ECI
AIR UNIVERSITY

CDC 49350B

COMMUNICATIONS-COMPUTER SYSTEMS CONTROL JOURNEYMAN

Volume 2. Communication Systems

Authors: MSgt Albert F. Dice Jr.
TSgt Joseph M. Myers
3410th Technical Training Group
USAF Technical Training School (ATC)
Keesler Air Force Base, Mississippi 39534-5000
DSN: 597-3870

Education Specialist: Ben A. Humphrey
Editor: Patricia D. Ayles
Extension Course Institute (AU)
Gunter Air Force Base, Alabama 36118-5643

DUE TO THE LARGE amounts of information that had to be covered to fulfill the requirements of your specialty training standard (STS), your career field career development course (CDC) has been constructed in two parts. This is the second volume of the second part. Again, like the 49350A CDC, one lesson will build on another lesson and progress from volume to volume to parallel the requirements of the STS. There may be times when you need to review some of the basic concepts presented in 49350A CDC; therefore, make use of your glossary supplement in locating these subject areas. You need to ensure you have a thorough understanding and knowledge of one lesson before proceeding to the next.

This second volume of CDC 49350B deals with communications systems found throughout the Defense Communications System (DCS). The information provided in this volume will begin to show you how various networks operate and what part you have in the overall system. Remember from our initial introduction to this CDC, we will continue to build and expand on material presented in previous volumes.

Unit 1 discusses very briefly the mission and organization of the Defense Communications Agency (DCA) and composition of the Defense Communications System. Unit 2 starts with a discussion of how the digital switched networks operate and what the future plans are for these networks. Unit 3 covers data networks, including AUTODIN and other major networks and their operation. Unit 4 discusses the Defense Satellite Communications System and the Air Force Satellite Communications System. Unit 5 lists the principles and operation of the local area networks and includes their topologies.

Foldout 1 is bound in the back of this volume. Use it as the text directs.

A glossary of terms used in this volume is included in the part B supplement. Use the supplement to refer to definitions of previously covered items.

Code numbers appearing on figures are for preparing agency identification only.

The inclusion of names of any specific commercial product, commodity, or service in this publication is for information purposes only and does not imply endorsement by the Air Force.

To get an *immediate response* to your questions concerning subject matter in this course, call the authors at DSN 597-3870 between 0800 and 1600 (CT), Monday through Friday. Otherwise, write the author at 3410 Technical Training Group, Keesler AFB MS 39534-5000, to point out technical errors you find in the text, Unit Review Exercises, or Course Examination. Sending subject matter questions to ECI slows the response time.

NOTE: Do not use the Suggestion Program to submit corrections for printing or typographical errors.

This volume is valued at 24 hours (8 points).

NOTE:

In this volume, the subject matter is divided into self-contained units. A topic page begins each unit, identifying the lesson headings and numbers. After reading the topic page and unit introduction, study the section, answer the self-test questions, and compare your answers with those given at the end of the unit. Then do the Unit Review Exercises (UREs).

Acknowledgement

PREPARATION of this volume was aided through the cooperation and courtesy of Datapro Research Corporation, TRW Information Networks Division, and AT&T Federal Systems.

Specifically, supporting technical data and illustrations have been reproduced from Datapro Reports on Data Communications by Datapro Research Corporation. Supporting technical data and illustrations also were reproduced from TRW Concept 2000, Local Area Network, Network Manager's Guide and Planning Kit. Supporting technical data and illustrations also were reproduced from Security-Plus, STU-III Communications Terminal by

AT&T Federal Systems
Guilford Center
P.O. Box 20046
Greensboro, NC 27420
Attn: Dept. 71GC094400
Phone: 1-800-262-3787

Permission to use the information from the above publications is gratefully acknowledged.

Please read the topic page for Unit 1 and begin. ➡

DEFENSE COMMUNICATIONS

In the early morning hours of 7 December 1941, the first wave of Japanese fighter aircraft began their attack on Pearl Harbor, Hawaii, launching the United States into World War II. The planes came in low and fast, striking their preselected targets with great accuracy. When the assault was completed, millions of dollars in damage had been done to key airstrips and other military installations, thousands of men were killed or injured, and our Pacific fleet was virtually destroyed.

The attack occurred while many of our soldiers and sailors were still sleeping and unaware of the impending danger. It did not have to be that way, though. Hours before the attack began, military authorities had drafted a message warning of possible hostile actions by the Japanese. Problems on the HF radio link from Washington to Hawaii that Sunday morning forced communications personnel to choose an alternate method for transmitting the message. Although several other Government communications links were available, the warning was sent by RCA commercial radio, arriving in Hawaii after the attack was already in progress.

This story gives some insight into the condition of our military communications structure as our country entered World War II. Since then, we have made tremendous advances in facilities, equipment, techniques, and organization. The organization gained momentum with the passing of the National Security Act of 1947. In that act, lawmakers included this declaration of purpose: To provide for the effective strategic direction and operation of the armed forces under unified command.

Effective strategic direction meant that efficient communications facilities would be needed. Moreover, they should be unified. In other words, what was needed was a common communications system that would link all defense activities together. The answer was the Defense Communications System (DCS).

To make sure the DCS became a reality, the Department of Defense (DOD) established the Defense Communications Agency (DCA) and gave it the task of creating and managing the worldwide military communications complex. In this unit, you will find information about the DCA in terms of its management of the DCS. Although we will be primarily discussing DCA, we cannot really separate *you* from the scene. In your job as a technical controller, you are part of the management team. You help manage the part of the DCS that passes through your Technical Control Facility (TCF). While doing so, you will be working within a framework of policies and procedures prescribed by DCA. Some of the most important of those managerial policies and procedures are covered in the sections that follow.

1-1. Mission and Organization of the Defense Communications Agency

DCA was organized in May 1960 to make sure that an integrated communications system would be established, improved, and operated to meet DOD needs. Portions of the communications assets of the three military services were placed under the control of DCA and then combined to form the DCS. Before that time the Army, Navy, and Air Force had operated three separate strategic communications systems. Each was independent of the other, except for a few minor links that were often technically incompatible. DOD Directive 5105.19 gives DCA authority to direct the DCS. DCA is undergoing restructuring and renaming and eventually will be named the Defense Information Systems Agency, or DISA.

200. The mission and structure of the Defense Communications Agency

Mission of DCA. Managing a large and complex system, such as the DCS is by no means an easy task. The list of management responsibilities and functions of DCA are found in DCAC 640-45-21, *DCA Organization and Functions Manual*. Briefly, though, the mission of DCA is to:

a. Do systems engineering for the DCS.

b. Make sure the DCS is planned, improved, operated, maintained, and managed effectively, efficiently, and economically.

c. Meet the long-haul, point-to-point, and switched telecommunications needs of the National Command Authorities, DOD, and other Government agencies, as authorized and directed.

While DCA is responsible for the proper management of the DCS, the operation and maintenance of the various components of the DCS are the responsibility of the military departments through their operation and maintenance (O&M) agencies.

Even though you are in the Air Force and assigned to a major command, your working relationship with various elements of DCA will be close; so close, in fact, that at times you may think you are working for DCA. This misconception is caused by the fact that DCA retains the authority to direct the operation of the DCS. In the following paragraphs, we will see how DCA directs the daily operation of the system.

Organization (DCA Operations Control Complex). The Director, DCA, exercises operational direction of the DCS through the Defense Communications Agency operations control complex (DOCC). The DOCC, as shown in figure 1-1, is composed of several levels of management centers that carryout the complex task of maintaining the DCS. The objectives of the DOCC are as follows:

a. Make sure of user-to-user communications support within the DCS.

b. Provide DCS status information in a useful form to let users and O&M agencies do their jobs and to prevent duplicate reporting.

c. Coordinate between the operating elements, user, commercial carriers, O&M agencies, military services, and other Government agencies, as directed, to identify communications problems quickly.

d. Make sure of restoration of the DCS under any adverse or catastrophic conditions.

e. Set up guidelines for transition to a wartime environment.

National Communications Agency Network Management Operations Center (NCANMOC). The DCANMOC is the central controlling element of the DOCC. Located at Headquarters DCA, it is responsible for exercising day-to-day operational direction over the world-wide DCS operations elements.

Area Communications Operations Center (ACOC). The ACOCs are responsible for the operational direction of a specific geographical area. There are three ACOCs: DCA Western Hemisphere, collocated with the DCANMOC at Headquarters/DCA; DCA Europe, located at Vaihingen, Germany; and DCA Pacific, located at Wheeler AFB, Hawaii. Current plans call for a fourth ACOC to be known as DCA Central.

Regional Control Facility (RCF). Due to the large geographic area of the Pacific, DCA Pacific (PAC) is divided into two regions, each with an RCF responsible for its operational direction. DCA Northwest Pacific (NWP) is located at Yokota AB, Japan, and DCA Southwest Pacific (SWP) at Clark AB, Phillipines.

As a technical controller, you will work closely with controllers at either an area communications operations center (ACOC) or an RCF, depending on the location of your facility. Although you do not work for them, it is important

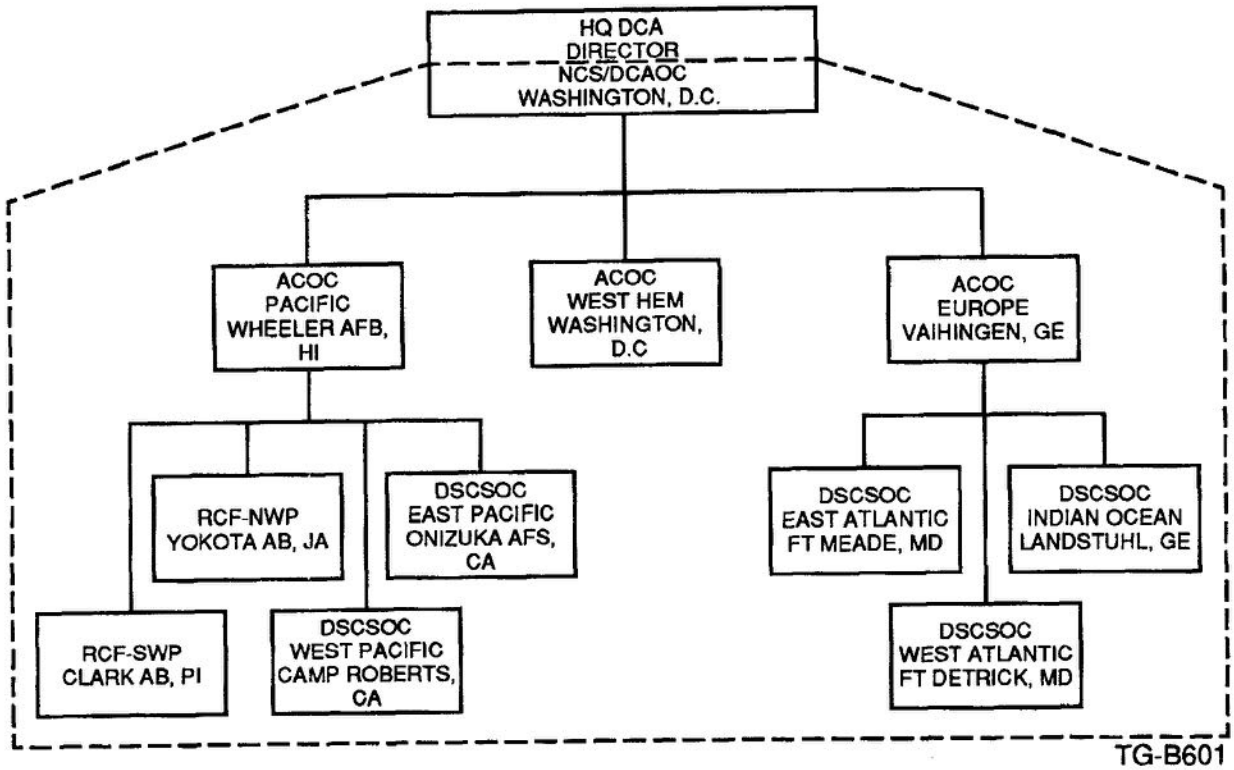


Figure 1-1. DCA operations control complex (DOCC).

that you maintain good relations with the controllers at the operations center you are working with. They are responsible for ensuring that the policies of the director of DCA are carried out efficiently.

All DCS reporting stations (technical control facilities) within an area are connected to one of the operations centers by *critical control circuits*. These control circuits are special *order wires* used by the DOCC in exercising operational direction over the DCS and in receiving DCS status reports.

Each operations center has a communications status activity, whose personnel maintain 24-hour-a-day surveillance of the status of the DCS within their area of responsibility. They do this by collecting, processing, and analyzing the reports submitted by stations under their control. To make this work more efficiently, the larger operations centers use computers to collect and process the status information.

By analyzing the contents of incoming status reports, operations center personnel decide whether *operational direction actions* are needed. They also use technical controller requests on recommendations and user complaints. If action is necessary, they decide what it should be and then pass directions and information to the right DCS element—your technical control facility, for example. Operations center personnel use the critical control circuits, on-call patches, and DSN calls to transmit directions. When situations are not urgent, they may use written messages sent through normal communications channels. Messages passed by any of the means we have just mentioned are known as *operational direction messages* (ODM).

An ODM is not merely an administrative message. On the contrary, it is usually a very important—sometimes vital—directive that normally requires immediate action by your technical control facility. While on duty, you may receive an ODM, perhaps passed over the critical control circuit or by DSN. Of course, it will not be addressed to you personally, but it might as well be. The person transmitting the ODM to your station will expect you to know what to do with it. If you receive a voice ODM, be certain to record the information exactly as given to you, then give it to your supervisor as soon as you can.

Your supervisor may prepare a reply to the ODM, called an *operational coordination message (OCM)*. OCMs can also be used to send nonaction information to an area or regional operations center and are transmitted the same way as ODMs.

Defense Satellite Communications System Operations Center (DSCSOC). The DSCSOCs are responsible for the operational direction of Defense Satellite Communications System Earth terminals in a given geographic area. The five DSCSOCs are located at Ft Meade and Ft Deterick, Maryland; Camp Roberts and Onizuka AFS, California; and Landstuhl, Germany. The DSCSOCs are manned by DCA personnel who report to the ACOCs as indicated in figure 1-1.

201. The worldwide digital systems architecture (WWDSA)

In May 1977, DOD tasked DCA, in coordination with the military departments, the TRI-TAC office, the National Security Agency, and other interested agencies and commands, to develop the WWDSA. The motivation for this effort stemmed from widespread concerns about the ability of DOD telecommunications systems to maintain acceptable levels of interoperability, survivability, and restorability on an end-to-end basis at a reasonable cost.

WWDSA was developed under DCAs leadership by the WWDSA working group; in December 1981, DCA issued the WWDSA final report, which documented the WWDSA goal architecture and the work done in its development. The report documents a transition strategy to achieve that architecture.

This transition strategy includes building on existing and planned programs, an enhanced command and control communications intelligence (C^3I) ability, an improved interoperability and standardization, exploitation of commercial developments, provision for continuity of service, incremental introduction of new services, and incremental improvements in management and control.

The improved systems will form an interoperable set of mutually supportive networks and facilities that are better able to cope with the challenges of supporting military operational needs throughout the full range of possible conflicts, including crises and contingencies, conventional warfare, limited nuclear warfare, and all phases of general nuclear warfare (preattack, transattack, postattack).

The WWDSA establishes evolutionary transition strategy for DODs telecommunications systems to achieve needed survivability and endurability that is affordable. The transition strategy incorporates 14 key objectives that are to be considered for incorporation in all DOD telecommunications systems as they are being planned or as improvements to existing systems are made. The key objectives of the WWDSA are:

(1) To obtain access to many sources of connectivity, including a variety of transmission media and switched networks, in order to achieve path and propagation diversity.

(2) To have the ability to use many sources of connectivity intelligently through improved routing strategies, processor augmentation, and extension of system capabilities closer to the users where possible.

(3) To have modularly expandable switches in capacity and features to allow low-startup cost. This composite switching ability is expandable to include such features as multilevel precedence and preemption (MLPP).

(4) To have interconnected voice and data (circuit-switched and packet-switched) networks for mutual support and improved reliability.

(5) To have improved internetwork systems control to improve call connect performance and system control responsiveness.

(6) To have a tandem switching ability to improve connectivity, provide a more distributed structure, and thereby increase survivability and responsiveness.

(7) To have a multirate ability (16 and 64 kbps) among switches for more effective use of digital transmission links. Tactical switches may be able to provide switching only at 15 kbps, but they should interface with 64 kbps switched networks. Secure voice at 2.4 kbps will be carried through the circuit switched network on 16 and 64 kbps channels through sub-multiplexing, multiple sampling, or bit-stuffing techniques. Trunking through HF radio will carry voice and data over 4-kHz analog channels.

(8) To enhance 2.4 kbps secure voice survivability through the use of packetized voice and the interconnection between circuit-switched and packet-switched networks.

(9) To have high-quality 16 kbps secure voice with an ability to tandem and conference with 2.4 kbps secure voice.

(10) To have a common proliferated survivability key distribution system for voice and data that will provide improved performance, security, and survivability of secure voice calls and secure data transfer.

(11) To have end-to-end encryption for classified data users over both circuit- and packet-switched networks.

(12) To have expanded and integrated use of satellite communications, including the use of small, extremely high-frequency/demand assignment multiple access (EHF/DAMA) satellite Earth terminals, both military and commercial, to supply wideband services and improve the mix of media at switching nodes.

(13) To have improved internetwork systems control between DCS, tactical, strategic, civil, commercial, and allied networks for normal operation, restoral, and reconstitution. Control will be made easier through the use of automated aids (network status indicators, facility reassignment algorithms, and data bases) useful to network management decision-makers. Critical users will have a systems control ability to help in the step-by-step restoral of fragmented networks.

(14) To have common standards for all networks and equipment, where practical, for improved interoperability. Emphasis on use of commercial standards where suitable.

Most of the current major architectures, plans, and programs are generally consistent with WWDSA, and only minor refinements are needed, in most cases, to bring our telecommunications systems into full alignment. While the WWDSA final report offers only general guidelines for transition, DCA is issuing more specific recommendations as they are developed.

Please write your response to unit self-test questions and then check the text answers at the end of the unit.

SELF-TEST QUESTIONS

200. The mission and structure of the Defense Communications Agency

1. Briefly, what is the mission of ~~DCA~~ DISA? Perform systems engineering for the DCS + ensure it is planned, improved, operated + maintained + managed

2. What organization is responsible for the operation and maintenance of the Air Force components of the DCS? O & M agency AFCC

3. How does the director/~~DCA~~ DISA exercise operational direction of the DCS? DOCC

4. What is the central controlling element of the DOCC? NCS/DACOC

5. How do the ACOCs and RCFs pass directions to technical control facilities? ODM

6. Who directs the operation of satellite Earth terminals? DSCOCs

201. The worldwide digital systems architecture (WWDSA)

1. What is the purpose of WWDSA?

2. What must be considered while planning new communications systems?

3. Who is developing specific guidelines for the transition strategy into WWDSA conformity?

1-2. Composition of the Defense Communications System

As you know, the DCS is a composite of DOD-owned and -leased telecommunications systems, subsystems, and networks composed of facilities, personnel, and material and is managed by DCA. It provides the long-haul, point-to-point, and switched network telecommunications needed to satisfy the requirements of DOD and selected Government agencies.

