1988

NEAR EAST UNIVERSITY

GRADUATION PROJECT

Subject : Network Security & Control

Submitted To : Prof. Dr. Fahrettin MAMEDOV

Prepared By : Aslı YAVUZ

Department : Computer Engineering

Student Number : 940726

INDEX 1

INTRODUCTION

Our subject in this project is Network Security and Control, Network Design Fundamentals. We had great knowledge while doing this project.

First of all this project will helpful for us at the real life for practising.

We took informations on the Internet, at so many books and also our teacher Mr. Mamedov gave us some of the source books that can help us to prepare our project.

We put figures to express the subject better. You can see them at the Appendix section.

Also we wish our project is helpful for students that are studying at the university.

We would like to thanks to Prof. Dr. Fahrettin Mamedov for his great helps to finish this project.

1) SECURITY AND CONTROL

This chapter identifies the 17 network control points that must be addressed for security and control. Specific hardware / software / protocol controls are reviewed.

Other control areas that are reviewed are: management controls, error control, recovery/back up/disaster, and the use of a matrix to identify, document, and evaluate security and control in a data communication network.

NETWORK SECURITY

In recent years organisations have become increasingly dependent upon data communication networks for their daily business communications, database information retrieval, and distributed data processing. This commitment to data communications/teleprocessing has changed the potential vulnerability of the organisation's assets.

This change has come about because the traditional security, control, and audit mechanisms take on a new and different form in data communication based systems. Increased reliance on data communications, the consolidation of many previously manual operations into computerised systems, use of database management systems, and the fact that on-line real-time systems cut across many lines of responsibility have increased management concern about the adequacy of current control and security mechanisms used in a data communication environment.

There also has been an increased emphasis upon computer network security because of numerous legal actions involving officers and directors of organisations, because of pronouncements by government regulatory agencies, and because the losses associated with computerised frauds are many magnitudes larger, per incident, than those from noncomputerized frauds. These factors have led to an increased vigilance with regard to protecting the organisation's information assets from many potential hazards such as fraud, errors, lost data, breaches of privacy, and disastrous events that can occur in a data communication network.

With regard to data communication networks, the organisation must be able to implement adequate control and security mechanisms within its facilities, including building facilities, terminals, local area networks, local loops, interexchange channel circuits, switching centres, network interface units (gateways), packet networks, hardware (modems, multiplexers, encryption devices, and the like), network protocols, network architecture software, test equipment, and network management control.

As an example, Figure 1-1 depicts a network typical of one that an organisation might develop.

In such a network all of the areas mentioned above would require a positive decision (policies and procedures) as to security and control. It should be noted that with this kind of network the organisation is vulnerable to many points of entry from an unwanted intruder. In fact, every terminal in the network is a potential entry point for an unauthorised intruder.

The rest of this chapter will be a discussion on each of the major portions of a data communication network, such as hardware and software, and a description of the various controls that relate to that specific area.

Finally, a matrix methodology for identifying network controls, documenting them, and evaluating their effectiveness will be presented. This is to provide the network manager with a good picture of the current controls, their effectiveness, and adequate documentation.

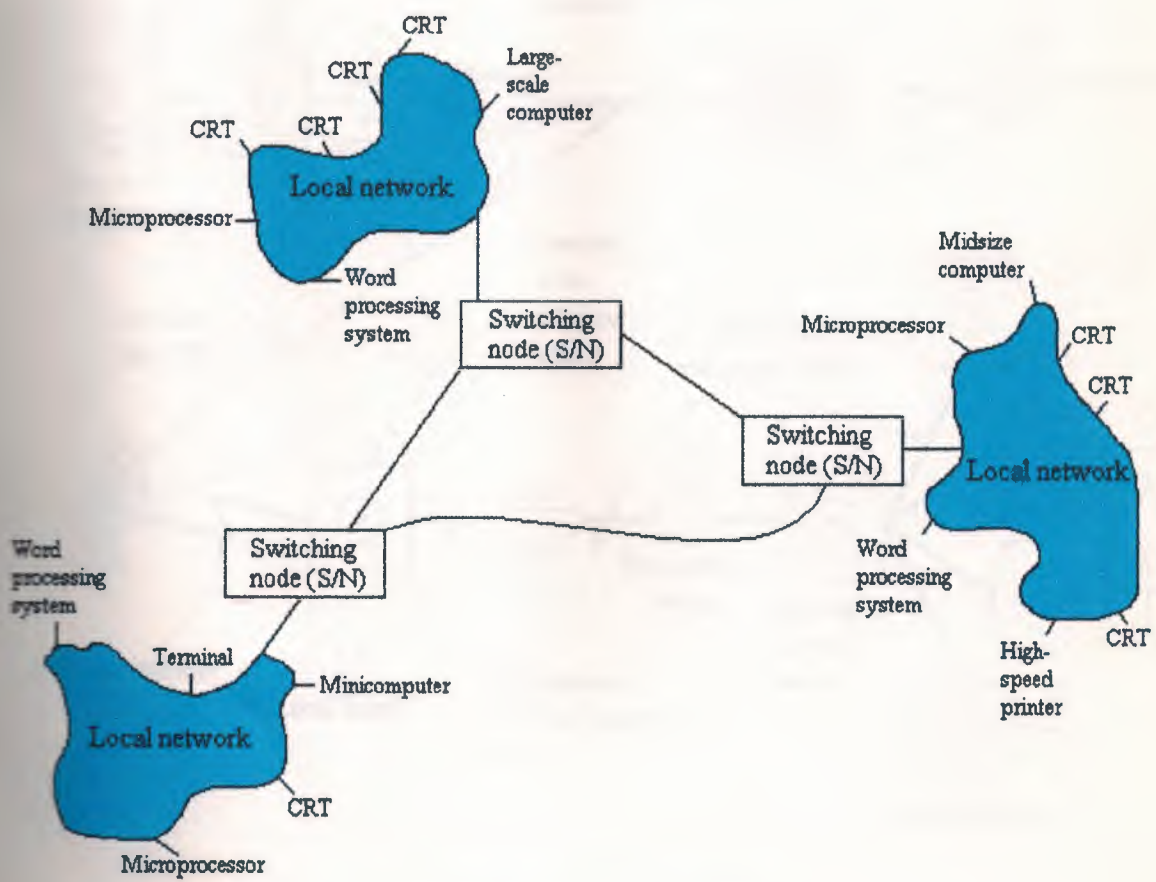


FIGURE 1-1 Future Network

NETWORK CONTROL POINTS

The 17 control points, or areas where control and security must be implemented, are depicted in Figure 1-2. The network manager, quality assurance personnel, security officer, or the organisation's EDP auditor should examine these areas to ensure that proper controls are implemented and are functioning properly. The numbers on Figure 1-2 are described in the following list.

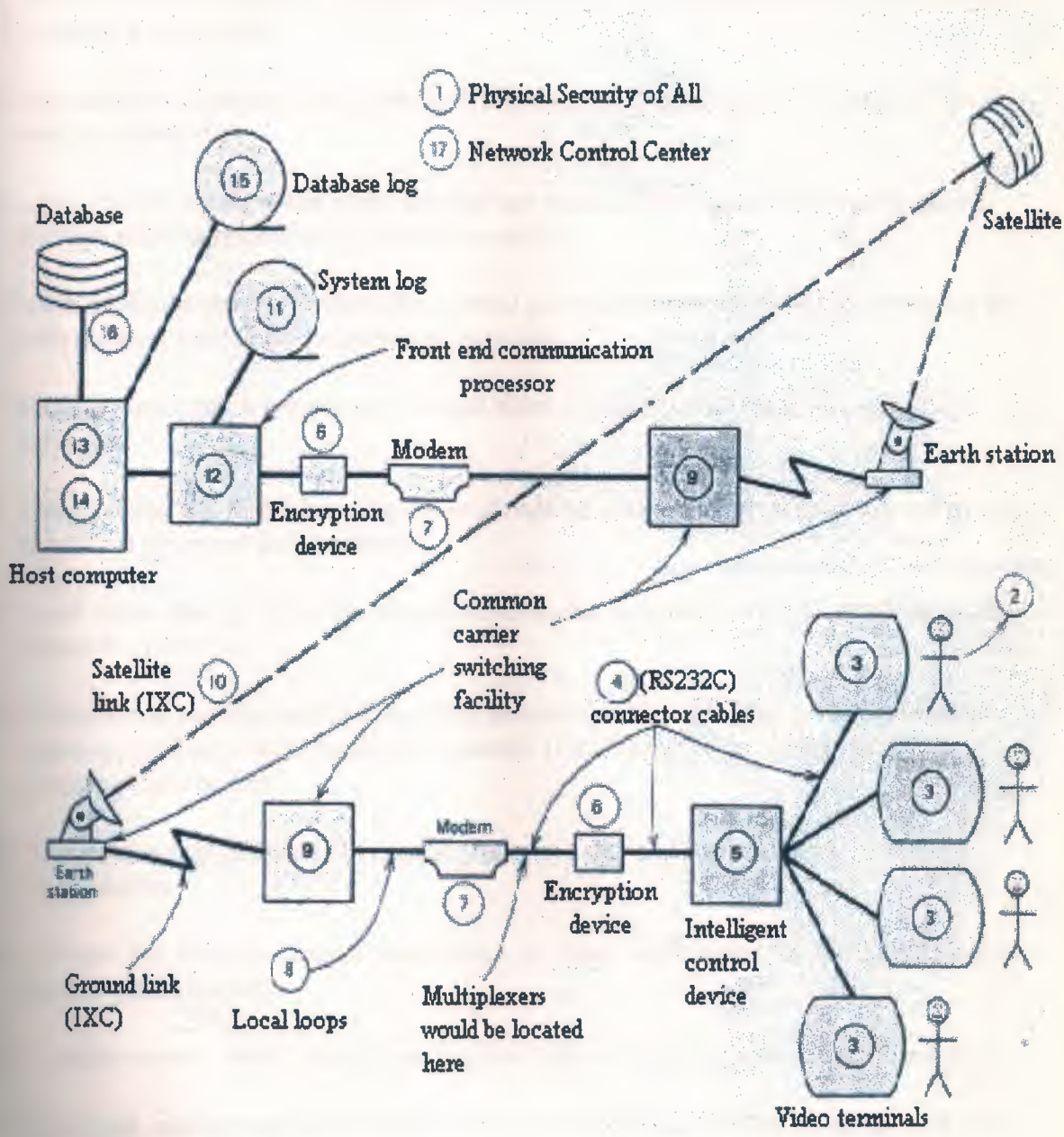


FIGURE 1-2 Network Control Points

1. Physical security of the building or buildings that house any of the hardware, software, or communication circuits must be evaluated. Both local and remote physical facilities should be secured adequately and have proper controls.

2. Operator and other personnel security involves implementation of proper access controls so that only authorised personnel can enter the closed areas where network equipment is located or can access the network itself.

3. Proper security education, background checks, and the implementation of error/fraud controls fall this area.

4. Terminals are a primary area where both physical and logical types of security controls must be enforced.

5. Local connector cables and wire pairs that are installed throughout the organisation's facilities must be reviewed for physical security.

6. Local intelligent control devices that control groups of terminals should be reviewed for both physical and logical programmed controls.

7. Hardware encryption is a primary control point, especially with regard to security of messages.

8. The modems and multiplexer hardware should be reviewed with regard to control and security at this point in the network.

9. Local loops that go from the organisation to the common carrier's switching facility should be reviewed.

10. The physical security and backup of the common carrier switching facility (telephone company central office) should be evaluated. If this facility were destroyed, all the circuits would be lost.

11. This review may include both central offices in a city and earth stations for satellite transmission.

12. Review the security control mechanisms in place with regard to the interexchange channel (IXC) circuits.

13. A major control point is the system log that logs all incoming and outgoing messages.

14. The front end communication processor is another major control point to review. At this point there may be a packet switching node (SN) that must be reviewed for security and control.

15. Within the host computer, any controls that are built into the software should be reviewed.

16. Also within the host computer, review for any controls that are designed into the host computer's hardware mechanisms/architecture.

17. Another major control point, only in database systems, is the database before-image/after-image logging tape.

18. This should be reviewed for any controls that may be in existence at this point. Many other security/control items of data are logged at this point.

19. With regard to database-oriented systems, another control point is the database management system (DBMS) itself.

20. The database management system software may have some controls that help with regard to security of the data communication network and the control of data/information flow.

21. The last control point is the network control centre itself. This area has controls that relate to management and operation, test equipment utilised, reports and documentation.

These 17 control points are the specific areas where control features can be implemented and maintained within a data communication network.

Now let's review the specific controls that can be used to secure your data communication network.

ENCRYPTION

Encryption is the process of disguising information by the use of many possible mathematical rules known as algorithms. Actually, *cryption* is the more general and proper term. Encryption is the process of disguising information, decryption is the process of restoring it to readable form. Of course, it makes no sense to have one process without the other. When information is in readable form, it is called *clear* or *plaintext.* When in encrypted form, it is called *ciphertext.*

The art of cryptography reaches far into the past and until recently has almost always been used for military and political applications. By today's exacting standards, such ciphers are insecure and therefore obsolete. They were usually alphabetic ciphers (rules for scrambling the *letters* in a message) and were designed for manual processing. Today's world of binary numbers and the speed of computers has given birth to a new class of cryption algorithms.

The acceleration of new research began during the Second World War and has continued into the present time for four reasons:

- Recognition of the necessity of encrypting communications for military purposes.
- The advent of high-speed computational electronics (computers).
- A growing interest in cryptography within academic circles.
- An interest on the part of private corporations, as well as governments, in protecting their proprietary information.

Interest in cryptographic protection runs highest in the world of communications. Of all the routes and resting places of information, communicated information is the most vulnerable to disclosure. Data stored on magnetic tapes, on disks, and in computer memory can be protected to a large extent by physical security, passwords, and other software access control systems.

Modern data communications takes advantage of existing public telephone circuits, microwave transmissions, and satellite relays. As a result, communicated information is highly exposed in a variety of forms. It can be captured at minimum expense and risk to the data thief, and at maximum loss to the organization.

A striking example of this exposure is the daily Electronic Funds Transfer (EFT) of billions of dollars between domestic and foreign banks over public links. The cover alteration of bank account numbers, amount of funds, and the like can have disastrous results.

There are always two parts to an encryption system. First there is the algorithm itself. This is the set of rules for transforming information. Second, there is always a key. The key personalises the use of the algorithm by making the transformation of your data unique. Two pieces of identical information encrypted with the same algorithm but with *different keys* produce completely different ciphertexts.

When using most encryption systems, it is necessary for communicating parties to share this key. If the algorithm is adequate and the key is kept secret, acquisition of the ciphertext by unauthorised personnel is of no consequence to the communicating parties.

The key is a relatively small numeric value (in number of bits) that should be easily transportable from one communicating node to another (see item 6 on Figure 1-2). The key is as it sounds. It is something that is small, portable, and with the aid of a good lock, the algorithm it keeps valuables where they belong.

Good encryption systems do not depend on keeping the algorithm secret. Only the keys need to be kept secret. The algorithm should be able to accept a very large number of keys, each producing different ciphertexts from the same cleartext. This large "key space" protects ciphertext against those who would try to break it by trying every possible key. There should be a large enough number of possible keys that an exhaustive computer search would take an inordinate amount of time or would cost more than the value of the encrypted information.

Almost every modem encryption algorithm transforms digital information. Scrambling systems have been devised for analogue voice signals, but it generally is agreed that their algorithms are not as strong as those used for digital signals made up of binary bits. The most recent advances in analogue signal protection have not been in newer and better algorithms. Instead, they have been in the technology of high-speed conversion of analogue signals to digital information bits in preparation for encrypting them with digital algorithms. In any case, the vast majority of today's proprietary information is digital. For this reason we will discuss only digital techniques.

Encryption algorithms may be implemented in software or hardware. The former has some advantages in protecting stored data files and data in the host computer's memory. However, hardware implementations have the advantage of much greater processing speed, independence from communication protocols, ability to be implemented on "dumb" devices (terminals, TELEX, facsimile machines, etc.), and greater protection of the "key" because it is physically locked in the encryption box.

Unauthorised tampering with the box causes erasure of the keys and related information. Hardware implementations have been reduced to the chip level because they are simply specialised microprocessors housed in small hardware boxes.

By far the most widely used encryption algorithm is the Data Encryption Standard (DES). It was developed in the mid-1970s by the U.S. government in conjunction with IBM. DES is maintained by the National Bureau of Standards (NBS) and is often referred to as NBSDES or DEA (Data Encryption Algorithm). The U.S. government recommends that DES be used for the encryption of commercial and unclassified military data. The American Banking Association has endorsed its use for the commercial banking industry.

This combination of credentials makes DES the technique of choice by private institutions. This concept of "choice" is somewhat misleading. DES is the only algorithm endorsed by the government. The academic literature is full of alternatives, but practical reasons, such as obtaining insurance against third party fraud, and the lack of mathematical sophistication on the part of encryption system users, presently leave little choice.

DES is classified as a *block cipher*. In its simplest form the algorithm encrypts data in independent 64-bit blocks. Encryption is under the control of a 64-bit key. DES expects a full 64-bit key but it uses only 56 of the bits (every eighth bit may be set for parity). Therefore, the total number of possible keys is 256 or over 72 quadrillion combinations.

DES ciphertext is composed of blocks containing highly randomised bit sequences. The algorithm is so thorough in its randomising of any 64-bit block (almost without regard to the cleartext of the key) that ciphertext almost always passes standard tests for randomness. The random quality of ciphertext is a crucial factor in the design of communication networks that will convey ciphertext. Communication control characters (for message routing or error detection) cannot be mixed with ciphertext because there is always some probability that DES will generate one of these control characters and thwart the communication system.

As a result, DES hardware usually is employed as shown in Figure 1-3. Communication protocols, parity, and checksums are in place with the message *before it* enters the originating DES hardware device. As is shown, this information may originate from a terminal, a front end, or a variety of communicating devices. The hardware encryption boxes usually are utilised on a link-to-link basis as depicted in Figure 1-3.

Placing the DES device between the modems can present a number of problems. First, most DES boxes are digital devices. They usually do not accept the analogue signals output by modems. Second, in asynchronous communications at least the start bit must be sent in the clear. Encryption can, and usually does, begin with the first data bit and end with the last. Similar problems can occur if synchronous timing signals are encrypted.

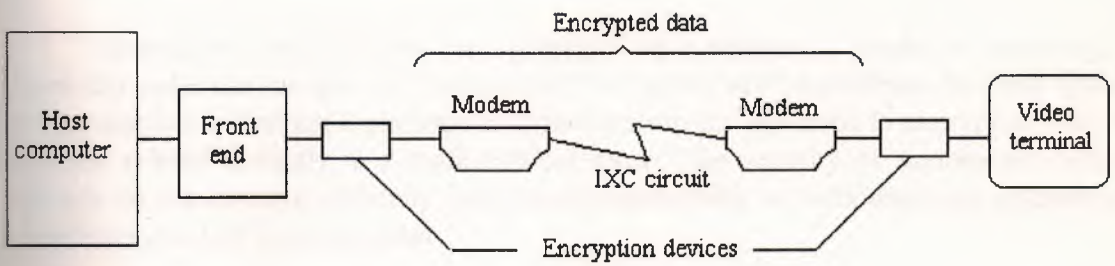


FIGURE 1-3 Encryption device location

The randomised information is now transmitted to a network switch, computer terminal, or other receiving device. The receiving DES hardware which must be loaded with the same key as the originating DES hardware then decrypts the information before it enters the receiving terminal device. Any communication protocols are verified *after* the decryption.

DES in some ways provides better error detection than standard parity or checksum techniques. If a single bit of any 64-bit ciphertext block is flipped during transmission, on decryption of that block the result will be 64 bits of random nonsense. This "error propagation" virtually ensures that parity and checksum will fail after decryption.

A more serious problem occurs if a bit is picked up or dropped during communication. The message loses 64-bit block "synchronisation" at the point of the dropped or added bit, and the message decrypts into nonsense. The result can be the loss of an entire message.

This magnification of communication errors is not without its price. Since the *minimum loss* of information is usually 64 bits, a retransmission almost always is required if there is a single bit communication error.

DES is a member of a class of algorithms known as "symmetric." This means that the key used to decrypt a particular bit stream must be the same as that used to encrypt it. Using any other key produces cleartext that appears as random as the ciphertext. This can cause some problems in the complex area of key management; keys must be dispersed and stored with great care. Since the DES algorithm is publicly known, the disclosure of a key can mean total compromise of encrypted messages.

1988

NEAR EAST UNIVERSITY

GRADUATION PROJECT

Subject : Network Security & Control

Submitted To : Prof. Dr. Fahrettin MAMEDOV

Prepared By : Aslı YAVUZ

Department : Computer Engineering

Student Number : 940726

INDEX 1

INTRODUCTION

Our subject in this project is Network Security and Control, Network Design Fundamentals. We had great knowledge while doing this project.

First of all this project will helpful for us at the real life for practising.

