = 13dB

Assume that the trunk-cable attenuation for this particular cable is 1.5 *dB*/100 meters. The 500 meters of cable attenuates the signal 7.5 dB. This leaves

13 - 7.5 = 5.5 dB

for the taps.

If 4-port taps with an insertion loss of 0.5 dB each are used, the number of taps that can be put on the trunk cable before the signal becomes too small is:

5.5/0.5 = 11

Since each tap has four ports, the number of stations is 44. If more taps are needed, then the cable length has to be shorter.

If the trunk cable length were zero, then all 13 dB of signal could be used for taps. The number of taps that could be on the network would be:

13/0.5 = 26

The number of stations would be 104.

The relationship between the number of taps and the trunk-cable distance is shown in Figure 7-2. This figure defines the maximum limits of a carrier-band network using the particular taps and trunk cable in this example. Other types of cable and other taps will have different characteristics. Any network to the left of and below the line will work within the IEEE Standard 802.4 limits; any network above and to the right of the line is out of the specifications of the Standard.

If terminating taps are used, the network's capability is increased.

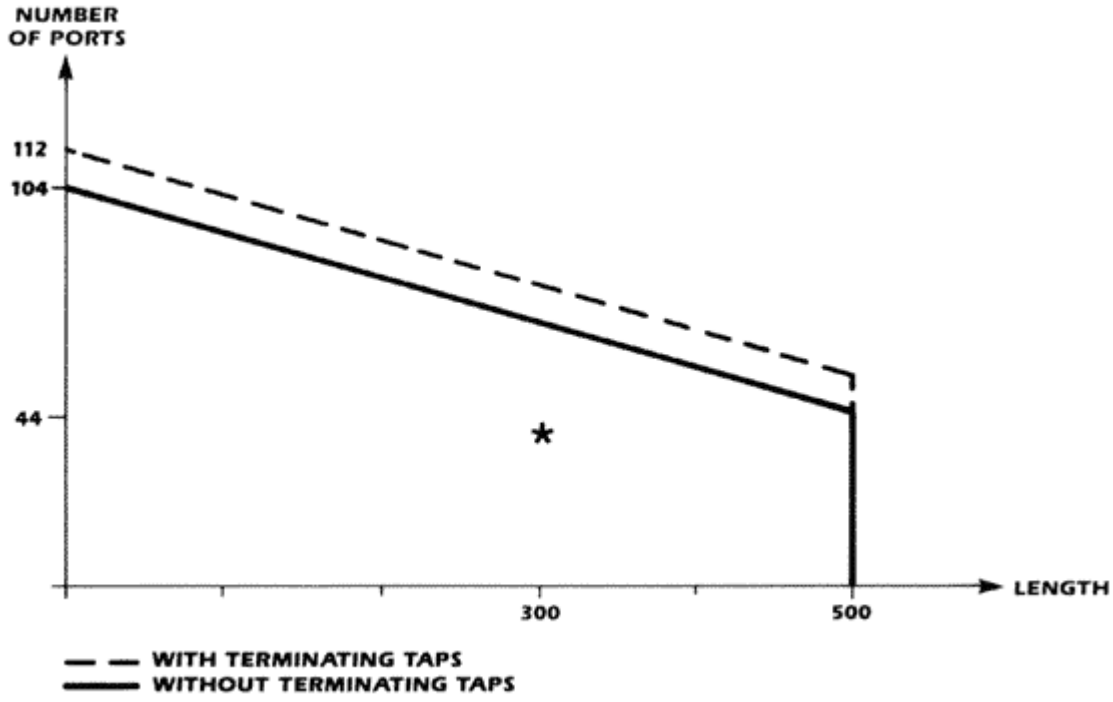

Figure 7-2. Network Size Limitations

If this cable and these taps were used in a particular situation where the cable had to be only 300 meters long and there were only 40 devices on the network (10 four-port taps), the operation point of the network would be as indicated by the asterisk in Figure 7-2. The further away from the maximum line that an actual network is operated, the more reliable it will be. The closer to these limits the network is operated, the less reliable it will be.

So far, only the attenuation of the trunk cable has been discussed. The drop cables also have attenuation, tilt, and group delay. Because the drop cables are generally short, these characteristics are negligible. During planning, however, the maximum length of the drop cables should be examined to make sure they are within the allowable limits. For the 300-meter-long trunk cable described above, if it is assumed that the drop cable is the same type as the trunk cable, the total length of cable between any two stations must be less than 500 meters because of the cable distance rating, as is shown in Figure 7-3.