You have already seen how the various elements of the DOCC direct the operation of the DCS. This section will provide an overview of the elements that make up the DCS and the facilities that have direct control responsibility over them.

202. Elements of the DCS

DCS facilities can be broken down into three general categories: fixed, transportable, and mobile.

Fixed. Most of the facilities in the DCS are fixed. These include, among other assets, switching facilities, such as the automatic digital network (AUTODIN), and automatic secure voice network (AUTOSEVOCOM), radio relay facilities, and most assets of the Defense Satellite Communications System (DSCS). These facilities are built permanently in place: in other words, they are not transportable or mobile. Some of these facilities will be discussed in detail in the remaining units of this volume.

Transportable. Some of the equipment in the DCS is transportable. This is equipment that can be moved by truck, rail, or other means. An example would be power generators used to support long-term, but not necessarily permanent, operations.

Mobile. Many technical controllers are assigned to mobile or tactical communications squadrons. The equipment these organizations use can be mounted on devices known as mobilizers or can be carried on trucks and trailers for rapid deployment in support of short-term military operations. Both mobile and transportable communications systems will be covered in Volume 3 of this course.

Also included in the DCS are the transmission media (including those commercially leased), circuits that provide user and subscriber connection to the switching and relay facilities of the DCS networks, and circuits that interconnect the switching and relay facilities of the DCS networks. All telecommunications required to interconnect the National Command Authority (NCA), the Joint Chiefs of Staff (JCS), and commanders of the unified and specified commands with the general purpose networks are DCS assets.

You should understand that some of the communications equipment and systems you encounter will not be part of the DCS. The communications networks for post, camp, or base operations are generally not considered part of the DCS, even though technical controllers who are assigned to a DCS facility help to maintain their proper operation. Also, the mobile and transportable communications facilities of the Army, Air Force, and Naval and Marine forces are not DCS assets. As you familiarize yourself with the particular facility you are assigned to, you should make it a point to know what your DCS assets are.

203. Responsibilities of DCS control facilities

In our discussion of the DOCC, we said that its various offices are responsible for the operational direction of the DCS. Understand that the DCS is a large and complex system that requires a wide dissemination of responsibilities to make

sure of its proper management. For this reason, many TCFs are chosen as control facilities and given management responsibilities that are more specific than those of the elements of the DOCC. The control facilities in the following discussion report their status to the right DOCC elements in their geographical area.

Facility Control Office (FCO)/Subregional Control Facility (SRCF). An FCO is assigned to supervise the operation and maintenance of communications links in given geographical areas. Certain TCFs will be assigned this responsibility based on their ability to access the systems and stations under their control. Essentially, the FCO is an added duty that some TCFs have. It should be noted that, at the time of this writing, DCA is undergoing a reorganization. The FCOs will slowly transition into SRCFs that will have responsibilities similar to those of the FCO.

Intermediate control office (ICO). If the layout of a particular segment of a communications circuit or trunk is such that the FCO/SRCF or circuit control office (CCO) is not in the best position to test and coordinate with other TCFs, one or more of the other TCFs may be chosen as an ICO for that particular segment. Each ICO is responsible for the general service condition of its segment of a circuit or trunk.

Circuit control office. One TCF is named CCO for each circuit in the DCS. Generally, the CCO is responsible for coordinating the initial activation of a circuit by the telecommunications service order (TSO), which establishes the circuit. The CCO coordinates any realignment or deactivation of the circuit. The CCO also is responsible for end-to-end out-of-service (customer denied service) quality control testing and for coordinating troubleshooting efforts during circuit outages or to maintain the engineered value stated in the TSO.

An application of the CCO plan with one TCF at each end of a circuit is shown in figure 1-2. Both TCFs are referred to as serving TCFs as they provide users with access to the DCS.

Another application of the circuit control plan may require the assignment of an ICO to help the CCO in testing, coordination, and other required actions. A TCF may be assigned as an ICO on the path of long or complex circuits with the configuration as shown in figure 1-3.

The TCF to which you are assigned may be given FCO/SRCF, ICO, or CCO responsibilities, or any combination of the three. Elements of the DOCC decide which TCFs fill these important positions, and they are named on the TSO for each circuit and system.

Figure 1-2. CCO assignment.

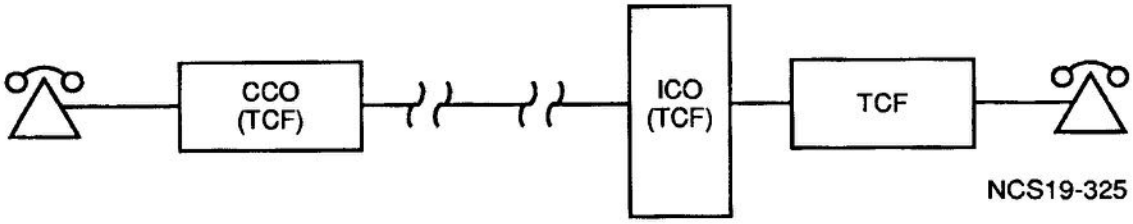


Figure 1-3. CCO assignment with ICO.

Please write your response to unit self-test questions and then check the text answers at the end of the unit.

SELF-TEST QUESTIONS

202. Elements of the DCS

1. What are the three general categories of DCS facilities? Fixed, transportable, & mobile

2. In which category would an AUTODIN facility be? Fixed

203. Responsibilities of DCS control facilities

1. To whom do control facilities report their status? DOCC

2. Which control office supervises the operation of transmission links in a given area? FCO

3. Who is responsible for the activation and testing of circuits? CCO

4. How many control office designations may a given TCF be assigned? All three

ANSWERS TO SELF-TEST QUESTIONS

200

1. To perform systems engineering for the DCS and ensure it is planned, improved, operated, maintained, and managed.
2. Its O&M agency, AFCC.
3. Through the DOCC.
4. The NC S/DCAOC.
5. By operational direction messages (ODM), via critical control circuits, on-call patches and DSN calls.
6. DSCSOCs.

201

1. To provide the ability for DOD telecommunications systems to maintain acceptable levels of interoperability, survivability, and restorability at a reasonable cost.
2. The 14-key objectives of WWDSA.
3. DCA.

202

1. Fixed, transportable, and mobile.
2. Fixed.

203

1. The DOCC element in their area.
2. FCO (SRCF).
3. The CCO.
4. All three.

UNIT REVIEW EXERCISES

Note to Student: Consider all choices carefully, select the *best* answer to each question, and *circle* the corresponding letter. When you have completed all unit review exercises, transfer your answers to ECI Form 34, Field Scoring Answer Sheet. **DO NOT RETURN YOUR ANSWER SHEET TO ECI.**

1. (200) What is the central controlling element of the National Communications Agency Operations Control Complex?

   a. The Regional Control Facility (RCF).
   b. The Technical Control Facility (TCF).
   c. The Area Communications Operations Center (ACOC).
   d. The National Communications Agency Network Management Operations Center (DCANMOC).

2. (200) Operational direction messages (ODM) may be sent in what ways?

   a. Critical control circuits, on-call patches, or Defense Switched Network (DSN) phone call.
   b. Defense Communications Agency (DCA) formatted report, critical control circuits, or AUTOVON phone call.
   c. AUTODIN, AUTOSEVOCOM, or other secure transmission.
   d. Mail, messenger, or carrier.

3. (201) What concerns motivated the development of the Worldwide Digital Systems Architecture (WWDSA)?

   a. The rising cost of maintaining DOD telecommunications systems.
   b. The need for a more secure digital communications network.
   c. The need to maintain acceptable levels of interoperability, survivability, and restorability.
   d. The need to redefine the organizational structure, goals, and programs of the Defense Communications Agency.

4. (202) What are the three general categories of Defense Communications System (DCS) facilities?

   a. Automated, manual, and passive.
   b. Fixed, transportable, and mobile.
   c. Terminal, relay, and tributary.
   d. Analog, digital, and analog/digital.

5. (202) Generally, what type facilities are AUTODIN, AUTOSEVOCOM, and most assets of the Defense Satellite Communications System (DSCS)?

   a. Digital.
   b. Tributary.
   c. Analog.
   d. Fixed.

6. (203) Who is responsible for the operation and maintenance of communications links for given geographic areas?

   a. The Area Communications Operations Center (ACOC).
   b. The Subregional Control Facility (SRCF).
   c. The Circuit Control Office (CCO).
   d. The Technical Control Facility (TCF).

Please read the topic page for Unit 2 and continue. ➡

DIGITAL DATA COMMUNICATIONS

Page

The business of communicating by data networks has grown immensely in recent years. The Automatic Digital Network (AUTODIN) was our first network to offer a secure means for the worldwide dissemination of data communications. Many users maintained their own individual networks to make sure of quick access for command and control of our military forces. The Defense Data Network (DDN) was developed to streamline this command and control by offering a secure, highly survivable, cost effective data communications network. It offers long-haul and area communications, interconnectivity, and the capability for interoperability to all existing Department of Defense automated data-processing systems and data networks. In this unit, we will discuss AUTODIN, some of the networks that make up the DDN, and weather networks.

2-1. Automatic Digital Network (AUTODIN)

AUTODIN provides the Department of Defense with an automatic electronic data communications service. The system is designed around remote, interconnected central-processing points called AUTODIN switching centers (ASC). The AUTODIN system use 15 such centers. Nine of these are located in the United States, and the remaining six are strategically located at various overseas points. The ASCs located in the United States are all commercially leased, and the overseas switches are Government-owned. The 15 ASCs are located in the following areas:

Norton CA (USAF)
McClellan CA (USAF)
Tinker AFB OK (USAF)
Gentile AFS OH (USAF)
Andrews AFB MD (USAF)
Fort Detrick MD (USA)
Hancock Field NY (USA)
Albany GA (USN)
Honolulu HI (USN)
Pirmasens, Germany (USA)
Coltano, Italy (USA)
Guam (USN)
Yokota, Japan (USAF)
Taegu, Korea (USA)
Croughton, England (USAF)

Although most of the narrative in this section is directed at the CONUS AUTODIN ASCs, there are many similarities between them and overseas ASCs. They do the three basic jobs of message switching, message processing, and message protection and bookkeeping in the same manner. Therefore, much of the information, except that concerning the actual hardware used, may be associated with overseas ASCs. The CONUS ASCs use RCA computers to do message switching; overseas ASCs use Philco-Ford computers.

204. ASC connectivity

ASC Interconnect. The interconnectivity of AUTODIN switching centers falls into two general categories: CONUS and overseas. Within the CONUS, the ASCs are connected by leased lines known as interswitch trunks (IST). The operating speed for CONUS ISTs is 9600 baud. The 9600 baud composite line is made up of two 4800 baud channels (A and B) combined through a modem. The A channel is considered the primary channel for message transmission. If a message is destined for another ASC, it is queued for the A channel. If, at the same time, another message is to be transmitted to the same ASC, the B channel is used. The B channel provides redundancy for the message path from ASC to ASC. One ASC treats the other ASCs as tributaries when processing message traffic. In figure 2-1, you can see that the CONUS ASCs are connected through other ASCs to form the AUTODIN CONUS matrix. This redundant connectivity provides for message protection in the event of complete ASC failure or saturation. Notice that on the East and West coast there are two ASCs, each operating as a gateway or entry point to the CONUS AUTODIN system. The reason for this is, again, redundancy.

The ASCs outside the CONUS use Government-owned facilities for communications media where possible. However, from an overseas ASC to the CONUS, leased lines are used. Again, redundant lines are provided in overseas locations for diverse routing in the event of ASC failure or saturation. The overseas ISTs operate in 1200 or 2400 baud single-channel operation. Where two lines are used to connect ASCs overseas, the method of message queuing (A and B channel) is identical to that of the CONUS ASCs.

Subscriber Connectivity. AUTODIN subscribers may be connected directly to one or more ASCs or, in some instances, to an intermediate switch. Each method of connectivity is described in the following paragraphs.

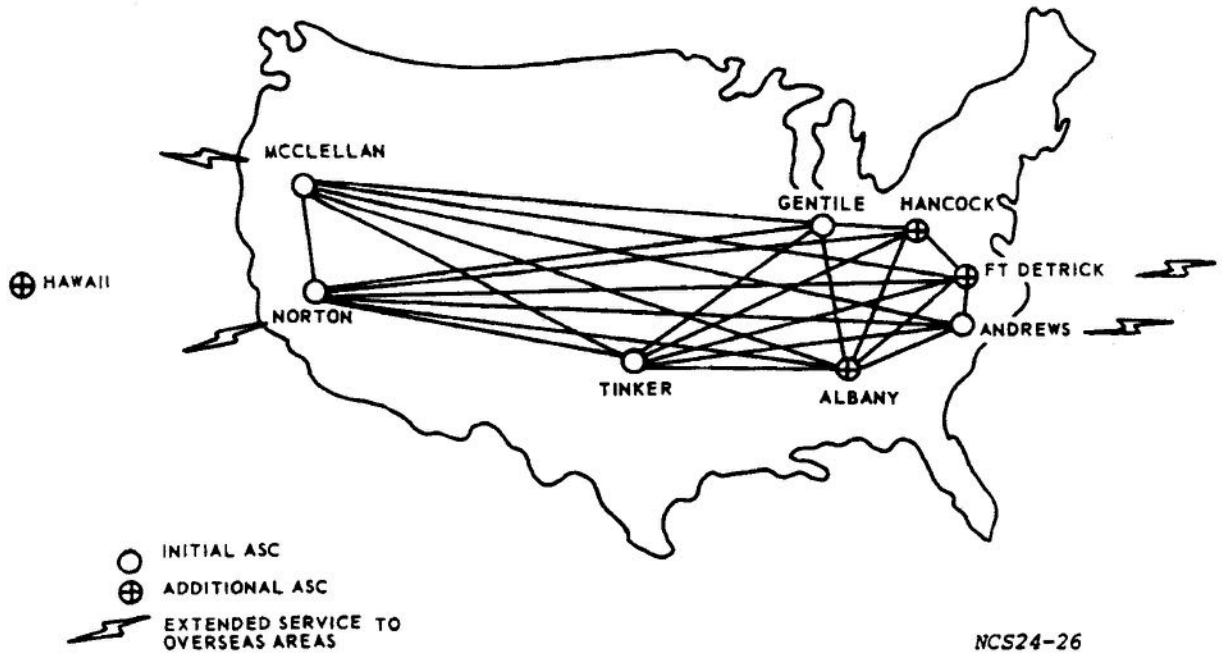


Figure 2-1. CONUS ASC connectivity.

Single home. A subscriber that is connected to only one ASC or intermediate switch is said to be "single-homed." Single-homed tributaries use either leased or Government provided lines for ASC connection (depending on location). This type subscriber is not provided a redundant path or switch connection due to either the priority of message traffic or the mission the subscriber serves. In cases where a single-homed subscriber is connected to an intermedi ate switch, the intermediate switch will normally be dual-homed.

Dual home. Dual-homed subscribers, as the term implies, are connected to two ASCs. This dual connection provides an alternate path for message transmission for the subscriber in the event of line or ASC failure.

Intermediate switch. In locations where an ASC is not in the immediate area of a subscriber or where several low-speed subscribers require access to the AUTODIN system, an intermediate switch is used. An intermediate switch is termed a nonautomatic relay center or NARC. Such terminals provide a collection point for message traffic and interface the AUTODIN system at much higher speeds than the subscriber would operate. This provides a more cost effective method of providing service to low-speed subscribers. Besides, since the number of lines for message switching is limited to 300 lines per ASC, the intermediate switch serves to extend this number.

205. AUTODIN switch services

Community of Interest. At present, the AUTODIN system is serving two different communities. The first, which has been with AUTODIN since its start in 1961, is referred to as the "General Service (GENSER)" or "R-community." The other, known as the Defense Special Security Communications System (DSSCS) or Y-community, began operation in 1972. The ASC message-switching program handles the two communities separately and will not let messages from one community crossover to the other.

YASC Services. The CONUS ASCs have the capability of serving 300 full-duplex lines and provide five types of service: (1) message switching (store and forward), (2) hybrid AUTODIN red patch service (direct user-user), (3) query response, (4) guaranteed sequential delivery, and (5) AUTODIN limited private service.

Message switching unit. The ASC message switching unit (MSU) program processes traffic for store-and-forward delivery according to traffic conditions and the handling precedence assigned by the originator. Proper message headings are generated when delivery to more than one address is required. Machine code and transmission speed conversion are carried out as required to prepare the message for delivery in a form suitable for reception by each individual tributary

station. In providing this service, the ASC does three basic jobs:

(1) Message switching. The message switching function of the system accepts messages from incoming channels of the ASC and delivers them to the proper outgoing channels.

(2) Message processing. Message processing consists of making such code and format conversion as is necessary to make the message compatible with the terminal device receiving them.

(3) Message protection and bookkeeping. The message protection and bookkeeping function makes sure of reliable delivery of the message once it enters the system.

Hybrid AUTODIN red patch service (HARPS). HARPS provides direct user-to-user service through a manual patch made by a technical controller in the AUTODIN patch and test facility (PTF) of the ASC. This service is limited to tributary stations that are high volume users, have compatible equipment, and operate at relatively high speeds. Normally, the tributary stations provided this service operate with the ASC on a store-and-forward basis (MSU). When HARPS is activated, the MSU service of the tributary stations involved is temporarily suspended and direct user-to-user service (HARPS) begins. At this point, the tributary stations involved are transmitting data directly to each other at high speeds without conforming to rigid message format requirements.

Query/response service (Q/R). Query response service lets Q/R terminals access Q/R host computers (data banks) through the AUTODIN system. This service, depending on the length of the Q/R message, will provide responses to queries in a matter of seconds. The high-speed trunk channels of the ASC make the speed of Q/R possible. Q/R service is provided for both the general service and DSSCS communities, and it is available for modes I, II, and V. (Modes are discussed later in this section.)

Guaranteed sequential delivery of multiple segmented messages. This service lets bulk data messages of unlimited lengths be transmitted and received between mode I terminals, with AUTODIN assuring the sequential delivery of each segment of the bulk data message. Thus, with guaranteed sequential delivery, the message length limitation of 40,000 characters or 500-line blocks is allowed to be exceeded.

AUTODIN limited privacy system (ALPS). ALPS operates in the same manner as store-and-forward, except that no record of the message is made on the ASC history tapes. Therefore, the ASC cannot edit or recover a message as in the case of a normal store-and-forward operation. However, journal entries about ALPS messages are made to a history disk. In circumstances where retrieval is necessary, the ALPS program will use journal entries to generate an automatic service to the originating station for retransmission purposes.

