Chapter

1

Transmission Network Fundamentals

1.1 Transmission Network Media

In telecommunications, information can be transmitted between two locations using a signal that can be either analog or digital in nature. In the telecommunications networks today, digital transmission is used almost exclusively, in which analog traffic, such as voice calls, is converted to digital signals (a process referred to as *sampling*) to facilitate long distance transmission and switching.

A high-pitched voice contains mostly high frequencies, while a low-pitched voice contains low frequencies. A loud voice contains a high-amplitude signal, while a soft voice contains a low-amplitude signal. Analog signals can be combined (i.e., multiplexed) by combining them with a carrier frequency. When there is more than one channel, this is called *frequency-division multiplexing (FDM)*. FDM was used extensively in the past but now has generally been replaced with the digital equivalent, called *time-division multiplexing (TDM)*.

The most popular TDM system is known as the Tier 1 (T1) system, in which an analog voice channel is sampled 8,000 times per second, and each sample is encoded into a 7-bit byte. Twenty-four such channels are mixed on two copper pairs and transmitted at a bit rate of 1.544 megabits per second (Mbps).

T1 in North America (E1 in the rest of the world) remains an important method of transmitting voice and data in the *public switched telephone network (PSTN)*.[1]

A talking path (i.e., a switched circuit) in the PSTN can be either analog or digital or a combination thereof. In fact, a digital signal can be transmitted over a packet-switched network as easily as a circuit-switched network. Digitized voice is similar to data; therefore, if data can be transmitted over a packet network, then so can digitized voice.

One of the most common applications is now known as *voice over IP (VoIP).* The challenge, of course, is to get the transmitted signal to the destination fast enough (delay-related issues), as in instances in which the conversation may be time sensitive. A second challenge is to get each packet, which is a small piece of a voice conversation, to its destination in the proper order.

Three types of media (physical layers) can be used in transmitting information in the telecommunications world:

- Copper lines (twisted-pair and coaxial cables), for low- and medium-capacity transmission over a short distance
- Fiber-optic transmission, for medium- and high-capacity transmission over any distance
- Wireless transmission, including:
  - Low (mobile radio) and medium-capacity (microwave point-to-point) over short and medium distances
  - Satellite for low- and medium-capacity transmission over long distances

The terms *transmission* and *transport* are used interchangeably in this text, as both are currently in use; the former is preferred in Europe, but the latter is more commonly used in North America. Sometimes *transmission* refers only to the physical media, while *transport* can include other OSI Model layers of the data transfer.

1.1.1 Wireline Systems

1.1.1.1 Copper Lines Years ago, copper wire was the only means of transporting information. Technically known as *unshielded twisted pair (UTP)*, it consists of a large number of pairs of copper wire of varying size within a cable. The cable did not have a shield, so the signal (primarily the high-frequency part of the signal) was able to leak out. In addition, the twisting on the copper pair was very casual, designed as much to identify which wires belonged to a pair as to handle transmission problems. Even with these limitations, it was quite satisfactory for use in voice communications.

Coaxial cable technologies were primarily developed for the cable TV industry. In the last few years, this technology has been extended to provide Internet services to residences. The high capacity of coaxial cable allows it to support multiple TV channels, and this capacity can also be used for high-speed Internet access. Like fiber optics, the cost of cable installation limits the deployment of new services, and current deployments are not typically in areas that allow this service to be offered to business offices.

1.1.1.2 Fiber-optic Systems Fiber optics constitute the third transmission medium, and this is unquestionably the high-bandwidth transmission medium of choice today. Fiber-optic cables can be placed in ducts, buried in the ground, suspended in the air between poles, installed as part of the ground wire on the high-voltage transmission towers *optical power ground wire (OPGW)*, and so forth. Transmission speeds of as high as 10 Gbps have become commonplace in the industry. Of course, laying fiber, on a per-mile basis, still costs somewhat more than laying copper, but on a per-circuit basis there is no doubt that fiber is more cost effective.

The huge capacity of fiber certainly makes for more efficient communications; however, placing so much traffic on a single strand, for point-to-point communications, makes for greater vulnerability. Most of the disruptions in the long distance network are a result of a physical interruption of a fiber run (called *backhoe fade*), and the *ring configuration* is the protection solution used most often in fiber-optic networks.

Dense wavelength division multiplexing (DWDM) is a fiber-optic transmission technique that employs light wavelengths to transmit data and can increase the bandwidth of the existing fiber-optic facilities. There is a huge emphasis on scalable DWDM systems enabling service providers to accommodate consumer demand for ever-increasing amounts of bandwidth. In order to squeeze more bandwidth out of their fiber networks, long-haul carriers are deploying DWDM to build backbones that might have dozens of channels riding on a single strand of fiber, with each channel operating at multigigabit speeds.

The cost of laying fiber-optic cable can easily reach $70,000 to $150,000 per mile in rural areas and could be much higher in the dense urban areas. This cost does not include any terminal equipment. For that reason, most users opt for either leasing fiber-optic facilities or building their own microwave network.

1.1.2 Wireless Systems

Wireless communications can take several forms: microwave (point-to-point or point-to-multipoint), synchronous satellites, low Earth orbit satellites (LEOs), cellular, personal communications service (PCS), and so on. For years, microwave radio transmissions have been used in the telecommunications industry for the transport of point-to-point data where information transmissions occur through carrier signals. Microwave carrier signals are typically relatively short in wavelength and can transmit information using various modulation methods.

To understand wireless technology, a basic understanding of the radio frequency (RF) spectrum is required. The RF spectrum is a part of the electromagnetic spectrum in which a variety of commonly used devices (including television, AM and FM radios, microwave radios, cell phones, pagers, and many other devices) operate. The electromagnetic spectrum has been used for communications for over 100 years, and it comprises an infinite number of frequencies, from AM radio at 1 MHz to the cellular/PCS band at 2 GHz.

Frequencies are measured in cycles per second, or hertz, which are inversely related to wavelength. At low frequencies wavelengths are long, while at higher frequencies wavelengths are very short. Given an equal power level, the longer the wavelength, the greater the distance the signal can travel. Whereas low-frequency signals (such as AM radio) can be transmitted for hundreds of miles, high-frequency signals (such as infrared) can travel only a few feet.

The *fixed-satellite service* basically involves four frequency bands: 4/6 GHz, 7/8 GHz (for military systems), 11/14 GHz, and 20/30 GHz. Although there are numerous bands above 30 GHz allocated to the fixed-satellite service, only one is presently being used. Microwave frequencies and "stationary" satellites allow the use of high-gain, directional antennas, much like the fixed service, reducing the power requirements for the satellite transmitters.

The fixed-satellite service includes international, domestic, and military systems and, although they often carry the same type of traffic, each group has its own set of users. International and domestic systems operate at 4/6 GHz and 11/14 GHz, while military systems use 7/8 GHz and frequencies near 20 GHz and 45 GHz.

Another of the wireless telecommunications technologies is the *low Earth orbit (LEO) satellite system*, which are satellites that communicate directly with handheld telephones on Earth. Because these satellites are relatively low (less than 900 miles above), they move across the sky quite rapidly.

In a LEO system the communications equipment on a satellite acts in much the same way as a cell site of a cellular system: it "catches" the call transmitted from Earth and usually passes it to an Earth-based switching system. Because of the speed of the satellite, it is frequently necessary to hand off a particular call to a second satellite just rising over the horizon. This is similar to a cellular system, except that in this case it is the cell site that is moving rather than the subscriber.

The RF spectrum in which these carrier transmissions occur is subject to regulation by the *Federal Communications Commission (FCC)* in the United States, *Industry Canada* in Canada, *Cofetel* in Mexico, and globally via the International Telecommunications Union (ITU). Countries that are members of the ITU generally follow the ITU spectrum allocation.

Within the RF spectrum, not all frequencies are subject to licensing requirements, and license-exempt bands include the industrial, scientific, and medical (ISM) band (the most widely used license-exempt frequency band) and the *Unlicensed National Information Infrastructure (UNII) band*.