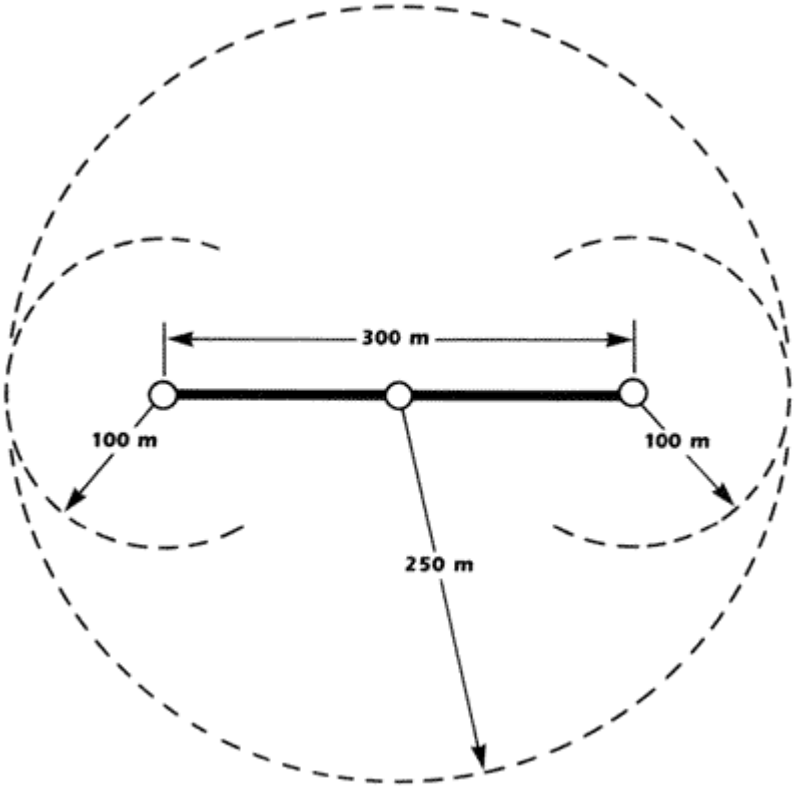

Figure 7-3. Area Limitation

Although the figure shows the trunk cable as a straight line, the trunk cable can be routed in any shape. The area served by the cable system can be in shapes other than the one shown.

Note: The IEEE 802.4 Standard limits the drop cable length to 50 meters. This limitation is based on the premise that the signal attenuation between drop cable ports on a tap may be 0 dB. Most taps, however, have an attenuation between drop cable ports of 20 dB. This means that the drop cables can be any length provided that the normal signal limitations are met.

Noise Limitation

The other major limitation is the noise environment in which the network can operate. The noise environment is very difficult to predict before a network is installed. The noise could come from stations that would be connected to the network after it is installed. Before the stations are operating, however, there is no noise. Even if the noise sources are present before the network is installed, noise is difficult to measure, and it is even more difficult to predict how it will affect the cable system. Perhaps the best way to deal with potential noise problems is to eliminate the ways in which noise can affect the network.

The maximum amount of noise on the drop cable at a station is allowed to be up to

- 10 dBmv. Noise is picked up mostly by the trunk cable because it is generally much longer than the drop cables. With 20 dB taps, the most noise on the trunk cable can be:

- 10 dBmv +20 dBmV = + 10 dBmv.

Assume that a trunk cable of questionable quality is used and the noise on the trunk cable is + 10 dBmv. The network operates, but on the edge of disaster. If a new piece of equipment is brought into the network area and adds to the noise, then the network operation becomes erratic and many errors are caused by the noise. If a quality armored cable is used instead, the noise on the trunk cable is reduced by as much as 50 dB. The noise voltage level could then increase several hundred times without affecting the network operation. One reason that armored trunk cable is recommended for the carrier-band network is that it is an insurance against present and future noise.

Section 9 gives a number of recommendations for reducing noise susceptibility with good cable installation practices. The important recommendation is: use a good-quality armored cable. The armored cable should be more than adequate for most environments unless there is equipment nearby that produces very large electric arcs, such as arc furnaces of power-switching yards. In that case, the cables should be put into conduits.

Data-Rate Limitation

The data rate of the carrier-band network, S Mbits/sec., is the theoretical

maximum capacity of the network. The time to pass the token and the time to get ready to send each frame must be subtracted from this maximum data rate. In the example in figure 8-1, the estimate of the network traffic was 230 frames/second and 43.206 octets, or about 350,000 bits/sec. If there is a 10-microsecond time delay between a station getting a token (or an implicit token) and actually starting to send data, for the 230 frames, the equivalent bit times added for the 230 frames would be:

10 μ sec. x 5 bits/μ sec. x 230 = 11,500

A token frame is 22 octets or 1 76 bits long. Assume that, after sending data, a station takes 10 microseconds to get ready to pass the token, and that a station sends only one data frame every time it holds the token. The amount of equivalent bit times it takes to pass the token every second is:

{176 + (10 μ sec. x 5 bits/μ sec.) } x 230 frames = 51,980 equivalent bit times.