ALPS service is available to both GENSER and DSSCS mode I, II, and V terminals that are specifically class-marked in the ASC program for ALPS.

206. AUTODIN modes of operation and subscriber terminal equipment

AUTODIN terminals will operate in one of three standard modes set up for AUTODIN operation. The modulation rates of the various modes of operation are 75, 150, 300, 600, 1200, 2400, and 4800 baud. Tributaries using modulation rates of less than 150 baud are limited in number to prevent traffic overloads resulting from slower rates of input or output. This is particularly true of ASC output. A description of the various operational modes follows. The modes may be block-by-block or continuous as described in the text.

Mode I. This is a duplex operation with automatic error and channel controls allowing independent, simultaneous two-way operation, using synchronous signals. This operation is done by control characters used to acknowledge receipt of valid line blocks or to return error information. A line block consists of 80 characters plus four-framing characters. The terminal (or switching center) responds automatically to these characters by continuing or stopping transmission or by displaying action information to the operator. Examples of terminal equipment using this mode of operation are compound terminals and magnetic tape terminals.

Mode I block-by-block. This is a transmission mode in which a line block (84 characters) is not transmitted until proper acknowledgement is received for the preceding line block. Acknowledgement 1 and 2 (ACK 1 and 2) are used alternately for each correctly received line block. This is done to avoid the loss of a line block during message transmission.

Mode I continuous. In the continuous mode, no pause in transmission is made between line blocks to await acknowledgement. However, if an acknowledgement is not received by the 83rd character of the second of two consecutive line blocks, further transmission is suspended until a reply is received for the first of the two line blocks.

These terminals operate at speeds ranging from 150 to 9600 baud. They offer error control and message-by-message acknowledgement. They may use paper tape, punched cards, magnetic tape, or any combination of these, depending on which model mode I terminal is in use.

Mode II. This is a duplex operation, normally associated with teletypewriter equipment, allowing independent and simultaneous two-way operation. There is no automatic error or channel control; message accountability is maintained through channel sequence numbers and service message actions. There are occasions when equipment is used for half-duplex operations (i.e., one-way send or receive). Mode II uses a continuous method of transmission only and requires no reply from the sender or receiver. This mode uses asynchronous signals in its operation and operates at various low speeds.

Mode V. This is a duplex operation, normally associated with teletypewriter equipment, allowing independent and

simultaneous two-way asynchronous transmission. Control characters are used to acknowledge receipt of messages and display limited information to the operator. Message accountability is maintained through the use of channel sequence numbers for message accountability, with automatic response using control characters, by the distant terminal/switching center (error control is not provided). Transmission is done on a message-by-message basis. Acknowledgements (ACK 1 and 2) are exchanged between the sender and receiver for messages correctly received. The acknowledgements are accepted and processed by a transmission control unit (TCU). The TCU is an integral part of the mode V terminal and will be discussed later in this section.

Most mode V terminals consist of a model 28 automatic send/receive teletypewriter set, model 28 receive only teleprinter, and a mode V TCU. These terminals have no error control.

As mentioned earlier, there are many models of terminals for modes I, II, V. It is your responsibility to understand each subscriber's equipment configuration and operating speed and their terminal's operating characteristics.

207. ASC support equipment

In the text to follow, we will discuss the various pieces of equipment that an AUTODIN tech controller must be familiar with. Your troubleshooting ability in an AUTODIN system will be greatly enhanced by your knowledge of the support equipment used.

Master Station Clock (MSC). The MSC is the single most important item of equipment within the ASC. All timing within the ASC is originated by the MSC.

The MSC is a modular, solid-state, rack-mounted piece of equipment. It has three separate oscillators. Each oscillator is powered by a DC power supply. Battery backup power is also provided for each oscillator.

The three oscillators each have an output frequency of 1.2288 MHz, which is monitored for amplitude, frequency, and phase. The amplitude of each oscillator is monitored by an amplitude detector network. If the square-wave output of the primary oscillator (usually the A oscillator) deteriorates, this detector network will automatically activate selection logic circuitry that will switch to a different oscillator and give a failure alarm indication.

The frequency of each oscillator is stable at 10^{-7} Hz per week. If the drift rate for the primary oscillator exceeds this standard, it will be detected and an alarm will be given. Detection is carried out by a phase comparator that beats the output of each oscillator against the other two oscillator outputs (e.g., A and B, B and C, A and C). If the count difference exceeds seven within a 2-minute period, the selection logic activates and switches oscillators.

The primary oscillator is fed into a triple-redundant binary chain divider, which has 14 stages. Each stage provides one of the 14 output-timing signals provided by the master station clock. The frequency of each stage and associated baud rate is as follows:

Baud	*Receive Timing Output*	*Transient Timing Output*
75	9.6 kHz	75 Hz
150	19.2 kHz	150 Hz
300	38.4 kHz	300 Hz
600	76.8 kHz	600 Hz
1200	153.6 kHz	1.2 kHz
2400	307.2 kHz	2.4 kHz
4800	614.4 kHz	4.8 kHz

Modem. Since most of digital data circuits connected to an ASC are transmitted over lines in a quasi-analog form and the ASC operates pure DC, some conversion is needed. The purpose of a modem is to convert quasi-analog or analog data signals to DC and vice versa. This conversion (within CONUS) takes place before the signal entering the ASC.

Shield Point Isolators. Shield point isolators are used on all circuits coming into and leaving the ASC. Refer to figure 2-2. These isolators are really RF filters used to prevent clear text signals from being inadvertently transmitted from the ASC and to prevent noise or other interference from entering the ASC.

Red/Black Isolators. Red/black isolators are used to isolate timing sources in red (clear text) areas from black (encrypted) areas. They are also used on circuits that do not require encryption and are routed through the red and black areas of the tech control, such as weather circuits.

DC Signal Converters. DC signal converters are used to provide conversion of high-level polar DC circuits to low-level polar or vice versa, depending on the subscribers' needs.

Crypto. There are five encryption devices in use in the AUTODIN system: TSEC/KG-13, TSEC/KG-34, TSEC/KG-84A, TSEC/KW-7, and TSEC/KW-26. All of these, except for the TSEC/KG-84A, are being slowly phased out of AUTODIN by a plan known as the KG-84A replacement program. (In fact, by the time this volume is in print, the replacements may be completed.)

The KG-84A has several distinct advantages over other crypto devices. There is a significant reduction in COMSEC maintenance personnel at the ASCs because of the reduced maintenance required for the KG-84A. Also, units are significantly smaller, a condition that gives added space for other equipment to be installed. Space has become an extremely valuable commodity with today's budget reductions and building limitations. The ability to replace parts at depot level is another advantage that speeds up repairs.

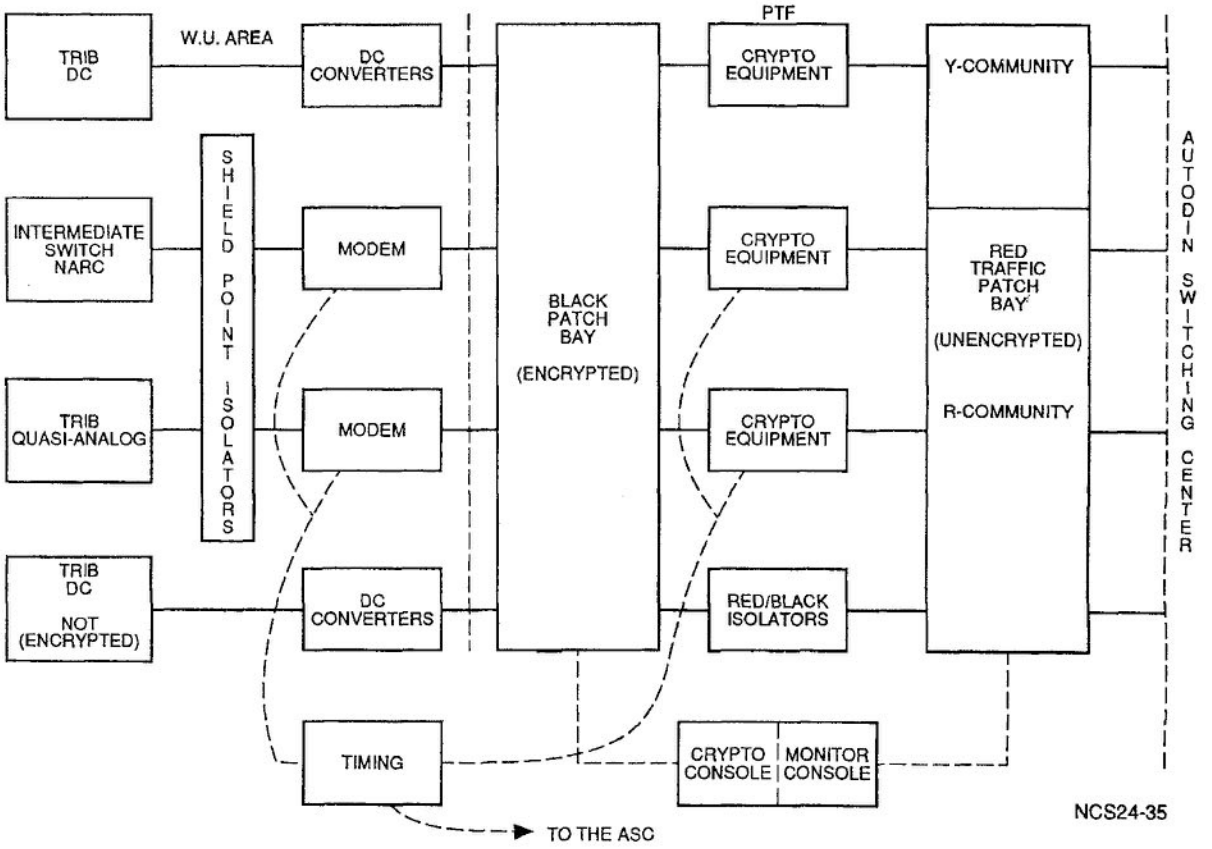


Figure 2-2. CONUS ASC PTS.

208. The AUTODIN patch and test facility

As a technical controller assigned to an AUTODIN facility, you must thoroughly understand how all links in the communications chain interrelate, so that you can swiftly isolate the cause of any interruption of traffic and start corrective action. Continuing efforts to upgrade AUTODIN patch and test facilities (PTF) worldwide have helped make sure that you are afforded every possible advantage in the preventive and corrective maintenance of ASCs. You should strive to learn everything possible about your PTF and its capabilities.

The PTF monitors performance and transmission quality, restores service following equipment failures, and provides manual rerouting for all communications connected to an AUTODIN switch.

The PTF is used for terminating communications lines, for interconnecting links between communication lines and the MSU equipment, and for monitoring and measuring instruments, cryptographic devices, and switching facilities. Monitoring and measuring instruments are used for indicating communications line continuity and signal quality. Cryptographic equipment provides communications security protection.

In CONUS ASCs, the modem area is considered separately from the PTF and is normally located in the Western Union (WU) area (fig. 2-2). Audio terminating and patching facilities are part of the modem area, so only DC lines appear in the PTF. For our discussion, we will use the CONUS AUTODIN PTF configuration.

Malfunctions in the ASC are reported to the PTF for proper action and reporting. The PTF reports directly to the DCA ACOC. The PTF has the capability to patch around faulty equipment to restore communications service to users. After restoring service, the controller will report the faulty equipment to maintenance for repair.

Following are some of the responsibilities of the patch and test facility:

a. Coordinate all trunk and access line outages to the primary TCF or commercial test board.

b. Coordinate with tributary station personnel on problems affecting operation and service.

c. Provide the ASC shift supervisor with details on failures and degradation of service.

d. Maintain a file of all trunks and access lines to include a functional diagram and equipment identification for each circuit.

e. Maintain an equipment list of each tributary in sufficient detail to define all on-line equipment and spare equipment.

f. Establish and assure effectiveness of a quality control program that will include all circuits and associated equipment.

g. Make sure that no security compromises are introduced through patching or equipment substitutions.

h. Maintain a patch-and-test facility log of circuit outages.

209. Signal flow through a CONUS AUTODIN patch and test facility

The functional structure of the communications area is illustrated in the simplified block diagram in figure 2-2. This area links the switching center to outlying stations through the circuits of the DCS AUTODIN system. The PTF is a very important part of the communications structure. Its primary function is to provide high-quality, error-free communications. Follow the signal flow in figure 2-2 as you read the paragraphs below.

Shield Point Isolators. All analog circuits entering the ASC area must enter through a shield-point isolator. The isolators are radiofrequency (RF) filters and prevent noise and RF from entering the ASC as well as preventing decrypted (clear text) signals from emitting from the building. From the isolators, signals flow to a modem.

Modems. The modems modulate/demodulate synchronous and asynchronous signals passing between the switching center and subscribers. Accurate timing is provided to all areas by the MSC. The modems are located in the GTE facility, which is located in the same facility as the PTF.

DC Converter. DC circuits entering the facility pass through a DC converter to convert signals from high to low levels. All DC signals entering the ASC must be low-level polar.

Black DC Patch Bay. All low-level DC signals entering or exiting the ASC PTF must pass through the black DC circuit patch bay. This enables the tech controller to test and/or reroute circuits to spare lines or equipment. This patch bay handles clear text unclassified and encrypted classified traffic.

Monitor Console. The monitor console provides the central point for the control and supervision of the PTF. As a tech controller, you will work and do most of your trouble-shooting at either this console or the crypto console. It provides access to all communications circuits and auxiliary communications (intercom, DSN, base telephone, etc.). The monitor console allows the tech controller to test or monitor both red (unencrypted, classified) and black (encrypted, classified) circuits. Special switches called *red switch* and *black switch* allow only one circuit at a time to be brought up to prevent security violations. The monitor console has dial-up access to an ASR teletypewriter model 28 and has a data analyzer, an intercom panel, and an oscilloscope (fig. 2-3). This unit allows the controller to inject or receive traffic for monitoring or testing purposes. The monitor console is connected so that it can monitor a circuit without interrupting traffic flow, or you may terminate the circuit into the proper test equipment.

Incorporated into the monitor console are DSN trunk lines. These lines are used for dial-up of data grade lines for reroute and restoral purposes. A switch associated with each DSN circuit provides the tech controller with the ability to control DSN circuits from the console.

Figure 2-4 shows three of the displays for the monitor console. Figure 2-4,A, is the protocol setup for a particular circuit. This display gives you information, such as the type code and parity used on the circuit. Once you know this information, you can analyze circuit outages by calling up a traffic analysis display. Figure 2-4,B, is one of the displays used in the PTFs data base. Notice that it is very similar to a DD Form 1441, Circuit Data.

Crypto Console. The crypto console is similar to the monitor console in size and design (fig. 2-3). It is the central point for the control and supervision of the crypto area as it pertains to the PTF. Appearances for 75 encryption unit controls and alarms are installed along with an oscilloscope and character reader.

An audible and visual alarm will activate when a circuit has lost crypto synchronization. This allows tech control to block the input to the ASC immediately and report the loss of sync to crypto maintenance. Tech control can reset crypto units remotely through the use of a crypto auxiliary unit (CAU). The CAU allows three tries for reset; if it will not make sync, then crypto maintenance will have to resync the circuit manually.

Crypto Area. The crypto area has the encrypting and decrypting devices necessary to provide for transmission of classified traffic. The encryption devices provide isolation between the encrypted area and the unencrypted area. When an encryption device is not used, a device called a *red/black isolator* is required.

Red/Black Isolators. Isolators are used for electrical separation between the red and black areas of unsecure (unclassified) traffic and associated timing. These isolators may be either electromechanical relays for low-speed circuits (75 baud) or fiber optic isolators used on circuits with rates higher than 75 baud.

Red Traffic Patch Bay. The output of the encryption devices will appear at one of two red patch bays. In the beginning of this section, we mentioned the communities of interest: the common user (R-community) and Defense Special Security Communications System (Y-community). Because these two signals cannot be intermingled, a special red patch bay was set aside for all Y-community circuits. This patch bay is identical to the one used for R-community traffic except that the jacks used are a different type. Y-community

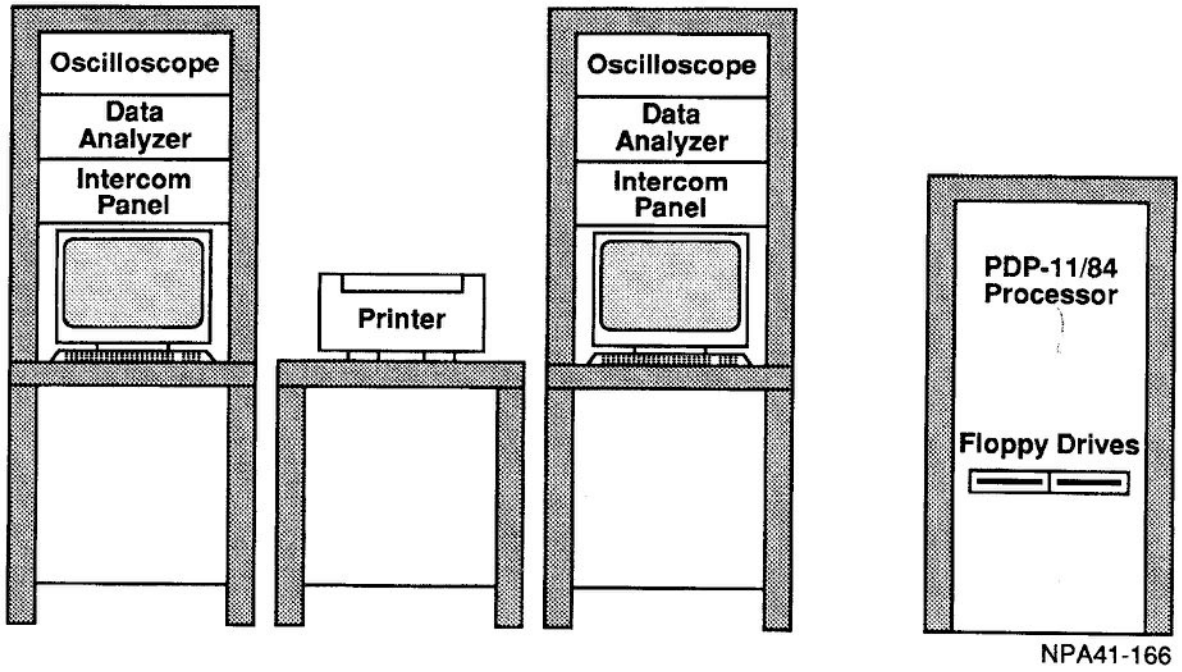


Figure 2-3. AUTODIN PTF and crypto monitor consoles.