The frequencies that are used for radio communications have slowly moved upward from lower to higher frequencies (shorter wavelengths). Back in the early days of radio, it was easier to generate carrier frequencies of sufficient power at the lower side of the frequency spectrum. With the advancement of new techniques, it became possible to develop new components that use higher and higher frequencies.

Microwave and millimeter-wave bands occupy frequencies from around 1 to 300 GHz, but this book discusses the characteristics of the bands for terrestrial microwave (and millimeter-wave) point-to-point systems from around 2 to 90 GHz.

1.1.3 Free-Space Laser Communications

Free-space laser communications systems are wireless, point-to-point connections through the atmosphere that employ the optical part of the frequency spectrum. Therefore, they cannot be categorized as either wireless or wireline systems in a classical sense. They work only under clear line-of-sight conditions between each unit, eliminating the need for securing rights of way, buried cable installations, and government licensing. Free-space laser communications systems can be quickly deployed, since they are small and do not need any radio interference studies.

Optical wireless is an attractive option for multigigabit-per-second short range links (typically from a few hundred meters up to 2 km) where laying optical fiber is too expensive or impractical, and where microwave systems do not provide enough bandwidth.

This type of optical communication, also known as *free-space optical (FSO)*, has emerged as a commercially viable alternative to RF and millimeter-wave wireless for reliable and rapid deployment of data and voice networks. (See Figure 1.1, which shows wireless transceivers mounted on rooftops.) RF and millimeter-wave technologies allow rapid deployment of wireless networks with data rates from tens of megabits per second (point-to-multipoint) up to several hundred

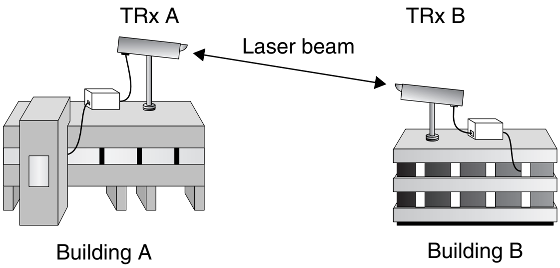

Figure 1.1 Optical wireless transceivers

megabits per second (point-to-point). However, spectrum-licensing issues at licensed and interference at license-exempt frequency bands can sometimes still limit their market penetration.

Although optical losses and space losses can introduce a significant attenuation of the optical signal, the main problem is atmospheric effects. As mentioned earlier, it is desirable to have as much excess margin as possible to mitigate atmospheric effects such as fog. On a sunny day, the atmosphere is clear, and the margin is useful to overcome fades caused by turbulence. On a foggy day, the margin is used to overcome signal attenuation.

The dominant atmospheric effect that affects optical communication is attenuation of the signal by scatter and absorption. Molecular scatter and absorption of major atmospheric constituents is relatively insignificant. Although rain and snow can cause attenuation up to approximately 40 dB/km and 100 dB/km, respectively, fog by far is the largest problem. In extremely heavy fog, attenuation as high as 300 dB/km (500 dB/mi) has been reported. Clearly, either link distance or link availability is compromised as part of the network design.

Some systems can operate through window glass but with reduced distance. Metallic glass coating prevents any type of radio propagation altogether.

Alignment is important both at the transmitter and the receiver. The transmitter has to be pointed accurately to ensure efficient delivery of energy to the receiver. The receiver has to be pointed properly to ensure that the signal entering the receiver aperture makes it to the detector. A great deal depends on how and where the transceivers are located and, in the case when a transceiver is mounted on the roof of a tall building, building sway contributes significantly to pointing error. A high-rise building can sway more than a meter (three feet), and the roof itself often houses air conditioning and ventilation units as well as elevators and other mechanisms that cause vibration in the low tens of hertz. Moreover, some roofs are not very solid and can deform when someone walks on them.

Temperature changes (diurnal and seasonal) and uneven heating by the sun can deform the mount enough to throw the pointing off. Some FSO users have indicated that they need to realign their transceiver units several times a year for this very reason. Optical wireless transceivers and their mounts have enough wind resistance that they can be tilted in heavy winds. To make things worse, building owners, for liability reasons, do not readily grant approval for the installation of penetrating mounts, and nonpenetrating rooftop mounts exhibit even greater pointing fluctuations.

Microwave and infrared transmission systems are both good alternatives for short distance network connections (less than two miles). Each system requires line-of-sight and has its advantages and disadvantages. The ease of obtaining frequency spectrum licensing, various weather and atmospheric conditions, topology of the area, and security should be evaluated to determine which system is used.

When frequency spectrum licensing is difficult and expensive to obtain, infrared transmission systems have a distinct advantage. Infrared systems are also advantageous if the weather is normally rainy, but not foggy, and there is little smog; when the conditions require spanning a large body of water; and when the area has high levels of electromagnetic interference (EMI). In addition, an infrared transmission system is less inclined to be intercepted.

Microwave transmission systems are advantageous in areas that are foggy and have a substantial amount of snow or smog, or if the conditions require spanning longer distances. Microwave systems are the preferred option anytime the distance exceeds two miles.

1.2 Basic Terminology

1.2.1 E1, T1, and J1

There are two standards for the first-order digital transmission systems. The T1 system, developed by Bell Laboratories, is used mainly in the U.S.A., Canada, Taiwan, Jamaica, and a few other countries. North American T1 service providers often refer to the signal interfaces between the user and the network as *DS1* signals. In the case of user-to-user interfaces, the term *DSX-1* is used to describe those DS1 signals at the “cross-connect” point; therefore, DSX-1 is a physical interface of the T1 circuit.

Most of the countries around the world use the E1 system defined by European Conference of Postal and Telecommunications Administration (CEPT).

Details of the T1 systems can be found in literature.[2] Here, only a brief description of T1 is given:

- There are 24 DS0 (64-kbps) time slots in a T1 line, providing a total bandwidth of 24 × 64 kbps = 1,536,000 bps (1,536 kbps).
- Another 8,000 bps are used as framing bits.
- Adding up the total bandwidth of the 24 DS0 channels and the 8-kbps framing bits yields a 1.544 Mbps T1 data rate.

The North American digital hierarchy (see Table 1.1) starts with a basic digital signal level of 64 kbps (DS0). Thereafter, all facility types are usually referred to as Tx, where x is the digital signal level within the hierarchy (e.g., *T1* refers to the DS1 rate of 1.544 Mbps). Up to the DS3 rate, these signals are usually delivered from the provider on twisted-pair or coaxial cables.

The basic format for transmission facilities in Japan (see Table 1.2) is similar to the North American ANSI standard and called *J1*. However, the CMI line coding used in Japan is different from the one used in North America.[3] Rather than using 50 percent duty cycle (half-width) "mark" pulses, continuous marks are transmitted, inverting the voltage after each mark. The spaces also have a transition, but in the middle of the pulse period. This ensures that there are always sufficient transitions to maintain synchronization, regardless of whether the signal is all zeros or all ones.

TABLE 1.1 North American Data Rates

Name	Rate
DS0	64 kbps
DS1	1.544 Mbps
DS1C	3.152 Mbps
DS2	6.312 Mbps
DS3	44.736 Mbps
DS4	274.176 Mbps

TABLE 1.2 Japanese Digital Hierarchy

Designation	Bit rate (Mbps)	Number of voice channels
DS1	1.544	24
DS2	6.132	96
DS3	32.064	480
DS4	97.728	1,440
DS5	400.352	5,760

TABLE 1.3 ITU Data Rates

Name	Rate
DS0	64 kbps
E1	2.048 Mbps
E2	8.448 Mbps
E3	34.368 Mbps
E4	139.264 Mbps
E5	565.148 Mbps

The CCITT Digital hierarchy's[4] basic level is the DS0 rate of 64 kbps (see Table 1.3). These signals are usually delivered from the provider via twisted-pair or coaxial cables. The following is a description of the CEPT digital hierarchy:

- There are 30 DS0 (64-kbps) time slots in an E1 line, providing a total bandwidth of 30 × 64 kbps = 1,920,000 bps (1,920 kbps).
- One 64-kbps time slot (TS0) is used for framing bits.
- Another 64-kbps time slot (TS16) is used for signaling of voice frequency channels.
- Adding up the total bandwidth of the 30 DS0 channels, framing, and signaling bits yields the 2.048 Mbps E1 data rate.