The total equivalent bit times that will be taken up for sending the estimated amount of data and passing the token is then:

350,000 + 11,500 + 51,980 = 413,480

Since this time is only about 8% of the total network capacity, the token will be going around many times before any station sends data. Low network utilization is good because the estimated data traffic is an average, not peak data traffic. Also, estimates tend to be low because not all possible cases are considered during the initial planning. One of Murphy's laws states that network traffic increases to use up the available capacity. As a rule of thumb, the network traffic should be kept below 50%.

If data traffic is too high, the network may need to be partitioned into several parts by a bridge or a router. Partitioning may be desirable for other reasons. Real-time requirements for one group of stations may be incompatible with other stations that use the network for file transfer between computers or for terminal-to-computer data. Also, segregation may be desirable for critical applications so that the failure of a non-critical station does not affect the critical stations.

A non-technical reason for partitioning a network into smaller parts may be an organizational consideration. For example, if two different functional areas of a factory that use the same network to report to different department heads, there may be problems such as, who pays for the network, who maintains it, and who gets blamed if the network fails.

Once the general requirements of the network are known and the basic limits of the network are understood, a number of questions can be answered:

Should the network be segmented by bridges or routers into smaller networks? What is the approximate trunk-cable length and the number of taps needed?

Once these questions have been answered, the analysis can be performed to see whether the proposed network can satisfy the requirements. When the general characteristics of the network are known, the detailed planning can begin. Keep the requirements and the analysis as part of the network record. If the network has to be expanded later, this record is a valuable starting point. Also, when the network is operating, measurements can be made to determine the actual data traffic on the network. The actual traffic can then be compared to the estimated traffic to provide feedback for future network planning.

Network Design

Before the detailed network design can begin, the final cable-system components must be selected including the trunk and drop cables and the taps.

Network Component Selection

Many different types of cable-system components can be used nominally for the carrier-band network. For example, almost any type of 75-ohm cable can be used. The common wisdom is to buy cable at the lowest price and save money, but a little reflection shows that this approach is not the best.

The cost of the cable is only a small fraction of the overall cable-system cost. A much larger cost is the installation of the cable system, as shown in Table 7-1 below:

Site survey and cable-system design	15%
Installation labor	45%
Materials	25%
Documentation and validation	15%

Table 7-1. Cable-System Installation Costs

An unreliable cable system costs more. In some factories, the cost of a network failing is estimated at $30,000 per minute in lost production alone. What does it cost to have maintenance people constantly fix the cable system? What does it cost to have to rewire the factory? These costs are often intangible before the network starts to fail. It is easy for a network designer or purchasing agent to specify a low-grade cable or other components to show management where a little money can be saved. It is easy for the cable-installation contractor to put in a lower-grade cable to make money on a low bid. It is difficult to justify the extra costs for quality components. It seems that there is never enough money to do it right the first time, but always enough money to do it over.

The recommended cable for carrier-band network for industrial use is the armored flexible cable or the semi-rigid cable installed by professional cable contractors. The taps should be industrial grade with the characteristics described in Section 2.

Plan to provide more drop ports than are needed for the immediate application of the network. By providing more drop ports, it will not be necessary to shut down the network to add another tap when new equipment is added. Also, provide extra unused ports for test points at critical locations on the network such as, at the ends of trunk-cable segments or at places where the trunk cable goes into difficult-to-access places.

Before determining the final routing of the trunk cable, try to identify areas which might be hostile to the network. Areas that have electric arcs can produce noise. Areas such as loading docks that use fork lifts are likely to cause mechanical damage to the cables. Although existing cable trays and conduits are useful for routing the trunk cable, try to keep the cable away from power lines because these can radiate a great deal of noise.

Put the taps near the stations to avoid long drop cables. Also, put the taps where they can be secured to a post or a wall. Taps hanging in mid-air will require messenger wires.

Too often when a simple network is installed, no one bothers to document it because it is so simple. As time goes by, however, the network is extended and more devices are added, or the original network designers or installers have left. Soon there is no record as to where the cables are routed, how long they are, how many taps there are, where they are located, etc. Network documentation is not all that difficult or cumbersome; it can fall out of the design process by use of a form such as that shown in Figure 7-4. In the figure, an example of Section 7.1 is shown as a hypothetical network being designed.