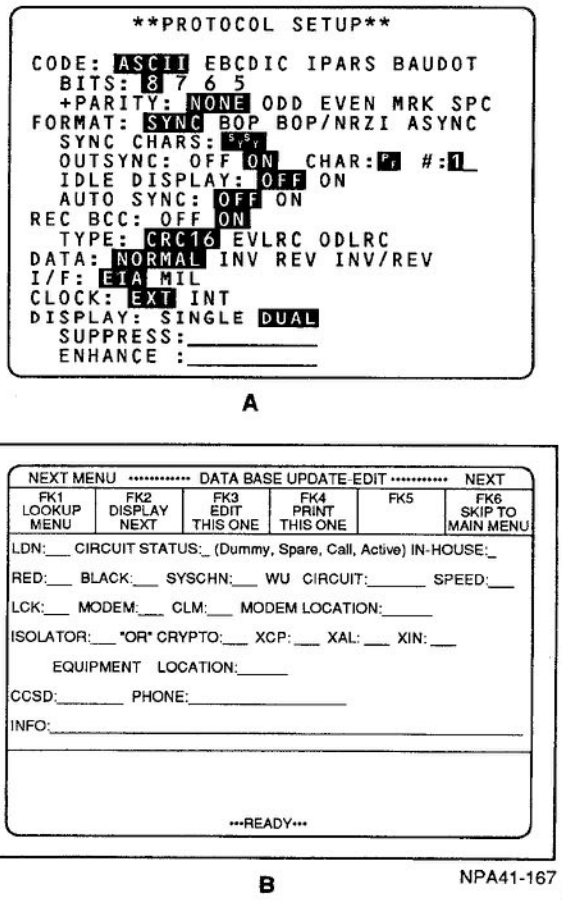


Figure 2-4. AUTODIN PTF monitor displays.

circuits use bantam jacks (miniature), and R-community circuits use normal 310 jacks.

Each send-and-receive data leg can be broken by a cut key in each circuit on the patch bay. Push-to-operate/push-to-release buttons have lamp indicators that light up when they are operating. These cut keys are used to interrupt traffic flow into and from the ASC. From the red digital patch bay, each circuit, depending on the speed, would be connected to a buffer.

210. The AUTODIN terminal concentrator

The AUTODIN terminal concentrator (ATC) is a minicomputer-based system that links the PTF with the integrated circuit communications data processor (ICCDP). Each AUTODIN switch has four ATCs. It also has an ATC switch whose function is to control which of the ATCs is on-line at any given time. An ATC has two primary components, as described below.

Line Termination Unit LTU. The LTU is the termination point for all data channels. Data is transferred to and from the tech control in serial form (bit-by-bit). The LTU gathers the serial bit data and assembles the bits into characters for transfer to the ATCs processor component, the PDP 11/84.

PDP 11/84. The PDP 11/84 collects and distributes messages from and to communications channels, through the LTU, and transfers them to the ICCDP. The PDP 11/84 provides the necessary control characters and intransit storage for data received over communications channels, stores them in memory, converts codes, adds framing characters,

and transfers data in line block form (84 character blocks) to the ICCDP memory for processing.

The PDP 11/84 also exercises control over individual channels by exchanging idle control and framing characters with terminal control units of tributary stations. For mode I circuits, an idle line pattern (fig.2-5,A) is sent when no traffic is being passed. These idles are used to maintain synchronization between terminal equipment and the ASC. Should the idle line pattern drop off, an out-of-sync alarm will appear at the receiving station. Mode II and V circuits use a mark in the idle state.

Framing and control characters are used to regulate the flow of line blocks and/or messages to and from the ASC. Two framing characters appear at the beginning of each line block, followed by 80 data characters and two framing characters, for a total of 84 characters.

Figure 2-5 shows some of the control characters. All control characters are variations of the idle sync pattern. If you were watching the idle sync pattern on an oscilloscope (fig. 2-5,A) and a control character were received, you would see only a blip on the scope as it changed from idle to the control character and back to the idle character again. Control characters are always sent as identical pairs that follow one another. The control characters are broken down into two areas. The transmit control characters are sent by the transmitting station to direct the receiving station to take some action. The receive control characters are those sent by a receiving station in response to transmissions of messages or transmit control sequences. Some of the transmit control characters are:

a. Discard message (DM). This directs the receiving station to discard the message being received. Cancel can also be sent between messages to setup the acknowledgement sequence (fig. 2-5,D).

b. Reply (REP). Directs the receiver to retransmit its last good control character or its current updated response (fig. 2-5,B).

c. Invalid (INV). Sent in response to receiving an unsolicited control character (fig. 2-5,C).

d. Enquire (ENQ). Sent to a distant ASC by another ASC requesting an identification.

Some of the receive control characters are:

a. Acknowledge 1 (ACK 1). Sent in response to a correctly received line block. Used alternately with ACK 2 (fig. 2-5,F).

b. Acknowledge 2 (ACK 2). Same as ACK 1. ACK 2 is the only correct response to a received cancel control character (fig. 2-5,G).

c. Negative acknowledgement (NACK). Sent in response to an errored line block (fig. 2-3,H).

d. Reject message (RM). Sent to reject an incoming message. The only proper response to a received RM is a cancel (fig. 2-5,D).

e. Wait before transmitting (WBT). Sent by a receiving station to prevent the transmitter from continuing to send traffic (fig. 2-5,E).

211. The integrated circuit communications data processor

The ICCDP is a large special-purpose computer that does the message-switching function of the ASC. Two ICCDPs are used in the ASC, one to do the on-line message-switching operation and the other in a standby state. The standby ICCDP will automatically assume on-line operation should the on-line ICCDP fail. The standby ICCDP can also be used to do various off-line routines and maintenance functions.

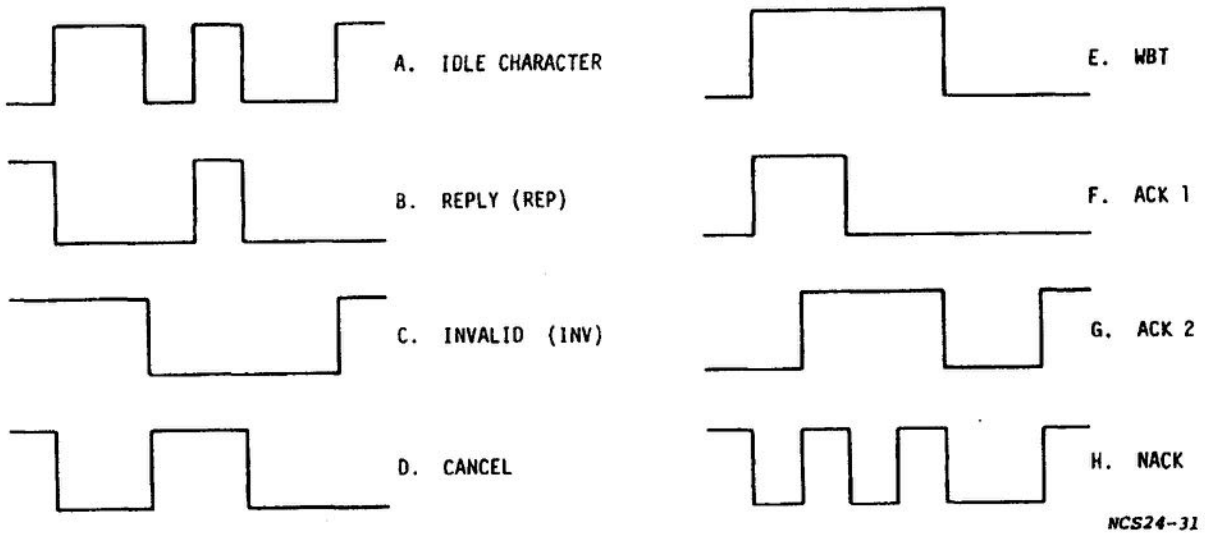


Figure 2-5. Control characters.

The main functions of the computer are:

a. Gathers line blocks of messages from the ATC.

b. Determines switching (routing) of messages.

c. Stores messages on the expanded memory support system (EMSS).

d. Retrieves messages from the EMSS as required for transmission and distributes them to the proper ATC output zone.

e. Does the required checking to guarantee complete and accurate transmission.

Three of the main components of the ICCDP are the high-speed memory (HSM), basic-processing unit (BPU), and transfer channels (TC).

The *high-speed memory* is a random-access, magnetic-core storage area for instructions and data. Because of limited size of this memory, only messages being processed for input/output are held within. If, for some reason, the message cannot be delivered, it is placed on an external storage device for later processing.

The BPU transfers data to and from high-speed memory and executes instructions from a computer program. This unit also controls transfer of data to and from the input/output devices. Because of the very high speed of the high-speed memory and the relative slowness of the peripheral devices, buffering action is necessary. This is the function of the transfer channels.

The *transfer channels* provide the means by which the computer can access several peripheral devices simultaneously and continue internal processing. This is necessary, since the computer is a high-speed device and the peripheral devices are relatively low-speed devices.

There are three peripheral devices associated with the ICCDP—the operator's console, the high-speed paper tape reader, and a monitor printer. The operator's console is used for monitoring the program internal to the ICCDP and for troubleshooting. Its control and visual displays are used mostly by maintenance personnel and not for general operation of the system.

212. Uses of the system console and the ASC service section

System Console. The systems console is the focal point of on-line system operation. Through displays, alarms, indicators, and on-line program printouts, the operator is kept informed of all happenings in the on-line system operation. The systems console also controls the standby ICCDP and, through its automatic switch monitor (ASM), signals the standby ICCDP to assume the on-line function should the normal on-line ICCDP fail. The systems console command switches associated with each ICCDP let the operator initiate various command instructions to the on-line program.

Essentially, the systems console is a monitoring and control device that provides the interface between operators and the on-line program. Through the systems console, operators are informed of the conditions encountered by the program in the processing of message traffic and the operation of the various peripheral devices associated with the on-line system. Based on information received from the system in program printouts and status displays at the systems console, operators insert commands through the systems console switches to make changes to the system operation. The operator at this console will work very closely with the PTF relaying information regarding alarms and the status of circuits.

ASC Service Section. The ASC service section handles various service queries from subscriber stations about transmission, etc. Also, courtesy copies of automatic service messages generated by the on-line ICCDP are sent to the service section for reference purposes. An automatic service message is generated when an incoming message is not correctly formatted. The service section also processes originating and terminating message traffic for the various staff elements of the center. To do these functions, the service section incorporates the following terminal equipments:

a. Digital subscriber terminal equipment (DSTE). The DSTE is a modular terminal that provides both card and paper tape capability and operates at 300 baud.

b. Mode V terminal. This unit provides for the transmission and reception of messages in paper tape format and operates at 75 baud.

213. The signal flow through the AUTODIN switching center

The sequence of events that takes place as messages process from a tributary station through the ASC may be followed by correlating the numbered paragraphs below with the numbered blocks of the block diagram (fig. 2-6).

(1) The message is prepared at the tributary in proper media (card, paper tape, or magnetic tape) and placed in the reading device. The characters of the message are then read to a control unit, which converts them from the native code of media being used to a line transmission code. The signal is then sent from the control unit in DC form to cryptographic equipment. The encrypted signal then enters modulation equipment, which converts it from DC to audio for transmission over the communications medium to the ASC.

(2) The audio signal enters a shield point isolator at the ASC to prevent noise and radiofrequency interference (RFI) from entering the ASC. From the shield point isolator, the signal enters the demodulation equipment (modem) at the ASC, where it is converted from audio to DC.

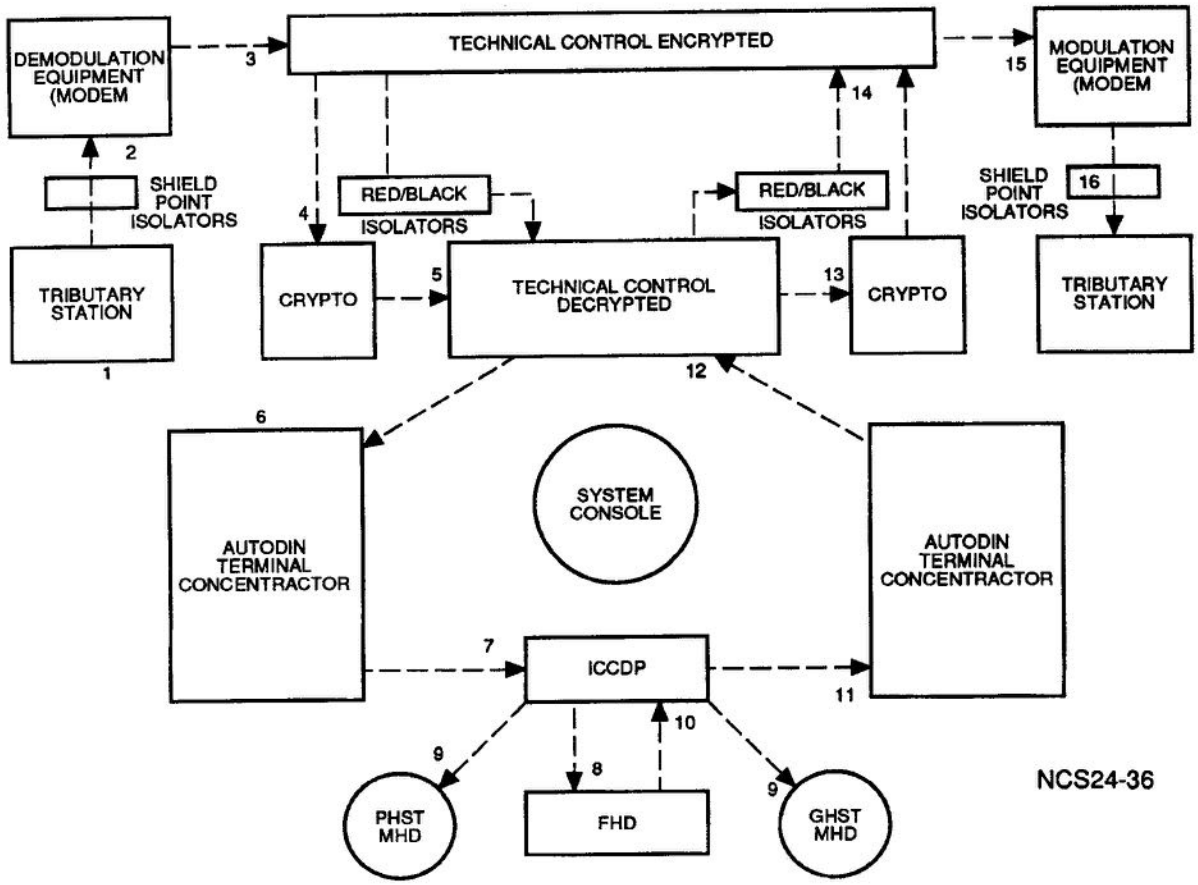


Figure 2-6. Block diagram of message path.

(3) The signal then enters the technical control encrypted side, where it can be monitored for quality at the black patch bay.

(4) Following this, the signal enters the crypto facility, where it is decrypted for acceptance into the system. If the signal is unclassified, it passes through a red/black isolator to provide electrical separation in place of an encryption device.

(5) After decryption, the signal enters the technical control decrypted side, and again the signal can be monitored and measured for quality.

(6) The signal now enters the ATC in serial form (bit-by-bit) and is accumulated until a character is formed. It is converted from line transmission code to extended field data code (ASCII) and stored to the input zone of the data magnetic core memory assigned to the channel. This process is repetitive for each character being transferred until a complete line block (84 characters) has been received and stored by the ATC. The line block is now checked for correct parity and, if correct, an acknowledgement (ACK 1 or 2) control character is sent to the control unit of the tributary station. On receipt of an ACK, the control unit will commence sending the next line block of the message. In the event the block is received with bad parity, the ATC will send an error control character instead of the acknowledgement, thus causing the control unit to retransmit the same block over again. If the error situation persists after three tries at automatic block retransmission, an alarm is activated at the systems console of the ASC. After enough line blocks have accumulated in the input zone of the ATC, they are transferred to the ICCDP.

(7) The line blocks transferred from the ATC are stored in the high-speed memory input/output buffer of the ICCDP, and the input-processing program begins. The input program validates the message header for accuracy. If the header format is incorrect, the ICCDP will instruct the ATC to send an reject message (RM) to the control unit of the tributary station. On receipt of the RM, the control unit will activate an alarm, necessitating operator intervention to correct and retransmit the message. If the message passes header validation, routing indicator processing begins. The program now checks the routing indicator against a routing indicator table stored in the high-speed memory for validity. In the event the routing indicator fails the validity check and the message is single-addressed, the ATC will be instructed to issue an RM signal as in the case of incorrect header format. In circumstances where the message is multiple-addressed and at least one routing indicator passes the validity check, the program will accept the message and process the valid

routing indicators. On those routing indicators that failed the validity check, an automatic service message will be generated by the program and sent to the tributary station advising that the message must be retransmitted only to those routing indicators that were found to be incorrect. After all input processing has been completed, the message line block segment is then transferred to the fixed-head disk (FHD) for storage.

(8) The message line block segment is now written into an area of the disk called a *chunk*. A message, depending on its length, may require one chunk or up to 72 chunks, as in the case of a 500-line block message. When the message has been completely received and stored on the FHD, it is retrieved, a chunk at a time, and transferred to the ICCDP for output processing.

(9) As the message segment is being stored and retrieved from the FHD, two history moving head disks (MHD) are simultaneously being written for file record purposes. These are the prime history moving head disk (PHST-MHD) and the ghost history moving head disk (GHST-MHD). The history MHDs contain such information as the actual message line block segment, the time the message entered the system, the time the message was transmitted out of the system, and various other statistics.

(10) The message line block segment is transferred from the FHD to the high-speed memory input/output buffer of the ICCDP, and the output-processing program begins. The output revalidates the message header to make sure nothing went wrong while the message was stored on the FPD. Should the validation program find an error, the message will be scrubbed. On completion of output processing, the message line block segment is transferred to the ATC.

(11) The message line blocks transferred from the high-speed memory input/output buffer are stored in the data memory output zone assigned to the channel. The ATC then extracts the data from the output zone on a character-by-character basis, converts codes by converting each character from ASCII to the proper line transmission code. When a line block has been transmitted, the ATC waits for an ACK from the control unit of the tributary station before transmitting the next line block of the message. In the event the control unit answers with an error control character rather than an acknowledgement because of bad parity, the ATC will automatically retransmit the same line block once again. If this is done three times on the same block, the ATC will cause an alarm to be activated at the systems console.

(12) The signal now enters the PTF decrypted side, where it can be monitored and measured for quality at the red patch bays..

(13) The signal then enters the cryptographic facility, where it is encrypted.

(14) After encryption, the signal reenters the PTF encrypted side and again can be monitored and measured for quality at the black patch bays.

(15) Leaving the PTF, the signal enters the modulation (modem) equipment, where it is converted from DC to audio. On the analog side of the modem, it passes though a shield point isolator to prevent clear text signals from emitting from the ASC.