We took informations on the Internet, at so many books and also our teacher Mr. Mamedov gave us some of the source books that can help us to prepare our project.

We put figures to express the subject better. You can see them at the Appendix section.

Also we wish our project is helpful for students that are studying at the university.

We would like to thanks to Prof. Dr. Fahrettin Mamedov for his great helps to finish this project.

1) SECURITY AND CONTROL

This chapter identifies the 17 network control points that must be addressed for security and control. Specific hardware / software / protocol controls are reviewed.

Other control areas that are reviewed are: management controls, error control, recovery/back up/disaster, and the use of a matrix to identify, document, and evaluate security and control in a data communication network.

NETWORK SECURITY

In recent years organisations have become increasingly dependent upon data communication networks for their daily business communications, database information retrieval, and distributed data processing. This commitment to data communications/teleprocessing has changed the potential vulnerability of the organisation's assets.

This change has come about because the traditional security, control, and audit mechanisms take on a new and different form in data communication based systems. Increased reliance on data communications, the consolidation of many previously manual operations into computerised systems, use of database management systems, and the fact that on-line real-time systems cut across many lines of responsibility have increased management concern about the adequacy of current control and security mechanisms used in a data communication environment.

There also has been an increased emphasis upon computer network security because of numerous legal actions involving officers and directors of organisations, because of pronouncements by government regulatory agencies, and because the losses associated with computerised frauds are many magnitudes larger, per incident, than those from noncomputerized frauds. These factors have led to an increased vigilance with regard to protecting the organisation's information assets from many potential hazards such as fraud, errors, lost data, breaches of privacy, and disastrous events that can occur in a data communication network.

With regard to data communication networks, the organisation must be able to implement adequate control and security mechanisms within its facilities, including building facilities, terminals, local area networks, local loops, interexchange channel circuits, switching centres, network interface units (gateways), packet networks, hardware (modems, multiplexers, encryption devices, and the like), network protocols, network architecture software, test equipment, and network management control.

As an example, Figure 1-1 depicts a network typical of one that an organisation might develop.

In such a network all of the areas mentioned above would require a positive decision (policies and procedures) as to security and control. It should be noted that with this kind of network the organisation is vulnerable to many points of entry from an unwanted intruder. In fact, every terminal in the network is a potential entry point for an unauthorised intruder.

The rest of this chapter will be a discussion on each of the major portions of a data communication network, such as hardware and software, and a description of the various controls that relate to that specific area.

Finally, a matrix methodology for identifying network controls, documenting them, and evaluating their effectiveness will be presented. This is to provide the network manager with a good picture of the current controls, their effectiveness, and adequate documentation.

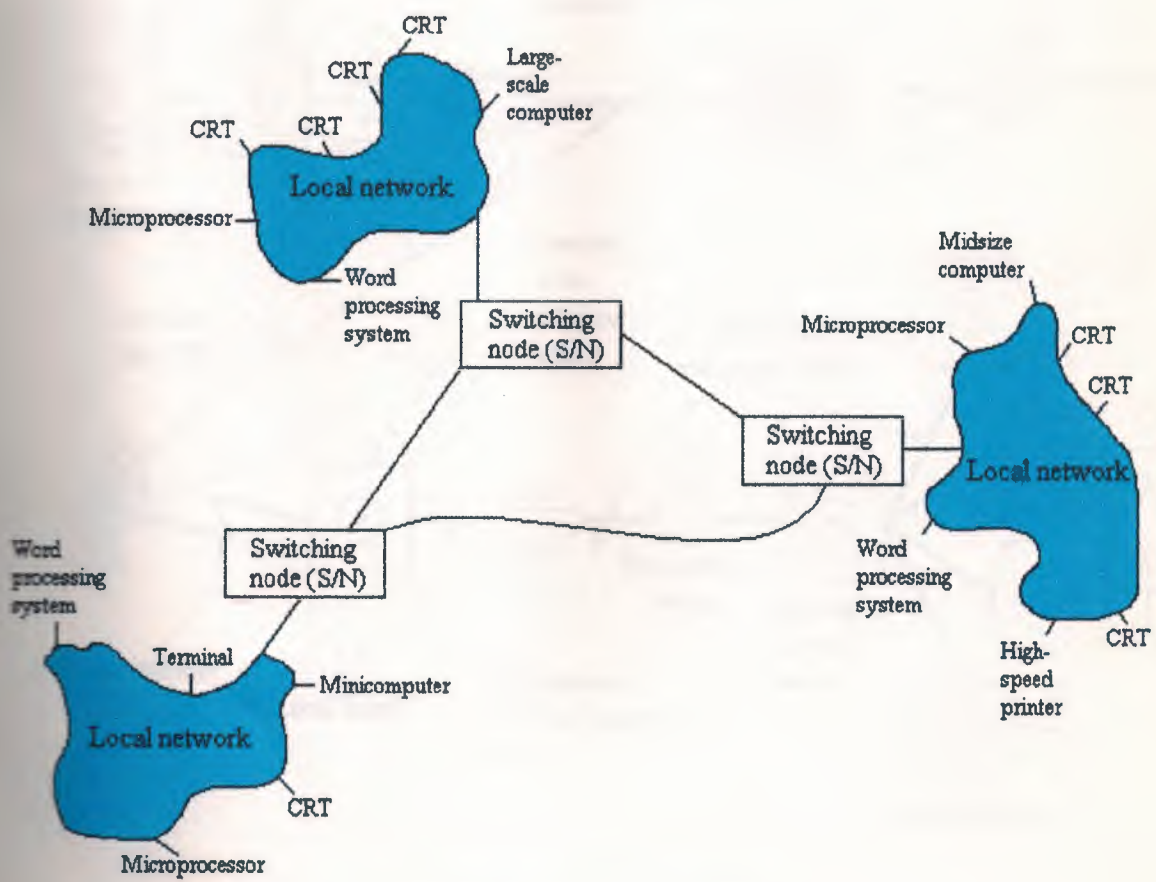


FIGURE 1-1 Future Network

NETWORK CONTROL POINTS

The 17 control points, or areas where control and security must be implemented, are depicted in Figure 1-2. The network manager, quality assurance personnel, security officer, or the organisation's EDP auditor should examine these areas to ensure that proper controls are implemented and are functioning properly. The numbers on Figure 1-2 are described in the following list.

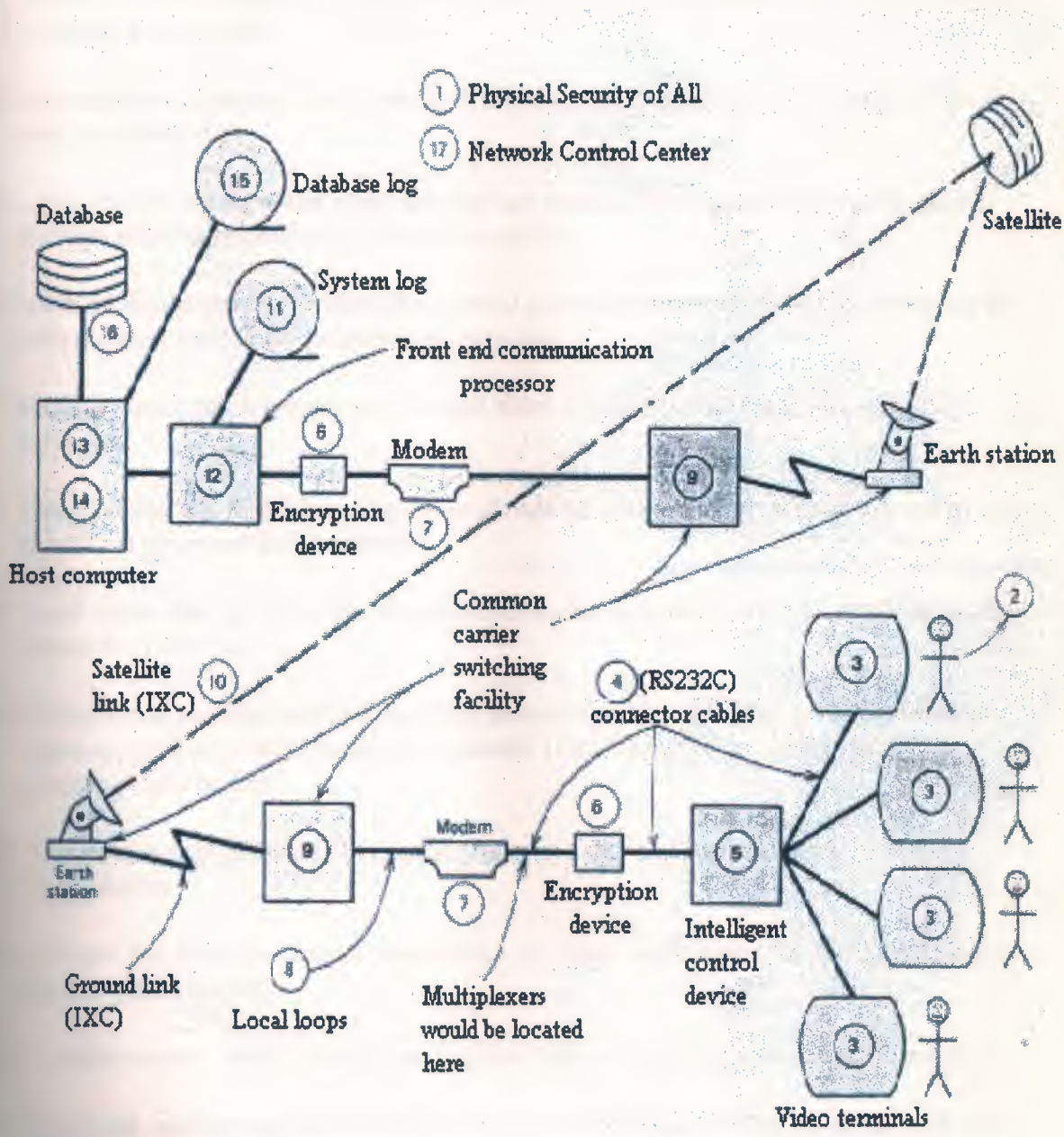


FIGURE 1-2 Network Control Points

1. Physical security of the building or buildings that house any of the hardware, software, or communication circuits must be evaluated. Both local and remote physical facilities should be secured adequately and have proper controls.

2. Operator and other personnel security involves implementation of proper access controls so that only authorised personnel can enter the closed areas where network equipment is located or can access the network itself.

3. Proper security education, background checks, and the implementation of error/fraud controls fall this area.

4. Terminals are a primary area where both physical and logical types of security controls must be enforced.

5. Local connector cables and wire pairs that are installed throughout the organisation's facilities must be reviewed for physical security.

6. Local intelligent control devices that control groups of terminals should be reviewed for both physical and logical programmed controls.

7. Hardware encryption is a primary control point, especially with regard to security of messages.

8. The modems and multiplexer hardware should be reviewed with regard to control and security at this point in the network.

9. Local loops that go from the organisation to the common carrier's switching facility should be reviewed.

10. The physical security and backup of the common carrier switching facility (telephone company central office) should be evaluated. If this facility were destroyed, all the circuits would be lost.

11. This review may include both central offices in a city and earth stations for satellite transmission.

12. Review the security control mechanisms in place with regard to the interexchange channel (IXC) circuits.

13. A major control point is the system log that logs all incoming and outgoing messages.

14. The front end communication processor is another major control point to review. At this point there may be a packet switching node (SN) that must be reviewed for security and control.

15. Within the host computer, any controls that are built into the software should be reviewed.

16. Also within the host computer, review for any controls that are designed into the host computer's hardware mechanisms/architecture.

17. Another major control point, only in database systems, is the database before-image/after-image logging tape.

18. This should be reviewed for any controls that may be in existence at this point. Many other security/control items of data are logged at this point.

19. With regard to database-oriented systems, another control point is the database management system (DBMS) itself.

20. The database management system software may have some controls that help with regard to security of the data communication network and the control of data/information flow.

21. The last control point is the network control centre itself. This area has controls that relate to management and operation, test equipment utilised, reports and documentation.

These 17 control points are the specific areas where control features can be implemented and maintained within a data communication network.

Now let's review the specific controls that can be used to secure your data communication network.

ENCRYPTION

Encryption is the process of disguising information by the use of many possible mathematical rules known as algorithms. Actually, *cryption* is the more general and proper term. Encryption is the process of disguising information, decryption is the process of restoring it to readable form. Of course, it makes no sense to have one process without the other. When information is in readable form, it is called *clear* or *plaintext.* When in encrypted form, it is called *ciphertext.*

The art of cryptography reaches far into the past and until recently has almost always been used for military and political applications. By today's exacting standards, such ciphers are insecure and therefore obsolete. They were usually alphabetic ciphers (rules for scrambling the *letters* in a message) and were designed for manual processing. Today's world of binary numbers and the speed of computers has given birth to a new class of cryption algorithms.

The acceleration of new research began during the Second World War and has continued into the present time for four reasons:

- Recognition of the necessity of encrypting communications for military purposes.
- The advent of high-speed computational electronics (computers).
- A growing interest in cryptography within academic circles.
- An interest on the part of private corporations, as well as governments, in protecting their proprietary information.

Interest in cryptographic protection runs highest in the world of communications. Of all the routes and resting places of information, communicated information is the most vulnerable to disclosure. Data stored on magnetic tapes, on disks, and in computer memory can be protected to a large extent by physical security, passwords, and other software access control systems.

Modern data communications takes advantage of existing public telephone circuits, microwave transmissions, and satellite relays. As a result, communicated information is highly exposed in a variety of forms. It can be captured at minimum expense and risk to the data thief, and at maximum loss to the organization.

A striking example of this exposure is the daily Electronic Funds Transfer (EFT) of billions of dollars between domestic and foreign banks over public links. The cover alteration of bank account numbers, amount of funds, and the like can have disastrous results.

There are always two parts to an encryption system. First there is the algorithm itself. This is the set of rules for transforming information. Second, there is always a key. The key personalises the use of the algorithm by making the transformation of your data unique. Two pieces of identical information encrypted with the same algorithm but with *different keys* produce completely different ciphertexts.

When using most encryption systems, it is necessary for communicating parties to share this key. If the algorithm is adequate and the key is kept secret, acquisition of the ciphertext by unauthorised personnel is of no consequence to the communicating parties.

The key is a relatively small numeric value (in number of bits) that should be easily transportable from one communicating node to another (see item 6 on Figure 1-2). The key is as it sounds. It is something that is small, portable, and with the aid of a good lock, the algorithm it keeps valuables where they belong.

Good encryption systems do not depend on keeping the algorithm secret. Only the keys need to be kept secret. The algorithm should be able to accept a very large number of keys, each producing different ciphertexts from the same cleartext. This large "key space" protects ciphertext against those who would try to break it by trying every possible key. There should be a large enough number of possible keys that an exhaustive computer search would take an inordinate amount of time or would cost more than the value of the encrypted information.

Almost every modem encryption algorithm transforms digital information. Scrambling systems have been devised for analogue voice signals, but it generally is agreed that their algorithms are not as strong as those used for digital signals made up of binary bits. The most recent advances in analogue signal protection have not been in newer and better algorithms. Instead, they have been in the technology of high-speed conversion of analogue signals to digital information bits in preparation for encrypting them with digital algorithms. In any case, the vast majority of today's proprietary information is digital. For this reason we will discuss only digital techniques.

Encryption algorithms may be implemented in software or hardware. The former has some advantages in protecting stored data files and data in the host computer's memory. However, hardware implementations have the advantage of much greater processing speed, independence from communication protocols, ability to be implemented on "dumb" devices (terminals, TELEX, facsimile machines, etc.), and greater protection of the "key" because it is physically locked in the encryption box.

Unauthorised tampering with the box causes erasure of the keys and related information. Hardware implementations have been reduced to the chip level because they are simply specialised microprocessors housed in small hardware boxes.

By far the most widely used encryption algorithm is the Data Encryption Standard (DES). It was developed in the mid-1970s by the U.S. government in conjunction with IBM. DES is maintained by the National Bureau of Standards (NBS) and is often referred to as NBSDES or DEA (Data Encryption Algorithm). The U.S. government recommends that DES be used for the encryption of commercial and unclassified military data. The American Banking Association has endorsed its use for the commercial banking industry.

This combination of credentials makes DES the technique of choice by private institutions. This concept of "choice" is somewhat misleading. DES is the only algorithm endorsed by the government. The academic literature is full of alternatives, but practical reasons, such as obtaining insurance against third party fraud, and the lack of mathematical sophistication on the part of encryption system users, presently leave little choice.

DES is classified as a *block cipher*. In its simplest form the algorithm encrypts data in independent 64-bit blocks. Encryption is under the control of a 64-bit key. DES expects a full 64-bit key but it uses only 56 of the bits (every eighth bit may be set for parity). Therefore, the total number of possible keys is 256 or over 72 quadrillion combinations.

DES ciphertext is composed of blocks containing highly randomised bit sequences. The algorithm is so thorough in its randomising of any 64-bit block (almost without regard to the cleartext of the key) that ciphertext almost always passes standard tests for randomness. The random quality of ciphertext is a crucial factor in the design of communication networks that will convey ciphertext. Communication control characters (for message routing or error detection) cannot be mixed with ciphertext because there is always some probability that DES will generate one of these control characters and thwart the communication system.

As a result, DES hardware usually is employed as shown in Figure 1-3. Communication protocols, parity, and checksums are in place with the message *before it* enters the originating DES hardware device. As is shown, this information may originate from a terminal, a front end, or a variety of communicating devices. The hardware encryption boxes usually are utilised on a link-to-link basis as depicted in Figure 1-3.

Placing the DES device between the modems can present a number of problems. First, most DES boxes are digital devices. They usually do not accept the analogue signals output by modems. Second, in asynchronous communications at least the start bit must be sent in the clear. Encryption can, and usually does, begin with the first data bit and end with the last. Similar problems can occur if synchronous timing signals are encrypted.

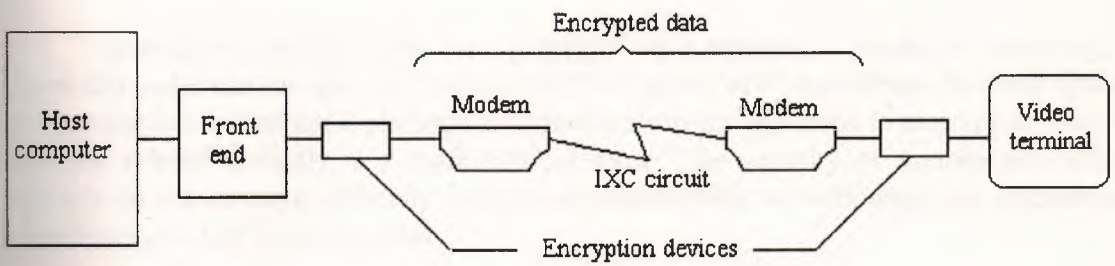


FIGURE 1-3 Encryption device location

The randomised information is now transmitted to a network switch, computer terminal, or other receiving device. The receiving DES hardware which must be loaded with the same key as the originating DES hardware then decrypts the information before it enters the receiving terminal device. Any communication protocols are verified *after* the decryption.

DES in some ways provides better error detection than standard parity or checksum techniques. If a single bit of any 64-bit ciphertext block is flipped during transmission, on decryption of that block the result will be 64 bits of random nonsense. This "error propagation" virtually ensures that parity and checksum will fail after decryption.

A more serious problem occurs if a bit is picked up or dropped during communication. The message loses 64-bit block "synchronisation" at the point of the dropped or added bit, and the message decrypts into nonsense. The result can be the loss of an entire message.

This magnification of communication errors is not without its price. Since the *minimum loss* of information is usually 64 bits, a retransmission almost always is required if there is a single bit communication error.

DES is a member of a class of algorithms known as "symmetric." This means that the key used to decrypt a particular bit stream must be the same as that used to encrypt it. Using any other key produces cleartext that appears as random as the ciphertext. This can cause some problems in the complex area of key management; keys must be dispersed and stored with great care. Since the DES algorithm is publicly known, the disclosure of a key can mean total compromise of encrypted messages.

Therefore, in order for two nodes in a network to establish communication of ciphertext, it is first necessary to define and communicate a common key over a secure channel or send it by personal courier.

Alternatives to DES have been proposed by a number of academic cryptologists. These fall under the category of "asymmetric" or "public key" algorithms. In these systems the key needed to decrypt a message *is different* from the one used to encrypt it. The two keys are related distantly in a mathematical sense. The security of asymmetric systems depends on the extreme difficulty (analytical impossibility or computational unfeasibility) of deriving one key from the other.

Asymmetric algorithms can greatly reduce the key management problem. Each receiving node has its publicly available key (hence the name "public key") that is used to encrypt messages sent by any network member to that node. These public keys may be listed in a telephone book type directory. In addition, each user has *a private key* that decrypts only the messages that were encrypted by its public key.