In using the form, first identify the network and the cable segment of the network if repeaters or bridges are used. List each tap and its location. Identify each port (taps have numbers on them) and list either the station to be connected to the port or mark it as a spare. Start the list from the tap at the control center if it is at the end of a cable segment. Otherwise pick an end of a segment. Leave room on the form for taps that may be added later.

Enter the distance from the each tap listed to the next one.

In the first entry, list the SIGNAL IN as the minimum signal, 63 dBmV, that would be presented to the tap. Since the particular type of tap to be used has been selected, the drop-to-trunk loss of the signal is known. In the example, the attenuation for the first tap at the control center is 20 dB so that the signal out is 43 dB. For the subsequent taps, calculate the attenuation of the trunk cable from the previous tap and list the SIGNAL IN to the tap. Again, since the tap insertion

loss is known, the SIGNAL OUT entry can be calculated. Proceed until the form is filled out.

NETWORK NAME: EXAMPLE NUMBER: 37

CABLE SEGMENT 1

TAP #	LOCATION	PORT	DIST.	SIG. IN	SIG. OUT
10	N37-B2	1 CONTROL CTR. 2 SPARE	7	63	43
16	N83-F7	1 CONTROLLER 2 SPARE 3 BRIDGE 4 SPARE	95	42.9	42.4
22	N90-F3	1 SPARE 2 SPARE	115	41	40.7
28	E15-F18	1 TM1 2 TM2 3 SPARE 4 SPARE	88	39	38.5
34	E21-H31	1 A 2 B	20	37.2	36.9
40	E35-G14	1 C 2 SPARE	25	36.6	36.3
46	E43-G19	1 SPARE 2 SPARE	X	36	

Figure 7-4. Sample Documentation Form

There are a few things to note about the example:

- The taps are consecutively numbered but spaces are left for additional taps that may be added so that the identification of the existing taps will not have to change.

- The location numbers in the example are arbitrary grid locations of a floor plan.

- A spare tap and a number of spare ports have been left so that the network can be expanded easily and so that there are test points for network maintenance. Adding up all the cable distances shows that the trunk cable

is 350 meters long, not the 300 meters originally estimated. This extra length usually results after all the twists and turns of the trunk cable are taken into consideration. The total length is still within the distance limitation of 500 meters.

- The cable-system components count can be easily extracted from the documentation.

- The network documentation can be used by the cable-system installers to route the cable, install the taps and mark them, and verify the signal strengths measured on the cable against the calculated values.

The plan is now ready and network components have been selected. The network is ready to install.

Chapter 8: Cable System Installation and Verification

If the network planning and design procedures outlined in Section 7 have been carried out, there is now a plan in place for the carrier-band cable-system installation. Depending on the type of cable that has been selected, the following recommendations apply.

Flexible Cable Installation

Flexible cable can be installed by any reasonably competent craftsman. The components for a flexible cable system have been designed to minimize the skill levels and the care needed to install the cable system properly. There are a number of suggestions here which will help get the job done and will result in a more reliable network.

As opposed to semi-rigid cable, flexible coaxial cable is relatively easy to install because it is flexible. Moreover, if the flexible cable is armored, it can be laid into cable trays, pulled into conduits, buried, or hung between poles with little worry about cable damage. Ordinary coaxial cable is more delicate.

Pre-Installation Testing

The trunk cable should all come from one spool- rather than several segments of cable from different spools or from different manufacturers all spliced together. The reason for using a cable from a single spool is that different cable segments

may be good by themselves but have slightly different characteristic impedances. At the places where these different cable segments are spliced, there will be impedance mismatches and signal reflections. Also, the splices themselves are a potential source of reliability problems.

The trunk cable installation is the most difficult and expensive part of the cable-system installation. For this reason, it is necessary to know if the cable on a reel is good. If bad cable is installed, it will have to be removed, and a new one put in. This time consuming, frustrating, and expensive problem can be avoided if the cable is tested before it is installed.

Some cable vendors test their cable before it is shipped. However, the cable can be damaged in shipping or by just being stored in a warehouse that is too hot or has rodents. For this reason it is a good idea to retest the cable before installation.

Measure the return loss from both ends of the cable. The return loss should be less then 26 dB. If the return loss is more than 26dB, the cable should not be used.

Measure the cable attenuation. The attenuation should be indicated next to the manufacturer's specification for the length of cable on the reel. For a 5 Mbit/sec. network, the attenuation is measured at 10 MHz; for a 10 Mbit/sec. network, the attenuation is measured at 20 MHz.