1.2.2 PDH, SDH, and SONET

Traditionally, transmission systems have been asynchronous, with each terminal in the network running on its own clock. In digital systems, clocking (timing) is one of the most important considerations. Timing means using a series of repetitive pulses to keep the bit rate of the data stream constant and to indicate where the ones and zeros are located in a data stream. Because these clocks are free running and not synchronized, large variations occur in the clock rate and thus the signal bit rate.

Asynchronous multiplexing uses multiple stages; lower-rate signals are multiplexed, and extra bits are added (bit-stuffing) to account for the variations of each individual stream and combined with other bits (framing bits) to form higher-level bit rates. Then bit-stuffing is used again to produce even higher bit rates. At the higher asynchronous rate, it is impossible to access these signals without multiplexing.

The *Plesiochronous Digital Hierarchy (PDH)* signals have the essential characteristics of time scales or signals such that their corresponding significant instants occur at nominally the same rate. The prefix *plesio*, which is of Greek origin, means "almost equal but not exactly," meaning that the higher levels in the CCITT (ITU today) hierarchy are *not* an *exact* multiple of the lower level. Any variation in rate is constrained within specified limits. The PDH systems belong to the first generation of digital terrestrial telecommunication systems in commercial use.

Synchronous network hierarchies were introduced in the late 1980s. The term *synchronous* means occurring at regular intervals and is usually used to describe communications in which data can be transmitted in a steady stream rather than intermittently. For example, if a telephone conversation were synchronous, each party would be required to wait a specified interval before speaking.

Synchronous Digital Hierarchy (SDH) is a newer technology in the field of digital transmission.[5] The transmission is carried out in a synchronous mode, hence the name. The most important advantage in adopting this synchronous technology is to enable the mapping of various user bit rates directly onto the main transmission signals, thus bypassing various stages of multiplexing and demultiplexing as was done in the case of earlier PDH technology.

North American *Synchronous Optical Network (SONET)* is a second-generation digital optical transport protocol. The fiber-based carrier network uses synchronous operations among such network components as multiplexers, terminals, and switches.

The number of new architectures and topologies are made possible as a result of this new technology. For instance, *add/drop multiplexers (ADMs)* have made it possible to use SONET/SDH terminals in a long chain with bit streams added or dropped along the way in an effective manner.[6] By closing the chain at two ends, a ring configuration is possible, which provides enhanced protection features.[7,8] SONET-based rings create a robust, high-availability network that can "heal" itself automatically by routing around failures. The optical fiber rings offer security, high bandwidth, low signal distortion, and high reliability.

Other advantages include support of network management systems, easy upgrade to high bit rates, and adaptability to the existing PDH. In synchronous networks, all multiplex functions operate using clocks derived from a common source.

The North American SONET system is based on multiples of a fundamental rate of 51.840 Mbps, called STS-1 (for synchronous transmission signal, level 1). The facility designators are similar but indicate the facility type, which is usually fiber-optic cable (e.g., OC-1 is an optical carrier supporting an STS-1 signal, whereas OC-3 supports a STS-3 signal, and so forth). Some typical rates are listed in Table 1.4.

The international SDH system is based on a fundamental rate of 155.520 Mbps, three times that of the SONET system. This fundamental signal is called STM-1 (synchronous transmission module, level 1). The typical transmission media is defined to be fiber, but the broadband ISDN specification does define a *user-network interface (UNI)* STM-1

TABLE 1.4 STS Data Rates

Name	Rate (Mbps)
STS-1	51.840
STS-3	155.520
STS-9	466.560
STS-12	622.080
STS-48	2,488.320

(155.520 Mbps) operating over coaxial cables. Some typical rates within this hierarchy are shown in Table 1.5.

Optical carrier (OC-n) levels describe a range of optical digital signals that can be carried on the SONET network. The general rule for calculating the speed of optical carrier lines is when a specification is given as OC-n, the speed will equal $n \times 51.840$ Mbps.

The rate in Table 1.6 is a *line rate,* referring to the raw bit rate carried over the optical fiber. A portion of the bits transferred over the line is designated as *overhead*. The overhead carries information that provides OAM&P (Operations, Administration, Maintenance, and Provisioning) capabilities such as framing, multiplexing, status, trace, and performance monitoring. The payload rate (line rate – overhead rate = payload rate) is the bandwidth available for transferring user data such as packets or ATM cells.

The SONET/SDH level designations sometimes include a "c" suffix. The "c" suffix indicates a *concatenated* or *clear* channel. This implies that the entire payload rate is available as a single channel of communications (i.e., the entire payload rate may be used by a single flow

TABLE 1.5 STM Data Rates

Name	Rate (Mbps)
STM-1	155.520
STM-3	466.560
STM-4	622.080
STM-16	2,488.320

TABLE 1.6 Optical Carrier Data Rates

Name	Rate (Mbps)
OC-1	51.840
OC-3	155.520
OC-3C	155.520
OC-12	622.080
OC-24	622.080
OC-48	2,488.320

of cells or packets). The opposite of concatenated or clear channel is a *channelized link*.

In a channelized link the payload rate is subdivided into multiple fixed rate channels. For example, the payload of an OC-48 link may be subdivided into four OC-12 channels. In this case the data rate of a single cell or packet flow is limited by the bandwidth of an individual channel.

One of the main advantages of the ITU-T SDH system is the fact that it may be the first compatible system used worldwide. A further advantage is the extremely high bit rate transmitted by the system (e.g., nearly 10 Gbps with STM-64). When used in conjunction with DWDM, even much higher rates can be handled. SDH is perfectly suitable to multiplex and transport the traffic of PDH networks, and it also can be used for data transport and leased lines. It follows further from the synchronizing feature that a low-level container, also including its content, can be accessed at any higher hierarchical level. However, a disadvantage of SDH is the necessity to establish a synchronization network.

SDH and SONET are both gradually replacing the higher order of PDH systems, but the evolution from PDH to SDH worldwide is a phased process because SDH based networks must have the flexibility to utilize existing PDH transport media. The advantages of higher bandwidth, greater flexibility, and scalability make these standards ideal for asynchronous transfer mode (ATM) networks as well.

To maximize the benefits of the SONET/SDH microwave radio, the radio must be capable of complementing a synchronous fiber-optic network. This means that for the microwave radio to integrate with fiber-optic network elements, its design must address a number of parameters, including capacity and growth, network management, maintaining pace with SDH/SONET standards evolution, interface, and performance.

Providing microwave radio with the optical interface will allow a microwave network to integrate with the fiber-optic network without the use of multiplexing equipment (unless drop and/or insert of the traffic is required). The same management tools are used for both media.

Common expectations for fiber *and* microwave elements are signal rates and interfaces, overhead processing, service channels, operations systems, and transmission quality. SONET/SDH microwave radios can easily integrate into a new or existing fiber-optic network (see Figure 1.2).

Digital microwave systems based on synchronous digital hierarchy (SONET/SDH) can meet the requirements for the high-capacity backbone transmission systems. SDH/SONET radios provide an economical solution when existing infrastructure (towers, shelters, and so on) can be reused, and when rights of way or adverse terrain make fiber deployment very costly or time consuming.