(16) The signal is then sent through the serving TCF and applied to a communications medium. While in the TCF, the encrypted signal is monitored, but the TCF does not have the monitoring control that the PTF has.

(17) The signal is then transmitted to the tributary station through the communications medium.

Please write your response to unit self-test questions and then check the text answers at the end of the unit.

SELF-TEST QUESTIONS

204. ASC connectivity

1. How is an ASC connected to other ASCs?
   inter switched trunk

2. What is the purpose of redundant lines?
   message protection in the event of a failure

3. Define the term "AUTODIN matrix."
   interconnectivity of all ASCS so the system will not degrade

4. What is a single-homed subscriber?
   subscriber mission & message priority

5. Determination of single- or dual-homed connection depends on what factors?
Subscriber mission & message priority

6. A subscriber can be connected by three methods to an ASC or ASCs. What are they?
single-homed, dual-homed, & intermediate switched

7. What is the purpose of an intermediate switch?
provide collecting point for message traffic & to interface the ASC at higer speeds

205. AUTODIN switch services

1. What are the five types of service provided by CONUS ASCs? message switching hybrid autodin red patch service,

2. What are the three basic functions of the AUTODIN switching centers? message switching, message processing, message protection & bookeeping

3. What basic function of the AUTODIN switching center permits messages from one community of interest to be transmitted to another community of interest?
message programming ✓

4. Define query/response service.
allows Q/R terminals to access Q/R host computers through the autodin system.

5. What is the purpose of guaranteed sequential delivery? This allows bulk data messages to be transmitted & received in sequential order.

6. Describe the hybrid AUTODIN red patch service (HARPS). a patch provides direct user-to-user service.

7. What is the difference in operation between the AUTODIN limited privacy system and normal store-and-forward service? store & forward system keeps a record of each message on a history tape for recovery.

206. AUTODIN modes of operation and subscriber terminal equipment

1. Differentiate between block-by-block and continuous operation. block by block must recieve an acknowlegement.

2. Name the three modes of operation used in AUTODIN.
modes I, II, V

3. Differentiate between mode II and mode V operation. mode II can operate fdl or half duplex
mode V operates full duplex

4. What are the advantages of mode I operation?
mode I allows independant & simultaneously

5. What are the disadvantages of modes II and V?
mode II has no automatic error detection
mode V has only partial channel control

207. ASC support equipment

1. What is the single most important item of equipment within the ASC? Master Station Clock

2. How does the frequency alarm detection circuitry work in the master station clock?
detection is accomplished by a phase comparator that beats the output of each oscillator

3. What device is located in the TCF area to convert analog signals to digital signals and vice versa?
MODEM

4. What is the purpose of the red/black isolators?
provide electrical isolation of clear text traffic from black areas to red areas to prevent security violations

5. When would we use a DC signal converter?
Convert a DC signal from high to low-level polar.

208. The AUTODIN patch and test facility

1. What type of rerouting service does the AUTODIN PTF provide? manual

2. What two facilities are located within the modem area of the AUTODIN PTF?
Audio terminating & patching facilities

3. In the event of a communications outage, who does the AUTODIN report PTF directly to?
DCA ACOC

4. Which section does the AUTODIN PTF have to coordinate with on all trunk and access line outages?
Primary TCF or Commercial test board

209. Signal flow through a CONUS AUTODIN patch and test facility

1. What devices provide isolation and prevent noise and RF from entering the ASC?
   Shield pair Isolators

2. What is the purpose of the DC converter on low-speed teletypewriter circuits?
   convert high level polar signals to low level & vise versa

3. What is the purpose of the monitor console?
   central point for control & supervision at the RPTF.

4. On the monitor console, what keeps red circuits separate from black circuits? Red or Black switch allows only one type of circuit to be brought up at a time

5. Name three types of test equipment located on the monitor console. O-scope, data analyzer, & intercom panel

6. The extra AUTOVON lines located in the RPTF are for what purpose? Reroute & restoral

7. What is one cause of an alarm on the crypto console?
   Loss of crypto sync

8. What component allows the controller to reset crypto units remotely when synchronization is lost?
   CAU

9. What is the purpose of red/black isolators?
   provide electrical isolation between red & black areas

10. Why are cut keys used on the red digital patch bay?
    Interupt traffic flow to & from

11. What is the purpose of having a red digital patch bay using bantam jacks and another using standard 310 jacks? seperation between R & Y community traffic.

210. The AUTODIN terminal concentrator

1. What does the AUTODIN terminal concentrator do?
   links tech control with ICCP

2. What are the two primary components of an ATC?
   An LTU & a PDP 11/84

3. How does a PDP 11/84 exercise control over individual channels? exchanging idle control & framing characters

211. The integrated circuit communications data processor

1. What is the main purpose of the ICCDP?
performs message switching function of the ASC

2. List the five main functions of the ICCDP.
Gathers line blocks of messages, determines routing of messages

3. Name three main components of the ICCDP.
High speed memory

4. List three peripheral devices associated with the ICCDP. operators console, high speed paper tape reader & monitor printer

212. Uses of the system console and the ASC service section

1. What is considered the focal point of the on-line system operation? systems console

2. In what capacity does the systems console function when it is providing interface between the operator and the on-line program? monitoring & control devices

3. What is the purpose of the ASC service section?
handles requests for message transmission, tracer action, & duplicate transmissions

4. What capability does the DSTE provide for the ASC section? card & paper tape

5. What is the purpose of the mode V terminal in the service section? provides for the TX & RX of messages in paper tape format at speeds of 75 baud

213. The signal flow through the AUTODIN switching center

1. What device is used on the analog signal at the ASC to prevent RFI from entering the switch?
shield point isolator

2. What device is used in the patch and test facility to provide electrical separation for clear text (unclassified) traffic? Red/Black isolator

3. What signal format is used at the ATC?
Serial

4. To where are the signal line blocks transferred after they leave the ATC?
ICCDP

5. What device is used in the ASC to do code conversion?
ATC

6. Where are the line blocks coming from the ATC stored for the processing in the ICCDP?
High Speed memory

7. What happens to a message if a validation error is found at the output buffer of the ICCDP?
not forwarded anyfurther

8. What happens when the ATC is requested to retransmit the same line block three times to the subscriber due to errors?
alarm will be activated at console

2-2. Defense Data Network (DDN)

In September 1981, the Director, Defense Communications Agency (DCA), initiated a study to assess the capabilities of the automatic digital network (AUTODIN II) and to evaluate a plan for an alternate network that could be used in its place. The purpose of the study was to describe a world-wide survivable, common-user, long-haul data communications system. After considerable evaluation, it was decided that packet switching technology was more attractive to the government than the AUTODIN II technology.

On April 2, 1982, the Department of Defense (DOD) directed DCA to proceed with the development of DDN, the designated DOD common-user data communications network using the packet switching technology. This development has been ongoing since then with a gradual building process taking place.

The following discussion is based on the most current information available on the Defense Data Network. The DDN is an extremely dynamic program with changes occurring on a daily basis. The network configuration, equipment, and software peculiarities at your location may vary somewhat from the material presented in this unit of instruction.

214. How packet switching was integrated into the Defense Data Network

Advanced Research Projects Agency Network (ARPANET). The first packet switching network (military or civilian) was designed under a 1969 Defense Advanced Research Projects Agency (DARPA) Research and Development (R&D) Program and was named the ARPANET. At first, the ARPANET was purely an experimental network, chartered to advance the state-of-the-art in computer resource sharing. It was designed to provide efficient communications between dissimilar computers so that hardware, software, and data resources could be shared conveniently and economically by a wide community of users. As the first R&D goals of the network were attained, users with operational needs rather than experimental needs began to use it.

By 1975 there were many operational users of the network, so responsibility for its operation was transferred to the Defense Communications Agency (DCA). In 1983, DCA divided the ARPANET into two separate networks, the MILNET and the ARPANET, thereby acknowledging the changing nature of the military communications environment and forming the unclassified segment of the DDN. ARPANET technology is the packet switching technique used in DDN.

Evolution of Military Packet Networks. Packet switching is a method for handling data as it is transmitted through a communications network. The switching nodes to which subscriber computers are attached subdivide information streams into small packets, then route and otherwise handle each packet as if it were a separate message, correctly reassembling the packet data at its destination.

Each packet switching node (PSN) receiving a packet from a neighbor node checks for errors and, should an error be found, requests retransmission from the neighbor until the data is received correctly. The node then either sends the packet to another node or delivers the packet directly to the addressee.

The more advanced packet switching networks, such as the DDN, route packets adaptively instead of using predetermined paths. With predetermined routing, data cannot be easily sent if any network component fails in the path over which the data must pass. With adaptive routing, switching nodes avoid portions of the network that are congested or damaged.

Packet switching is particularly well-suited to military data communications and was developed specifically for

computer communications. It can support the real-time communications required by computer systems and can provide high levels of circuit use. Furthermore, because packet switching nodes typically operate without an attendant, and because they are small, reliable, and inexpensive, they can be installed in large quantities and at many locations, thus providing greater survivability. Because of these characteristics, packet switching has been implemented in several military and commercial networks.

215. Defining the classified and unclassified segments of the Defense Data Network

Classified Segment. The DDN is composed of a classified and an unclassified segment. The DDN program objective to integrate several classified networks into one classified segment is in the developmental stage. When DDN is fully implemented, user traffic will be protected by KG-84As on the interswitch trunks (IST) as well as all host and terminal access lines. A host access line is connected to a computer that may have any number of terminals attached to it, maybe a network of terminals. On the other hand, a terminal access line would be just that, an access line connecting one individual terminal.

The classified segment is made up of three distinct subnets. These subnets are DSNET1 (Defense Secure Network) for processing secret data, DSNET2 for processing Top Secret WWMCCS data, and DSNET3 for processing Top Secret/SCI data. These networks are working separately at present but eventually will be integrated together and will be known as DISNET. These networks were formerly known as:

a. DSNET1—DDN Integrated Secure Network (DISNET).

b. DSNET2—The Worldwide Military Command and Control System (WWMCCS) Intercomputer Network (WIN) Communications Subsystem (WINCS).

c. DSNET3—Sensitive Compartmented Information Network (SCINET).

With the introduction of *BLACKER* technology, the three separate classified subnets will be merged into a single multilevel secure classified network (referred to as DISNET). BLACKER equipment has some bugs to be worked out and is not fully available at this time.

BLACKER is an encryption device that will encrypt from host-to-host. This means the data will (except for the routing information) be encrypted out of the user equipment and will again be encrypted by KG-84 crypto before entering the system. So the data undergoes double encryption.

Unclassified Segment. The unclassified segment is known as the military network (MILNET). User traffic on the unclassified segment is protected by KG-84A encryption devices on both the ISTs and host access lines. Terminal access lines are protected by low-cost encryption and authentication devices (LEAD). Foldout 1 shows the MILNET worldwide topology.

It is expected that, after the classified portions of DDN merge together, the unclassified MILNET will eventually merge with them. This will produce one all-encompassing network for all digital traffic.

Security and Privacy. The DDN safeguards the security of traffic by using link and end-to-end encryption and by taking physical and procedural security measures. User traffic on the unclassified segment cannot use the resources of the classified segment; however, NSA gateway devices may be used to let classified networks use the resources of the unclassified segment.

A gateway, as the name implies, is a point at which one network (e.g., DSNET1) may enter another network such as MILNET. In order for this to be possible, however, an internet protocol must be available for use in a subscribers system.

Each subscriber access line to the classified segment will operate at a single, system high-security level; for example, Secret or Top Secret. Furthermore, the lines from subscribers handling special categories of Top Secret, such as SCI and SIOP, will be secured separately from other Top Secret traffic.

End-to-end encryption devices will keep the traffic of different security levels or communities of interest separate. Thus, through end-to-end encryption techniques, each network user will be able to communicate only with other users belonging to the same subscriber community; that is, those users who have and use the same cryptographic key. For instance, if DSNET1 uses key A and the MILNET uses key D, they will not be able to de-encrypt the data from each other. MILNET will only be able to de-encrypt data from other MILNET hosts using key D.

Network Monitoring and Control. Fault diagnosis and system maintenance isolation for the DDN is controlled by network monitor centers (MC). There are regional MCs in Europe, the Pacific, and the continental United States for the MILNET, and MCs for every other separate network. Each MC has a minicomputer with special applications software. The personnel at the MCs monitor the status of the network, do fault isolation and diagnosis, and support hardware and software maintenance of the packet switches, TACs/NACs and other network-provided components.

216. Interoperability of subscriber systems

Interoperability. First of all, what do we mean by interoperability? Interoperability is the ability to transfer meaningful information between equipment produced by different vendors (e.g., IBM to Burroughs). Computers work very well when connected to other computers like themselves, but not when connected to computers using a

different language format. Suppose you call a random phone number in Germany, you do not know German, and whoever answers the phone does not know English or any of the other languages in which you are conversant. You will not be able to converse; to put it another way, you will not have interoperability.

DOD standard protocols used by subscriber host computers to achieve interoperability are shown in figure 2-7 and described below.

(1) X.25 is the standard network access protocol for new subscribers.

(2) DOD standard transmission control protocol/internet protocol (TCP/IP) permits the end-to-end flow of data between two computer systems or between a host system and a terminal access controller (TAC) or network access controller (NAC).

(3) Telnet is a virtual terminal protocol to which traffic from different terminal types is converted, resulting in the use of a common virtual terminal format throughout the system.

(4) File transfer protocol (FTP) is a protocol that enables files to be transferred between computer systems.

(5) Simple mail transfer protocol (SMTP) is a protocol that supports the reliable and efficient transfer of electronic mail over a network.

Not all DDN terminals will have these protocols. The protocols used will depend on the needs of each subscriber. For example, some subscribers will not need to use any other network than the one they are presently tied to. Therefore, an internet protocol (IP) would not be required. If electronic mail is not required, SMTP will not be used, etc.

DOD Protocol standards to interoperability. Office of Secretary of Defense (OSD) policy requires host systems to implement at least one of the DOD standard protocol suites, i.e., military standard protocols or protocols specified by the Government open systems interconnection profile (GOSIP) (Federal Information Processing Standard 146). The DDN supports connection of user systems with either protocol suite. Since GOSIP does not provide a full set of protocols and the standard is relatively new, the network provides greater services for the military standard protocols than the GOSIP protocols, e.g., GOSIP does not specify a virtual terminal protocol. Plans are underway to provide interoperability between the two suites and to provide support to GOSIP protocols that is equal to that provided for military standard protocols.

Besides the use of standard protocol suites, subscriber systems must provide compatible applications programs that make use of the standard protocols.

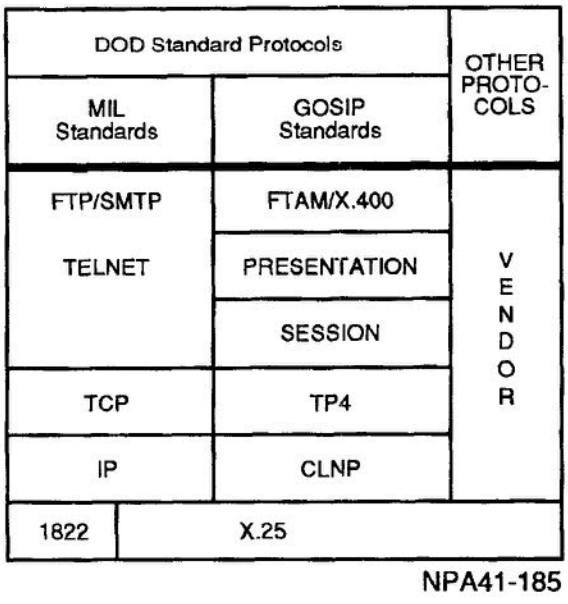


Figure 2-7. Protocols Supported by the Defense Data Network.

217. What are the performance characteristics of DDN?

Undetected Bit Error Rates. For DDNs purposes, communications errors are any errors caused by access lines, trunks, or switching nodes and TACs. The network is designed to decrease the communications errors by use of error detection and correction mechanisms. A cyclical redundancy check (CRC) of 16 bits is associated with host messages on access lines and packets on trunks to deal with the burst errors that typically occur. A 16-bit checksum is also used on an end-to-end basis within the switch subnetwork.

To protect against memory failure in the switches, error detection and correction hardware is used. An added protection mechanism used in the switches is the checksumming of critical data structures and portions of the data code before transmission.

The total user-to-user undetected bit error rate depends upon the network protocol access scheme of the user. In all cases, though, the performance exceeds the undetected bit error rate requirements defined for AUTODIN II A.

Misdelivery. DDN is designed to deliver data units according to the addressing information specified to the originating switch by the originating subscriber. Misdelivery is defined as the delivery of a data unit in violation of the originally specified addressing information. DDN misdelivery analysis shows a better host-to-host delivery rate than AUTODIN II A.

Availability. DDN is designed for essentially continuous operation to support real-time handling of all user traffic. The network provides an availability of at least 99 percent to any pair of single-homed users that want to communicate with each other. This includes all network components between the source and destination host or terminal.

Users have the capability to enhance network availability either by dual access (two access lines to the same switching

node) or by dual-homing (a single access line to two switching nodes). Dual-homed subscribers have a network availability of at least 99.95 percent.

Precedence and Preemption Capabilities. DDN assigns the proper precedence and preemption mechanisms depending on the user priority levels. The mechanisms operate so that higher priority users are assigned scarcely used network resources ahead of lower priority users. Also, portions of the system resources, such as TAC input buffers, are reserved to guarantee availability to high-priority users.

Originating hosts and terminals define their traffic by one of four precedence levels. These precedence levels are used by the switching nodes and TACs as a criterion in the processing and transmission of communications traffic. Category I (flash and flash override) traffic is given the highest precedence and is processed without being preempted. The other three precedence levels are:

(1) Category II (immediate).
(2) Category III (priority).
(3) Category IV (routine).

The precedence and preemption capabilities of the DDN allow the network to cope with system failures and surges in traffic and to respond efficiently to critical users while under peacetime or stress conditions.

Survivability. The DDN is a highly distributed network with adequate built-in features to make sure of its survivability. The principal survivability features are summarized in the following paragraphs.

Redundancy. Eventually there will be over 200 fixed packet switching nodes (PSN), nine fixed Network Monitoring Centers (NMC), and five mobile reconstitution nodes equipped with an NMC capability. Critical users are dual-homed to the network, through many interconnected trunks, to provide redundancy at all possible points in the network.

Dispersion. The switching nodes are widely dispersed over the network and, whenever possible, located away from primary target areas.

Dynamically adaptive routing. DDNs routing procedure automatically routes traffic around congested, damaged, or destroyed switches and trunks and allows the system to keep on functioning over the remaining portions of the network.