The net result is that if two parties wish to communicate with each other, there is no need to exchange keys beforehand. Each knows the other's public key from the public directory and can communicate encrypted information immediately. The key management problem may be reduced to each user's being concerned only with the on-site protection of its private key.

It is expected that the National Bureau of Standards will endorse a public key algorithm by 1985.

In order to visualise how a public key algorithm works, look at Figure 1-4. At the top of this figure there is a public directory which contains all of the public keys for each organisation utilising public key encryption. Our public directory contains five different banks.

In order to use the public key encryption methodology, a bank also has a secret key known as a private key; therefore, there are two separate keys, the private (secret) key and the public key. In this case, the bank places its public key into the public directory and carefully secures its own copy of the private key.

The middle of Figure 1-4 shows what an encrypted message would look like. When bank 4 wants to send a message to bank 1, it encrypts the message with the bank 1 public key, which is obtained by bank 4 from the public directory. This represents a straightforward encryption of a message between bank 4 and bank 1. Obviously, when the message is received at bank 1, it decrypts the message using its secret private key.

For more complex encryption, bank 4 can include its signature so bank 1 also can verify the signature or, in other words, be sure that the message originated from bank 4.

In order to perform a signature verification (see the bottom message of Figure 1-4), bank 4 first encrypts its ID (signature) plus some of the "key-contents"' of the message, using the bank 4 private key. This is its own private key and is known only to bank 4.

Next, bank 4 encrypts both the message contents and the already encrypted bank ID using the bank 1 public key from the public directory. This means that the bank 4 ID has been double encrypted, first using the bank 4 private key and then a second time using the bank 1 public key. The message is then transmitted to bank 1.

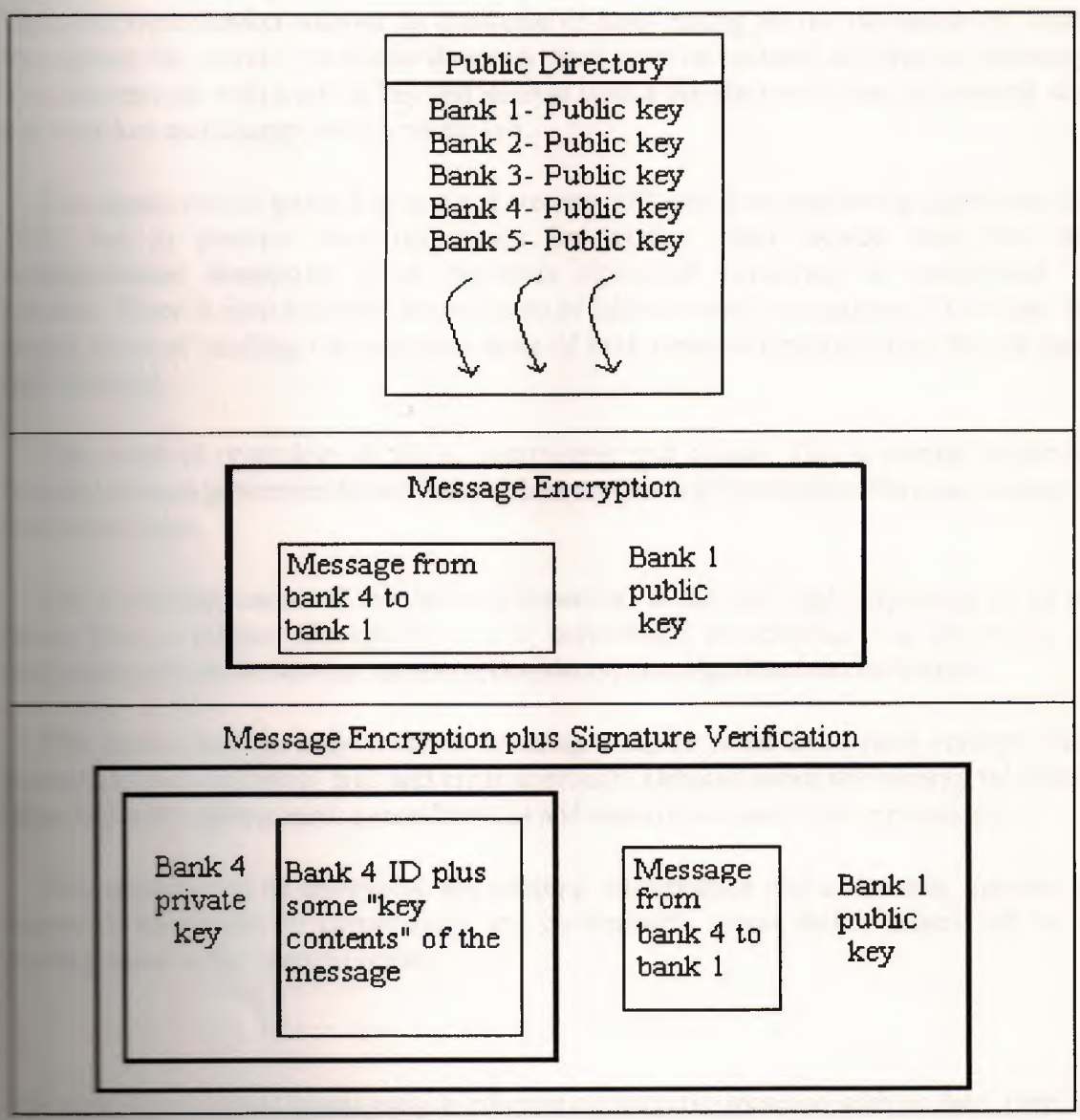


FIGURE 1-4 Public encryption

Upon receipt of the message, bank 1 uses its private key to decrypt the entire message. At this point, bank 1 is able to read the contents of the message, except for a block of data that is still encrypted (unidentifiable). Because the message was received from bank 4, bank 1 assumes that bank 4 secretly encrypted its ID plus some "key-contents" of the message for signature verification purposes.

At this point, bank 1 takes the Bank 4 public key (from the public directory) and decrypts the trailing block of data that contains the bank 4 ID plus some "key-contents" [1] of the message.

In this way, the public key system encrypts messages and also offers electronic signature identification without an exchange of keys among all the thousands of banks throughout the world. The public directory need only be updated as often as necessary. You can encrypt with a public key and decrypt with a private key or you can encrypt with a private key and decrypt with a public key.

The algorithms for public key systems are very different from symmetric algorithms like DES, but in practice their ciphertexts are similar when viewed from the data communication standpoint. Each produces ciphertext consisting of randomised bit patterns. There is almost always some degree of inherent error propagation. Therefore, the practicalities of handling the communication of both types of ciphertexts are for the most part identical.

The world of cryptology is full of controversy and debate. This is caused in part by tension between governments and independent academic cryptologists. National security is always the issue.

The underlying cause of this tension, however, is the fact that cryptology is an art rather than a science. Except for a few noteworthy exceptions, it is impossible to mathematically *prove* whether an encryption/decryption algorithm can be broken.

This means that the only route to breaking a cipher is an artful (and perhaps time-consuming and expensive) trial and error approach. Debates about the security of ciphers often end with mathematical generalisations and seat-of-the-parts type expressions.

This combination of embryonic but exciting mathematics and a dramatic increase of interest in encryption by corporations and governments means that it indeed will be an exciting arena in the years to come.

[1] The term *key-contents* means unique information from the message such as date, time, or dollar amount. It does not refer to the public/private keys.

HARDWARE CONTROLS

This section describes the hardware controls found in a network. The pieces of network hardware are discussed in terms of the controls that relate to them. We will review controls that relate to front end processors, packet switching controllers, modems, multiplexers, remote intelligent controllers, and terminals.

1. Front End Processors

The front end processor that controls a centrally controlled data communication network can be one of the single most important areas for security and control. It is only a piece of hardware, but within it are software programs/protocols that control the access methods for data flow.

Some specific controls that might be housed within the front end communication processor are:

- Polling of the terminals to ensure that only authorised terminals are on the network.
- Logging of all inbound and outbound messages (systems log) for historical purposes and for immediate recovery should the system fail.
- Error detection and retransmission for messages that arrive in error.
- Message switching that reduces the possibility of lost messages (there also can be circuit switching or packet switching).
- Store and forward techniques help avoid lost messages (although storing and the forward opens up the possibility of a network programmer's copying messages from the storage disk).
- Serial numbers for all messages between all nodes.
- Automatic call-back on dial-up facilities for preventing the host computer from the being connected to an unauthorised dial-up terminal.
- Systems editing such as rerouting of messages, triggering of remote alarms if the certain parameters are exceeded or if there is an abnormal occurrence.
- Collection of network traffic statistics for long-term control of the total network.

2. Packet Switching Controllers

A packet switching controller or switching node (SN) is similar to a front end communication processor, but it has some specialised features that pertain to the operation of a packet network.

It is possible for a packet switching controller to perform any of the control functions previously mentioned for front ends. In addition, it performs other specific control functions such as the following:

- It keeps track of messages between different nodes of the network.
- It controls the numbering of each packet to avoid lost packets, messages, or illegal insertions.
- It routes all messages. It may send different packets, containing parts of the same message, on different circuits (unknown circuit path).
- This may prevent an unauthorised user/perpetrator from receiving all parts of a sensitive message.
- It contains global and/or local databases that contain addresses and other sensitive data pertaining to each node.
- These databases can be cross-referenced with other written documentation when network nodes are reviewed for security.
- On dial-up packet networks, it keeps track of the sender of each message that is delivered.
- It can either restrict the users to dial-up or allow use of leased circuits into the packet network.

3. Modems

The modem may be an interface unit either for broadband (analogue) communication circuits or for baseband (digital) communication circuits. It does not matter which because these hardware units can perform any of the controls listed below, depending upon the features installed by each manufacturer.

Modems can offer loopback features that allow the network manager to isolate problems and identify where they are occurring in the network. Some modems contain automatic equalisation microprocessor circuits to compensate for electronic instabilities on transmission lines, thereby reducing transmission errors.

Some modems have built-in diagnostic routines for checking their own circuits. Mean Time Between Failure (MTBF) statistics should be collected for modems because low MTBF indicates that downtime is excessive.

Some dial-up modem controls include changing the modem telephone numbers periodically, keeping telephone numbers confidential at both user sites and the central data centre, possibly disallowing automatic call receipt at the data centre (using people to intercept), removing telephone numbers from both local and remote dial-up modems, and requiring the use of terminals that have an electronic identification circuit for all dial-up ports.

Finally, it may be desirable to utilise a *dial-out-only facility,* whereby the act of dialling into the network and entering a password automatically triggers a disconnect; the front end or host computer then dials the "approved" telephone number that matches the password used during the original dial-in. In other words, dial-in triggers a dial-out.

4. Multiplexers

Because many multiplexer sites are at remote locations, a primary control is to prevent physical access to the multiplexer.

Another consideration is whether the multiplexer should have dual circuitry and/or backup electrical power since loss of a large multiplexer site can knock out several hundred terminals. Because time division statistical multiplexers have internal memory space, and some have disk storage, special precautions must be taken.

Memories and disk storage make illegal copying of messages easier. Other controls include logging all messages at the remote multiplexer site before transmission to the host computer and manually logging all vendor service call visits.

5. Remote Intelligent Controllers

A remote intelligent controller can be a special form of multiplexer or a remote front end communication processor that is located several hundred miles from the host computer.

These devices usually control large groups of terminals. All of the controls that were mentioned for multiplexers also apply to remote intelligent controllers.

A review of software controls that can be programmed into this device is suggested. For example, daily downline loading of programs can help ensure that only authorised programs are in this device.

Another control is the periodic counting of bits in the software memory space. This identifies a minor program change so that a new one can be downline loaded immediately. Each controller should have its unique address on a memory chip (instead of software) to anyone who wants change hardware addresses.

Remote logging of each inbound/outbound message should be considered seriously. If hardware encryption boxes are located in the same facility as the remote intelligent controllers, then access to these devices should be controlled by implementation of strict physical control procedures and locked doors.

6. Terminals

There are two basic areas that must be considered with regard to the control of terminals in a data communication network. The first is *human error prevention controls* and *the second is security controls*. Each is listed below:

a) Human Error Prevention Controls

- Ensure adequate operator training with regard to self-teaching operator manuals and the periodic updating of these manuals.

- Keep dialogue simple between the operator and the application system (menu selection might be utilised).

- Terminals should be easy to use and have functional keyboards.

- Consider preprinted forms for printing terminals and a fill-in-the-blank format (preprinted forms on a video screen) for video terminals.

- Instructions should be preprogrammed and available for recall when an operator needs help.

- Secured systems, where assistance should be more difficult to obtain, may be an exception.

- Operators should have restart procedures that can be used for error recovery during a transaction.

- Work area extremes in light, noise, temperature, and so on must be minimised if operators are to reduce errors to a minimum.

- Reasonably fast response times reduce errors because longer response times produce error-causing frustration in operators. Long response times also reduce productivity.

- Intelligent terminals can edit for logical business errors and verify data before transmission.

- When video terminals are used, they should have the largest dot matrix screen to reduce operator eyestrain (10 times 14 is easier to read than 5 times 7), screens should have an anti-glare surface, characters should not jitter on the screen, and the cursor should be visible at 8 feet.

- Reverse video (black on white as compared to white on black) provides a choice for individual operators. Yellow/green screens are easiest to see, and terminals that have brightness/focus/contrast adjustments are preferred by terminal operators.

b) Security Controls

- Terminals can have a unique electronic chip built in that provides positive identification. With chips, the front end or host identifies each terminal electronically.
- Physically lock terminal on/off switches or have locks that disable the screen and keyboard.
- Keep terminals in a physically secure location.
- Lock off all of the communication circuits after hours (positively disable the communication circuits).
- Each system user should have an individual password.
- Each user could have a plastic identification card that runs through an identification card reader. Such cards replace the need for individual passwords.
- Utilise special log-in numbers that can entered only by a key person in the department.
- Consider using one of the newer types of personal identification such as signature identification, fingerprint identification, voice identification, hand image identification.
- Transaction code each terminal. This prevents any transaction that is not related to the work area in which the terminal is located. In other words, the terminal is made transaction specific.
- Develop a security profile of the types of data being entered and the user login procedures. If a violation occurs, the terminal that was used can be shut down automatically. In addition, a terminal security report should be delivered the next day to the manager of the user work area.
- Restrict terminals to read-only functions.
- Sequence number, time stamp, and date all messages.
- Passwords should not print when they are typed.
- Ensure proper disposal of hard copy terminal output.
- Allow intelligent terminals to perform editing transactions before they are transmitted.
- When looking at the control and security of dial-up terminals, review the controls for dial-up modems that were listed previously in the section on modems.

CIRCUIT CONTROLS

Some of the communication circuits that must be reviewed are the wire pairs and cables that are placed throughout the user facility, the local loops that go between the user facility and the common carrier (telephone company), and the interexchange channel (IXC) circuits between cities.

The wire pairs and cables within the user facility should be made as physically secure as possible, because this is where anyone wanting to tap the system would enter. It is 100 times easier to tap a local loop than it is to tap an interexchange channel. Ensure that the lines are secured behind walls and above ceilings, and that the telephone equipment and switching rooms are locked and the doors alarmed.

With regard to local loops, there is not much that can be done except to visit the common carrier switching facility. This provides some idea as to the physical security, fire protection, and disaster prevention controls implemented by the common carrier. If these are inadequate, about the only thing that can be done is to split local loops among your facility and two or three different common carrier switching facilities (telephone company end offices).

For security on interexchange channels, encryption of messages is the only dependable method. If the data/information is so sensitive that a breach of privacy or the insertion/modification of a message cannot be allowed, then encryption must be considered.

With regard to internal cables within your user facility, the use of fiber optics might be considered. Fiber optic cable uses light-emitting diodes or laser light to transmit pulses of light through hair-thin strands of plastic or glass. These devices offer security through their immunity to electrically generated noise, their resistance to taps, their isolation, and their small size. They also have some special benefits in an environmental sense.

Because optical fibers are immune to electrically generated noise such as radio interference, they offer a bit error rate of approximately 10-9 as compared with 10-6 for metallic connectors.

Fiber optic cable is an attractive security measure because it is almost totally immune to unauthorised access by tapping. Taps can be made only by breaking the cable, polishing it off, and inserting a splice or nicking into the core, to detect the light.

The first method, using a T-splice adapter, does give a detectable power loss in the optic fiber system, so it can be detected easily.

The second method, nicking, might be possible with a step index cable, which has a silica core and a plastic cladding around it. The plastic cladding could be nicked so that the light could leak out, although if too much light leaked out the signal would be lost.

The nicking technique is almost impossible to accomplish in a graded index fiber, however, because the core and the cladding are one piece of silica.

A graded index fiber is made of silica and the cladding is also silica, but it has a different index of refraction and therefore reflects light down the cable. Because these two are melted together during manufacture, nicking would be almost impossible (the glass would crack).

With regard to isolation, optical fiber cables provide complete isolation between transmitters and receivers, thus eliminating the need for a common ground. This structure provides electrical isolation from hardware and eliminates problems such as ground loops within an installation. It also reduces the amount of electrical noise that produces errors on data communication circuits.

For communications in a dangerous atmosphere, such as a petroleum refinery or a paint factory, it has another advantage because static spark is eliminated.

The small size and light weight of fiber cables offer users better opportunities to secure this medium physically. Because fiber optic cable is non-conductive, it is free from electromagnetic noise radiation and therefore is resistant to conventional passive tapping techniques.

Finally, in most cases fiber optic cable is less restricted under harsh environmental conditions than its metallic counterparts. It is not as fragile or brittle as might be expected and it is more corrosion resistant than copper. The only chemical that affects optical fiber is hydrofluoric acid. In case of fire, an optical fiber can withstand greater temperatures than copper wire.

Even when the outside jacket surrounding the fiber has melted, a graded index fiber optic system can still be operational in an emergency signalling system. One word of warning, however: care must be taken when pulling these cables through the building so the cable is not separated because its tensile strength is exceeded.

One more caution with regard to control and security of the connector cables against surreptitious taps. The maximum 50-foot cable length of the RS232C or the 4,000-foot cable length of the RS449 could be prime targets.

The RS449 offers extra control features such as special circuits for moving from a primary private line service to a packet switched service when backup is needed or simply to access another database that is not normally used. This eliminates manual patching, switching keys, and so on. The RS449 can invoke tests to isolate problems with either the local or remote data circuit-terminating equipment (DCE) or the communication circuit itself.

PROTOCOL CONTROLS

Protocols are simply the rules by which two machines talk to each other. The word "protocol" comes from the greek *protokollon,* which is the first sheet glued to a papyrus roll; it was the table of contents.

The International Organisation for Standardisation (ISO) has developed a seven-layer (OSI model) protocol. These layers and some ideas for their control are as follows :

- **Layer 1: The Physical Link Control**

The physical layer is concerned with transmitting raw bits over a communication channel. It describes the physical, electrical and functional interchange that establishes, maintains, and disconnects the physical link between data terminal equipment (DTE) and data circuit-terminating equipment (DCE).

At this layer controls are needed to physically protect the connector cable. An example might be that an RS449 cable offers more control pins than an RS232C cable (see Figures 4-4 and 4-5). The goal at this layer is to control physical access by employees and vendors and to try to identify breaches of security and/or restrict entry to the system at this physical layer, as well as each of the following six layers.

- **Layer 2: Data Link Control (DLC)**

Data link control contains the functions that transfer data over the link established by layer 1. The task of the data link layer is to take a raw transmission facility and transform it into a circuit that appears free of transmission errors to the network layer (layer 3). It accomplishes this task by breaking the input data into *data frames,* transmitting the frames sequentially, and processing the acknowledgement frames back to the original sender.

At this layer the protocol should contain controls such as sequence counting of frames, error detection and retransmission capabilities, identification of lost frames, reduction of possible duplicate transmissions to zero.

It should solve problems caused by damaged/lost/duplicate frames, prevent a fast transmitter from drowning a slow receiver in data, provide limited restart capabilities in case of abnormal termination situations, ensure that some of the transmitted data are not misinterpreted as line control characters, increase flow control efficiency to ensure that the maximum number of frames can be sent without requiring an acknowledgement, properly terminate a session, and the like.

- **Layer 3: Network Control**

Network control provides for the functions of internal network operations such as addressing and routing.

This is probably the software located in the terminal or intelligent controller at the remote end and the front end communication controller at the host end, although it may be in the packet switching node (SN).

Layer 3 determines the chief characteristics of how packets (the units of information) are exchanged and routed within the network. The major issue here, which is confusing, is the division of labour between the host computer and the front end processor.

Some of the controls to be questioned in this layer involve who should ensure that all packets are received correctly at their destinations and in the proper order. This layer of protocol should accept messages from the host convert them to packets, and see to it that the packets get directed toward their destination. Packet routing should be controlled here; there also might be some global or local databases at this layer that should be kept secure.

Control of congestion, such as too many packets on one channel, should be controlled by this layer. Also, this layer can contain billing routines for charging users and should be reviewed for possible problems such as error, theft of time, or improper message charges.