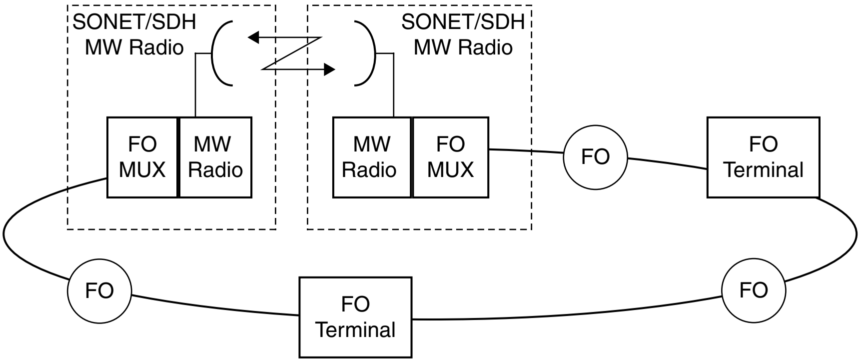

Figure 1.2 Hybrid microwave/fiber-optic ring

SONET/SDH radio technology is capable of delivering bandwidth-efficient bandwidth of 8 bits/s/Hz. For example, the 512-state *quadrature amplitude modulation (QAM)* technique can pack two STM-1 streams into a single 40-MHz channel using a single carrier. By adding channels in an *N+1* configuration, system capacities of up to 14 protected STM-1s can be achieved within one frequency band (for example, in the upper 6-GHz band, 8 bidirectional channels are available).

By deploying a dual-band configuration (such as lower 4- and 5-GHz bands) system, capacities of STM-16 and greater are achievable. Although theoretically possible, this can be done only if the spectrum governing bodies allow more than one channel to be accessed by the same user.

1.2.3 ATM

Asynchronous transfer mode (ATM) is the complement of *synchronous transfer mode (STM).* STM is a circuit-switched networking mechanism whereby a connection is established between two termination points before data transfer commences and torn down when it is completed. In this way, the termination points allocate and reserve the connection bandwidth for the entire duration, even when not actually transmitting data.

ATM is a transmission technology that uses fixed-size packets called *cells*. A cell is a 53-byte packet with 5 bytes of header/descriptor and 48 bytes of payload, or user traffic (voice, data, video, or their combination). Today, telecommunications companies are deploying fiber optics in cross-country and cross-oceanic links with gigabits-per-second speeds. They would like to carry, in an integrated way, both real-time traffic such as voice and high-resolution video, which can tolerate some loss but not delay, as well as non-real-time traffic such as computer data and file transfer, which may tolerate some delay, but not loss.

The obvious problem with carrying these different characteristics of traffic on the same medium in an integrated fashion is that the requirements of these traffic sources may be quite different. In other words, the data comes in bursts and must be transmitted at the peak rate of the burst, but the average arrival time between bursts may be quite large and randomly distributed. For these connections, it would be a considerable waste of bandwidth to reserve a bucket for them at their peak bandwidth rate for all times when, on the average, only 1 in 10 buckets may actually carry the data. Thus, using the STM mode of transfer becomes inefficient as the peak bandwidth of the link, peak transfer rate of the traffic, and overall burstyness of the traffic (expressed as a ratio of peak/average) all go up.

Terms such as *fast packet, cell,* and *bucket* are used interchangeably in ATM literature. ATM networks are connection-oriented packet-switching networks.

Future telecommunication networks, including wireless networks, must be able to offer today's range of services as well as services with new features; e.g., variable bit rates. The requirements of modern networking involve handling multiple types of traffic (voice, video, and data), all with individual characteristics that make very different (and often opposed) demands on the telecommunication channel. The second requirement is reliability and flexibility in the communication links.

The greatest problem is that transmissions occur at statistically random intervals with variable data rates. A way of solving this problem is to use a service that takes packets on the transport layer from a higher layer and fragments them in small packets of a fixed size. The delays produced by each packet are going to be short and probably fixed, so, if voice and video traffic can be assured priority handling, they can be mixed with data without diminishing any reception quality. The service that solves this problem is called the *ATM adaptation layer (AAL)*. A new adaptation layer is required to provide the flexibility for network operators to control delay on voice services and to overcome the excessive bandwidth needed by using structured circuit emulation.[9]

The AAL2 was designed specifically for cost-effective voice transport. AAL2 is used in 3G wireless networks as a backhaul connection between *radio base stations (RBSs)* and *base station controllers (BSCs)*.

Over the last ten years, more and more transmission systems, especially those in wireless networks, have been using ATM over the microwave networks. These radio systems carrying packetized traffic (ATM or frame relay) have to be designed in a way that takes into account the behavior of this kind of traffic. Because ATM is primarily designed for an essentially error-free environment, in the wireless arena, the sources of errors and their consequences on ATM traffic and its Quality of Service (QoS) are being studied today.

ATM traffic requires a very high-quality transmission medium with a good *background error rate* (also called *Residual BER* or *RBER*). Microwave radio and fiber optics are ideal from this perspective, as they both offer in the order of 10^{-13} background error rates. Microwave radio is subject to fading for a small period of time but, by proper design, this is limited to a specified time period (typically 99.99 percent availability or better).

ATM is designed for low BER links, and radio links with a moderate BER can cause unacceptable high cell loss and *misinsertion* rates.[10] By definition, a misinserted cell is a received cell that has no corresponding transmitted cell on the considered connection. Cell misinsertion on a particular connection is caused by defects on the physical layer affecting any cells that were not previously associated with this connection.

Although IP-based networks are becoming more and more widely used, ATM still has its applications and will be around for quite some time (the same goes for TDM networks and circuits).

1.2.4 Ethernet Backhaul

1.2.4.1 About the OSI layers The *Open System Interconnection Reference Model* (OSI Reference Model or *OSI Model*) is a description of layered communications and computer network protocol design. Basically, it divides network architecture into seven layers which, from top to bottom, are the *application*, *presentation*, *session*, *transport*, *network*, *data link*, and *physical layers*. It is therefore often referred to as the *OSI Seven Layer Model*.

Internetworking devices such as bridges, routers, and switches have traditionally been categorized by the OSI layer they operate at and the role they play in the topology of a network:

- **Layer 2** Bridges and switches operate at Layer 2 (data link layer)
- **Layer 3** Routers operate at Layer 3 (network layer)

Bridges and switches extend network capabilities by forwarding traffic among LANs and LAN segments with high throughput. Layer 2 refers to the layer in the communications protocol that contains the physical address of a client or server station. It is also called the data link layer or MAC layer. Layer 2 contains the address that is inspected by a bridge, switch, or PC NIC.

The *Layer 2* address of every network device is unique, fixed in hardware by its manufacturer and usually never changed. Traditionally, products that were called switches operated by forwarding all traffic based on its Layer 2 addresses.

The *spanning tree protocol*, implemented in many Layer 2 switches, prevents forwarding loops in switched networks. Unfortunately, this is achieved by shutting down redundant connections and never using them. In contrast, routers are able to keep redundant connections active and make use of this built-in redundancy to increase network reliability and performance. With Layer 2 switching reaching the limits of its potential, the multilayer switch represents the next stage in the evolution of internetworking devices.

Multilayer switching is simply the combination of traditional Layer 2 switching with Layer 3 protocol routing in a single product, usually through a fast hardware implementation.

Routers perform route calculations based on Layer 3 addresses and provide multiprotocol support and WAN access, but typically at the cost of higher latency and much more complex administration requirements. Layer 3 refers to the layer in the communications protocol that contains the logical address of a client or server station. It is also called the *network layer*.

Layer 3 contains the address (such as IP or IPX) that is inspected by a router that forwards the traffic through the network. The Layer 3 address of a network device is a software setting established by the user network administrator that can and does change from time to time; only devices that need to be addressed by Layer 3 protocols, such as IP, have Layer 3 addresses. Traditionally, routers operated solely on Layer 3 addresses.

1.2.4.2 Carrier Ethernet TDM networks are reliable, well developed technology with guaranteed and predictable service levels. Unfortunately, they are not suitable for the Ethernet transport and introduction of new, bandwidth-intensive services. Technology—and the cost of course—is driving the migration to IP-based networks, and the new IP services are critical to improving operators' revenue; therefore, new generations of wireless networks will be IP-based.