Graceful degradation. The high degree of active redundancy coupled with the ability to automatically monitor the status of switching nodes, trunks, and access lines, enables the DDN to degrade gracefully when a few of transmission paths, switching nodes, or monitoring centers are down. In fact, a person using DDN will, most likely, notice little or no difference in the quality of a path if trouble occurs somewhere in the system.

Precedence and preemption. The four-level capability discussed earlier allows the network to provide continuous service to critical users during stress periods.

Hardening and HEMP protection. Communications is affected by the degrading effects of nuclear and electronic warfare emissions. To provide a degree of shielding, all DDN hardware is high-altitude electromagnetic pulse (HEMP) protected with EM shielding and with line isolation and surge-arresting protection. Too, selected node sites are on the uninterrupted power supply (UPS) system to provide continuous operation during power surges or failures.

Reconstitution. To make rebuilding easier during postattack periods, DDN will eventually include five mobile reconstitution nodes equipped with an NMC capability. These elements will be prepositioned in nontargetable areas to rapidly replace a damaged or destroyed node or NMC.

218. The packet switching node (PSN)

At the heart of the DDN backbone network are over 200 PSNs located at about 100 locations around the world known as node sites. It is these PSNs (fig. 2-8) that make packet switching in the DDN possible. The primary function of the PSN is to store and forward message packets between host users, other PSNs, or network gateways.

A PSN, sometimes called an interface message processor (IMP), is a Bolt, Baranek and Newman (BBN) C/30 or C/30E microprogrammed minicomputer designed for unattended, highly reliable operation. A PSN terminates trunk circuits, called interswitch trunks (IST), with transmission rates of 9600 to 56,000 bps. It provides the sequenced functional capabilities to receive, transmit, and control data between attached devices to include:

a. Terminal Access Controllers (TAC).
b. Mini-TACs.
c. Host Front End Processors (HFEP).
d. Terminal Emulation Processors (TEP).

These devices are connected to the switching nodes using either X.25 or ARPANET (1822) access protocols. These devices will be covered in more detail later. But first, let's take a closer look at the PSN.

Figure 2-9 shows the front of the PSN. Refer to the figure as we discuss each portion of the PSN.

Cassette Drive/Control Panel. The cassette drive/control panel is located in a recess at the top of the PSN. The control panel has several controls and an indicator light.

Cassette drive (cassette loader and drive). Loads the software cassette tape. The cassette tape should remain in the loader at all times.

Tape motion (indicator light). Indicates when the tape in the cassette drive is being read or rewound.

Power (push button switch and indicator). Turns the PSN on or off. When the PSN is off, pressing the POWER switch once will turn it on. Pressing the POWER switch again will turn the PSN off. The POWER switch should be left on at all times.

The node site coordinator (NSC) should be aware that the POWER switch may be enabled or disabled by the processor rack power distribution unit (PDU) on and off switch. If the

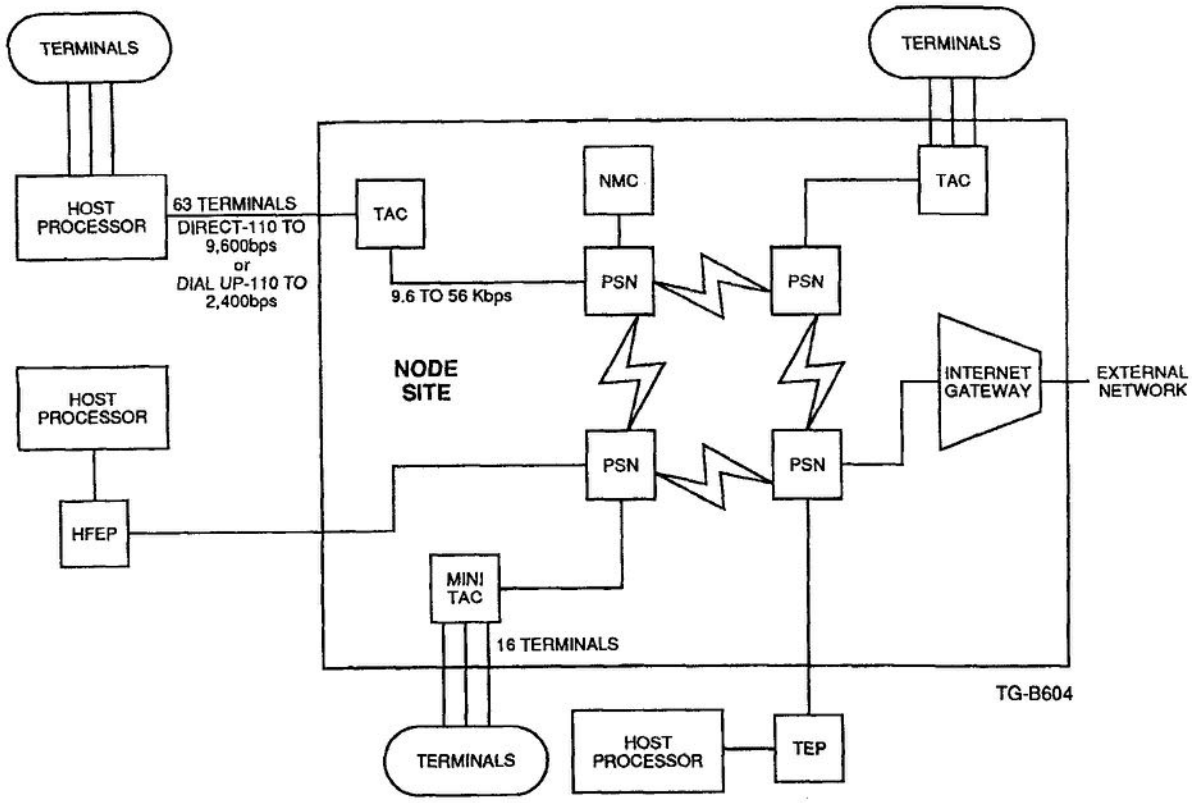


Figure 2-8. DDN node site connectivity.

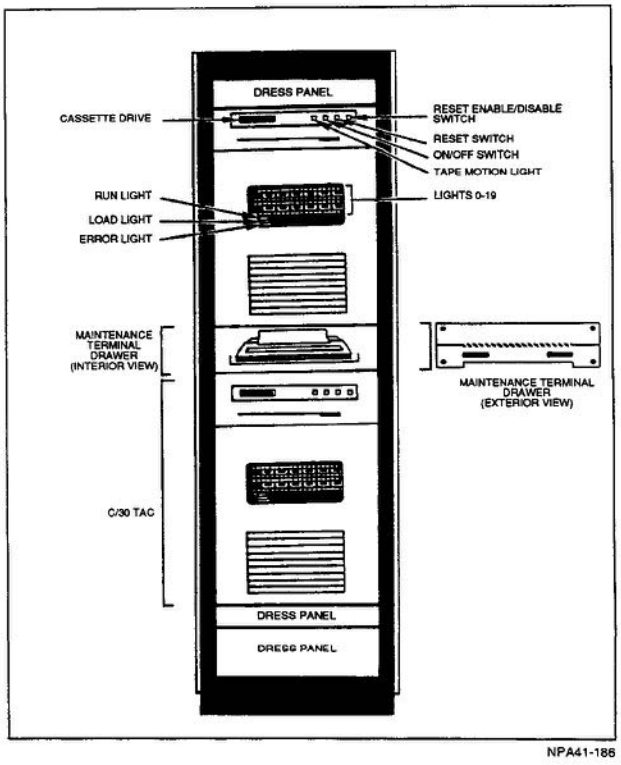


Figure 2-9. PSN front panel features.

PDU switch is set to on-remote, the push button switch located on the PSN front panel will control power to the PSN. If the PDU switch is set to on-local, the NSC will have to use the PDU on and off switch to control PSN power.

Reset (push button switch). Resets the PSN. Pressing this button causes the PSN to reset, clearing all memory, rereading its software cassette tape, and then requesting a software reload from a neighboring node. This button should *NEVER* be pushed unless directed by the MC.

Reset enable/disable (key switch). Enables or disables the reset switch on the front panel. This switch is used as a safeguard to prevent the inadvertent resetting of the PSN.

Light Panel. The PSN light panel is located on the flat piece of glass below the cassette drive and control panel. It has several indicator lights.

Lights 0 to 19 (indicator lights). Indicate different information depending on the different machine states. The MC may ask the NSC to report on the appearance of light displays in order to diagnose a network problem. The following is an introduction to interpreting the light panel.

The PSN front panel lights alternate between showing normal host status information and trunk modem status information. If lights 17, 18, or 19 are on, host status is displayed to indicate:

- 19—hosts 0 to 15 are indicated by lights 0-15.
- 18—Hosts 16 to 31 are indicated by lights 0-15.

- 17-hosts 32 to 47 are indicated by lights 0-15.

Different host statuses are indicated by whether the light is on, off, or flashing. Figure 2-10 illustrates the PSN light panel appearance when the PSN shows host status. When lights 17, 18, and 19 are off, trunk modem statuses 0 to 15 are indicated by lights 0 to 15. Just like the host status indications, different modem statuses are indicated by whether the light is on, off, or flashing. Figure 2-11 illustrates the light panel when the PSN shows trunk modem status.

PSN reading its cassette. When the PSN reads its cassette tape, front panel lights 0 through 19 are OFF, and the front panel LOAD light flashes. The PSN reads its cassette automatically after a crash, machine reset or power failure, or when it receives a command from the MC. After about 3 minutes, the PSN completes the cassette tape load and then requests a software reload from the neighbor node. No NSC intervention is required. Figure 2-12 shows how the PSN front panel lights appear while it is reading its cassette tape.

PSN requesting a software reload. After the PSN has read its cassette, it automatically requests a software reload from a neighbor node. When the reload request is sent, lights 16 to 19 are steadily on. One of the lights 0 to 13 is also on, indicating the trunk modem on which the reload request is being made. The PSN starts with the lowest numbered modem being used (e.g., 0). If the reload is not received shortly, the PSN turns off that modem and repeats the request on the next modem (e.g., 1), skipping the unused modem. The PSN cycles through the modems until the reload is received.

Figure 2-13 illustrates how the PSN front panel lights appear during a PSN request for a software reload. The

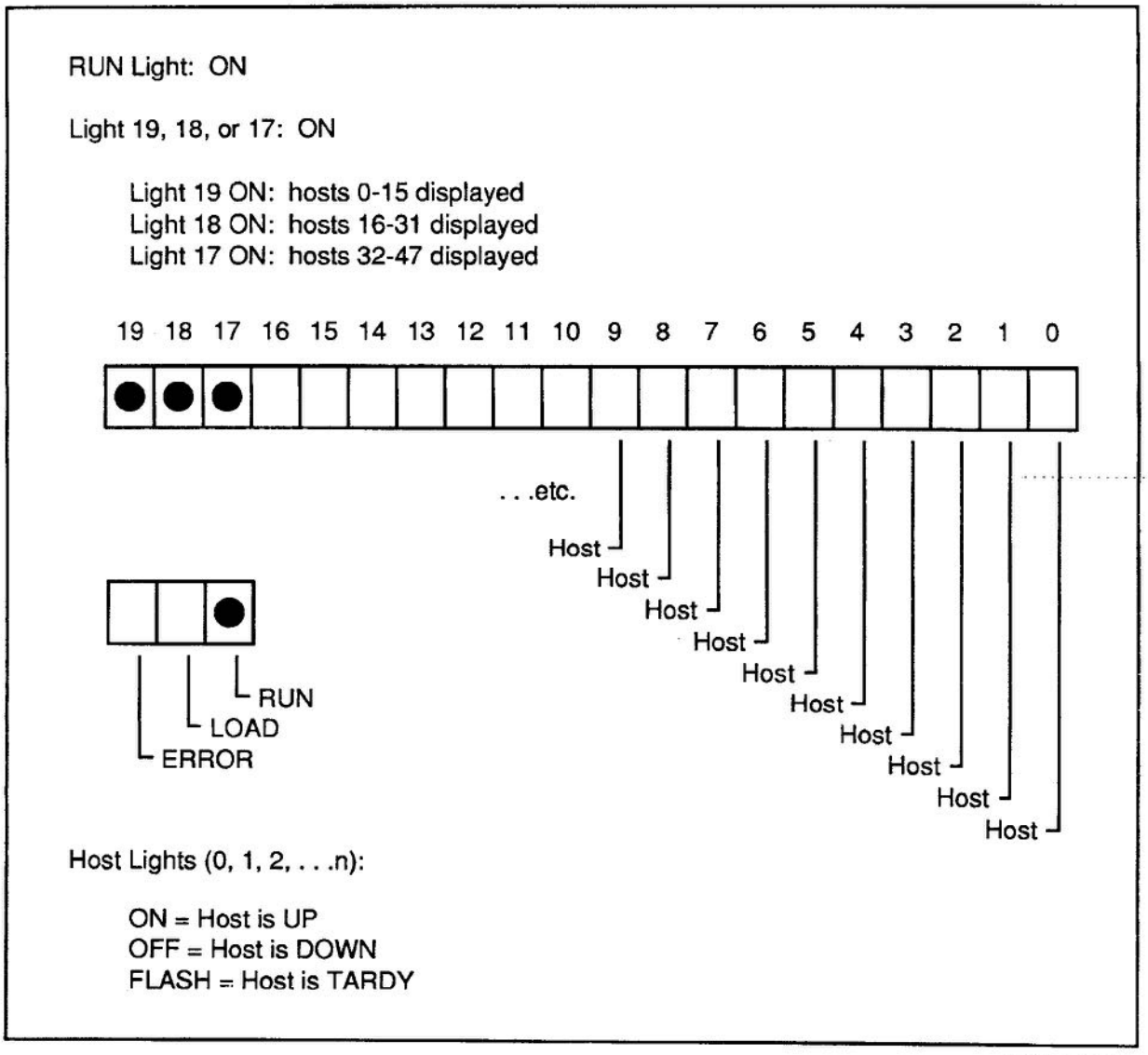


Figure 2-10. PSN host status display.

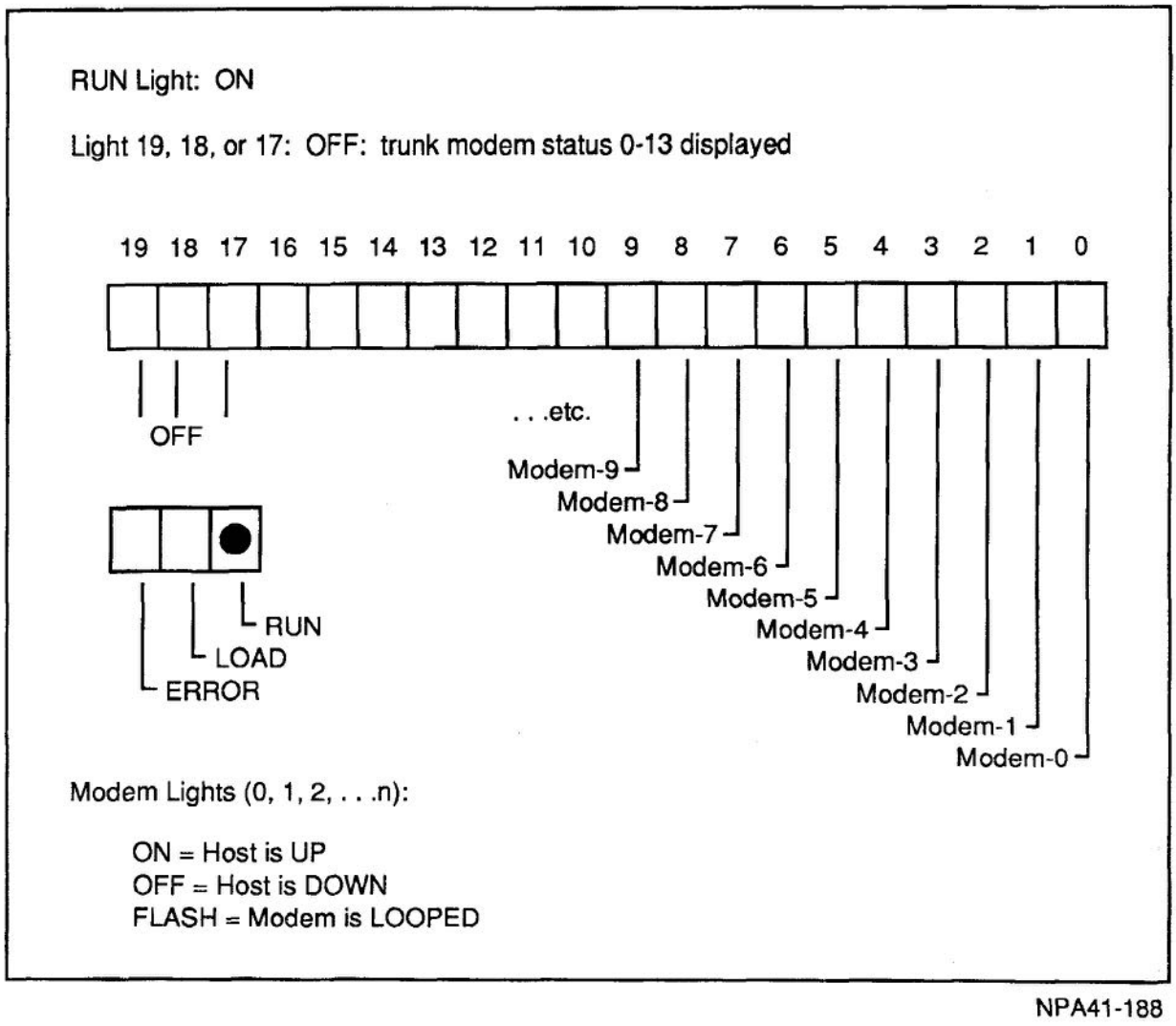


Figure 2-11. PSN trunk modem status display.

question mark refers to the fact that the PSN cycles through each configured (used) modem, skipping unused modems.

PSN running its loader/dumper program. The PSN runs its loader/dumper program automatically after a crash, machine reset, or power failure recovery, or when it receives a command from the MC. The loader/dumper program allows the MC to load run-time or diagnostic software into the PSN, dump PSN memory to a file at the MC, or restart the PSN run-time program, all without the NSCs intervention or help. When running its loader/dumper program, the PSN's front panel lights indicate the count (in binary) of packets received during a software reload or packets sent during a memory dump. Figure 2-14 shows how the PSN front panel lights appear while the PSN is running its loader dumper during a software reload or memory dump.

After the reload, the entire light panel will go dark. Light 19 will come on, blinking slowly. Then the PSN will return to displaying host and modem status.

PSN Rear Panel Features. PSN rear panel features are discussed below and shown in figure 2-15. The rear panel RESET and POWER controls duplicate the same switches found on the front control panel. The NSC may not have to use rear panel controls, but should have a basic familiarity with them.