- **Layer 4: Transport Control**

Transport control provides transport services to the users for network independent interfacing from source to destination (end-to-end) across the network. At this layer we are out of the area of message protocols and into the area of software and network architectures. Layers 4 through 7 involve network architectures, whereas layers 1 through 3 involve basic message protocols.

Layer 4 is unique because it can be either protocol or network architecture software. The basic function of the transport layer (also known as the host-host layer) is to accept entire messages from the session layer (layer 5), split it into smaller units, pass these to the network layer (layer 3), and ensure that all the pieces arrive correctly at the other end.

Some of the controls that should be checked at layer 4 are related to network connections because the transport layer might have to create multiple network connections in order to get the required number of circuit paths. At this layer multiplexing might be invoked, so multiplexing controls should be reviewed.

At this layer also a program on a source machine carries on a conversation with a similar program on the destination machine using headers and control messages; therefore, some of the controls might be in the application programs.

At the lower layers (layers 1-3) the protocols are carried out by each machine and its immediate neighbours rather than the ultimate source and destination machines, which may be separated by many hardware devices and circuit links.

Another needed control is one that determines if the software at this level can tell which machine belongs to which connection. Other controls that are performed at this level, even though they may be performed elsewhere as well, are source/destination machine addressing and flow control (here it is flow of messages rather than flow of packets) so one machine cannot overrun another.

- **Layer 5: Session Control**

Session control supports the dialogue within a session. Operating system supervisors traditionally support this function. The session layer is the user's interface into a network. It is at this layer that the user negotiates to establish a connection with a process on the other machines.

Controls that should be examined at this layer are the typical controls that relate to a terminal (dedicated or dial-up), such as passwords, log-in procedures, terminal addressing procedures, authentication of terminals and/or users, correct delivery of the bill, and so on.

Another control occurs when the transport control (layer 4) connections are unreliable; the session layer may be required to attempt to recover from broken transport connections. As another example, in database management systems it is crucial that a complicated transaction against the database never be aborted halfway through the routine because this leaves the database in an inconsistent state.

The session layer often provides a facility by which a group of messages can be set aside so that none of them is delivered to the remote user until all of them have been completed.

This mechanism ensures that a hardware or software failure within the subnetwork can never cause a transaction to be aborted halfway through. The session layer also can provide for sequencing of messages when the transport layer does not.

- **Layer 6: Presentation Control**

Presentation control provides for the transformation or conversion of data formats. Examples are compaction, encryption, peripheral device coding, and formatting. The presentation layer performs functions that are requested sufficiently often as to warrant finding a general solution for them.

At this layer there are controls such as software encryption, text compression, text compaction, and conversion of incompatible file formats/file conversions so two systems can talk to one another.

Also this layer can take incompatible terminals and modify line and screen length, end-of-line conventions, scroll versus page mode, character sets, and cursor addressing to make them compatible. Simple errors at the remote terminal might be caused by the software at this layer.

- **Layer 7: Application Control**

The application control layer performs the application programs and system activities in support of the business functions.

The content of the application layer is up to the individual user/organisation.

This layer has controls that are related logically to the business system under review. Controls in the application layer are the typical day-to-day logical controls that are built into business systems.

The most common protocol that you might have to review is the international standard for packet switching networks. It is called X.25.

NETWORK ARCHITECTURE / SOFTWARE CONTROLS

Controls that relate to network architecture/software typically are associated with layers 4 through 7 of the OSI model. Additional architecture/software controls relate to computer operating systems, teleprocessing monitors, telecommunication access programs, databases, and security software packages.

Teleprocessing monitors are programs that relieve the operating system of many of the tasks involved in handling message traffic between the host and remote terminals, such as line handling, access methods, task scheduling, and system recovery. System throughput is increased by offloading these data communication functions from the operating system to the teleprocessing monitor.

Some of the controls that should be reviewed for teleprocessing monitors are access controls, who can sign onto a terminal, and who can access program routines (sometimes called *exits*). With regard to these exits, the code of each exit routine should be checked for correctness and security. These exit program modules should be placed in software-controlled libraries.

The vendor's "system generation" manuals or the teleprocessing monitor should be reviewed to determine if any security controls were built into the monitor by the vendor.

Telecommunication access programs are vendor-supplied programs that control the transmission of data to and from the host computer and various data communication devices. The telecommunication access programs are more likely to reside in a front end communication processor but they can reside in the host computer.

Some controls for the telecommunication access program may be documented in the vendor's "system generation" manuals. The controls that were built in by the software vendor should be evaluated. As with teleprocessing monitors, user program routines (exits) and access methods need to be examined.

Another area that interfaces with the teleprocessing monitor is the very sensitive network control database. For example, there might be *a system database* containing global information about addresses and logical names of all peripheral devices, locations of system files, system timing parameters; task locations and priorities, peripheral device control tables, and system supply command lists. Because of its importance to the security of the entire system, data in the system database must be protected adequately from copying or destruction.

Another database is the *network database*. It contains data such as the number of stations, polling/selecting lists, current station identifier, communication control port addresses, logical terminal identifiers, terminal device list, terminal poll/call sequences, dial-up numbers, message and process information, and the like. The network database also must be protected from unauthorised copying.

The network database can be used to cross-check against manual documentation. Because it contains information such as the number of stations and logical terminal identifiers, a copy of the database can be matched against the written network documentation as a means of verifying the currency of the documentation.

The impact of any security software packages that restrict or control access to files, records, or data items should be reviewed. These packages are independent of the data communications software.

Finally, software should be protected in case of a disastrous situation such as a power failure. Restart recovery routines should be available, and the system should only have one master input terminal for entering sensitive or critical commands. All default options should be identified, and the impact of default options that do not operate properly should be assessed to determine whether adequate software maintenance is available. Also all sensitive tables (passwords) should be protected in the memory.

ERROR CONTROL IN DATA COMMUNICATIONS

There are two categories of errors. The first category involves corrupted (changed) data, and the second involves lost data. With regard to selecting an error control system, some of the following factors should be considered:

- The extent and pattern of error-inducing conditions on the type of circuit used.
- The effects of no error control, or error detection/retransmission and of automatic error detection and correction (forward error correction).
- The maximum error rate that can be tolerated.
- Comparison of the cost of increased accuracy with the present cost of correcting errors.
- Comparison of different application systems as to the overall transmission accuracy currently being achieved.
- Cost of errors remaining in the received station to flag them and reenter them.

1) Data Communication Errors

Errors are a fact of life in today's data communication networks. Depending on the type of circuit/line, they may occur every few minutes or every few seconds or even more frequently. They occur because of noise on the lines. No data communication system can prevent all these errors from occurring, but most of them can be detected and many corrected by proper design. Common carriers that lease data transmission lines to users provide statistical measures specifying typical error rates and the pattern of errors that can be expected on the different types they lease.

Normally, errors appear in bursts. In a burst error more than one data bit is changed by the error-causing condition. This is another way of saying that 1-bit errors are not uniformly distributed in time. However, common carriers usually list their error rates as the number of bits in error divided by the number of bits transmitted, without reference to their nonuniform distribution. For example, the error rate might be given as 1 in 500,000 when transmitting on a public voice grade telephone circuit at 1,200 bps.

The fact that errors tend to be clustered in bursts rather than evenly dispersed has both positive and negative aspects. If the errors were not clustered (but instead were evenly distributed throughout the day), with an error rate of 1 bit in 500,000 it would be rare for two erroneous bits to occur in the same character, and consequently some simple character checking scheme would be effective. But this is not the case, because bursts of errors are the rule rather than the exception. They sometimes go on for time periods that may obliterate 50 to 100 or more bits.

The positive aspect is that, between bursts, there may be rather long periods of error-free transmission. Therefore no errors at all may occur during data transmission in a large proportion of messages. On the other hand, if errors are concentrated in bursts, it becomes more difficult to recover the meaning and much more reliance must be placed on knowledge of message ########[2] or on special logical/numerical error detection and correction methods.

It is possible to develop data transmission methodologies that give very high error detection and correction performance. The only way to do the detection and correction is to send along extra data. The more extra data that are sent, the more the error protection that can be achieved. However, as this protection is increased the throughput of useful data is reduced. Therefore, the efficiency of data throughput varies inversely as the desired amount of error detection and correction is increased.

Errors will even have an effect on the length of the block of data to be transmitted when synchronous transmission is used. The shorter the message blocks used the less likelihood there is of needing retransmission for any one block. But the shorter the message block, the less efficient is the transmission methodology as far as throughput is concerned. If the message blocks are long, a higher proportion may have an error and have to be resent.

In transmissions over the dial-up switched network, a considerable variation in the error rate is found from one time of the day to another. The error rate is usually higher during the periods of high traffic (the normal business day). In some cases the only alternative open to the user of these facilities is to transmit the data at a slower speed because higher transmission speeds are more error prone.

Dial-up lines are more prone to errors because they have less stable transmission parameters than private leased lines, and, because different calls use different circuits, they usually experience different transmission conditions. Thus, a bad line is not necessarily a serious problem in dial-up transmission; a new call may result in getting a better line.

Line conditioning, a service that is not available on dial-up lines, but only on private leased lines, consists of special electrical balancing of the circuit to ensure the most error-free transmission.

2) Line Noise and Distortion

Line noise and distortion can cause data communication errors. In this context we define noise as undesirable electrical signals. It is introduced by equipment or natural disturbances and it degrades the performance of a communication line. If noise occurs, the errors are manifested as extra or missing bits, or bits whose states have been "flipped," with the result that the message content is degraded. Line noise and distortion can be classified into roughly 11 categories: white noise, impulse noise, cross talk, echoes, intermodulation noise, amplitude changes, line outages, attenuation, attenuation distortion, delay distortion and jitter.

White or Gaussian Noise :

Is the familiar background hiss or static on radio and telephones. It is noise caused by the thermal agitation of electrons and because of this, it is inescapable. Even if the equipment utilised were perfect and the wires were perfectly insulated from any and all external interference there would still be some white noise. White noise is usually not a problem unless its level becomes so high that it obliterates the data transmission. Sometimes noise from other sources such as power line induction, cross modulation from adjacent lines, and a conglomeration at random signals resembles white noise and is labelled as such even though it is not caused by thermal electrons.

Impulse Noise (Sometimes called Spikes) :

Is the primary source of errors in data communications. An impulse of noise can last as long as 1/100th of a second. An impulse of this duration would be heard as a click or a crackling noise during voice communications. This click would not affect voice communications but it might obliterate a group of data bits, causing a burst error on a data communication line. At 150 bps,1 or 2 bits would be changed by a spike of 1/l00th of a second, whereas at 4,800 bps, 48 bits would be changed.

Some of the sources of impulse noise are voltage changes in adjacent lines or circuitry surrounding the data communication line, telephone switching equipment at the telephone exchange branch offices, arcing of the relays at older telephone exchange offices, tones used by network signalling, maintenance equipment during line testing, lightning flashes during thunderstorms, intermittent electrical connections in the data communication equipment.

Cross Talk :

Occurs when one line picks up some of the signal travelling down another line. It occurs between line pairs that are carrying separate signals, in multiplexed links carrying many discrete signals, in microwave links where one antenna picks up a minute reflected portion of the signal from another antenna on the same tower, and in any hard-wire telephone circuits that run parallel to each other, are too close to each other, and are not electrically balanced.

You are experiencing cross talk during voice communication on the public switched network when you hear other conversations in the background. Cross talk between lines will increase with increased communications distance, increased proximity of the two wires, increased signal strength, and higher frequency signals. Cross talk, like white noise, has such a low signal strength that it is normally not bothersome on data communication networks.

Echoes and Echo Suppression :

They can be a cause of errors. An echo suppressor causes a change in the electrical balance of a line and this change causes a signal to be reflected so it travels back down the line at reduced signal strength. Whenever the echo suppressors are disabled, as in data transmission, this echo returns to the transmitting equipment. If the signal strength of the echo is high enough to be detected by the communication equipment, it will cause errors. Echoes, like cross talk and white noise, have such a low signal strength that they are normally not bothersome.

Intermodulation Noise :

Is a special type of cross talk. The signals from two independent lines intermodulate and form a product that falls into a frequency band differing from both inputs. This resultant frequency may fall into a frequency band that is reserved for another signal. This type of noise is similar to harmonics in music. On a multiplexed line, many different signals are amplified together and slight variations in the adjustment of the equipment can cause intermodulation noise. A maladjusted modem may transmit a strong frequency tone when not transmitting data, thus yielding this type of noise.

Amplitude Noise :

It involves a sudden change in the level of power. The effect of this noise depends on the type of modulation being used by the modem. For example, amplitude noise does not affect frequency modulation techniques; this is because the transmitting and receiving equipment interprets frequency information and disregards the amplitude information.

Some of the causes of amplitude noise may be faulty amplifiers, dirty contacts with variable resistances, sudden added loads by new circuits being switched on during the day, maintenance work in progress, and switching to different transmission lines.

Line Outages :

They are a catastrophic cause of errors and incomplete transmission. Occasionally a communication circuit fails for a brief period of time. This type of failure may be caused by faulty telephone branch office exchange equipment, storms, loss of the carrier signal, and any other failure that causes an open line or short circuit.

Attenuation

Is the loss of power that the signal suffers as it travels from the transmitting device to the receiving device. It results from the power that is absorbed by the transmission medium or is lost before it reaches the receiver. As the transmission medium absorbs this power, the signal gets weaker, and the receiving equipment has less and less chance of correctly interpreting the data. To avoid this, telephone lines have repeater/amplifiers spaced through their length.

The distance between them depends upon the amount of power lost per unit length of the transmission line. This power loss is a function of the transmission method and circuit medium. Also, attenuation increases as frequency increases or as the diameter of the wire decreases.

Attenuation Distortion :

It refers to high frequencies losing power more rapidly than low frequencies during transmission. The received signal can thus be distorted by unequal loss of its component frequencies.

Delay Distortion :

It can cause errors in data transmission. Delay distortion occurs when a signal is delayed more at some frequencies than at others. If the method of data transmission involves data transmitted at two different frequencies, then the bits being transmitted at one frequency may travel slightly faster than the bits transmitted at a different frequency. A piece of equipment, called an *equaliser*, compensates for both attenuation distortion and delay distortion.

Jitter :

It may affect the accuracy of the data being transmitted. The generation of a pure carrier signal is impossible. Minute variations in amplitude, phase, and frequency always occur. Signal impairment may be caused by continuously and rapidly changing gain and/or phase changes. This jitter may be random or periodic.

3) Approaches to Error Control

Error control implies (1) techniques of design and manufacture of data communication transmission links and equipment to reduce the occurrence of errors (an area that is outside the scope of this book), and (2) methodologies to detect and correct the errors that are introduced during transmission of the data.

In the sense of the second meaning of error control, the methodologies fall into three categories, and possibly four if you consider the option of ignoring the errors.

- Loop or echo checking
- Error detection with retransmission
- Forward error correction (FEC)

4) Loop or Echo Checking

Loop or echo checking does not use a special code. Instead, each character or other small unit of the message, as it is received, is transmitted back to the transmitter, which checks to determine whether the character is the same as the one just sent. If it is not correct, then the character is transmitted a second time.

This method of error detection is wasteful of transmission capacity because each message (in pieces) is transmitted at least twice and there is no guarantee that some messages might not be transmitted three or four times. Also, some of this retransmission of characters for a second or third time might not be necessary since the error could have occurred on the return trip of the character. This would require the transmitter to retransmit the character even though it was in reality received correctly the first time.

Loop or echo checking is usually utilised on hard-wire, short lines, with low-speed terminals. This type of error checking does give a high degree of protection but it is not as efficient as other methods. It is sometimes confused with full duplex transmission.

5) Error Detection with Retransmission

Error detection and retransmission schemes are built into data transmitting and receiving devices, front end computers, modems, and software. These schemes include detection of an error and immediate retransmission, detection of an error and retransmission at a later time, or detection of an error and retransmission for up to, say, three tries and then retransmission at a later time, or the like.

Error detection and retransmission is the simplest, and if properly handled, the most effective and least expensive method to reduce errors in data transmission. It requires the simplest logic, needs relatively little storage, is best understood by terminal operators, and is most frequently used.

Retransmission of the message in error is straightforward. It is usually called for by the failure of the transmitter to receive a positive acknowledgement within a pre-set time. Various methods are used to determine that the message that has just been received has, in fact, an error imbedded in it. Some of the common error detection methods are parity checking, constant ratio codes, and polynomial checking.

a) Parity checking :

If you examine a character from the ASCII coding structure, it soon becomes apparent that 1 of the 8 bits encoding each character is redundant-i.e., its value is solely determined by the values of the other 7 and is therefore unnecessary. Since this eighth bit cannot transmit any new information, its purpose is the confirmation of old information.

The most common rule for fixing the value of the redundant bit uses the "parity" (evenness or oddness) of the number of 1s in the code. Thus, for an even parity code system using ASCII:

. Letter "V" is encoded 0110101. Since the number of 1s is 4, already an even number, a zero is added in the parity (eighth) position, yielding V = 01101010.

. Letter "W" is encoded 0001101, which has an odd number of 1s. Therefore a 1 is added in the parity position to make the number of 1s even, yielding W = 00011011.

A little thought will convince you that any single error (a switch of a 1 to a 0 or vice versa) will be detected by a parity check but that nothing can be deduced about which bit was in error. If the states of two bits are switched, the parity check may not sense any error.

Of course, it may be possible to sense such an error because the resulting code, although correct as far as parity is concerned, is a code that is "forbidden," e.g., undefined or inappropriate in its context. Such detection, of course, requires more circuitry or software.

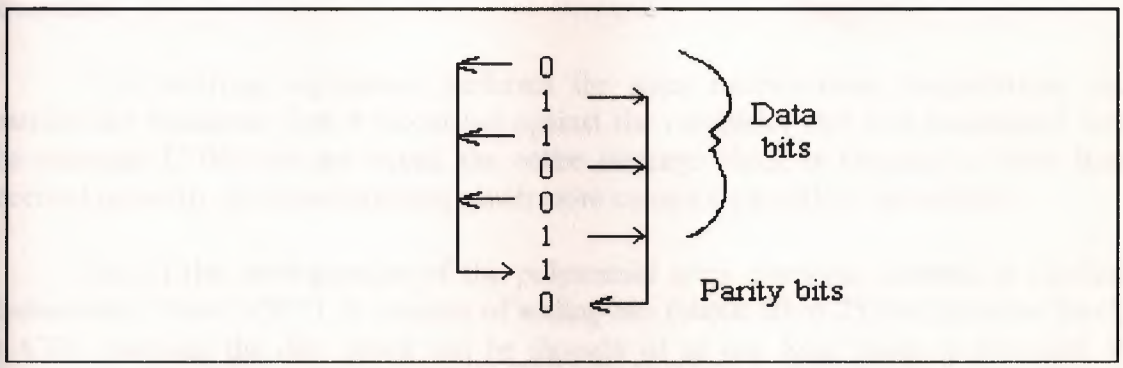


FIGURE 1-5 Cyclical parity check for a 6-bit code

Another parity checking technique is the *cyclical parity check* (sometimes called *interlaced parity*). This method requires two parity bits per character. Assuming a 6-data bit code structure, the first parity bit would provide parity for the first, third, and fifth bits, and the second parity bit would provide parity for the second, fourth, and sixth bits. Figure 1-5 shows an even parity cyclical parity check on a 6-bit code.

b) Constant ratio codes :

N out of M codes are special data communication codes that have a constant ratio of the number of 1 bits to the number of 0 bits. N out of M codes detect an error whenever the number of 1 bits and 0 bits are not in their proper ratio. For example, in the 4-of-8 code there are always supposed to be four 1 bits and four 0 bits in the received bit configuration of the character.

Whenever this ratio is out of balance the receiving equipment knows that an error has occurred. N out of M codes are not widely utilised because they are inefficient. As an example of their inefficiency, consider that the 4-of-8 code has 70 valid character combinations while a 7-bit ASCII code has 128 valid character combinations (27 = 128).

c) Polynomial checking :

Polynomial checks (also called *Cyclical Redundancy* Check or CRC) on blocks of data are often performed for synchronous data transmission. In this type of message checking, all the bits of the message are checked by application of a mathematical algorithm. For example, all the 1 bits in a message are counted and then divided by a prime number (such as 17) and the remainder of that division is transmitted to the receiving equipment.

The receiving equipment performs the same mathematical computations and matches the remainder that it calculated against the remainder that was transmitted with the message. If the two are equal, the entire message block is assumed to have been received correctly. In actual practice, much more complex algorithms are utilised.

One of the most popular of the polynomial error checking schemes is *Cyclical Redundancy Check* (CRC). It consists of adding bits (about 10 to 25) to the entire block. In CRC checking the data block can be thought of as one long binary polynomial, **P**. Before transmission, equipment in the terminal divides **P** by a fixed binary polynomial, **G**, resulting in a whole polynomial, **Q**, and a remainder, **R/G**.

$$\frac{P}{G} = Q + \frac{R}{G}$$

The remainder, **R**, is appended to the block before transmission, as a check sequence *k* bits long. The receiving hardware divides the received data block by the same **G**, which generates an **R**.