Pre-testing the taps is less critical than cable testing. The taps are checked during the cable-system installation as part of the installation procedure. If a bad tap is found, it can be replaced at that time.

Trunk Cable Installation

Every facility is different and local ordinances for wiring installation may vary. For this reason, a complete installation procedure cannot be given. The suggestions given here, however, apply to most situations.

Do not overstress cable during installation. If the cable is not pulling in easily there is a reason why it is stuck. Pulling harder will not remove the obstacle but only damage the cable.

Do not bend the cable around sharp corners. The minimum bend radius for RG-11 type cable is 7 inches.

Do not stretch the cable between posts without adequate support. The maximum unsupported cable length for unarmored RG-11 cable is 100 feet and for the armored RG-11 150 feet. If longer distances are needed, use messenger wires.

Some cable slack should be left along the way. If changes are needed, they can be accommodated without having to splice in new cable.

Secure the cable to posts, walls, or other building structural members that will not move and do not vibrate. In time, other cables, pipes, and conduits will be installed by other people. If the network wiring in not secured, it will be moved by the other installation people and may be damaged.

When securing the cable, do not overstress it or crush it with the attachment devices. The Product and Services section in the back of the Handbook lists some cable attachment fixtures that avoid these potential problems.

Ground the metal armoring of the cable in as many places as is practical. This grounding increases the noise immunity of the cable system. In grounding the armoring, do not ground the inner shield of the cable.

If the cable is spliced, seal the splice joints and connectors, and secure them mechanically so they will not be bent or stressed.

Once the trunk cable has been installed, test the cable system before the taps are installed. This testing will identify any trunk cable problems that may have been caused by improper installation. The trunk cable segment ends should be terminated at this time. If the trunk cable ends are left in accessible places, as suggested in Section 8, the testing should be easy. The trunk cable should be tested for return loss. The return loss should be less than -24 dB.

Tap Installation and Testing

In order to install a tap, the trunk cable has to be cut and connectors attached to both ends of the cut cable. This step presents a good opportunity to test the trunk cable and any other taps that have already been attached to it.

Install a tap at one end of the trunk cable. Put a signal generator on a drop port at the end of the cable. Call this direction on the trunk cable "A"; call the other direction "B" Both ends of the trunk cable should be terminated.

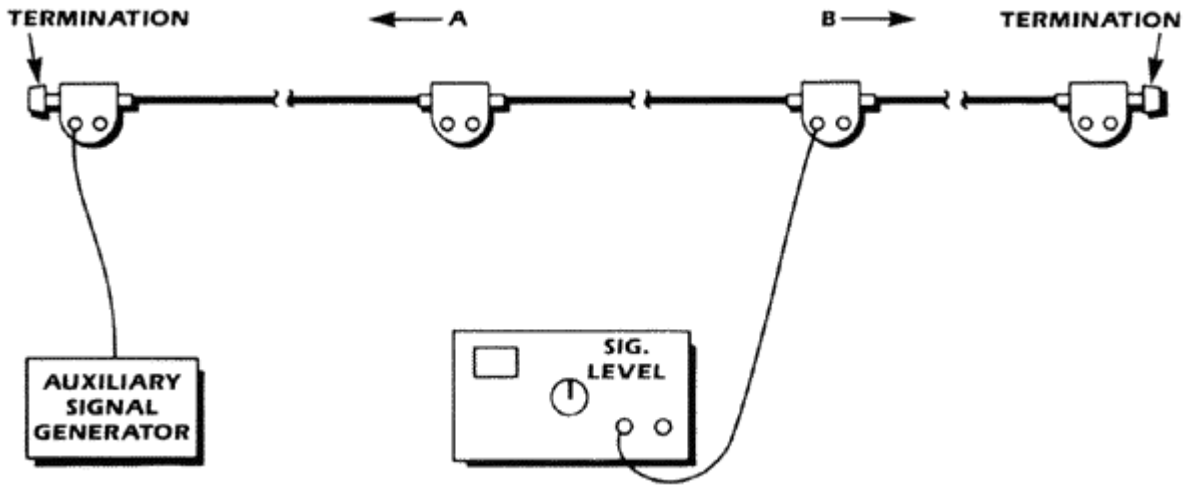

Figure 8-1. Signal Generator and Signal Level Meter

Cut the trunk cable at the place a tap is to be installed and attach the connectors. Measure the return loss of the trunk cable in both direction A and B. For the return loss, the measurement should 24 dB or greater as the first taps are installed. The measurement should show 22 dB or more as the last tap is installed.