Network providers are upgrading their IP networks to support not only existing best-effort services but also real-time services and existing Layer 2 services. Best-effort services such as e-mail are able to withstand the significant delay, packet reordering and outages common on most IP networks. On the other hand, real-time services, such as voice-over-IP (VoIP), video, streaming media and interactive gaming, demand a higher level of network performance with low latency and high network availability. Essential services that currently reside on ATM and frame-relay switches cannot be transitioned to a network that is not stable and does not deliver the *Quality of Service (QoS)* service-level agreements require.

As real-time applications continue to increase, network outages will become more visible, and service providers will have to react or lose customers to other carriers. For IP networks to support demanding real-time applications and converged legacy networks, carriers must overcome a number of obstacles; poor router reliability, lack of link protection, disruptive operations, slow convergence time, and multiservice support are just some of the challenges.

Even though Ethernet/IP provides significantly cheaper bandwidth, in terms of cost per bit, than legacy ATM and TDM, the technologies so far have rarely been used for transport in mobile access networks, in part due to the lack of sufficient QoS and resilience to guarantee the required service level. Different QoS requirements for voice, data, and video services must be supported by a well-designed IP and Ethernet based network.

Driven by the MEF (*Metro Ethernet Forum*[11]), a de facto standard "high quality" transport service labeled *Carrier Grade Ethernet* has been defined to meet these needs. The standard supports high QoS characteristics and a hard SLA (Service Level Agreement). With the increasing importance of Class of Service standards, Carrier Class Ethernet certification, and real-time applications, assuring QoS is a critical element in offering revenue-generating Ethernet services. This assurance comes from properly testing all of the differentiated services using multistream traffic generation and prioritization techniques that did not play a large role in traditional point-to-point services.

Carrier Ethernet is a ubiquitous, standardized, carrier-class service defined by five attributes that distinguish it from the regular LAN-based Ethernet. Carrier Ethernet attributes are scalability, standardized services, service management, quality of service, and reliability. In wireless networks, mobile backhaul Ethernet can be delivered over a variety of access technologies (see Figure 1.3).

MEF has defined the requirements put on network reference points including the *user-network interface (UNI)* and *network-to-network interfaces (NNI)*. The MEF architecture is based on *Ethernet virtual connections (EVC)*, where an EVC is an association of two or more UNIs over one or more *metro Ethernet networks (MEN)* that transport Ethernet frames. Each EVC has a set of service attributes (service type, multiplexing support, bandwidth profiles, and performance assurance) that are used to define services in a flexible way and to standardize SLAs.

4G mobile networks require a single, all-IP, packet-based backhaul infrastructure, providing carriers with a significant cost advantage. However, the number of mobile devices and multitude of services, such as traditional voice, voice conferencing, image sharing, video,

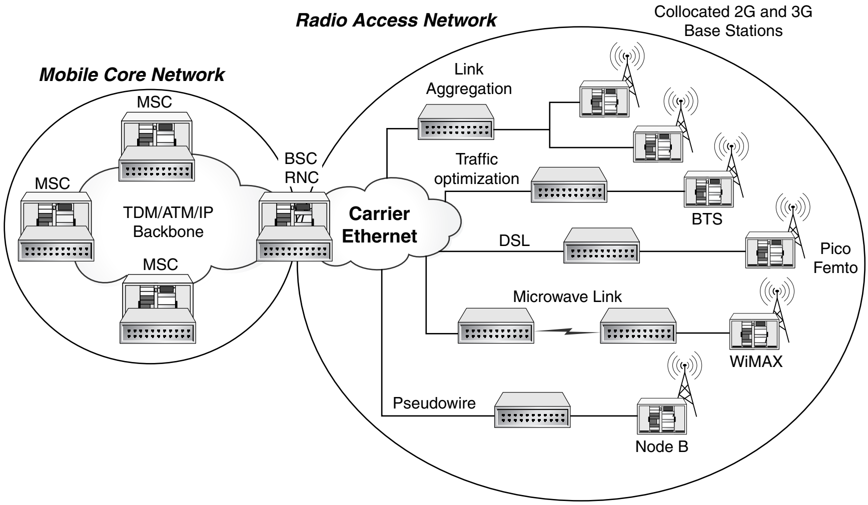

Figure 1.3 Carrier Ethernet in mobile backhaul

and high-speed data, strains the infrastructure. Carrier Ethernet will deliver cost, scalability and flexibility of Ethernet networks, but with *TDM Carrier Class reliability*.

New generations of *Ethernet microwave radios* equipped with adaptive modulation, link aggregation, and *XPIC (Cross-polarization Interference Canceller)* are already delivering high-speed *GigE (Gigabit Ethernet)* links. Ethernet microwave radios, adaptive modulation, link aggregation, and XPIC are discussed in more details in other chapters of this book.

1.3 Transmission Network Topology

The main objectives of the transmission network are to connect all the points of interest, satisfy the capacity demands, and provide reliable service using different media (microwave, copper, fiber optics, or satellites). During the transmission network build-out, it is an imperative to establish a transmission network plan that will include all present traffic requirements as well as future expansion.

As wireless carriers move to 4G mobile technology, huge demands are being placed on carrier backhaul infrastructure. The multiple, high-bandwidth, quality-sensitive services that carriers have planned for 4G require an infrastructure that is packet-based, scalable, and resilient, as well as cost-effective to install, operate, and manage.

Network operators worry about two things: how to start deploying the network in phases without spending capital before it is needed, and how to grow these small, initial segments once they see growth coming down the road. That is why scalability is a very important factor. The transmission network topologies can be divided into two groups:

- The *flat network* is a single entity, which means that it can be optimized to have high network utilization. A drawback is that the network topology is sensitive to changes in the traffic distribution. A change in the distribution changes the earlier, well-optimized network to being nonoptimized.
- The *layered network* facilitates the design of a network and its subsequent expansion, as the total network is modular. Modular design also makes the network and the traffic routing easy to understand, thus simplifying operation and maintenance (O&M), which will reduce the operator's O&M costs in the future.

A layered network is divided into various network layers, which are connected via gateways. The layered/modular network is designed subnetwork by subnetwork; i.e., the total demand matrix is divided into demand matrixes for each subnetwork. The new, smaller matrixes are easier to handle and understand than the large ones.

In the future, as the services offered to the end user become more and more flexible, the layered approach might be the most suitable topology—assuming that the initial cost is not considered.

In wireless networks, the size of the network is assessed based on the number of cell sites and/or required backhaul capacity. Many successful mobile operators protect transmission by using automatic traffic rerouting, assuring additional reliability in normal situations, such as when microwave radio access links suffer cut-off as a result of poor weather conditions, possible fiber-optic cable cuts, or any other human error. With a flexible rerouting transmission system, backup capacity can pass via physically separate routes, given that the problem is not likely to interrupt both routes simultaneously.

Rerouting can be arranged for all sites or only critical sites, such as base stations that are labeled as higher priority—for example, a hub site. Hub sites are those sites that collect traffic from more than one other site (typically three to four other sites) and carry that traffic toward the BCS (Base-station Controller) location or fiber-optic ring hub site.*

* In wireless networks, BSC is the brain of the entire network.

For a larger transmission network, using a resilient ring configuration as a high-capacity backbone that carries traffic to the switch is recommended. The ring architecture is considered to be a reliable communication facility, as it provides automatic protection against the following:

- Site hardware (batteries, towers, antenna systems) failures
- Radio, switch, or multiplexer (MUX) equipment failures
- Propagation failures in the microwave network
- Cable cuts in the fiber-optic network

Ring architecture also provides basic user features such as simple operation, fault location, and maintenance. Ring configuration automatically provides alternative routing of E1/T1 traffic and no loss of E1/T1 traffic due to a single failure. Each E1/T1 circuit must be dedicated completely around the ring, and reuse of the same E1/T1 in the opposite direction is not possible. For ultimate reliability, both directions can be 1+1 hardware protected.