The receiving hardware checks to ascertain if the received **R** agrees with the locally generated **R**. If it does not, the data block is assumed to be in error and retransmission is requested. In ARQ systems, a 25-bit CRC code added to a 1000-bit block allows only three bits in 100 million to go undetected. That is, for a 2.5% redundancy, the error race is 3 x 10-8.

6) Forward Error Correction

This approach uses codes that contain sufficient redundancy to permit errors to be detected and corrected at the receiving equipment without retransmission of the original message. The redundancy, or extra bits required, varies with different schemes. It ranges from a small percentage of extra bits to 100% redundancy, with the number of error-detecting bits roughly equalling the number of data bits.

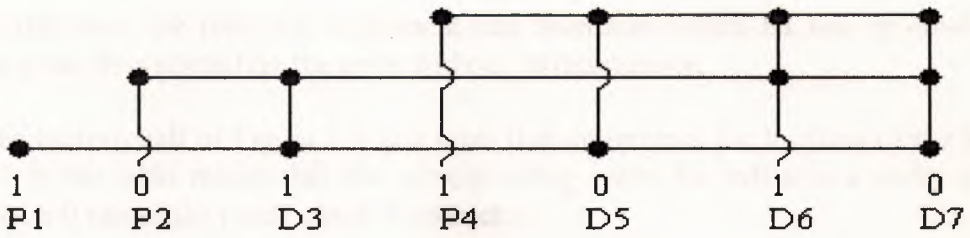
One of the characteristics of many error-correcting codes is that there must be a minimum number of error-free bits between bursts of errors. For example, one such code, called *a Hagelbarger Code,* will correct up to six consecutive bit errors provided that the 6-bit error group is followed by at least 19 valid bits before further error bits are encountered.

Bell Telephone engineers have developed an error correcting code that uses 12 check bits for each 48 data bits, or 25% redundancy. Still another code is the *Bose-Chaudhuri Code,* which, in one of its forms, is capable of correcting double errors and can detect up to four errors.

To show how such a code works, consider this example of a forward error checking code, called *a Hamming Code* [3], after its inventor, R. W. Hamming.3 This code associates even parity bits with unique combinations of data bits. Using a 4- data-bit code as an example, a character might be represented by the data bit configuration 1010. Three parity bits **P1**, **P2**, and **P4**, are added, resulting in a 7-bit code, shown in the upper half of Figure 1-6. Notice that the data bits (D3 D5, D6, D7,) are 1010 and the parity bits (P1, P2, P4) are 101.

As depicted in the upper half of Figure 1-6, parity bit P1, applies to data bits D3, D5, and D7. Parity bit P2 applies to data bits D3, D6, and D7. Parity bit P4, applies to data bits D5, D6, and D7. For the example, in which D3, D5, D6, D7,= 1010, P1, must equal 1 since there is but one 1 among D3, D5, and D7, and parity must be even. Similarly P2, must be 0 since D3, and D6 are 1s. P4, is 1 since D6 is the only 1 among D5, D6, D7.

[3] William P. Davenport, *Modem Data Communication-Concepts*, Language, and *Media* (New York: Hayden Book Company, Inc.,1971).



Checking Relations Between Parity Bits (P) and Data Bits (D)

0 = Corresponding parity check is correct 1 = Corresponding parity check fails			Determines in which bit the error occured
P4	P2	P1	
0	0	0	no error
0	0	1	P1
0	1	0	P2
0	1	1	D3
1	0	0	P4
1	0	1	D5
1	1	0	D6
1	1	1	D7

Interpreting Parity Bit Patterns

FIGURE 1-6 Hamming Code for forward error correction

Now, assume that during the transmission, data bit D7, is changed from a 0 to a 1 by line noise. Because this data bit is being checked by P1, P2, and P4, all three parity bits will now show odd parity instead of the correct even parity. (D7, is the only data bit that is monitored by all three parity bits, therefore whenever D7, is in error, all three parity bits will show an incorrect parity.)

In this way, the receiving equipment can determine which bit was in error and reverse its state, thus correcting the error without retransmission.

The bottom half of Figure 1-6 is a table that determines the location of the bit in error. A 1 in the table means that the corresponding parity bit indicates a parity error. Conversely, a 0 means the parity check is correct.

These 0s and 1s form a binary number that indicates the numerical location of the erroneous bit. In the example above, P1, P2, and P4, checks all failed, yielding 111, or a decimal 7, the subscript of the erroneous bit.

Error detection and correction methodologies come in many varieties. The data communication network designer must give careful consideration to all facets of the system being designed and make appropriate use of the various methodologies to control and correct errors.

MANAGEMENT CONTROLS

Network management involves setting up a central control philosophy with regard to the overall network functions. The network manager should be independent of the other managers in the data processing environment or even independent of the information systems department itself. Some of the general responsibilities of this job function would be design and analysis, network operations, failure control, and testing/problem management.

Some network management controls include the following. The network management team should have a national account with the common carrier when possible. There should be a central call number to log all problems in regard to who, what, where, when, why, the telephone number, date, and time of a problem.

The failure control group should compile statistics for their hardware such as Mean Time Between Failures (MTBF). The network hardware vendor often can supply these data. The network management people also should maintain statistics on the time from failure to recovery. In its most detailed form this is comprised of the Mean Time To Diagnose (MTTD) plus the Mean Time To Respond (MTTR) plus the Mean Time To Fix (MTTF).

In addition to the central control for problem reporting on the network, the network management group should maintain other statistics such as the cumulative network downtime, subnetwork downtime, circuit utilisation reports, response time analysis, queue length descriptions, histograms of daily usage (such as number of characters transmitted per day per circuit), failure rates of the circuits such as the number of retransmitted messages, local host and file activity statistics, local device error activities, network gateway failures, distribution of character and packet volume, distribution of traffic by time of day and location, peak volumes, and a statistical profile of all time-related network traffic. These reports, or similar ones, should be available for managing the network.

With regard to network documentation (some of this can be cross-checked for currency in the global or local network databases), a good network management team should have some or all of the following: circuit layout record, network maps, hardware/software cross-references, all network vendor maintenance records, software listings by network task and component, all user site telephone numbers and names of individuals to contact, an interface component maintenance history log, circuit controlled telephone contact index, maintenance history by component, inventory by serial number of network components, network redundancy locations and switching criteria, vendor contracts and vendor contacts, and a current list of personnel working in the network centre.

A control review of network management should ascertain the existence of appropriate operational manuals and a comprehensive description on how the network operates. There should be adequate recovery procedures, backup procedures and disaster plans.

With regard to communication test equipment, not much can be done to control it because it is in continuous use. Network management must recognise that misuse can allow breaches of privacy or the insertion of illegal messages.

A network monitor is mandatory when bit-oriented protocols such as **X.25** are used. The only control that can be put on such a device is a keylock for its switch. The keylock should be turned off and the key removed when the equipment is not being used. This prevents people from browsing over data as they pass through the data communication network.

Loopback test equipment should be used to diagnose the location and cause of problems.

Microprocessor based network analysers permit checks for poll-to-poll or poll-to-response times. Such checks aid network management in assessing polling efficiency.

Other, smaller hand-held test devices, such as break-out boxes, allow test personnel to send test patterns of data bits to a modem through the RS232C or RS449 cable.

The primary control for test equipment is to ensure that only qualified people use this equipment and that they use it only when necessary.

RECOVERY/BACKUP/DISASTER CONTROLS

Recovery and backup controls within the data communication network encompass many areas. The person who is reviewing these controls may start at either end of the network (remote terminals or central host computer). The object is to check for recovery procedures and backup hardware throughout the network.

- Perhaps the most important question to ask is this: Is it cost effective to back up each piece of hardware encountered between a remote terminal site and the central host computer?
- A related question is: Are there software procedures for recovery of data files, network databases, network software, and the like?
- Use of Figure 1-2 during the review of recovery/backup/disaster controls will help ensure that all network control points are considered.

One important area involves backup of the communication circuits. One option is to lease two separate physical circuits (that have been alternately routed) in order to have one for backup.

Another option is to utilise dial-up communication circuits as backup to leased circuits. Of course, another alternative is to have manual procedures that can be used if the circuit is down for a very short period of time, perhaps several hours at the maximum.

There should be recovery and restart capabilities in the event of either a hardware crash or a software crash. Backup facilities should include backup power, possibly at both the local and remote sites.

With regard to a data communication network disaster plan, a separate plan for each of six different areas should be developed.

These disaster plans are for (1) the data communication network control centre, (2) the communication circuits, (3) remote switches/concentrators/intelligent terminal controllers, (4) common carrier (telephone company) facilities, (5) electric power for the data communication facilities and user terminals/lights, and (6) the user application systems.

A data communication network disaster plan should spell out the following details:

- The decision-making manager who is in charge of the disaster recovery operation. A second manager should be indicated in case the first manager is unavailable.
- Availability and training of backup personnel with sufficient data communication knowledge and experience.
- Recovery procedures for the data communication facilities. This is information on the location of circuits, who to contact for backup data circuits and documentation, as well as preestablished priorities as to which data circuits will be reconstructed first.
- How to replace damaged data communication hardware and software that is supplied by vendors.
- Outline the support that can be expected from vendors, along with the name and telephone number of who to contact.
- Location of alternate data communication facilities and equipment such as connector cables, local loops, IXCs, common carrier switching facilities, and other public networks.
- Action to be taken in case of partial damage or threats such as bomb threat, fire, water, electrical, sabotage, civil disorders, or vendor failures.
- Procedure for imposing extraordinary controls over the network until the system returns to normal.
- Storage of the disaster recovery procedures in a safe area where they will not be destroyed by the catastrophe. This area must be accessible, however, by those who need to use the plans.

MATRIX OF CONTROLS

In order to be sure that the data communication network has all the necessary controls and that these controls offer adequate protection, it is advisable to build a two-dimensional matrix that incorporates all the controls that *currently* are present in the network.

This matrix is constructed by identifying first all threats facing the network and second, all the network's component parts.

- ***Errors and Omissions*** - The accidental or intentional transmission of data that is in error, including the accidental or intentional omission of data that should have been entered or transmitted on the on-line system. This type of exposure includes, but is not limited to, inaccurate data, incomplete data, malfunctioning hardware, and the like.

- ***Message Loss or Change*** - The loss of messages as they are transmitted throughout the data communication system, or the accidental/intentional changing of messages during transmission.

- ***Breach of Privacy*** - The accidental or intentional release of data about an individual, assuming that the release of this personal information was improper to the normal conduct of the business at the organisation.

- ***Security/Theft*** - The security or theft of information that should have been kept confidential because of its proprietary nature. In a way this is a form of privacy, but the information removed from the organisation does not pertain to an individual.

- ***Reliability (Uptime)*** - The reliability of the data communication network and its "uptime." This includes the organisation's ability to keep the data communication network operating and the mean time between failures (MTBF) as well as the time to repair equipment when it malfunctions. Reliability of hardware, reliability of software, and the maintenance of these two items are chief concerns here.

- ***Recovery and Restart*** - The recovery and restart capabilities of the data communication network, should it fail. In other words, How does the software operate in a failure mode? How long does it take to recover from a failure? This recovery and restart concern also includes backup for key portions of the data communication network and the contingency planning for backup, should be a failure at any point of the data communication network.

- ***Error Handling*** - The methodologies and controls for handling errors at a remote distributed site or at the centralised computer site. This may also involve the error handling procedures of a distributed data processing system (at the distributed site).

- ***Data Validation and Checking*** - The validation of data either at the time of transmission or during transmission. The validation may take place at a remote site (intelligent terminal), at the central site (front end communication processor), or at a distributed intelligence site (concentrator or remote front end communication processor).

FIGURE 1-7 General threats.

- A ***threat*** to the data communication network is any potential adverse occurrence that can harm the network, interrupt the systems that use the network, or cause a monetary loss to the organisation. For example, lost messages are a potential threat.

- A ***component*** is one of the individual pieces that, when assembled together, make up the data communication network.

- A ***component*** can be viewed as the item that is being reviewed or the item over which we are attempting to maintain control.

- Thus, the components are the hardware, software, circuits, and other pieces of the network.

In Figure 1-7 several *general* threats to a data communication network are shown. Figure 1-8 identifies several *general* component parts for a data communication network.

- ***Host Computer*** - Most prevalent in the form of a central computer to which the data communication network transmits and from which it receives information. In a distributed system, with equal processing at each distributed node, there might not be an identifiable central computer (just some other equal-sized distributed computer).

- ***Software*** - The software programs that operate the data communication network. These programs may reside in the central computer a distributed-system computer the front end communication processor a remote concentrator or statistical multiplexer and/or a remote intelligent terminal. This software may include the telecommunications access methods, an overall teleprocessing monitor, programs that reside in the front end processors, and/or programs that reside in the intelligent terminals.

- ***Front End Communication Processor*** - A hardware device that interconnects all the data communication circuits (lines) to the central computer or distributed computers and performs a subset of the following functions: code and speed conversion, protocol, error detection and correction, format checking, authentication, data validation, statistical data gathering, polling/addressing, insertion/deletion of line control codes, and the like.

- ***Multiplexer Concentrator Switch*** - Hardware devices that enable the data communication network to operate in the most efficient manner. The *multiplexer is a* device that combines, in one data stream, several simultaneous data signals from independent stations. The concentrator performs the same functions as a multiplexer except it is intelligent and therefore can perform some of the functions of a front end communication processor. A switch is a device that allows the interconnection between any two circuits (lines) connected to the switch. There might be two distinct types of switch: a switch that performs message switching between stations (terminals) might be located within the data communication network facilities that are owned and operated by the organisation; a circuit or line switching switch that interconnects various circuits might be located at the telephone company central office.

- ***Communication Circuits (Lines)*** - The common carrier facilities used as links (a link is the interconnection of any two stations/ terminals) to interconnect the organisation's stations/terminals. These communication circuits include satellite facilities, public switched dial-up facilities, point-to-point private lines, multiplexed lines, multipoint or loop configured private lines, and many others.

- ***Local Loop*** - The communication facility between the customer's premises and the telephone company's central office or the central office of any other special common carrier. The local loop is usually assumed to be metallic pairs of wires.

- ***Modems*** - A hardware device used for the conversion of data signals from terminals (digital signal) to an electrical form (analogue signal) which is acceptable for transmission over the communication circuits that are owned and maintained by the telephone company or other special common carrier.

- ***People*** - The individuals responsible for inputting data, operating and maintaining the data communication network equipment, writing the software programs for the data communications, managing the overall data communication network, and those involved at the remote stations/terminals.

- ***Terminals/Distributed Intelligence*** - Any or all of the input or output devices used to interconnect with the on-line data communication network. This resource would specifically include, without excluding other devices, teleprinter terminals, video terminals, remote job entry terminals, transaction terminals, intelligent terminals, and any other devices used with distributed data communication networks. These may include microprocessors or minicomputers when they are input/output devices or if they are used to control portions of the data communication network.

FIGURE 1-8 General components

1. Ensure that the system can switch messages destined for a down station/terminal to an alternate station/terminal.

2. Determine whether the system can perform message switching to transmit messages between stations/terminals.

3. In order to avoid lost messages in a message-switching system, provide a store and forward capability. This is where a message destined for a busy station is stored at the central switch and then forwarded at a later time when the station is no longer busy.

4. Review the message or transaction logging capabilities to reduce lost messages provide for an audit trail, restrict messages, prohibit illegal messages, and the like. These messages might be logged at the remote station (intelligent terminal), they might be logged at a remote concentrator/remote front end processor, or they might be logged at the central front end communication processor/central computer.

5. Transmit messages promptly to reduce risk of loss.

6. Identify each message by the individual user's password, the terminal, and the individual message sequence number.

7. Acknowledge the successful or unsuccessful receipt of all messages.

24. Consider the following special controls on dial-up modems when the data communication network allows incoming dial-up connections: change the telephone numbers at regular intervals; keep the telephone numbers confidential; remove the telephone numbers from the modems in the computer operations area; require that each "dial-up terminal" have an electronic identification circuit chip to transmit its unique identification to front end communication processor; don't allow automatic call receipt and connection (always have a person intercept the call and make a verbal identification); have the central site call the various terminals that will be allowed connection to the system; utilise dial-out only where an incoming dialled call triggers an automatic dial-back to the caller (in this way the central system controls those telephone numbers to which it will allow connection).

FIGURE 1-10 Controllist.

Identifying and documenting the controls in a network require the task of identifying the *specific* threats and components that relate to whatever network is used by the organisation. After identifying the organisation's specific threats and components, the individual controls that are in place can be related to these threats and components.

Once the threats and component parts of the network have been identified, the next step is to place a short description of each threat across the top of the matrix. Likewise, a short description of each component is placed down the left vertical axis of the matrix as shown in Figure 1-9.

When the horizontal and vertical axes have been labelled, the next step is to identify all of the specific controls that are being used currently in the data communication network. These "in-place" controls should be described and placed in a numerical list. For example, assume 24 controls have been identified as being in use in the network.

Each one is described and they are numbered consecutively 1 through 24. The numbered list of controls has no ranking attached to it: the first control is number 1 just because it is the first control identified. Figure 1-10 shows what a list of in-place controls looks like.

Next, each of the controls that has been identified is placed into the proper cell of the matrix. This is accomplished by reading the description of each control and the controllist and then asking the following two questions:

1. ***Which threat or threats does this control mitigate or stop?***

2. ***Which component or components does this control safeguard or control?***

For example, if the description of control 1 is "ensure that the system can switch messages for a down station/terminal to an alternate station/terminal," then the number 1 should be placed in the very first cell in the upper left corner (see Figure 1-11). This is because a control that ensures that the system can switch messages when a station is down helps control *errors,* and it also is a control that safeguards or resides in the host computer and/or front end.

Figure 1-11 also shows control 1 in the cell that intersects between Message Loss or Change and Host Computer. Control 1 also appears in several other cells. The point is that by answering these two questions, you can place each control in the proper cells of the matrix.

The finished matrix with controls (Figure 1-11) shows the interrelationship of each "in-place" control [4] to the threat that it is supposed to mitigate and the component that it safeguards or controls.

The last step in designing a custom matrix of controls for your specific data communication network involves a personal evaluation as to the adequacy of the controls. This is accomplished by reviewing each subset of controls as it relates to each threat and component area of the matrix. For example, the subset of controls that are listed down a column below a threat are evaluated.

The object of this step is to answer the specific question, "Do we have the proper controls and are they adequate with regard to each specific threat?" Using Figure 1-11, look down the column under errors and omissions. The matrix clearly defines the specific subset of controls that relate to the threat area Errors and Omissions. They are 1, 2, 3, 4, 7,12,18, and 5.

This type of review also can be performed for various other subsets of controls. For example, individual subsets of controls can be evaluated as they relate to:

* ***Threats (columns)***
* ***Components (rows)***
* ***Individual cells***
* ***Empty cells***

Looking at Figure 1-12, we see a pictorial diagram describing the above four areas that should be reviewed. The matrix approach offers a perfect tool for a detailed microanalysis of the controls in a data communication network.

The matrix clearly shows the relationship between various subsets of controls and specific threat areas, component parts, individual cells, and empty cells.

[4] *Internal* Controls for *Computerised* Systems by Jerry FitzGerald, published by Jerty FitzGerald and Associates, 506 Barkentine Lane, Fed- wood City, Calif. 94065.

LISTS OF DATA COMMUNICATION CONTROLS

In order to help you construct a matrix of controls that relate to your organisation's data communication network, we have supplied 14 specific lists of controls. Each list has a definition of that particular area and is followed by its own set of controls [5] . The areas that are addressed are:

- Software controls (data communication)
- Disasters and disruptions (data communication)
- Modems
- Multiplexer, concentrator, switch
- Communication circuits (lines)
- Error handling (data communication)
- Local loop (lines)
- Data entry and validation (data communication)
- Errors and omissions (data communication)
- Restart and recovery (data communication)
- Message loss or change (data communication)
- People controls (data communication)
- Front end communication processor
- Reliability / uptime (data communication)

RISK ANALYSIS FOR NETWORKS

Management sometimes requests that a risk analysis be performed on the network. Risk analysis can be used to show the potential "average annual loss." This loss figure can be used to justify the cost of controls, to formulate insurance requirements, and to visualise potential loss that the organisation *might* suffer should one or more of the threats actually occur.

Risk analysis that produces actual "dollar loss" figures involves many estimates because some figures are not available, such as exact loss suffered in a fire, fraud loss, fraud occurrence rate, or other probabilities.

[5] These lists of controls were taken from the book, *Designing Controls into* Computerised Systems by Jerry FitzGerald, published by Jerry FitzGerald and Associates, 506 Barkentine Lane, Redwood City, Calif. 94065.