PSN FPI fantail (PSN ports). Connects trunk and host access lines to the PSN. The FPI fantail is a slotted backplane into which trunk and host access lines connect. Lines attached to TACs and hosts connect to these PSN fantail ports. Port 15 is reserved for maintenance terminal connection to the PSN. Port 16 is used to connect the cassette drive unit to the PSN.

FD4 fantail (PSN ports). Connects host access lines to the PSN. The FD4 fantail is a slotted backplane into which host lines connect. The FD4 fantail allows connection of four "V.35" plugs and four "RS-232" plugs.

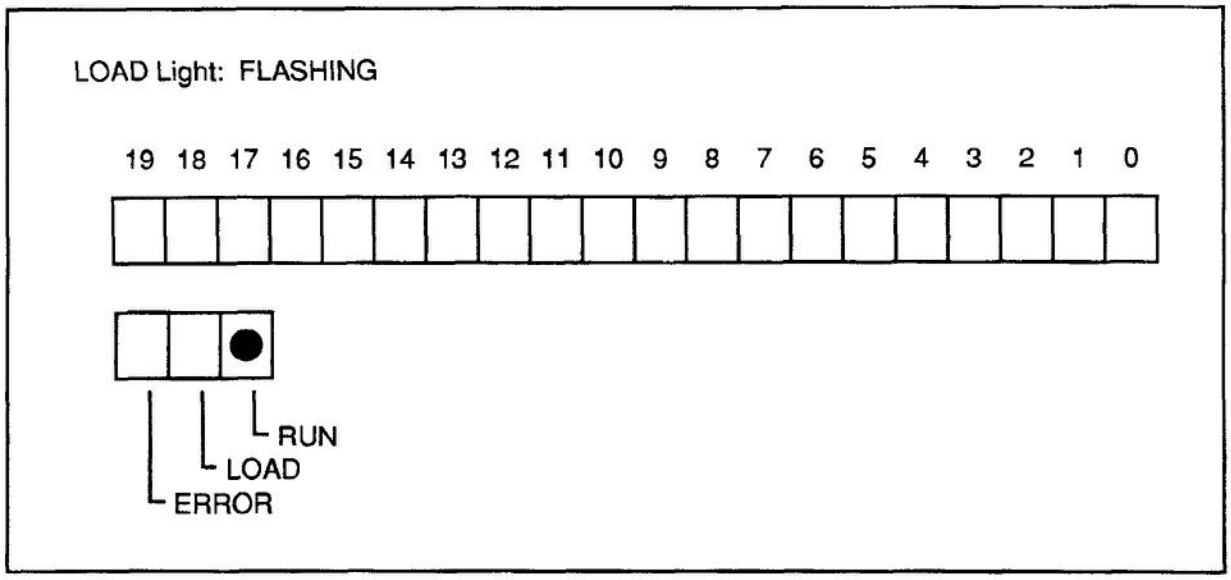


Figure 2-12. PSN reading its cassette.

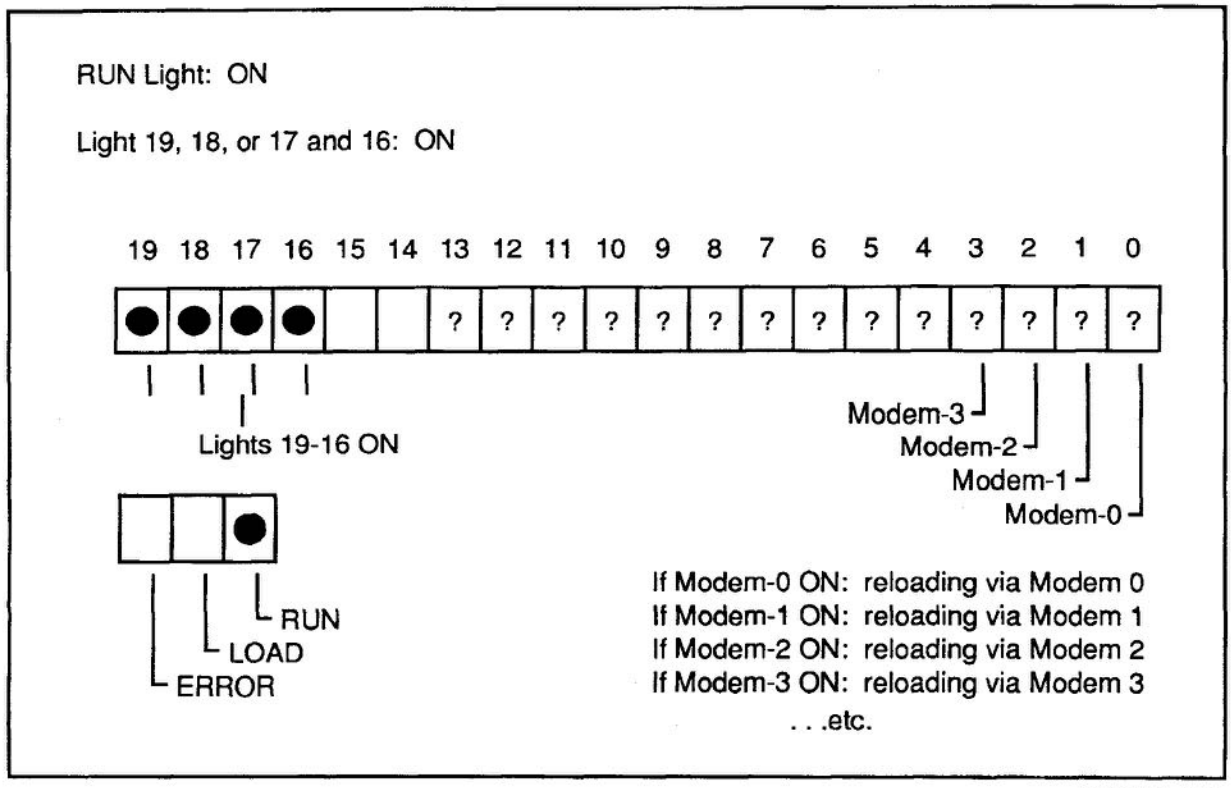


Figure 2-13. PSN requesting a software reload.

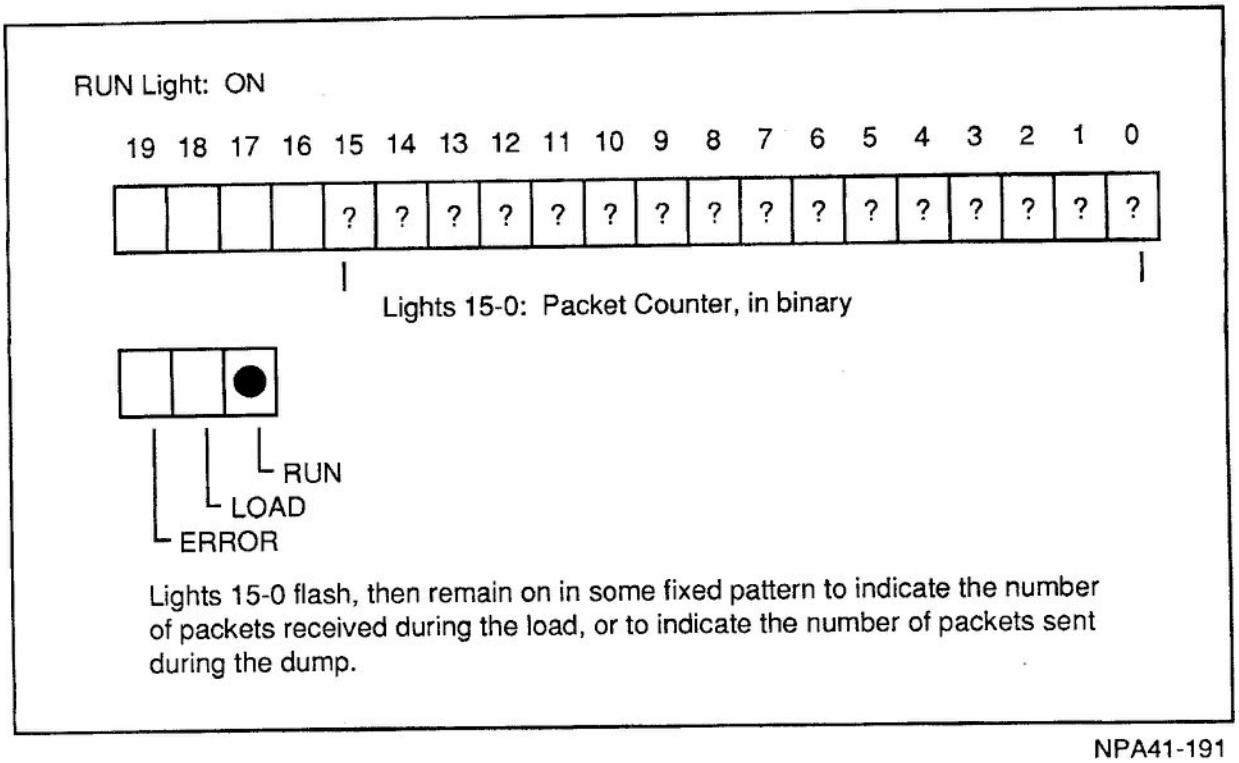


Figure 2-14. PSN in its loader/dumper.

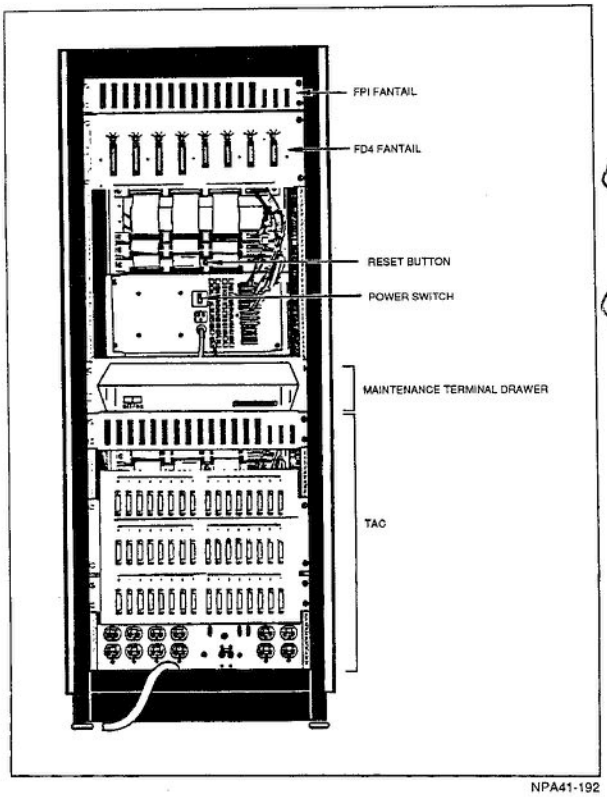


Figure 2-15. PSN rear panel features.

219. Operating principles of the terminal access controller (TAC)

Asynchronous terminal users are allowed access to the network either directly, through a TAC, or indirectly, through a host connected to a TAC. Each TAC has 63 ports for inputs from terminals, and a 64th port for maintenance control.

Terminals and hosts are connected to TACs either by direct lines at speeds from 110 to 9600 bps, or by dial-up lines at speeds of 110 to 2400 bps. The output of each TAC is connected to a PSN by a direct line that operates at speeds from 9600 to 56,000 bps.

The network can be considered as a way for a remote computer (host) and the user's terminal to communicate. With the TAC, the user at a terminal can open a communications connection to a distant host. The TAC acts as the user's window through the DDN to a host where the user has an account to log in to. The user may also open a communications connection to a service program on the Network Information Center's computer to obtain information.

The front of the TAC contains both a cassette drive/control panel as well as a light panel, which displays information about the TAC processing, much the same as the PSN. The controls and indicators on the TAC front panel are shown in figure 2-16.

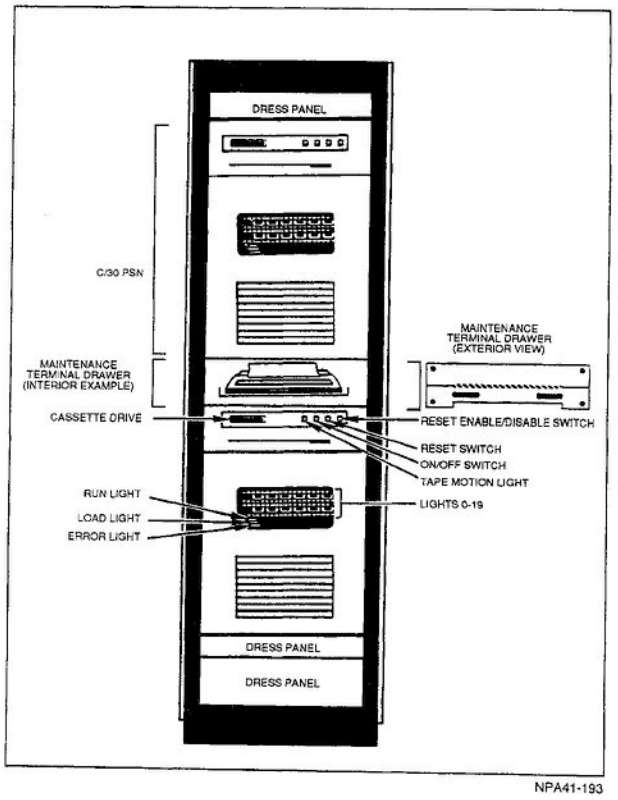


Figure 2-16. TAC front panel features.

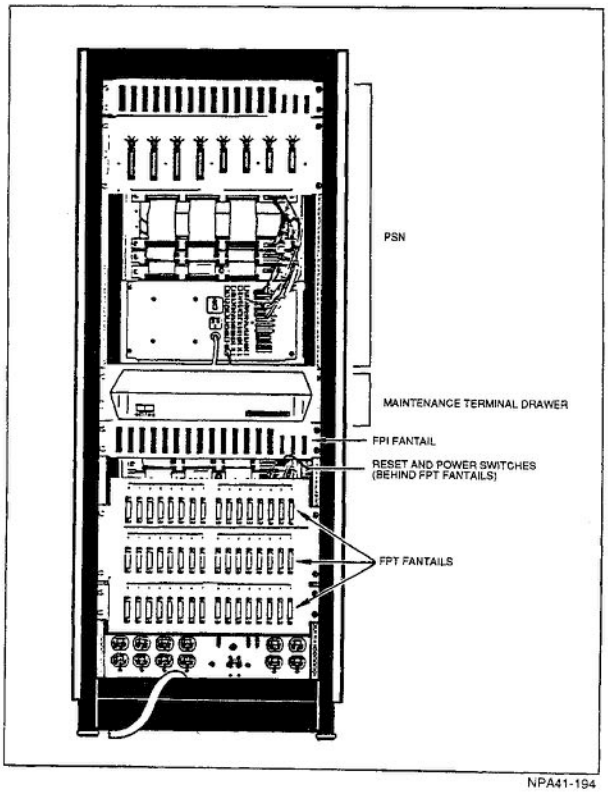


Figure 2-17. TAC rear panel features.

The rear panel features are shown in figure 2-17. The rear panel RESET and POWER controls duplicate the same switches found on the front control panel. The node site coordinator may not have to use rear panel controls, but should be familiar with them.

Protocols. To maintain the connection between a terminal and a host during network operation, the TAC and the host use a set of conventions called protocols to communicate with each other. Generally, protocols are transparent to the terminal end user. (Computers and terminals that cannot understand the DDN protocols will not work on this network.) The TAC supports transmission control protocol (TCP) for communicating with remote hosts. TCP is responsible for ensuring that data sent between the terminal and the host arrives error free. The TAC is able to connect only to hosts that support the TCP protocol.

The TAC does not restrict a user's connections to hosts that are on the same network the TAC is on. By using internet protocol (IP), the TAC allows connections to hosts on other networks. These other networks are part of a system of networks (an internet) joined by gateways.

TAC configuration. Before a user at a terminal can use the TAC, the TAC has to be informed of some of the important features about the terminal. Each TAC port is setup originally (configured) to expect certain characteristics in the terminals connected to it. This information about terminal characteristics, the *TAC configuration*, is contained in the TAC site file, a software file that resides in the TAC memory. These configurations are set up for each port when the TAC is first installed or when a port is activated for a new user in response to a telecommunications service request (TSR). Default configurations are maintained to allow maximum user flexibility.

The initial configuration concerns terminal characteristics that are associated with the physical connection between the terminal and the TAC. The physical connection and characteristics associated with the physical connection are collectively called the TAC port.

If the configuration of the TAC port does not meet the user's special needs, the user may negotiate a change to the initial TAC port configuration for the duration of the session only, by using configuration commands. When the session is over, the port will return to the initial configuration defined in the site file. If the user wishes to return to the initial configuration during the TAC session, the reset to initial configuration (RIC) command is provided.

In some cases, TAC configuration commands are not allowed. In these cases, using configuration commands will produce the "can't" error message.

TAC Commands. A good explanation of TAC commands can be found in DCAC 310-P70-74 (*Terminal Access Controllers User's Guide*). It covers such things as what commands are available, how to input a command to the TAC, and what each command will do when entered. Some

of the specific parameter options that can be tailored for TAC ports may be new to you, so let's look at some of them.

Hunting. Hunting is the ability of the TAC to determine the terminal's input and output rate. The TAC can hunt for certain standard rates from 110 to 9600 baud. Legal rates for hunting are: 110, 150, 300, 600, 1200, 1800, 2400, 4800, and 9600 baud. (TAC ports used for dial-in access to DDN may be set to hunt for 300 or 1200 baud).

Padding. Padding is defined as the addition of blank, extra, or nonsignificant characters to the data being transmitted. Data is padded if the network configuration requires it. For example, some terminals and lineprinters need extra time after commands, such as [RETURN] [LINEFEED] for the print head to return to the margin. This extra time is provided by padding the data. Other devices, such as terminals called GRTs, need no padding.

Parity. Parity is a method of ensuring accurate transmission of data by adding up bit values and checking them before and after transmission of a message. Parity is either even or odd. Certain terminals, especially the Teletype Model 37, require even parity.

Flow control. Flow control is the ability of a device, in this case the TAC or terminals connected to the TAC, to wait before sending or receiving more information than its internal storage mechanism (called a buffer) can contain. If either side is missing data, flow control may be needed. Too, certain devices, such as lineprinters, need a means of preventing their internal buffers from overflowing when data are sent from the TAC at a rapid rate. In this case (when using the lineprinter), turn on output flow control. Likewise, the TAC may need a means of keeping its buffers from overflowing when data are sent at too rapid a rate from a device (such as a terminal with internal buffer transmission capability or a microcomputer) connected to the TAC. In this case (rapid transmission of data from the terminal), turn on input flow control. The TAC supports two types of flow control: XON/XOFF and EIA RS-232.