In legacy PDH networks, additional hardware with built-in intelligence to assess the T1/E1 quality and switch circuits is required. This hardware has to be added at every site, and it is useful for small networks. SONET/SDH have incorporated several protection/switching techniques from their inception. These include linear APS, path-switched rings, line-switched rings, and virtual rings, providing the ability for a network to detect the problem (under 10 ms) and heal itself automatically in the case of failure, with the restoration time less than 50 ms.

Self-healing schemes use fully duplicated transmission systems and capacity for alternate routing of today's time division multiplexed (TDM) or synchronous transfer mode (STM) circuit facilities. The restoration capacity and the associated transmission systems are essentially unused except in the rare occasions of network failure.

Two adjacent rings might be interconnected via shared node.

Although expensive and relatively complex to implement, the *dual-homed ring* architecture is the choice for high-capacity digital service providers. This architecture uses a drop-and-continue feature that ensures that traffic is available to pass between adjacent rings at two separate nodes (i.e., since two rings share two nodes, we say that rings have a shared link). If an entire node is lost, the receiving ring equipment will select traffic from the other node. Although it looks expensive, actually network survivability has a great potential for cost reduction in the future.

The new Recommendation ITU-T G.8032/Y.1344 (06/2008) defines the automatic protection switching (APS) protocol and protection switching mechanisms for Ethernet ring topologies. Ring protection switching occurs based on the detection of events on the transport entity of each ring link. The events are defined within equipment Recommendations ITU-T G.8021.

Ethernet ring protection shall support up to 255 ring nodes and in the event of a single ring node or link failure, it will have protection switching time of less than 50 ms.

1.4 Transmission Network Performance

In today's networks, with converged voice and data, performance degradation may be as dangerous and costly as hardware failures. Degraded transmission networks can result in unacceptable signal transmission quality, loss of information, and dropped connections. High availability does not mean just preventing catastrophic failures; it also means preventing quality and performance degradation.

High availability (and quality) of the transmission network is an end-to-end network goal. A network management system (NMS) can help identify critical resources, traffic patterns, and performance levels. Transmission network survivability is usually measured in terms of its long-term availability or average network uptime. Most operators expect their network to be continuously available (or at least with as little downtime as possible) to minimize potential loss of revenue.

The survivable network has an infrastructure of transmission facilities and reliable network elements that are used to manage them. High network availability at the transport level may be achieved using millisecond restoration schemes provided by self-healing network configurations such as SONET/SDH rings or *fast facility protection (FFP)*. *Digital access cross-connects (DACS)* in combination with SONET/SDH ring configurations will ensure network availability and survivability.

An FFP network comprises two physically diverse routes with identical transmission systems (route diversity). Each route carries half of the working traffic and half of the restoration traffic. The restoration traffic on each route is the duplicate of the working traffic on the other route. If the media on these routes are different (for example, one is fiber optic and the other one is microwave), we call it *media diversity.* These highly reliable solutions do not come cheap and, in many cases, a compromise between the cost of the network and its deployment time and reliability has to be made.

Regardless of the transmission network medium and topology, hardware redundancy is an option when designing the transmission network. Protection types usually employed are 1+1, where one card or module serves as a protection for another one, or N+1, where one card or module protects N other units. The same fiber or frequency is used for working and protection equipment.

Linear 1+1 protection switching is different from 1+1 hardware redundancy and means that identical payloads will be transmitted on the working and protect fibers, or working and protect frequencies in case of the microwave system. Linear N+1 protection switching assumes the existence of one protect fiber/frequency for N working fibers/frequencies.

A rule of thumb is that, if all the hardware is protected with a 1+1 and/or N+1 configuration, fewer spare parts are needed (discussed in more details later in Chapter 5). In the case of hardware failure, protection will kick in, and the operator will have sufficient time (which may be days or weeks) to order replacement parts from the supplier. In addition, the ring configuration could provide protection against hardware failures as well, so additional hardware protection might not be required. This is something that transmission engineers have to decide, and the decision will be based on both technical and budgetary requirements.

It is also important to remember the distinction between terms like *performance, availability, quality,* and so on. Although the network is operational (available), network performance can still be poor with increased levels of BER, for a number of reasons. In voice networks, that may mean reduced sound quality; in data networks, it can cause constant data retransmissions, incorrect information, and so forth. In other words, the quality of such a network is low and unsatisfactory.

For the network operators, one of the key factors to the success is its ability to maintain a high standard of network performance, which can only be achieved by adopting the appropriate QoS metrics and measurement tools. *Five nines*, the jargon term that means a piece of equipment will function reliably 99.999 percent of the time (statistically, about five minutes of downtime per year), is used widely in the legacy TDM networks but may not be good enough in a world of always-on mobile devices and ever-increasing video consumption.

Table 1.7 shows some of the commonly used percentage values for unavailability. The five nines requirement, correctly or incorrectly, has been applied to almost everything—from the telecommunications equipment to microwave paths, fiber-optic links, and sometimes even to the all-inclusive end-to-end link.

When talking about availability it is a good idea to define what exactly these five nines include. Unfortunately, to make things even more complicated, five nines will mean different things to different people; so, when we bring up the five nines requirement, it is advisable to have it precisely defined from the get-go.

TABLE 1.7 Unavailable Time per Year

Availability (% of time)	Unavailability (% of time)	Unavailable Time per Year (min)
99.9999	0.0001	0.5256
99.9995	0.0005	2.628
99.9990	0.0010	5.256
99.9950	0.0050	26.28
99.9900	0.0100	52.56
99.9500	0.0500	262.8
99.9000	0.1000	525.6
99.5000	0.5000	2,628
99.0000	1.0000	5,256

In North America, it is quite common that, sometimes arbitrarily, network designers assign the same requirement of 99.999 percent of time availability to the microwave path (regardless of its length and number of paths in the system) and a guarantee of bit error rate (BER) better than 10^{-3} (or 10^{-6}) during that period. In many cases, designers neglect an actual quality of the link due to increased BER and focus only on the availability; the fact that the microwave link (or any other network connection) is available does not mean that the link (and therefore the entire network) is working properly.

From that prospective, ITU methods and models, developed and continuously revised over the last 20 years or so, will go a step further and try to incorporate all the possible factors (including equipment) that may affect the network availability, quality, and reliability.

Some of the main causes of IP network downtime are router hardware and software failures. In contrast to traditional central-office equipment such as voice and ATM switches, IP routers were not designed to support carrier-grade 99.999 percent availability; typical large IP networks achieve only between 99.95 and 99.99 percent availability. This is much more downtime than the five nines availability benchmark of legacy data networks.

New generations of routing platforms have achieved 99.999 percent availability by providing full hardware and software redundancy in a single router; in addition, hitless software upgrades are essential to the delivery of 99.999 percent availability because they eliminate router downtime associated with software upgrades.

Studies have shown that link failures accounted for more than 30 percent of the outages in a large IP network. This is not particularly surprising, since IP networks traditionally have been built without locally protected links. Instead, these networks have relied on the ability of routers to route the traffic around failed links, producing unacceptable disruption to real-time and converged services.

1.5 Network Synchronization

1.5.1 Synchronization Terminology

Digital systems require all signals within a given transmission level to maintain a frequency relationship. If this relationship is not maintained, information will be lost, or transmission capacity will be underutilized. In addition, varying transmission times, inaccurate timing, and unstable network equipment can also cause bits traveling in a transmission path to arrive at a time that is in variance with their expected arrival. Solving timing-related problems is part of *network synchronization*.

To date, two approaches have been dominant in achieving network synchronization: *plesiochronous*, used in PDH networks, and *synchronous*, used in SDH and SONET networks.