2) NETWORK DESIGN FUNDEMANTELS

This chapter presents the fundamentals of designing data communication networks. A step-by-step systems approach is used and 13 individual steps are described. The systems approach starts with a feasibility study and goes through planning, current system review, designing, geographical considerations, message analysis, circuit loading, security controls, configurations, software/hardware, cost analysis, and implementation. Other features in this chapter are a listing of evaluation criteria, various forms/ charts, and seven types of cost analysis.

THE SYSTEMS APPROACH TO DESIGN

When planning for a completely new data communication network, enhancement of a current network, or the use of publicly available networks, you should use the systems approach. Whether the network achieves success or just marginal utilization may be determined before a single piece of software or hardware is ordered. The key ingredient for success lies in planning based on the "system's interface with the users." Far too often, data processing-oriented personnel take an equipment-oriented approach or a technical software-oriented approach. In today's world of data communications the designer must take a user systems application approach.

For example, there are two major classes of users for a data communication network/system. These are the organization's "management" and "user" personnel.

Managers must accept the system and believe in it, or they will not trust the data/information/response they receive from the system. If the information received by management is not Consistent, Accurate, Timely, Economically feasible, and Relevant, then the system will not be accepted by management.

The "user" personnel who work with the system on a day-to-day basis must be able to accept the system or their productivity will fall drastically. When productivity falls, the cost of carrying out basic office functions may increase the cost of the final product or service by 10 to 50 percent.

Office productivity recently has taken on added importance because we have been moving from a society that has most of its people engaged in manufacturing to one in which the majority of the people are engaged in information-type processes (service oriented). In other words, proportionately more people are involved in information-related work than in manufacturing/assembly work. We now need the industrial engineers from the factory environment to move into the automated business office.

These changes are the reason this book promulgates the systems approach to designing data communication networks. The discussions and recommended steps encompass the process needed to design a new network. If a current network is being enhanced, perhaps some of the steps can be omitted. If the decision has been made to use one of the publicly available networks, then it may also be possible to omit some of the steps. However serious consideration should be given to all of the following 13 steps. Each step has a detailed explanation on how to carry it out. The 13 steps are:

1. *Make a feasibility study*
2. *Prepare a plan*
3. *Understand the current systems*
4. *Design the data communication network*
5. *Identify the geographical scope*
6. *Analyse the messages*
7. *Determine traffic/circuit loading*
8. *Develop a control matrix*
9. *Develop network configurations*
10. *Consider software*
11. *Consider hardware*
12. *Do a cost analysis*
13. *Sell and implement the network*

MAKE A FEASIBILITY STUDY

The first point that must be made with regard to a feasibility study is that it may not be necessary to conduct one. It may have already been performed by management in order to identify the problem or the purpose/objectives of the proposed system. Perhaps the scope of the proposed system already has been defined. Furthermore, it is entirely possible that either management or the realities of the economic/business environment have dictated that an on-line data communication network will be developed.

For example, can you imagine any major airline deciding that a network costs too much or does not meet its objectives? If one decided against a network, it would cease to be competitive with the other airlines; therefore, the feasibility of a "go/no go" network decision is decided even before the airline starts to think about a feasibility study.

Of course, in this case we are talking about a feasibility study that helps determine whether or not to proceed with a network, rather than a more elaborate feasibility study to identify which specific network should be set up. The decision as to which network is covered in the next 12 steps.

In proceeding with a feasibility study, a primary responsibility is to define the problem clearly and put it in writing. Problem definition involves identifying all the problems that have led to the need for a data communication network. Any of the following factors may be analysed to determine if they contribute to the need for this new network.

- Increased volumes of inputs/outputs
- Inadequate data processing
- Obsolete hardware/software
- Inadequate file structures (database)
- Unsatisfactory movement of data/information throughout the organisation
- Inadequate interfacing between application systems and staff within the organisation
- Documentation not being available in a timely manner
- Current systems being unreliable
- Inability to maintain current systems
- Inadequate security/privacy
- Decreasing productivity
- Inadequate training
- Future growth requiring new methods
- Competition forcing the change
- Negative effect of old system on employee morale
- A new system being viewed as having a positive effect on investments, cash flow, etc.
- Inadequate floor space for personnel/ files
- Future cost avoidance
- Need for more timely access to information for improved decision making
- Increasing flow of information/paperwork
- Need for expanded capacity for the business functions/manufacturing
- Necessity for increasing level of service quality/performance
- International operations requiring new methods and better exchange of information
- Reduction of inventories
- Need for a paperless office
- Desire to take advantage of the technology of the 1990s.

Once the problem has been defined in this way the purpose and objectives of the new system are identified, the scope or boundaries that the system will encompass are established, and perhaps some preliminary "magnitudes" of cost are identified for the proposed data communication network.

The feasibility study might include some preliminary work on the geographical scope of the network, or the physical areas of the organisation that will be interconnected by it. It may be appropriate to develop a rough draft geographical map of the intended network.

At the completion of this data gathering, a short feasibility study written report should be generated. This report is the medium by which you tell management what the problem is, what you have found its causes to be, and what you have to offer in the way of a solution. The feasibility study results might be presented verbally as well. This type of presentation provides management with an opportunity to ask questions or discuss issues that may have a bearing on whether to proceed.

Your solution is probably a "go/no go" decision as to whether a full program should be started for the design and development of a new data communication system. The feasibility study written report should contain:

- A statement of the problem that clearly demonstrates your understanding of it.

- A concise description of the purpose and objectives of the network. It is important to remember that the purpose is to improve inventory control, effect an improved cash flow, process orders faster, and the like, not to install modems or communication circuits.

- A clear statement of the scope or boundaries. Which application systems will use the network? At this point it may be appropriate to add the preliminary review of the geographical scope or the physical locations that will be interconnected.

- A clear statement of the various "magnitudes" of cost for such areas as software, hardware, communication circuits, restructuring of the internal business organisation, and the redesign of current application systems. Any political problems or organisational costs should also be considered. For example, combining voice and data communications into one department has a political cost.

- Highlighting of special attention areas, unusual situations, or the interrelatedness of problems that were not seen before.

- Description of the entire system in generalities so management can visualise the overall data communication system.

- Recommendations as to whether a new system should be designed. In fact, at this point you should be able to recommend whether to enhance the current communication system, design a totally new communication system, or subscribe to a public packet data communication network.

- A suggested timetable, including some general milestones. Try to estimate the cost of reaching each milestone.

PREPARE A PLAN

At this point the feasibility study has been completed and management has given its approval to proceed with the design and development of a data communication network.

In developing the plan, remember that a successful plan always takes into account the following three factors:

* *Technical feasibility* of the network.

* *Operational feasibility* by the "users" who conduct their daily business using the network, and by "management" who has to rely on its reports.

* *Economic feasibility* to keep it within budgetary limitations.

The first step is to take the statement on the purpose/objectives of the network and write it down into three distinct goal areas. The *major* goal is the reason that the data communication network is being built. The objective is to ensure that the network meets these requirements. Next, *intermediate* goals are other gains the system can make while serving its major purpose, hopefully with little or no extra expense. Finally, minor goals are the functions that a communication network, along with data processing applications, can perform for the organisation but for which it is not quite ready (future requirements). The major goals are mandatory. The intermediate goals are desirable. The minor goals are "wish list" items.

There is no way to outline the exact steps the plan should follow because it must be custom tailored to the organisation and application systems that the network must service. The goal the network is to achieve should provide the framework for the plan. For example, referring to the three goals above, the major goal might be to speed up order entry and achieve improved cash flow through better collections. The intermediate goal might be to interface all of the accounting applications with the order entry operations. A minor goal might be to set up a voice mail/electronic mail system for the future. All too often network designers forget their priorities and concentrate on minor goals because of personal interest. Committing the goals to writing serves as a constant reminder to avoid this trap.

The first step in developing a "custom" plan might be to identify the various sources of information, types of information to be collected, and a schedule for performing various activities. It is likely that the designer will emulate the 13 key steps already listed.

Finally, as the design begins, develop some evaluation criteria. If evaluation criteria are developed at the beginning, then there is a yardstick at completion so the design, development, and implementation of the data communication network/ system can be measured. The following evaluation criteria should be considered.

- **Time** This could be elapsed time, transaction time, overall processing time, response time, or other operational times.

- **Cost** This may be the annual cost of the system, per unit cost, maintenance cost, or other cost items such as operational, investment, and implementation.

- **Quality** Is a better product or service being produced? Is there less rework because of the system? Has the quality of data/information improved?

- **Capacity** This involves the capacity of the system to handle workloads, peak loads, and average loads, as well as long-term future capacity to meet the organisation's needs in the next decade.

- **Efficiency** Is the system more efficient than the previous one?

- **Productivity** Has productivity of the user (information provider) and management (information user) improved? Is decision making faster and more accurate because of the information provided by this system?

- **Accuracy** Are there fewer errors? Can management rely on this system more than the old one?

- **Flexibility** Can the new system perform diverse operations that were not possible before?

- **Reliability** Are there fewer breakdowns of this system compared with the previous one? Is uptime very high with this system? The reliability/uptime of an on-line network is probably the number one criterion by which to judge its design and development.

- **Acceptance** Evaluate whether both the information providers and the information users have accepted the system.

- **Controls** Are adequate security and control mechanisms in place in order to prevent threats to the system such as errors and omissions, fraud and defalcation, lost data, breaches of privacy, disastrous events, and the like?

- **Documentation** Does the system have adequate written/pictorial descriptions documenting all of its hardware, protocols, software, circuits, and user manuals?

- **Training** Are training courses adequate and are they offered on a continuous basis, especially for terminal operators? Are training manuals adequate and updated on a regular basis?

The above evaluation criteria can be used to evaluate the new data communication network after it has been developed. Also, it may be advisable to evaluate your own performance during the design and development of this new network.

In that case, examine items as whether development time schedules were on target.

- *Were development costs within budget or was there a large cost overrun?*

- *Were any deviations from the original purpose/objectives and scope documented?*

Consider interactions with those affected by the system:

- *Do they feel they were treated fairly and are they satisfied with you and your design?*

- *Was there a lot of turnover on the project team during the design and development?*

In summary, as the plan is prepared (step-by-step approach), also develop evaluation criteria for the data communication network as well as the evaluation criteria by which to judge your own design efforts. If you ignore this step, someone else may do it and you may be judged by a set of criteria that do not relate well to your effort.

UNDERSTAND THE CURRENT SYSTEMS

The objective of this step of the design effort is to gain a complete understanding of the current operations (application system/messages) and any network that is functioning. This step provides a benchmark against which future design requirements can be gauged. It should provide a clear picture of the present sequence of operations, processing times, work volumes, current communication systems, existing costs and user/management needs.

In order to be successful at this stage, begin by gathering general information or unique characteristics of the environment in which the system must operate. Next, identify the specific applications that will use the data communication network and any proposed future applications.

Learn something about the background of the industry in which the network will function (what competitors are doing in this regard), as well as about your individual company and about the departments that are responsible for the applications.

Determine if there are any legal requirements, such as local, state, federal, or international laws that might affect the network.

With regard to the people in different departments who will be affected by the system, do not overlook the fact that there are formal organisations as shown on the organisation chart, and there are also informal organisations within a specific department.

It is important to be aware that company politics might affect the design effort; people may tell you what they want for their personal interests rather than what is in the best interests of the organisation.

Develop an input, processing, output model for each system that will utilise the data communication network. Figure 2-1 shows a typical input, processing, output model. Your task is to identify each generic input to the application system, the typical processing steps that are performed, and each generic output. Describe and list each input/process/output on the model in Figure 2-1.

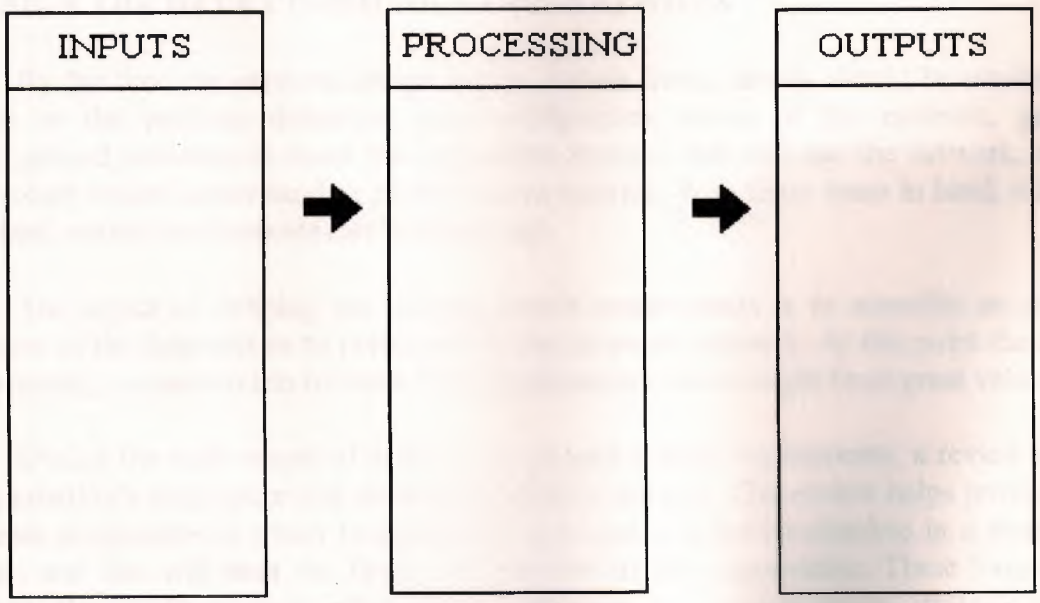


FIGURE 2-1 Input / Processing / Output Model

Also, identify the "file formats" so database planners can start to design the database and database access methodologies. Transmission volumes increase dramatically when the network is used for database retrieval transactions.

Techniques used to complete this step might include interviewing user personnel, searching a variety of current records for message format and volumes, estimating and sampling for timings and volumes, and possibly comparing current systems with others that have been put on a data communication network.

The documentation gathered during each of the above tasks can serve as a future summary of the existing system. A written summary also should be developed. This summary should include everything of importance learned during this step of the design. It is your written understanding of the existing systems. It should include any design ideas, notes on whether currently used forms or transmittal documents are adequate or inadequate, who was helpful, who hindered progress, and any other overall impressions gained from interviews, meetings, records, flow charts, sampling, and the like. In general, the written summary, should contain information that can be referred to during the detailed design steps for development of the data communication network. It is the benchmark to be used for later comparisons.

DESIGN THE DATA COMMUNICATION NETWORK

By the time the network design begins, certain items already should be established, such as the problem definition, purpose/objectives, scope of the network, general background information about the application systems that will use the network, and a thorough written understanding of the current systems. With these items in hand, a list of general system requirements can be developed.

The object of defining the general system requirements is to assemble an overall picture of the functions to be performed by the proposed network. At this point the input, processing, output models for each of the application systems might be of great value.

During the early stages of defining the general system requirements, a review of the organisation's long-range and short-range plans is advised. This review helps provide the proper perspective in which to design a system that will not be obsolete in a couple of years and that will meet the future requirements of the organisation. These long/short-range plans indicate such information as changes in company goals, strategic plans, development plans for new products or services, projections of changing sales, research and development projects, major capital expenditures, possible changes in product mix, emphasis on security, and future commitments to technology.

Once the system requirements have been identified, they should be prioritised. That is, they should be divided into mandatory system requirements, desirable system requirements, and wish list requirements. This information enables you to develop a minimum level of mandatory requirements and a negotiable list of desirable requirements that are dependent upon cost and availability. Match these against your major, intermediate, and minor goals mentioned earlier.

System requirements should be as precise as possible. For example, rather than stating "a large quantity of characters," state requirements in more precise figures such as "50 character per minute plus or minus 10 percent."

At this point, avoid presenting solutions; only requirements are needed. For example, a requirement might state that circuit capacity should be great enough to handle 5000 characters per minute which will triple by 1986. It would be a mistake to state this as a solution by saying that a 9600 bit per second, coaxial cable, voice grade circuit is required. Solutions should be left for later, during development of network configurations when software/hardware considerations must be interrelated with those configurations.

By definition, to design means to map out, plan, or arrange the parts into a whole which satisfies the objectives involved.

IDENTIFY THE GEOGRAPHICAL SCOPE

The scope of the applications systems that are to be included on the network have now been identified. The "very rough draft" geographical map that was developed during the feasibility study should be examined at this point, and a more detailed and accurate version should be prepared.

A data communication network has four basic levels of geographical scope:

- International (world-wide network)
- Country (within the boundaries and laws of a single country)
- City (within the boundaries of a specific city, state/province, or local governmental jurisdiction)
- Local facility (within a specific building or confined to a series of buildings located upon the same contiguous property)

Usually it is easiest to start with the highest level, international. Begin by making a network map drawing of all the international locations that must be connected. At this level it is necessary only to interconnect the major countries and/or cities around the world. It is sufficient to have a map that shows lines going between the countries/cities. Details such as the type of circuit, multiplex, multidrop, concentrators, and the like have not been decided yet. If the network does not cross international boundaries, then obviously this step can be omitted.

The next map you *might* prepare is the country map for each country. Interconnections should be drawn between all cities within the country of countries that require interconnection. Again, a single line drawn between the cities is quite adequate because the type of configuration has not yet been decided upon. Figure 2-2 is a typical example of a country map intermixed with an international map because of the closeness of the two countries.

The next map to prepare is one of the city or state/province. This can be divided into two levels. The first level uses a state map. It has lines drawn showing the interconnection among various cities within the state. City maps are used at the second level. They show interconnection of various "local facility" locations within the city. When two maps are used, it does add another level. The advantage, however, is that it also decreases the complexity of simultaneously trying to design both intrastate circuits and intracity circuits. If either of these levels is omitted, the state level maps may be the less vital. The city level maps are needed to identify concentrator sites and/or multidrop locations, as well as individual terminal locations. At this point, only lines are drawn between the various interconnect points because configurations have not been decided upon.

The local facility "maps" are really pictorial diagrams because usually blueprints or drawings of the building floor layouts are used. Specific terminal locations can be identified on these pictorial diagrams. It is too early to identify concentrator/multiplexer sites, so this should be left until a later time. It is appropriate at this point to identify the location of current telephone equipment rooms for incoming communication circuits (voice and data).

There are tentative locations for individual terminals and circuit paths for the local facility, intracity, intrastate country and international needs. To date, little is known about the volume of data that must be transmitted; nor is anything known about the type of hardware/software that might be utilised by this system.

The next step is to analyse the specific messages although this can be done simultaneously with the development of the geographical maps and pictorial diagrams.

ANALYZE THE MESSAGES

This step may be combined with the previous step on identifying the geographical scope, but it is more often combined with the following step, "determining traffic/circuit loading." The reason it is identified here as a separate step is so that you will understand clearly the level of detail that must be obtained during this very important step.

In this step each message that will be transmitted or received from each application system at each terminal location is identified. Also, each *message* field (data item/ attribute) is identified, along which the average number of characters for each field.

Further, it is necessary to identify message length and the volumes of messages transmitted per day or per hour. It probably will be necessary to visit each location where there is a system that will utilise the data communication network. These site visits are required in order to identify clearly each and every message type that will be transmitted or received.

If the system is a manual one, these messages might be forms in the current system, although they already might be electronically generated messages or video screen formats on terminals. Each message should be described by a short title, and a sample of the message should be attached if there is a current equivalent. If there is not an equivalent, all of the fields that will make up the message must be identified. Message analysis sometimes reveals that the system will have to handle a greater volume of data than was previously thought.

Before proceeding to the next step, we should discuss further the various fields/ data items of the message. After each message is described and samples collected of messages that are in the current system, this data must be recorded. A simple form should be used to record this data, such as the one shown in Figure 2-3. The name of each individual message is listed along with the name of each field/ data item that makes up that message. For each field in the message list the average number of characters in each field/data item. Most data items have only an average number of characters per message; few have a peak number. It is always worth the effort to determine if some of the individual data items have a peak number of characters per message. Peaks may occur during certain days of the year or hours of the day or any other time that is unique to the business situation.

TELLER INQUIRY SYSTEM			
Message Name	Message Fields (data item)	Average Characters/ Field	Peak Characters Field
Passbook savings inquiry	Password	4	4
	Customer account #	9	9
	Dollar amount	6	12
	Transaction code	3	3
	Total	22	28
Loan balance inquiry	Password	4	4
	Customer loan #	16	16

FIGURE 2-3 Message Contents

Once the messages have been described and recorded, the average/peak number of characters for each message can be calculated for each application system. The most important figure is the average number of characters per message, although sometimes peak numbers of characters per message must be taken into account.

It should be noted here that most systems are built using the average number of characters for their basis, because few organisations can afford the cost of a system built on the basis of the peak number of characters. The use of averages is even more prevalent when the choice is between average number of messages per day and peak number of messages per day.