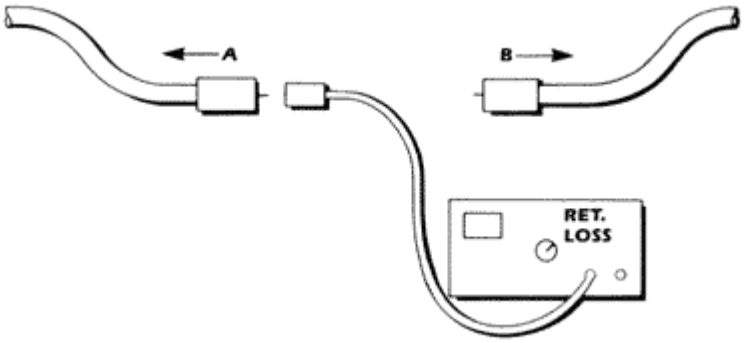

Figure 8-2. Trunk Return Loss Measurement

Attach the tap to trunk cable segment A. Measure the return loss and the signal level at the unconnected tap trunk cable port. For the return loss, the measurement should show 22 dB or greater. On the trunk cable port of the tap, the signal level should be between 32 and 47 dBmV. Be sure that the drop cable connectors on the tap are terminated during the measurement.

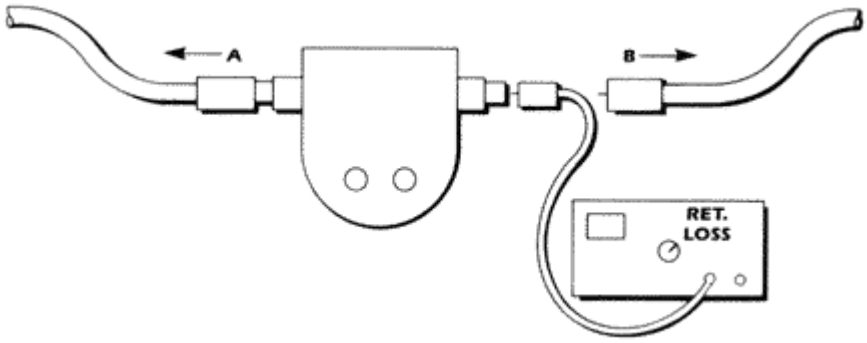

Figure 8-3. Tap and Trunk Return Loss

Attach trunk segment B to the tap. Measure the signal levels at each of the drop cable ports. The signal level should be between 12 and 27 dBmV. Be sure that the unused drop cable connectors are terminated during the measurement.

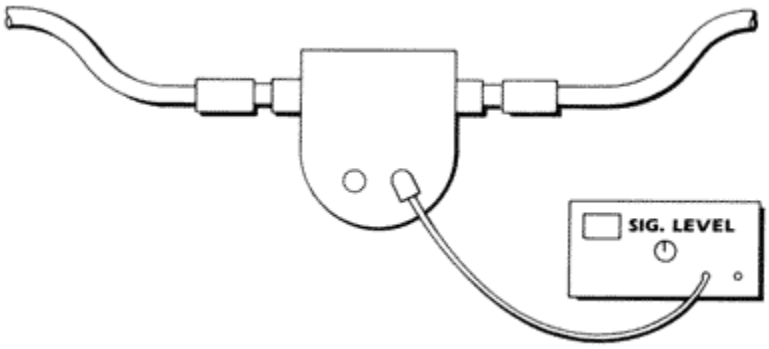

Figure 8-4. Signal Levels at Drop Ports

At this point, all the necessary measurements have been made on the particular tap being installed and the cable system. Now a determination can be made if everything is as it should be.

A way to make this determination easier is to have a form in which the signal values that are expected have been entered after the cable-system design. There should be places in the form for entering the measured values during installation. If the measured values do not agree with the calculated ones, the reason for the difference can be determined right away and corrected. Figure 8-5 shows a form from the example used in Section 8.

In this example, all the values are reasonably close, except for the return loss at the newly installed tap. Closely examining the attachment of cable segment to the tap revealed that the connector had not been tightened. Once this problem was corrected, the return loss values were as they should be.

Save the completed form for a record of how the cable system was at the time of installation.

Performing the testing and evaluation at installation time saves a lot of work later on. If the cable system is completely installed and then found to be outside the specifications, then a determination has to be made of where the fault or faults might be. This determination may require that the cable system be taken apart at several places. Taking the cable system apart may introduce other faults.