Digital network connectivity depends on the availability of a reliable synchronization source to provide a timing reference to the network elements. Synchronization networks provide timing signals to all synchronization network elements at each node in a digital network. Buffer elements at important transmission interfaces absorb differences between the average local frequency and the actual short-term frequency of incoming signals, which may be affected by phase wander and jitter accumulated along the transmission paths.[12]

A *slip* in T1 is defined as a 1-frame (193 bits) shift in time difference between the two signals in question. This time difference is equal to 125 μs (microseconds), and these slips are not a major impairment to trunks carrying voice circuits. The lost frames and temporary loss of frame synchronization results in occasional pops and clicks being heard during a call in progress. However, with advancements in DS1 connectivity, these impairments tend to spread throughout the network. To minimize them, a hierarchical clock scheme was developed whose function was to produce a primary reference for distribution to switching centers so as to time the toll switches.

In carrier telecommunications systems, *stratum* is used to describe the quality of a clock used for synchronization. The ANSI[†] Synchronization Interface Standard T1.101 defines profiles for clock accuracy at each

[†] ANSI-American National Standards Institute.

stratum level, as does ITU standard G.810, and Telcordia/Bellcore standards GR-253 and GR-1244.

- **Stratum 1** Defined as a completely autonomous source of timing that has no other input other than perhaps a yearly calibration. The usual source of Stratum 1 timing is an atomic standard or reference oscillator. The minimum adjustable range and maximum drift is defined as a fractional frequency offset of 1×10^{-11} or less. At this minimum accuracy, a properly calibrated source will provide bit-stream timing that will not slip relative to an absolute or perfect standard more than once every 4 to 5 months. Atomic standards, such as cesium clocks, have far better performance.

  A Stratum 1 clock is an example of a *primary reference source (PRS)* as defined in ANSI/T1.101. Alternatively, a PRS source can be a clock system employing direct control from *coordinated universal time (UTC)* frequency and time services such as *global positioning system (GPS)* navigational systems. The GPS may be used to provide high-accuracy, low-cost timing of Stratum 1 quality.
- **Stratum 2** Tracks an input under normal operating conditions and holds to the last best estimate of the input reference frequency during impaired operating conditions. A Stratum 2 clock system provides a frame slip rate of approximately one slip in seven days when in the hold mode.
- **Stratum 3** Defined as a clock system that tracks an input as in Stratum 2 but over a wider range. Sometimes Stratum 3 clock equipment is not adequate to time SONET network elements. Stratum 3E, which is defined in Bellcore documents, is a new standard created as a result of SONET equipment requirements.
- **Stratum 4** Defined as a clock system that tracks an input as in Stratum 2 or 3 but has the wider adjustment and drift range. In addition, a Stratum 4 clock has no holdover capability and, in the absence of a reference, free runs within the adjustment range limits.

Any stratum clock will always control strata of lower-level clocks. Inadequate timing may produce problems in any digital network, so the objectives have to be set very early in the planning process. The master timing sources that are possible to use and recommended are as follows:

- **PRS DS1** Timing is received from a collocated primary reference source such as a GPS or LORAN-C receiver, which is Stratum 1 level.
- **Dedicated DS1** Timing is obtained by terminating a DS1 dedicated to synchronization.

- **Traffic-carrying DS1** Timing is extracted from a traffic-carrying DS1 (PDH or copper medium and not carried over from SDH/SONET) coming into a site.
- **SDH** Timing is extracted from the SDH line signal where there is no influence from the pointer movements phase steps.
- **SONET DS1** Timing is obtained by deriving a nontraffic-carrying DS1 from SONET network elements, an OC-N multiplexer.

1.5.2 Synchronization in Wireless Networks

Telecommunications equipment (for example, cellular base stations) receive their timing signals from the worldwide GPS, an array of satellites that beam timing signals accurate to within 300 ns (nanoseconds) to receiving stations located around the globe. If the link fails, a backup system must be in place to maintain timing accuracy; if there is no backup, the cell goes down and communication is lost, which is an unacceptable condition. The GPS time standard is downlinked from the satellite as long as it is in range of the GPS receiver. However, there are intervals of time when a satellite is not in range (overhead), and no GPS time standard is available. This period without any GPS time update is called the *GPS holdover time*.

One major problem encountered after designing a timing network is evaluating its performance, as any problems related to synchronization can be difficult to detect and even more difficult to troubleshoot.

The digital microwave radios and high-level multiplexers are not considered in the synchronization plan, since they internally synchronize on a per-hop basis. Synchronous microwave radios on the market provide a transparent transmission media, which in SDH terms runs in a default *regenerator section termination mode (RST)*. In this mode, the radio obtains synchronization from the aggregate 155 Mbps input into the radio, and it does not offer or require any additional synchronization options.

Ethernet and IP are rapidly replacing traditional TDM circuit infrastructure in the communication networks. This creates *timing islands* in the network, potentially causing service impairments. Mobile services are especially vulnerable as they require precise synchronization at base stations.

There are two mobile wireless network synchronization schemes; the first one uses the same technology as a wired network (from T1/E1 circuits). This standard is used to provide *frequency-division duplex (FDD)* radio-based mobile wireless network synchronization signals for ingress/egress of data and accurate radio frequency (WCDMA, for example).

The second is synchronization of *time-division duplex (TDD)* radio-based mobile wireless networks, requiring frequency accuracy, phase alignment, and, in certain cases, time alignment between all base stations in the cell network. Examples of TDD radio systems are CDMA, cdma2000, Mobile WiMAX 802.16e, and Long-Term Evolution (LTE). The traditional wired ("circuit" oriented) synchronization signal delivery system cannot be used because there is no phase or time relationship between signal termination points on the clock distribution network.[13]

The migration toward a packet-based transport network poses the challenge of providing the level of synchronization requirements defined in the 3GPP, 3GPP2 (LTE), and IEEE 802.16e (WiMAX) specifications. The requirements for mobile wireless network synchronization depend on having an inter-base-station aligned timing reference. This is essential to guarantee transport channel alignment for handoff and guard band protection.

3GPP-specified FDD systems require frequency accuracy better than 50 parts per billion (ppb). The 3GPP TDD systems require an inter-base-station time alignment of 2.5 µs to IS-97's 10 µs, in addition to the 50 ppb frequency accuracy.

The IEEE 802.16e mobile WiMAX requirements are 20 ppb of frequency accuracy and 1 µs of phase alignment. Ensuring the fulfillment of these requirements reduces the call drop rate and improves the quality of services by decreasing packet loss.

IEEE 1588v2 (2008), also known as *Precision Time Protocol (PTP)*, is the new standard for providing precise timing and synchronization over packet-based, Ethernet networks. Accuracy within the nanosecond range can be achieved with this protocol when using hardware generated timestamps, although the protocol itself has no quality requirement. The transmission of the clock information over a packet network eliminates the need for alternative mechanisms, such as GPS or prohibitively expensive oscillators placed at the receiving nodes and thus providing significant cost savings in network equipment as well as in ongoing installation and maintenance.

This synchronization solution transmits dedicated timing packets, which flow along the same paths with the data packets, reducing the cost of synchronization and simplifying implementation.

Although IEEE 1588v2 systems add a small amount of additional traffic to the network load, they have several advantages; for example, they work in the data path, the most redundant and resilient part of the network, resulting in reliable operation. In addition, multiple transmission paths reduce redundant clock system costs. They also use a single synchronization session for all base-station traffic.

It is important to note that IEEE 1588v2 protocol cannot improve the performance of synchronization or calibration through existing networks unless every network node is replaced with a node that supports an IEEE 1588v2 boundary clock or transparent clock. With IEEE 1588v2 techniques implemented in every node, the network will experience less packet delay variation, which in turn, means that less stable oscillators may be used in network nodes.

The IEEE 1588v2 master function will typically be located at switching offices, while the IEEE 1588v2 slave function will be integrated into the base stations and receive the timing packets. The slave function consists of a clock recovery algorithm that works in tandem with the base station's high-quality oscillator.