The system designer should note that a pure character count may be misleading with regard to the number of characters contained in the transmitted message. Header characters (identifying overhead-type characters within the message) and the data communication network control characters must be taken into account. The control characters can be items such as a consecutive message number, the synchronisation characters, carriage returns or tabulation characters when appropriate, and line control characters for the protocol utilised (although the protocol may be unknown at this point). As a rule of thumb, 20 or 30 line control characters might be added to each message transmitted, although when messages are transmitted in contiguous groups, this figure might be closer to 20 or less. There is no rule of thumb for message header characters. The best way to identify message content control information is probably to interview the people who run the current manual or computerised application system.

Determining the volumes of messages is critical. Now that the average number of characters for each message has been determined, the next step is to learn how many messages will be transmitted per day or per hour.

The first item in the upper left-hand corner is the identifier of a network link. This is nothing more than a first cut at determining where messages will go when users transmit from their local facility work area. The second column shows the name of the individual message type. The third and fourth columns show the average characters per message and the peak characters per message (if appropriate). The fifth and sixth columns show the average number of messages per day and the peak number of messages per day. The seventh and eighth columns show the average number of characters transmitted per day and the peak number of characters transmitted per day; these numbers are obtained by multiplying the characters per message by the number of messages per day.

Finally, when possible, these traffic statistics (characters transmitted per day) should be broken down into the hourly number of characters transmitted throughout the work day. This information can be used to help spot any problems with hourly peak volumes as the design progresses. For example, if a column total of the hourly number of characters transmitted between 9 to 10 A.M. has a volume that is 50 times the capacity of a single circuit network link, then a problem exists.

The problem can solve itself if you have some messages transmitted later, such as during the next several hours. Other solutions are to have some people work overtime or to design a network link that has the capacity to meet that very high one-hour volume, although cost may prohibit the latter solution.

Even though the most important figure is the average number of characters transmitted per day, there may be important factors that cause peak volumes at various times during the day, various days during the week, or various times during the month. There also may be seasonal times of peak volumes because of holidays or legal requirements. Recall that legal requirements were identified earlier during the understand the current system phase.

The designer should plan for varying volumes at different hours of the day. For example in an on-line banking network traffic volume peaks usually are in the midmorning bank opening and just prior to closing. Airline and rental car reservation system designers look for peak volumes or messages during holiday periods or during other vacation periods. A military system designer might look for extreme peaks in volume during crisis situations.

You can calculate message volumes or counting current messages in a current system or by estimating future messages. Whenever possible take a random sample for several weeks of traffic and actually count the number of messages each day at each location.

On-line system is operating currently network monitors analysers may be able to provide an actual circuit character count or the volume transmitted per hour or per day. Take care when selecting the sample of working days to ensure that it is not an "out of normal" situation. When estimating message volumes for a system that does not currently exist. You can use conglomerate estimating, comparison estimating, detailed estimating, or modelling.

- With ***conglomerate estimating***, representatives from each application system that will use the network confer to develop estimates based on past experience.

- With ***comparison estimating***, the network designer meets with people inside or outside the organisation who have a similar system so they can supply estimates from their network.

- With ***detailed estimating***, the network designer makes a detailed study of the overall application system and its future needs in order to develop subestimates, which are then totalled into the total volume of messages just as we have described above.

- ***Modelling networks/response time.***

When making estimates of volumes, be sure to take future growth into account so the system will meet needs of the next decade. Do not worry about the accuracy of estimates at this point, although you should make them as accurate as possible. Accuracy may not be a major concern, because of the stairstep nature of communication circuits. For example, assume a situation in which a voice grade circuit is used. It can be used to transmit at 16,000 bits per second, but to meet data volumes, you need to transmit at 20,000 bits per second. This would require the lease of two voice grade circuits. The combined two voice grade circuits now have a maximum capacity of 32,000 bits per second, greatly exceeding the needed 20,000 bits per second. This example demonstrates that if actual message volumes are higher than estimated, there is plenty of spare capacity. On the other hand, the opposite problem may occur if estimates are too optimistic; the organisation may be forced to lease two voice grade circuits when only one is needed.

Now that individual message contents and the network link traffic table have been developed, there should be some feeling for the total volume of characters per day transmitted on each link of the proposed network. These are the volumes of characters transmitted from and to each local facility (nodes) where terminals will be located. The next step, which usually is carried out simultaneously with this step, is to determine traffic/circuit loading.

DETERMINE TRAFFIC/CIRCUIT LOADING

Now that average/peak characters transmitted per day per link have been identified, work can begin on determining the circuit capacities that will be required to carry that traffic. They are based on the number of characters per message and the number of messages transmitted per hour or per day.

At this point return to the geographical maps and pictorial diagrams (local facilities).

Does this map or pictorial diagram still seem reasonable in light of the vast amount of further information that has been gathered during the message analysis?

At this time some of the maps or pictorial diagrams might be reconfigured slightly in order to further solidify the geographic configuration of the network. Remember to evaluate all the geographical maps: international, country, city/ state, and local facilities.

The next step is to review all of the network links over which data will travel. This may have been done when the network link traffic table was completed. If so, double-check at this time to verify that each message type was cross-referenced to the proper network link (columns 1 and 2 in Figure 2-4). If the hour-to-hour variation is significant, it may be necessary to take hourly peaks into account or adjust working schedules and work flows.

Match the characters per day for each network link in Figure 2-4 with each network link that was shown on the country map (Figure 2-2). It will be helpful, when examining alternate configurations, if you list characters per day for each link shown on Figure 2-2.

It is the column totals (Figure 2-4) that really count. If the total number of characters transmitted in a single day on a single link is 330,000 or 405,000 then the network link has to operate at a speed that permits transmission of the 330,000 or 405,000 characters during the normal working hours. If it cannot meet this limit, certain adjustments have to be made. Now look at Figure 2-5. It shows: San Francisco/Miami, 890,000; San Francisco/Houston, 1,250,000; and Houston/Miami, 770,000 characters per day. Later in the design, if the San Francisco/Miami traffic is multidropped through Houston, the total traffic on the Houston/Miami link will be 1,660,000 characters per day (890,000 + 77O, OOO).

To establish the circuit loading (the amount of data transmitted), the designer usually starts with the total characters transmitted per day on each link, or if possible, the number of characters transmitted per hour if peaks must be met.

Starting with the total characters transmitted per day, the system designer first determines if there are any time zone differences between the various stations. This might be an international or a national system that has time zone differences that must be taken into account. For example, there is a three-hour time difference between Toronto and San Francisco. This means that if a host computer in Toronto operates from 7 A.M. until 4 P.M. (Toronto time), under normal circumstances there is only a five-hour working day in San Francisco, even assuming that someone is working through the lunch hour. By the time the people arrive at work in San Francisco at 8 A.M. it is already 11 A.M. in Toronto. Then Toronto shuts down its computer at 4 P.M. and it is still only 1 P.M. in San Francisco. This leaves the San Francisco facility with a workday that extends only from 8 A.M. until 1 P.M. The practical effect of this time difference is that the 1,460,000 characters (SF/TOR link of figure 2-5) of data must be transmitted during a five-hour period rather than the eight-hour day you might expect. These effects have to be taken into account or work schedules must be changed. Obviously, the Toronto host computer operating hours can be extended or the San Francisco staff can start work earlier. There is no perfect solution to time zone differences, but the system designer must account for them.

Other major factors that affect circuit loading include the basic efficiency of the code utilised and TRIBs. Synchronous transmission is more efficient than asynchronous transmission. The number of line control characters involved in the basic protocol affects line loading. The application systems/business future growth factor must be considered so the system will have a reasonably useful lifetime. Forecasts should be made of expected message volumes three to seven years in the future. This growth factor may vary from 5 to 50 percent and, in some cases, exceed 100 percent for high-growth organisations.

Some extra time should be allowed for transmission line errors (error detection and retransmission) which may result in the retransmission of 1 to 2 percent of the messages. Retransmissions may be even higher where small common carriers are used or if transmission is into or out of developing countries.

The network designer also should consider a 10 to 20 percent contingency factor for the "turnpike effect." The turnpike effect results when the system is utilised to a greater extent than was anticipated because the system is found to be available, is very efficient, and has electronic mail features. In other words, the system is now handling message types for which it was not originally designed.

Other factors to consider when evaluating line loading might be whether to include a message priority system. High-priority messages may require special identification and therefore may increase the number of characters per message. If the message mix changes and, over a period of time, most messages become high priority, then more characters will be transmitted during a working day.

Also, a greater throughput may have to be planned to ensure that lower-priority messages get through in a reasonable period of time. The learning curve of new terminal operators may also affect line loading. Operator errors and retransmissions are greater when a new system is being learned.

Another factor that might affect circuit loading is an inaccurate traffic analysis (confidence intervals). Try to account for any business operating procedures that might affect the system and the volumes of data transmitted.

Other factors that must be taken into account include extra characters transmitted with regard to the system operation (line control characters) such as polling characters, turnaround time/synchronisation characters, control characters in message frames and/or packets, modem turnaround time on half duplex circuits, message propagation time subtracts from the total useful hours for transmission of data, any printer time for carriage return/tabulation/form feeding, lost time when statistical time division multiplexers are overloaded, and periods of high error rates caused by atmospheric disturbances.

At this point the system designed should review and establish some of the response time criteria. These are required to meet the basic needs of the application systems that will utilise the network.

Finally, begin recording, on the network maps and/or pictorial diagrams, some of the bit per second transmission rates that will be required for each circuit link. Sometimes it is useful to show the transmission capacity required for each link. In Figure 2-5 we show the characters per day per link. Now add the bit per second transmission rate necessary for each circuit link. This will help when alternative network configurations and software/hardware considerations are being developed and evaluated.

DEVELOP A CONTROL MATRIX

Because the network probably will be the "lifeline" of the entire information flow within the organisation, security and control are mandatory. All of the security and control mechanisms that will be included in this data communication network must be taken into consideration during the design phase. It must be protected from all types of threats such as errors and omissions, message loss or change, disasters and disruptions, breaches of privacy, security/theft, unreliability, incorrect recovery/restart, poor error handling, and lack of data validation.

DEVELOP NETWORK CONFIGURATIONS

During this step of the system approach to designing a data communication network, the designer utilises all of the information collected to date. Of special value are the network maps and the traffic/circuit loading data. These are used to configure the network in such a way as to achieve the required throughput at a minimum circuit cost. Begin this step by reviewing the maps and pictorial diagrams that show the links between the station/ node locations.

The object of this step is to configure the circuit paths between users and the host computer. The decision involves moving the stations/nodes about, and making judgements with regard to software and hardware. In reality, this step is performed simultaneously with the next two steps, "consider software" and "consider hardware." Some goals that the network designer tries to achieve with regard to an efficient and cost-effective network include:

- Minimum circuit mileage between various stations/nodes. Computer programs help.
- Adequate circuit capacity to meet today's data transfer needs as well as those required three to seven years in the future.
- Reasonable response times at individual terminals and the response time needs must be met for each application.
- Reliable hardware that offers minimum cost, adequate speed and control features, a high mean time between failures (MTBF), and good diagnostic/serviceability features.
- Efficient software/protocols that can be used on a variety of circuit configurations including satellite circuits. One of the newer bit-oriented protocols that can interface with various international standards (X.25) might be used. This permits the network to interface which national/international networks as well as with electronic mail postal systems, to utilise multivendor hardware, and to connect to public packet switched networks.

- A "very high" level of reliability (network uptime) must be met. This may be the most important factor. The network designer should always remember that, when business operations move into an on-line, real-time data communications network, it is as if the company has closed its doors for business when the network is down.

- Reasonable costs (not necessarily the absolute lowest).

- Acceptance of the network by both day-today "user" personnel and "management" who utilise data/information from the system.

When one is developing different network configurations, there are a variety of choices. In other words, there is a "choice set" which is a set of all available alternatives. Each alternative is a different system or a slightly modified version of another alternative. During the deliberations, the following decisions must be considered:

- Determine the choice set, that is, all possible network configurations.

- Divide the choice set into attainable and unattainable sets. The attainable set(s) contain only those alternatives that have a reasonable chance of acceptance by management. Acceptance might be predicated on costs, software, hardware, circuit availability, or political factors within the organisation.

- Review the attainable set of alternatives and place them in a ranked sequence from the most favoured to the least favoured, taking into account your evaluation criteria for choosing the most favoured. Evaluation criteria were identified during the plan preparation phase.

- Present the most highly favoured alternatives to management for review and, it is hoped, approval.

There is one other consideration in selecting the different network alternatives. The network designer must know whether the proposed alternative is going to maximise something, optimise something, or satisfice something, or if it will be a combination of the three.

To *maximise* is to get the highest possible degree of use out of the system without regard to other systems.

To *optimise* is to get the most favoured degree of use out of the system taking into account all other systems; an optimal system does just the right amount of whatever it is supposed to do, which is not necessarily the maximum.

To *satisfice* is to choose a particular level of performance for which to strive and for which management is willing to settle.

Finally, the network designer also must be aware that individual job tasks within the network may have three levels of dependence upon each other.

- ***Random dependence:*** a job task is required because of some other job tasks.
- ***Sequential dependence:*** one particular job task must follow another job task.
- ***Time dependence:*** a job task is required at a set time with regard to another job task.

The network designer should assess various job tasks during the development and design of network configurations. Job task interrelationships must be studied with regard to future needs and growth. Job tasks that are dependent today may not be after a new application is completed next year. Job tasks require an open-ended approach.

Now that the network maps/pictorial diagrams and traffic/circuit loading have been reviewed, line controls and modes of operation can be considered. This probably involves software and such factors as full duplex versus half duplex, whether a satellite link is used, statistical multiplexers versus pure (transparent) multiplexers, modem speeds, intelligent terminal controllers, and how different configurations operate such as central control versus interrupt, multidrop, or point-to-point.

Various alternative configurations are shown in Figures 2-2 2-6,2-7,2-8 and 2-9. Figure 2-2 shows a point-to-point configuration where each terminal node has its own communication circuit between all other nodes. Figure 2-6 shows the same configuration using a multidrop circuit with New York as a switching centre. Figure 2-7 shows the same configuration again, using a multiplexed arrangement. The Houston site multiplexes San Francisco/Miami/Houston data to Chicago. Then Chicago multiplexes that data with the Chicago/Calgary/Toronto data and on to New York. Notice how the different configurations change overall circuit mileage. Circuits are paid for on the basis of dollars per mile per month; therefore, a minimum mileage configuration is also a minimum circuit cost configuration. Also notice that different numbers of modems are required in different configurations.

Figure 2-8 shows a packet switching satellite network. This can be a public packet switcher or a private packet network. Figure 2-9 shows a combination of a local network, a packet satellite network, point-to-point, multiplex, and multidrop configurations.

This step involves choosing among various network alternatives. The main constraints are the availability of software packages, available hardware, and available circuit links. These three factors are all interconnected and must be considered along with the "performance and reliability" that must be obtained. All of these factors are also interrelated with regard to cost. Therefore, when alternative network configurations are developed, you must consider the software, hardware, circuits, performance, reliability, and interrelate these five factors through your cost/benefit analysis.

CONSIDER SOFTWARE

With regard to software, the type of host computer may be a major constraint. The protocols that the host can handle may limit the types of terminals or other hardware that can be utilised. This limitation may be overcome through the use at protocol converters and/or the purchase of a new front end communication processor that can interface with the host and a variety of software and hardware.

At this point the software will determine the line control methodology/mode of operation. Decisions must be made as to whether operations will be in full duplex or half duplex, asynchronous or synchronous and at what speeds. For a new system one of the newer bit-oriented protocols should be selected, such as X.25, SDLC, HDLC, or the like. The older byte-oriented protocols (such as Binary Synchronous Communications-BSC) probably are not a good choice because of their limitations on satellite links, slow half duplex operation and inability to meet international standards. It is desirable to select a protocol that is compatible with the International Organisation for Standardisation (ISO) seven layers, although reality might dictate that in order to be compatible with existing hardware another protocol must be utilised.

In addition to protocol/software, other network architecture/software that resides in the host computer and in the front end communication processors have to be considered. For example, telecommunication access programs and the teleprocessing monitors may affect network operations. Security software packages in the host computer also can be a constraint. Finally, the host operating system itself may be a constraint to network control and operation, as might be the database management system software.

Any software programs that are located out in the network should be reviewed. These may be at remote concentrators, remote intelligent terminal control devices, statistical multiplexers, and terminals (microprocessor terminals). Microprocessor terminals also raise the question of distributed data processing/remote application programs.

The network designer can make a major contribution to the future by selecting a protocol that can grow, that is compatible with an internationally recognised standard, and that will not have to be changed for at least five to ten years. The protocol is crucial because the host computer network architecture must be able to interface with it. For example, the telecommunication access programs and teleprocessing monitor should be compatible with international standards. This means that the International Organisation for Standardisation seven-layer model should be used as the basic skeleton when protocols are interfaced to host computer/front end software packages. Also, you might want to interface with a local area network sometime in the future.

Finally, software diagnostics and maintenance must not be overlooked. Determine how quickly either in-house people or the vendor can diagnose software problems and also how quickly they can fix these problems.

CONSIDER HARDWARE

Hardware that interacts with the alternative network configurations is easier to handle than software because hardware is a tangible item. Some of the pieces of hardware that need to be considered are:

- Terminals/microprocessors
- Intelligent terminal controllers
- Modems (analogue/digital)
- Multiplexers
- Intelligent multiplexers (STDM)/concentrators
- Line-sharing devices
- Protocol converters
- Hardware encryption boxes
- Automated switching devices
- PBX/CBX switchboards
- Various communication circuit types
- Port-sharing devices
- Front end communication processors
- Host computers
- Testing equipment

With this in mind, the designer uses representations of the pieces of hardware and moves them about on the various network maps and pictorial diagrams. This experimentation with configurations should take into account the protocol/software considerations. The result should be a minimum-cost network that meets the organisation's data communications (throughput) requirements. This is no trivial task. Many organisations use computer simulation and modelling to carry out this task successfully.

Before ordering hardware, the design team should decide how to handle diagnostics, troubleshooting, and repair. It should be remembered that MTTD, MTTR, and MTTF always apply to hardware because hardware usually fails more often than software. Vendor estimates of MTBF (Mean Time Between Failures) should be obtained by the design team. Issues that should be addressed include the types of test equipment that are necessary and the organisational structure of the network management group. Some hardware may have built in diagnostic capabilities for its own internal electronic circuits, as well as the ability to identify problems on the communications circuit.

Diagnostics go hand in hand with network service. The vendor's MTBF and ability to respond to service calls are essential factors that affect downtime of the network.

In summary, a network configuration must be developed that takes both hard-ware and software into account. Costs are also analysed during this effort.

CONCLUSION

This project provides the network manager a good picture of the current controls, their effectiveness, and adequate documentation.

In this project a step - by -step systems approach is used and all individual steps are described in detailed with examples and pictures.

Finally computer industry is growing rapidly. Every people are changing their systems to the computer systems.

While these systems are using there may occur some errors because of the wrong usage, bugs, and less security systems.

So, you have to know network security and control systems for giving service to the companies.

We think that a computer engineering student should have to know network security and control to be successful at the real life.

APPENDIX

	Errors & Omissions	Message Loss of Change	Disasters and Disruptions	Breach of Privacy	Security/ Theft	Reliability (Uptime)	Recovery and Restart	Error Handling	Data Validation & Checking
Host Computer or Central System									
Software									
Front End Communication Processor									
Multiplexer, Concentrator, Switch									
Communication Circuits (Lines)									
Local Loop									
Modems									
People									
Terminals/ Distributed Intelligence									

FIGURE 1-9 Blank Matrix

	Errors & Omissions	Message Loss of Change	Disasters and Disruptions	Breach of Privacy	Security/ Theft	Reliability (Uptime)	Recovery and Restart	Error Handling	Data Validation & Checking
Host Computer or Central System	1,2,3,4,7	1,2,3,4, 5,7	1,8,11,13,16	6,8,24	6,8,24	1,13,16			6,24
Software	1,2,3,4,7	1,2,3,4, 5,7	1,8,16	6,8,24	6,8,24	1			6,24
Front End Communication Processor	1,2,3,4,7	1,2,3,4, 5,7	1,8,13,16	6,8,24	6,8,24	1,13,16			6,24
Multiplexer, Concentrator, Switch	1,2,3,4,7	1,2,3,4, 5,7	1,8,13,16	6,8,24	6,8,24	1,13,16			6,24
Communication Circuits (Lines)	12		10,15,16,18			15,16			
Local Loop	12								
Modems	12,18	18,24	8,9,10,11,13, 14,15,16,18	24	24	9,10,11,13,14, 15,16,17,18	9,10,11,1 4,15	18,19,20, 22,23	
People	5	5,7		6,8,24	6,8,24				6
Terminals/ Distributed Intelligence		2		6,8,24	6,8,24	1			6,24

Figure 1-11 Matrix with Controls

THREATS

COMPONENTS

	Errors & Omissions				Security/ Theft	Reliability (Uptime)	Recovery and Restart	Error Handling	Data Validation & Checking
Host Computer or Central System	1,2,3,4,7	1,2,3,4, 5,7	1,8,11,13,16	6,8,24	6,8,24	1,13,16			6,24
Software	1,2,3,4,7	1,2,3,4, 5,7	1,8,16	6,8,24	6,8,24	1			6,24
Front End Communication Processor	1,2,3,4,7	1,2,3,4, 5,7	1,8,13,16	6,8,24	6,8,24	1,13,16			
Multiplexer, Concentrator, Switch	1,2,3,4,7	1,2,3,4, 5,7	1,8,			13,16			6,24
Communication Circuits (Lines)	12		10,15,16,18			15,16			
Local Loop	12								
Modems	12,18	18,24	8,9,10,11,13, 14,15,16,18	24	24	9,10,11,13,	9,10,11,14	18,19,20 ,23	
People	5	5,7		6,8,24	6,8,24				6
Terminals/ Distributed Intelligence		2		6,8,24	6,8,24				6,24

This shows the subset of controls that mitigate the threat, Errors and Omissions.