Once a tap has been installed successfully, attach the drop cables and secure them so that they do not put stress on the connectors. Be sure to terminate the drop cable ends. The drop cable terminations are a problem. When the cable system is first installed, the drop cables are terminated. However, when stations are attached to the cable system, the terminations are taken off and the stations themselves terminate the drop cables. When the station is moved, the drop cable becomes unterminated and may be left unterminated by the oversight of the operators in charge of the network. For this reason, it is a good idea to use self-terminators at the ends of the drop cables. These devices automatically terminate the drop cable when no station is connected. When a station is connected, the self-terminator disconnects itself and the station's termination is used.

Once the tap installation has been completed successfully, the trunk and the drop cable connectors can be sealed. Use shrink tubing or gel tape to seal off the trunk cable connectors. If the environment is not too hostile with corrosives, the drop cable connectors can be sealed with simple rubber sleeves.

NETWORK NAME: EXAMPLE NUMBER: 37

CABLE SEGMENT 1

TAP #	LOCATION	PORT	R/L A	R/L B	SIG. EXP.	SIG. MEAS.
10	N37-B2		35	29		
		1 CONTROL CTR.			23	23
		2 SPARE			23	23
16	N83-F7		33	29		
		1 CONTROLLER			23	23
		2 SPARE			23	23
		3 BRIDGE			23	23
		4 SPARE			23	23
22	N90-F3	*	18	29		
		1 SPARE				21
		2 SPARE				21

*Indicates faulty tap #16 installation.

Figure 8-5. Measurement Form Example

If the trunk cable and tap installation and testing procedures described above have been followed and the measured values agree with the calculated ones, then the cable system has been verified to be good.

After a network has been operating for a while or if the network starts to experience many errors, the cable system should be verified again.

Cable-system verification requires the stations on the network to be shut down so that they do not put signals on the trunk cable while the measurements are being made. If new taps have not been put on the trunk cable or segments added, the verifications can be as simple as measuring the return loss at each end to the trunk cable segments. Again, having the trunk cable segment ends readily available helps verify the cable system.

Grounding

The cable-system armoring and inner coax cable shields should be grounded. The grounding procedure is complicated by the conflicting requirements of good noise rejection practices and safety requirements. For best noise performance, the cable system should be grounded at only one point. If the network covers a large area, however, there may be ground potential differences between equipment in the area. These voltage differences present a potential hazard to personnel who may touch the cable system and a station at the same time. To solve this safety problem, ground everything in as many places as possible.

While this is not a comprehensive grounding guide, here are a few suggestions:

Ground the taps so that the drop cables do not have to carry any ground currents.

Use a grounding wire that has a current carrying capacity equal or greater than that of the trunk cable outer conductor. For RG-11 cable, the ground wire should be 14 ga. or larger; for 1/2" semi-rigid cable, the ground wire should be 8 ga. or larger.

Attach the ground wires to the grounding facilities provided in the building. Do not rely on building structures, conduits, cable trays, messenger cables or other metal objects that may not be grounded.

Station Attachment

After the cable system has been installed, stations can be connected and the network operation can be started.

Before connecting a device to the cable system, power the device on and let it execute its self-test. Most stations have some form of self-test capability built in. If the device powers up correctly, it will start sending out signals to get the token

so it can get on the network. Connect the signal meter to the station and determine that the output signal is between 63 and 66 dBmV.

If there are other devices already operating on the cable system, measure the signal level on the drop cable to which the new device will be attached. The signal level should be at least + 10 dBmV.

Glossary of Networking Terms

The number at the end of each definition designates the Section in which the term was first used.

Acknowledgment, ACK: An LLC response frame that indicates that a data frame has been received correctly. 5

Acknowledged Connectionless: The Type 3 LLC service where frame delivery is guaranteed and the sending user is notified of the success to the transmission. 5

Address: An identification of a station. 4

Armor: Protective cladding over a cable. 2

Attenuation: Signals getting smaller as they travel on a cable. 2

Backbone: A network that interconnects other networks. 1

Baseband: A type of network wiring that supports only one signal at a time. 1

Bit Error Rate: The number of bits received in error divided by the total number of bits sent. 3

Bridge: A device used to transparently interconnect two similar networks and to separate the data traffic between them. 1, 6

Broadband: A type of network wiring that can support many signals at the same time on different channels. 1

Broadcast Medium: The cable system that is shared by all stations; one station can transmit and all the others can receive signals. 3

Bus: A linear network topology. 2

Characteristic impedance: The ratio of voltage to current of the signal on a cable. 2

Carrier-band: A type of baseband network used in the factory. 1

Collision: The result of two or more stations transmitting simultaneously on a shared cable and getting the signals garbled. 4