1.6 Network Delays

Signal *propagation delay* or *latency* describes the delay of a transmission from the time it enters the network until the time it leaves; *low latency* means short delays, whereas *high latency* means long delays. Low latency is essential for real-time transmissions. These include live voice conversations (but not voicemail messages, which are time insensitive) and live two-way video (but not entertainment video clips, which also are time insensitive). Latency is a phenomenon not only of mobile networks, but also an outcome of all the networks, terminals, and devices through which transmissions may pass, plus the bottlenecks (and, therefore, delays) they may encounter.

Delay can cause protocol time-outs, retransmissions, and disruptions in data circuits and can inhibit voice transmissions. All types of transmission equipment, such as multiplexers, packet assemblers, microwave radios, and digital access cross-connects (DACS), add small amounts of delay as a result of their internal buffering, and satellite links add significant delay to a signal. ATM switches introduce up to a 2 ms delay, and there is a concern about the number of times ATM compression can be used in a tandem link before the overall delay objective is exceeded.

Wireless CDMA networks are very sensitive to delays, and vendors recommend that backhaul delay between the cell site and the BSC be below certain limits. For example, the end-to-end delay allowable from the user equipment to a UMTS (WCDMA) radio network controller (RNC) is 7 ms. Values of around 12 ms are used in the cdmaOne and CDMA2000 networks.

The emerging set of voice and video services being delivered by 4G networks typically has an end-to-end latency budget of about 10 ms. If 5 ms of this latency budget is allocated to the fiber network, there is 5 ms of delay for the wireless backhaul network. About half of this is allocated to the Ethernet switch layer, leaving about 2.5 ms for the wireless links. In a ten-hop microwave system, this leaves a maximum latency of 0.25 ms per link, requiring a very low latency microwave Ethernet system.

TABLE 1.8 Typical Delay Values for the Microwave Hop

Capacity (Mbps)	Delay (μsec)
2×2	100
4×2	75
8×2	50
16×2	40
300 Mbps (Ethernet)	100

In addition, utility companies using microwave systems to carry their SCADA (Supervisory Control and Data Acquisition) signals require a very low delay. That is one reason why electrical utility companies still keep their old-fashioned analog microwave systems: they introduce smaller delays than digital microwave systems.

The main processing delay in a microwave radio is forward error correction (FEC) buffering, which decreases with an increase in the capacity of the radio link. Total latency of the microwave link is a combination of the radio, free-space, and multiplexer delays. Some typical delays in microwave radio hardware for a point-to-point connection (entire hop) without considering the free-space transit time shown in Table 1.8. Microwave radio manufacturers should be able to supply these numbers for their equipment.

1.7 Security and Encryption

Digital information is often the target of computer hackers, international spies, and criminals. In order to protect the information, in 1977 the National Security Agency (NSA) and the National Bureau of Standards (NBS) adopted the Data Encryption Standard (DES) to protect sensitive, unclassified, nonmilitary digital information from unauthorized access. Encryption is the intentional scrambling or masking of digital data to protect it from compromise.

Modern microwave radios often come with some kind of built-in security mechanism, like traffic encryption, for example. It is important to keep in mind to avoid proprietary security and encryption methods.

1.7.1 Data Encryption Standard (DES)

The Data Encryption Standard (DES) algorithm is the most widely used encryption algorithm in the world. For many years, and among many people, "secret code-making" and DES have been synonymous. DES works on bits, or binary numbers—the 0s and 1s common to digital computers. Each group of four bits makes up a hexadecimal, or base 16, number. Binary 0001 is equal to the hexadecimal number 1, binary 1000 is equal to the hexadecimal number 8, 1001 is equal to the hexadecimal number 9, 1010 is equal to the hexadecimal number A, and 1111 is equal to the hexadecimal number F.

DES works by encrypting groups of 64 message bits, which is the same as 16 hexadecimal numbers. To do the encryption, DES uses "keys," which are also apparently 16 hexadecimal numbers long or apparently 64 bits long. However, every 8th key bit is ignored in the DES algorithm, so that the effective key size is 56 bits. In any case, 64 bits (16 hexadecimal digits) is the round number upon which DES is organized.

In cryptography, Triple-DES is a block cipher formed from the DES cipher by using it three times. Given a plaintext message, the first key is used to DES-encrypt the message. The second key is used to DES-decrypt the encrypted message and, since the second key is not the right key, this decryption just scrambles the data further. The twice-scrambled message is then encrypted again with the third key to yield the final ciphertext. In general, Triple-DES with three different keys has a key length of 168 bits: three 56-bit DES keys (with parity bits 3TDES has the total storage length of 192 bits), but due to the meet-in-the-middle attack the effective security, it provides only 112 bits.

Triple-DES is slowly disappearing from use, largely replaced by its natural successor, the Advanced Encryption Standard (AES). One large-scale exception is within the electronic payments industry, which still uses Triple-DES extensively and continues to develop and promulgate standards based upon it, guaranteeing to keep Triple-DES an active cryptographic standard in the future. By design DES, and therefore Triple-DES, suffer from slow performance in software; on modern processors, AES tends to be around six times faster.

Triple-DES is better suited to hardware implementations, and indeed where it is still used it tends to be with a hardware implementation (e.g., VPN appliances and some cellular and data networks), but even there AES outperforms it. Finally, AES offers markedly higher security margins, a larger block size, and potentially longer keys.

1.7.2 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a symmetric key encryption technique that is slowly replacing the commonly used Data Encryption Standard (DES). It was the result of a worldwide call for submissions of encryption algorithms issued by the U.S. Government's National Institute of Standards and Technology (NIST) in 1997 and completed in 2000[14]. The winning algorithm, Rijndael, was developed by two Belgian cryptologists, Vincent Rijmen and Joan Daemen.

AES provides strong encryption and has been selected by NIST as a Federal Information Processing Standard in 2001, and in 2003 the U.S.

Government (NSA) announced that AES is secure enough to protect classified information up to the Top Secret level, which is the highest security level and defined as information that would cause "exceptionally grave damage" to national security if disclosed to the public.

The AES algorithm uses one of three cipher key strengths: a 128-, 192-, or 256-bit encryption key (password). Each encryption key size causes the algorithm to behave slightly differently, so the increasing key sizes not only offer a larger number of bits with which you can scramble the data, but also increase the complexity of the cipher algorithm. AES is fast in both software and hardware, is relatively easy to implement, and requires little memory; as a new encryption standard, it is currently being deployed on a large scale.

1.8 References

1. Lehpamer, H., *Transmission Systems Design Handbook for Wireless Networks,* Norwood, MA: Artech House, 2002.
2. Larus Corporation, *Transmission Engineering Tutorials,* 1996.
3. Flanagan W. A., *The Guide to T1 Networking,* 4th ed., Telecom Library Inc., 1990.
4. ITU-T Recommendation G.702, *Digital Hierarchy Bit Rates.*
5. ITU-T G.803, "Architecture of transport networks based on the synchronous digital hierarchy (SDH)," 03/2000.
6. Goralski, W., *SONET,* 2nd ed., New York: McGraw-Hill, 2000.
7. Zhou, D., "Survivability in Optical Networks," *IEEE Network,* Nov./Dec. 2000.
8. Lewin, B., "SONET Equipment Availability Requirements," *IEEE,* 1989.
9. Malis, A. G., "Reconstructing Transmission Networks Using ATM and DWDM," *IEEE Communications*, Vol. 37, No. 6, June 1999.
10. Bates, J., *Optimizing Voice in ATM/IP Mobile Networks,* New York: McGraw-Hill, 2002.
11. http://metroethernetforum.org/, accessed 07/13/2009.
12. Larus Corporation, *Digital Network Timing and Synchronization,* 1997.
13. Diamond, P., *Packet Synchronization in Cellular Backhaul Networks*, Semtech White paper, October 2008.
14. Federal Information Processing Standards, *Publication 197, Announcing the Advanced Encryption Standard (AES)*, November 26, 2001.