This shows the subset of controls that control the component, Communication Circuits (Lines)

Empty cells show a lack of control which may be a serious problem.

Some individual cells may be more sensitive to your network or your company, therefore, the control in these cells should be reviewed very closely.

FIGURE 1-12 Matrix evaluation of the controls

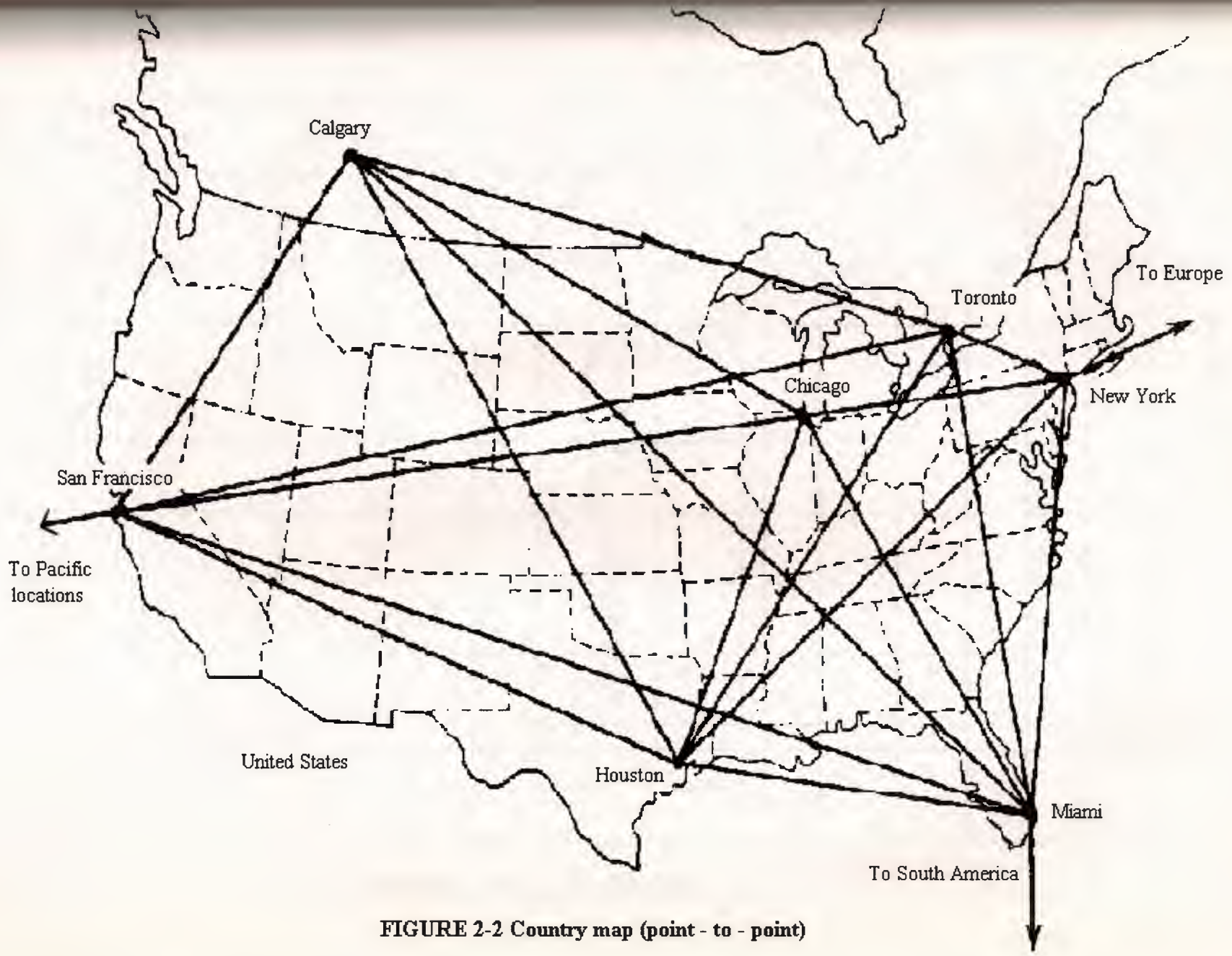


FIGURE 2-2 Country map (point - to - point)

Network Link	Message Type	Characters /Message		Message /Day		Characters /Day		Characters Transmitted Hourly # of						
		Average	Peak	Average	Peak	Average	Peak	8-9	9-10	10-11	11-12	12-1	1-2	2-3
Calgary to San Francisco	Passbook Savings Inquiry	22	28	1500	1650	33000	46200		12500	4000	4000	2000	1500	9000
	Loan Balance Inquiry					SUM OF THIS COLUMN								
DOWN TOTALS						330000	405000							

FIGURE 2-4 Network Link Traffic Table

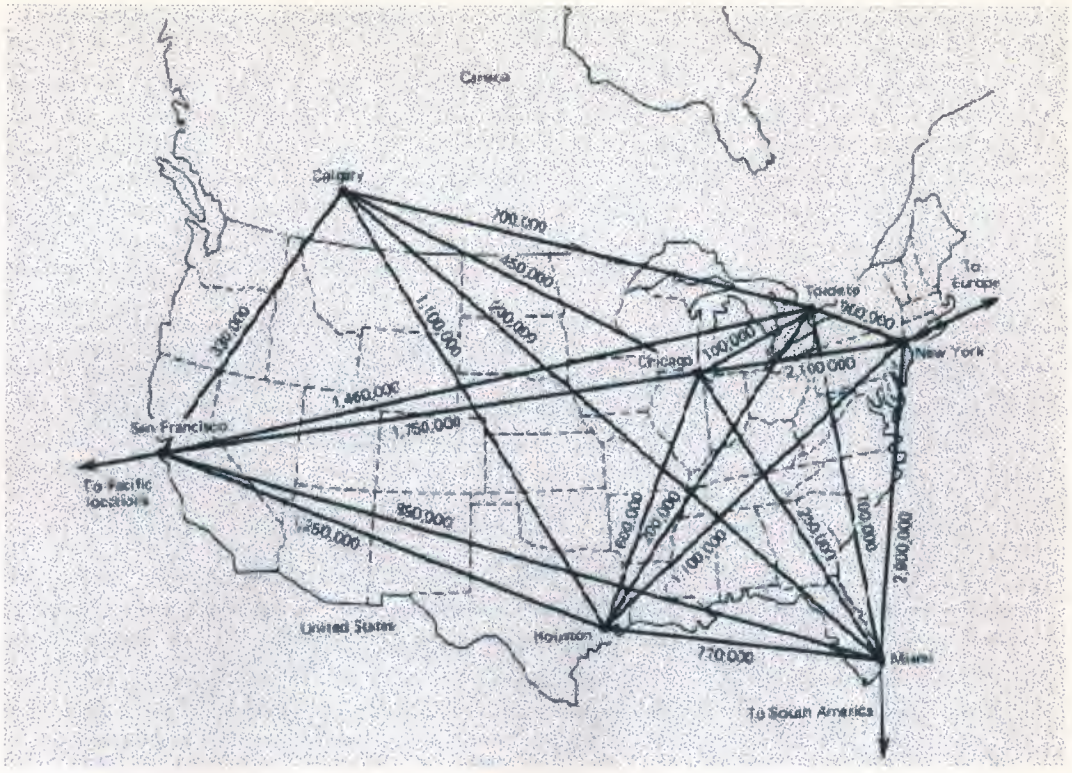


FIGURE 2-5 Link loading in Characters per day

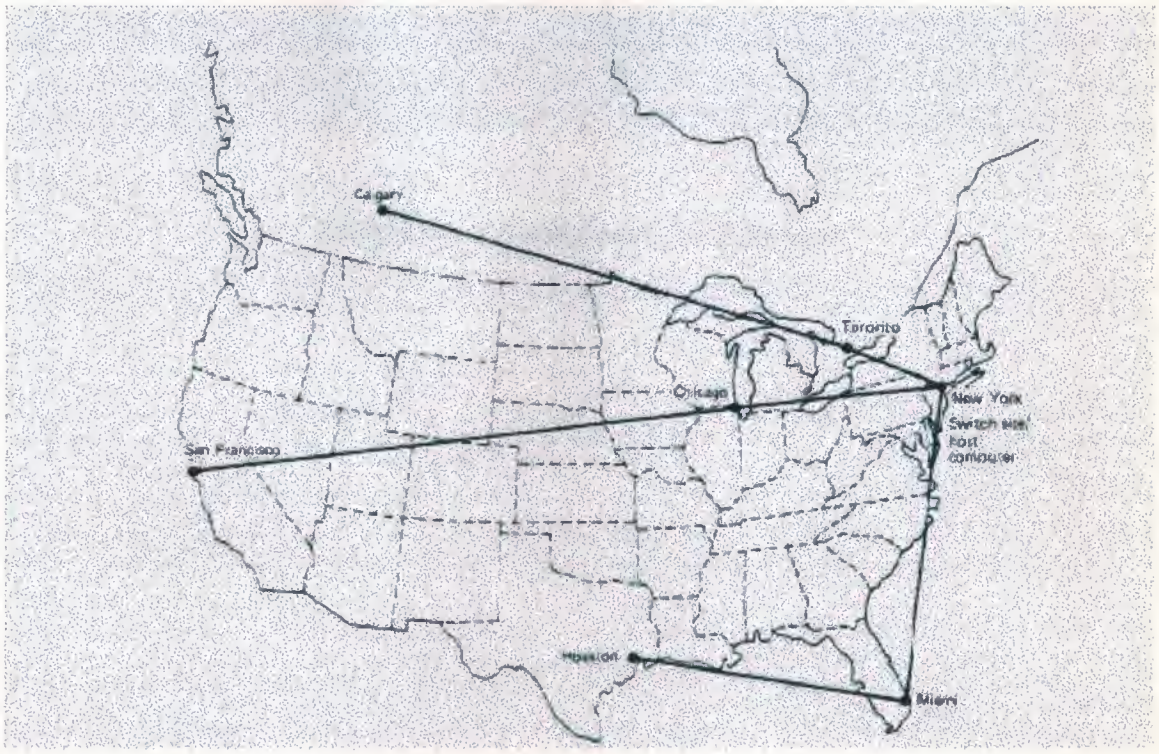


FIGURE 2-6 Multidrop Configuration

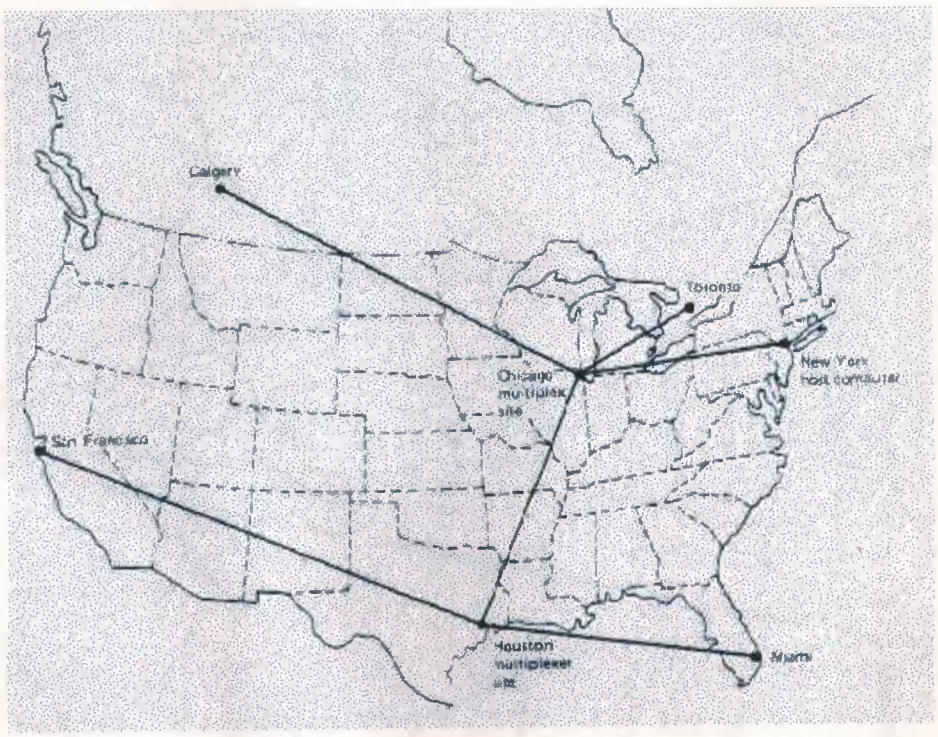


FIGURE 2-7 Multiplexed Configuration

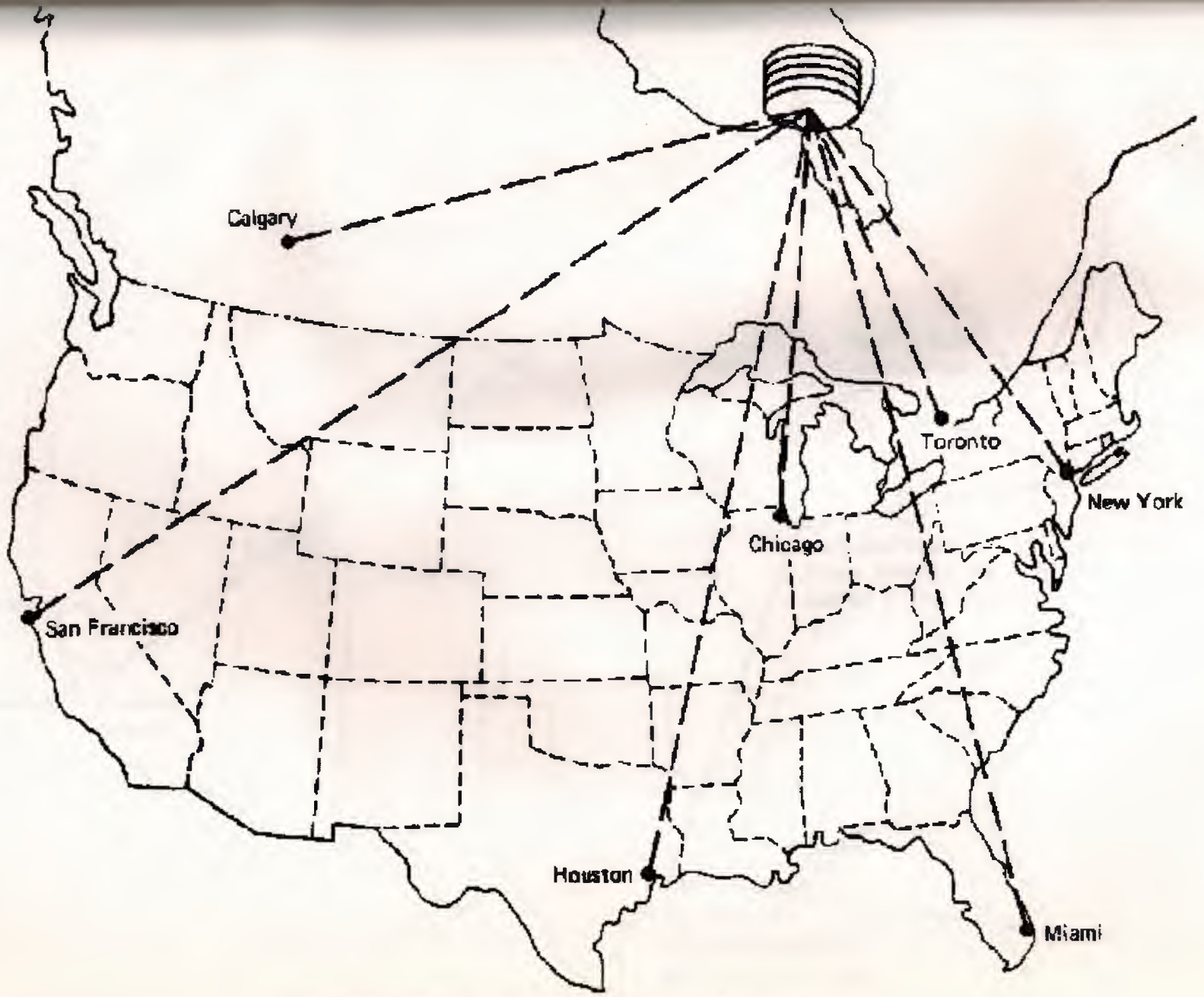


FIGURE 2-8 Public packet switching satellite configuration

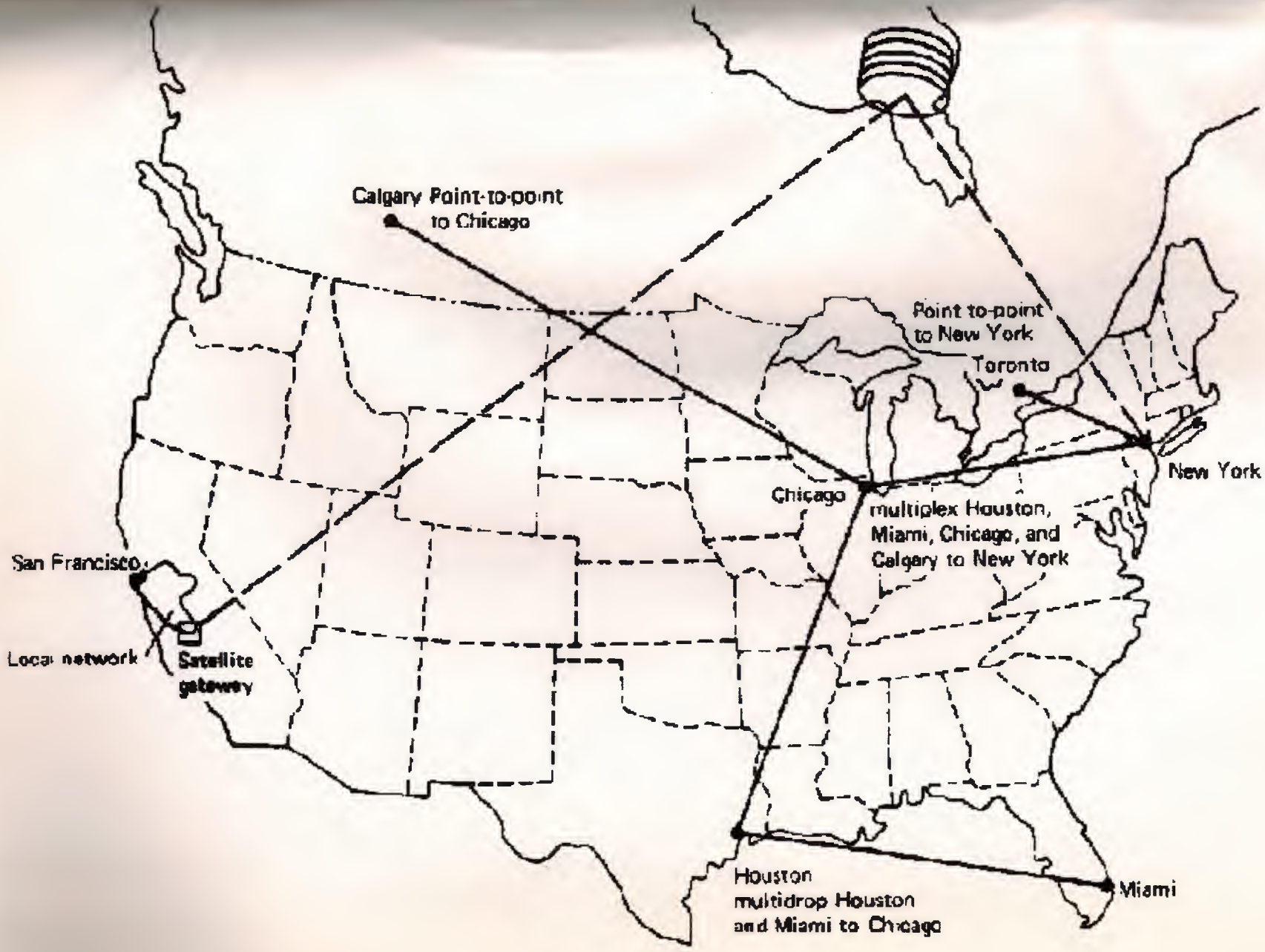


FIGURE 2-9 Multiple configurations