Contention: The process by which multiple stations attempt to get into the logical ring during the same response window. 4

Control Field: A field which identifies the type of service the LLC protocol performs. 5

DTE-DCE interface: The standard interface between a modem and the station. 3

dBmV: A measure of signal strength. 2

Destination Address: The address of the station for which a frame is intended. 4

Destination Service Access Point, DSAP: The identification of the destination user of the LLC. 5

Deterministic: A network in which the time between when a station needs to transmit and when it can do so can be calculated. 4

Drop Cable: The cable between the tap and the station. 2

Duplicate Frame: A frame received twice because an acknowledgment frame was lost. 5

End Delimiter: An octet that defines the end of a frame. 4

Flow Control: The ability of the destination LLC user to send a status frame to the source LLC user indicating that it is out of buffer space. 5

Frame: A group of contiguous bits. 4

Frame Check Sequence, FCS: A code that is used to determine whether a frame was received correctly. 4

Frame Control: An octet in a MAC frame that identifies the type of the frame. 4

Frequency Shift Key, Phase Coherent: The signaling method used on the carrier-band network. 2

Gateway: A station use to interconnect two different types of networks and to translate application protocols. 6

Head-end: A common signal processing device in a broadband network. 1

Insertion Loss: The amount of loss of signal going through a tap on the trunk cable. 2

Jabber Inhibit: Part of the modem that detects excessive transmission and inhibits it. 3

Jitter: The timing uncertainty of the signal crossing zero voltage. 2

LAN: Local Area Network. a data communications network for a limited area. 1

Link Service Access Point, LSAP: A field within the frame that identifies the users of the LLC service. 5

Logical Link Control, LLC: The protocol responsible for identifying users of the network and the provision of reliable frame delivery. 5

Logical Ring: A group of stations that pass the token to each other. 4

Loopback: The ability of one station to send data to another station with the request that the same data be returned. 5

Medium: The entire cable system: wiring, taps and splitters. 3

Medium Access Control, MAC: The part of a station that performs the protocols needed for sharing the cable. 4

Modem: Part of the station that transmits and receives signals from the medium. 3

Noise: Unwanted electrical signals on the cable. 2

Non-directional: Signal from drop cable splits equally in both directions from a tap onto the trunk cable. 2

Octet: An 8-bit byte. 4

Port: A drop cable connector on a tap. 2

Preamble: The initial signal of a frame used to get the modem ready to receive. 4

Priority: Ability to give transmission preference to more important frames. 4

Protocol: Rules that all stations must follow in order to communicate. 4

Redundant Media: Two or more cable systems carry the same signals. 3

Repeater: A device used to extend the distance of the cable by interconnecting two cable segments and regenerating the signals between them. 6

Reply Service: An LLC type 3 service where one station can ask another for data. 5

Response Window: Time during which a new station is admitted into the logical ring. 4

Retransmission: The repeated sending of a frame if an ACK is not received by the source LLC. 5

Retransmission Time: The amount of time that a source LLC waits for an ACK before it retransmits a frame again. 5

Retry Count: The number of times that a source LLC will try to send a frame before it gives up. 5

Return Loss: The amount of signal reflected from an impedance discontinuity. 2

Router: A station between two similar or dissimilar networks used to route data through possibly many interconnected networks. 1, 6

Sequence Number: A number in each data frame that is used to identify duplicate frames. 5

Service: A group of tasks that one part of a station performs for another part of the station. 4,5

Slot Time: The worst-case time between when a station sends a frame and the time it can get a response. 4

Source Address: The address of the station sending a frame. 4

Source Service Access Point, SSAP: The identification of the source user of the LLC. 5

Start Frame Delimiter: An octet that defines the start of real data in a frame. 4

Station: A computer device on a local area network. 1

Status Field: A part of the ACK frame sent by the destination LLC to the source LLC used to indicate reception of data or other status. 5

Tap: A device for connecting the station to the trunk cable. 2

Termination: A device which absorbs signals at the end of a trunk cable. 2

Tilt: The difference in attenuation of two different frequency signals. 2

Token: The right to transmit on a shared medium. 4

Token Passing: A deterministic protocol for gaining access to a shared cable. 4

Token Rotation Time: The time it takes for a token to be passed around the logical ring. 4

Transfer Impedance: A cable's ability to reject noise. 2

Type 1 Service: Sending of frames without expecting acknowledgment. 5

Type 3 Service: Sending of frames and expecting acknowledgment or retransmitting the frame again. 5

Unacknowledged: Type 1 service where frames are sent but not necessarily received correctly. 5