XON/XOFF. The TAC provides XON/XOFF flow control for the input (terminal to TAC) and output (TAC to terminal) directions. XON/XOFF protocol is a fairly standard protocol; it is used by many manufacturers of computer systems. Because it uses two of the few ASCII codes for the stop-go signaling, these codes must not be used elsewhere. In particular, when using input XON/XOFF flow control, the TAC traps and discards any instance of these two characters sent by the host to the user. Similarly, the TAC absorbs and does not transmit these two characters when receiving from the terminal with output XON/XOFF flow control enabled.

EIA RS-232. This type of flow control uses lines on the EIA RS-232 connector to signal stop and go. It is offered as an alternative type of flow control for compatible devices able to use it. EIA RS-232 flow control can be used only with terminals that are directly connected to the TAC and that use special-purpose modems that pass the relevant EIA RS-232 signals. If EIA RS-232 type flow control is configured in the site file in the TAC port for the terminal, the flow control cannot be changed by user command.

Echo. Echoing is the process of displaying characters on the terminal screen that were typed as input by the user. This process can occur at the terminal (echo half-duplex command), in the TAC (echo local command), or in the remote host (echo remote command).

Intercept character. An intercept character is basically a signal to the TAC when you want to say something to it. In other words, it gets the TACs attention. The standard intercept character for DDN (Defense Data Network) is the at sign (@), which is put in front of a command word when inputting to the TAC. For instance, the command; @CLOSE [RETURN], means, "Hey TAC! I'm done now."

There are some instances when the (@) sign cannot be used. For example, some personal computers use the (@) sign for another purpose, or there may be files containing an (@) sign to be transmitted to a host. The user has the option to change the intercept character for the duration of the network session.

220. Functions and characteristics of elements of the DDN backbone

Besides the PSN and TAC, there are other elements of the DDN that must be looked at. Depending on the specific needs of the local subscribers to DDN, you may encounter any number of the following.

Network Access Controller (NAC). A NAC is any one of three microprocessor-based components that allow terminals access to the DDN. The first of these, the miniterminal access controller (mini-TAC), is a DCA supplied and supported component of the DDN. The host front-end processor (HFEP) and terminal emulation processor (TEP), however, are not DCA-supported components of the DDN backbone, and they must be purchased and supported by the host that wishes to use them. The three NACs are described below.

Miniterminal access controller (mini-TAC). Terminals may access the network directly through a mini-TAC. A mini-TAC provides synchronous and/or asynchronous access for up to 16 terminals. The speeds for the ports connecting the mini-TACs to individual terminals, and for the direct lines to the PSNs, are identical to those for a TAC.

Asynchronous support is provided for terminals with EIA-RS-232-C, RS-422-A, RS-423-A, RS-449, MIL-STD-188C, and MIL-STD-188-114 electrical interfaces. Various types of synchronous, vendor-unique terminals are supported based on user needs and priorities.

The same data rates are used for both the inputs and outputs with timing provided either by the mini-TAC or the user terminal. The mini-TAC will provide automatic speed detection for its asynchronous terminals.

Host front end processor (HFEP). The primary function of the HFEP is to provide an alternate method to interface a host to a PSN by off-loading the communications package from a host processor. The protocol of a host processor, which gathers the data from its terminals, is not compatible with that of the DDN. The HFEP, a component owned and supported by a host, provides the proper software to interface DDN protocols.

An HFEP uses the same hardware base and the same software and supports the same network protocol as a mini-TAC. The major difference between the two is the protocol used to communicate with the host processor.

Terminal emulation processor (TEP). A TEP allows access to the network for those terminals, through their host processor, that do not require interoperability with other networks of the DDN. It requires no modification of the host's software, thus allowing interoperability only with compatible terminals within the DDN.

The role of the TEP is to emulate a collection of local terminals. Since the TEP emulates terminals, a host connected to the network using this approach can regard the network only as a set of locally attached terminals. Therefore, the host generally cannot take advantage of the full set of network services. The primary advantage of the TEP option is that no modification of the host's system software is needed.

Statistical Multiplexers. At some sites, the number of terminals requiring connection to the DDN does not justify the collocation of a mini-TAC or similar device. These sites will connect to a remoted mini-TAC through voice grade communications lines. Access can be provided using a statistical multiplexer and modem at each end of the access line.

Internet Gateway. An internet gateway, sometimes referred to as a "mail-bridge," exchanges "mail" between the various networks of the DDN by providing access to the ISTs. It should be noted that the DDN must provide connection to a growing number of networks outside the DDN. These include local area networks, regional networks, tactical data networks, broadcast satellite networks, and packet radio networks. The DDN must provide interconnection of these networks as outlined by the WWDSA goal architecture.

(46) **Network Monitoring Center (NMC).** An NMC monitors the status of network components, measures network performance, and provides a limited fault isolation and diagnostic capability. It consists of at least one BBN C/70 microprocessor plus peripherals. Each NMC is capable of monitoring multiple network segments; however, each DDN segment and cryptographically separated community of interest (COI) has a separate NMC. NMC operational functions include the following:

a. Measures network performance.
b. Monitors the status of network components.
c. Provides access to network components.
d. Maintains a DDN data base.
e. Provides a means for network configuration control.
f. Generates system event reports.

Node Site. Tech controls or other facilities that house a PSN and associated equipment are named DDN node sites. While tech controllers are being assigned the duty of node site coordinator, the full-scale of duties for that position are still being ironed out. The AFCC Project Management Office for DDN, however, foresees this role as being a major one. What is known of these duties will be covered in one of the following lessons.

221. The Air Force Concentrator

Description. Networks can be characterized by their size or geographic distribution, such as the local area network (LAN) or a wide area network (WAN). A local area network (LAN) may service a single office, a building, or possibly an entire Air Force base. Wide area networks typically serve large geographic areas like all bases throughout the world (e.g., DDN). A base may have several local area data communications networks. These data communications networks can be connected together, allowing subscriber systems on one network to share information with subscriber systems on another (provided the subscriber systems use compatible communications software). Local networks may also connect to larger wide area networks in order to reach other bases. Gateway devices called internet protocol routers (IPR) can connect local networks to each other and connect local networks to wide area networks. The DDN concentrator is a device designed to do these things.

(47) **Components.** The AF DDN concentrator consists of two basic components: the Codex 6510 IXP (an X.25 packet switch), and the Cisco Systems MGS Gateway Server.

Medium-to-large multi-user computer systems on a base connect to the Codex 6510 IXP and form a local area X.25 network. It will provide up to 20 X.25 ports for host connections. These connections are made with RS-232 (DB25) cables and, if necessary, short- or long-haul modems. If connected computer systems use compatible communications software, they may share information among themselves. Note that only hosts are connected to the concentrator. Individual terminals require a TAC. Terminals cannot be connected directly to the concentrator.

The Codex 6510 IXP acts much like a multiplexer. In fact, part of the Codex 6510 IXP is a multiplexer that accepts up to 20-host ports, multiplexes them, and provides one input to the Cisco Systems MGS Gateway Server.

(48) The Cisco Systems MGS Gateway Server is an IPR as described above. It connects a base's local area X.25 network to the DDN. In this way, the AF DDN Concentrator will become the base's primary method of connecting UNCLASSIFIED computer systems into the DOD internet (in some cases the only method). Therefore, its proper operation must be viewed as mission essential. Figure 2-18 illustrates how the Air Force concentrator fits into the DDN system.

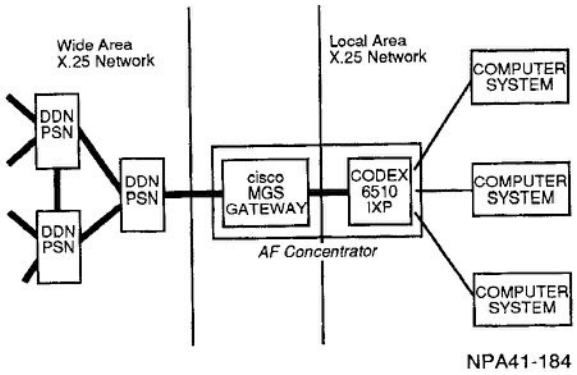


Figure 2-18. AF Concentrator connectivity.

Physical Characteristics. The Air Force concentrator is built into two standard 19-inch communications cabinets (fig. 2-19). From the front, the left cabinet houses the Codex 6510 IXP, the Cisco Systems Gateway Server (IPR), two RS-232 digital patch panels, and an interface converter/ synchronous modem eliminator (SME) cage. The right cabinet is available for mounting modems and related equipment required for host connections. This cabinet contains the analog patch panel, RJ-11 modem taps, and a terminal used to check or configure the concentrator.

The monitor terminal is located inside the rear door of the concentrator analog or modem cabinet. The terminal's video screen is on a large shelf, with its keyboard on a smaller shelf lower and to the front of it. A three-position matrix switch is permanently mounted in the shelf between the keyboard and video screen. This switch is used to connect the monitoring terminal to either the Codex 6510 IXP or the Cisco Systems MGS Gateway Server (IPR) control ports. Under normal operating conditions, this switch should be set to the middle position.

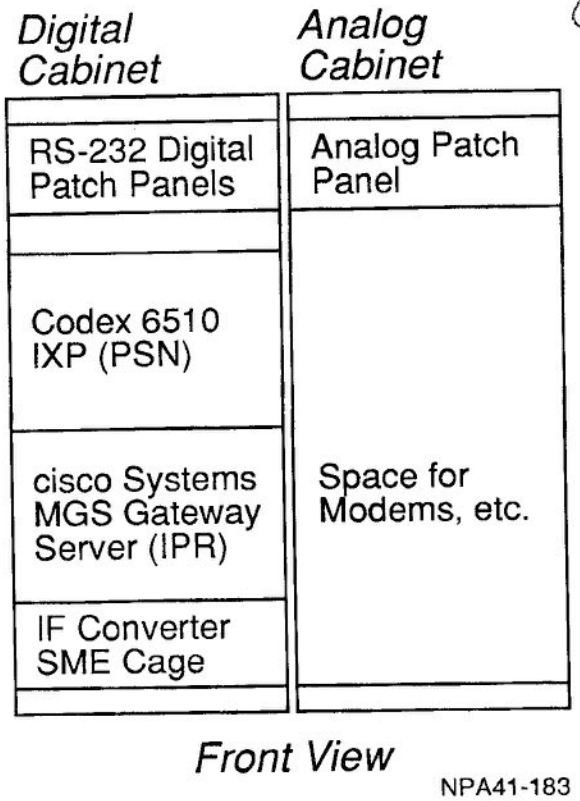


Figure 2-19. AF concentrator cabinets.

222. What is the role of a DDN node site coordinator?

Overview. DCA has wisely come to the decision that DDN node site coordination duties should be done by technical controllers. A node site coordinator (NSC) is the person named to make sure of continuous operation of a node site. While the NSC may delegate some tasks to other personnel, he or she is responsible to the network for all node site matters.

Primary Responsibilities. As an NSC, your primary responsibility is to provide the network with local site help in case of node hardware or circuit degradation or outages. You will also have several administrative responsibilities, as well as general technical control duties. These three types of responsibilities are detailed in the following paragraphs.

Local site assistance responsibilities. The NSC must provide, or arrange for provision of, local site aid to NMC controllers on a 24-hour, 7-days-a-week basis. In those isolated cases where a node site is located in a facility that is not manned 24 hours a day, the NSC must make sure that someone can provide local site help within 2 hours.

Administrative responsibilities. An NSC is responsible for the administration of a node site in four general areas.

(1) *Hardware and software accountability.* The NSC provides for the care and safekeeping of all installed node site equipment, all onsite spare parts contained in the installation checkout (INCO) kits, and accountability and access control of the PSN and TAC system cassette tapes.

(2) *Site access control and security.* The NSC coordinates personnel access to the node site through the use of site access rosters and makes sure that installed node site equipment is not altered, tampered with, or moved without proper authorization.

(3) *Maintenance and installation coordination.* The NSC coordinates and monitors the installation and implementation of node hardware, software, and circuits. Also, he or she coordinates and monitors emergency or scheduled preventive maintenance as directed by DCA or the NMC.

(4) *General administration and coordination.* The NSC maintains operating instructions issued by DCA and the Network Information Center (NIC), such as DCACs and DDN management bulletins. You must also act as liaison to representatives of organizations with whom coordination is

necessary for the efficient operation of the node site. To support both liaison and local site help functions, the NSC must maintain a list of telephone numbers for the NMC, the host administrator for each connected host, and others as necessary.

Technical control responsibilities. Besides specific node site coordinator responsibilities, tech controllers filling these positions must do general circuit actions tasks, such as circuit activation, deactivation, and changes. We are responsible for in-service and out-of-service quality assurance and fault isolation for both the equipment of the node sites and all connected circuitry. As was pointed out in an earlier lesson, you can look for changes in this role to be spelled out in DCAC 310-P70-76 (the DDN node site coordinators guide) and DCAC 310-70-1.

Please write your response to unit self-test questions and then check the text answers at the end of the unit.

SELF-TEST QUESTIONS

214. How packet switching was integrated into the Defense Data Network

1. What packet switching technology was used as a basis for the DDN? ARPANET technology

2. How is information routed under the packet switching concept? The information stream is subdivided into small packets which are routed as seperate messages through a network of packet switching nodes.

3. How do each of the PSNs handle message traffic? When a PSN receives a packet it checks for errors. If none are found, the packet is forwarded to another PSN, or delivered to the addressee.

4. What is the advantage of using "adaptive" routing? Portions of the network which are congested or damaged are by passed

215. Defining the classified and unclassified segments of the Defense Data Network

1. How are the ISTs, host access lines, and terminal access lines protected on the classified segment of the DDN? KG-84A encryption devices

2. How are the ISTs, host access lines, and terminal access lines protected on the unclassified segment of the DDN? ISTs & host access lines are protected by KG-84As

3. What precautions are taken to provide security for message traffic in the DDN? Both link & end to end encryption are employed. Physical & procedural security measures are used.

216. Interoperability of subscriber systems

1. What is interoperability? the ability to transfer meaningful information between equipment produced by different vendors

2. List the DDN protocols used to achieve interoperability. X.25 TCP/IP, Telnet, FTP, & SMTP

3. What two protocol suites are usable on DDN? GOSIP

217. What are the performance characteristics of DDN?

1. How are characteristic burst errors detected on DDN access lines and trunks? 16 bit CRC

2. What is used to protect against memory failure in DDN switches? Error detection

3. What is the network availability of the DDN for single- and dual-homed subscribers?
99% single homed
99.5% dual homed

4. What category of DDN message traffic is given the highest precedence level treatment?
Category I

5. How is network reconstitution facilitated during postattack periods?
use of 5 mobile preassigned reconstitution nodes.

218. The packet switching node (PSN)

1. What is the primary function of a packet switching node? store & forward message traffic

2. What is another name for the PSN?
IMP

3. What are the traffic rates of DDN ISTs?
9600 - 56,000 bps

4. When should you push the RESET button?
only when directed to do so.

219. Operating principles of the terminal access controller (TAC)

1. How are host terminals connected to a TAC?
   direct lines at 110 -9600bps
   dial up 110-2400 bps

2. Which protocol is required for the TAC to a host?
   TCP

3. What is "hunting?"
   TAC determining terminals input output rate

4. How does the TAC provide flow control?
   XON/XOFF protocol
   RS 232 connectors

220. Functions and characteristics of elements of the DDN backbone

1. What are the three types of network access controllers? Mini-TAC, HFEP, & TEP

2. Describe the protocol interface capabilities of a host front end processor (HFEP). compatable with that of the hosts terminal while the HFEP's output uses DDN protocol

3. How are terminals connected to the DDN when their location cannot justify collocation of a mini-TAC?
   ~~stat.~~ muxes & modems are used

4. What device provides access to the various networks of the DDN? gateway

221. The Air Force Concentrator

1. What two components make up the Air Force concentrator? Codex 6510 IXP & cisco systems MGS Gateway server

2. How many ports on the Codex 6510 IXP are available for connection to host computers?
   20 X.25 ports

3. What part of the concentrator connects a base's local area X.25 network to the DDN?
   cisco systems MGS Sever

222. What is the role of a DDN node site coordinator?

1. What is the primary duty of a DDN node site coordinator? local site assistance to the network.

2. If you are assigned DDN NSC responsibilities at a location which does not operate 24 hours a day, what response time are you required to provide for local site assistance? 2 hours response time

3. What are the four general areas of administrative responsibilities for a DDN NSC? Hardware software accountability site access & control security.

2-3. Weather Networks

Our military history is chocked full of reminders of the importance to the battlefield commander of knowing what the weather situation is like at all times. A prime example was "Operation Overlord," or "D-Day." American and British troops stood poised for days awaiting favorable weather conditions for a crossing of the English Channel to attack forces of the Third Reich. On 5 June 1944, American weather forecasters predicted good weather for the following day. The troops were readied for the assault and, on 6 June, Allied forces launched the greatest military operation in the history of warfare. A full understanding of the weather conditions was crucial to the success of this mission.

In the sections that follow, we will discover that our network of weather information services is quite complex and is designed to keep operational commanders fully aware of weather conditions at virtually any location in the world, 24 hours a day. Our discussion will cover the Air Force Digital Graphics System, the Automatic Digital Weather Switch, and the High-Frequency Regional Broadcast System.

50

223. The Air Force digital graphics system

Purpose of the Air Force Digital Graphics System (AFDIGS). AFDIGS provides worldwide weather forecast information to operational commanders and other Government activities, in support of their individual mission requirements. These weather products, in the form of facsimile representations, are transmitted on a given schedule for each scheduled transmission. Weather updates may occur more frequently for areas where there is a specific military, political, or special operations situation, such as space shuttle operations, requiring increased emphasis on the monitoring of weather conditions.

Operational Configuration. As shown in figure 2-20, AFDIGS is an extensive system that centers around the Air Force Global Weather Central (AFGWC) facility at Offutt AFB, Nebraska. AFGWC employs a large staff of highly skilled weather data analysts and a state-of-the-art computer and communications configuration to send out the data.

AFDIGS Weather Data Sources. AFGWC gathers data from several different sources, analyzes it, and produces weather forecasts in the form of hand-drawn paper maps or computer-generated maps on magnetic tape. The sources of data used by AFGWC are discussed below.

Fleet numerical weather service (FNWS). FNWS, located in Monterey, California, supplies ocean weather map products to AFGWC. This data is received by AFGWC in completed facsimile map form and is processed by computer for immediate retransmission over the AFDIGS network.

National weather service (NWS). NWS is located in Suitland, Maryland. It supplies information used by the CONUS and Alaskan areas only and, like FNWS data, it is received in completed map form and processed by the AFGWC computer for retransmission.

Automatic digital weather switch (ADWS). The ADWS, to be discussed in the next section of this unit, is located at Carswell AFB, Texas. It gathers data from weather intercept control units (WICU) at RAF Croughton, England, and Hickam AFB, Hawaii, and then sends this data to AFGWC for analysis.

Defense meteorological satellite program (DMSP). AFGWC can access the DMSP using its own satellite acquisition equipment and direct satellites to take

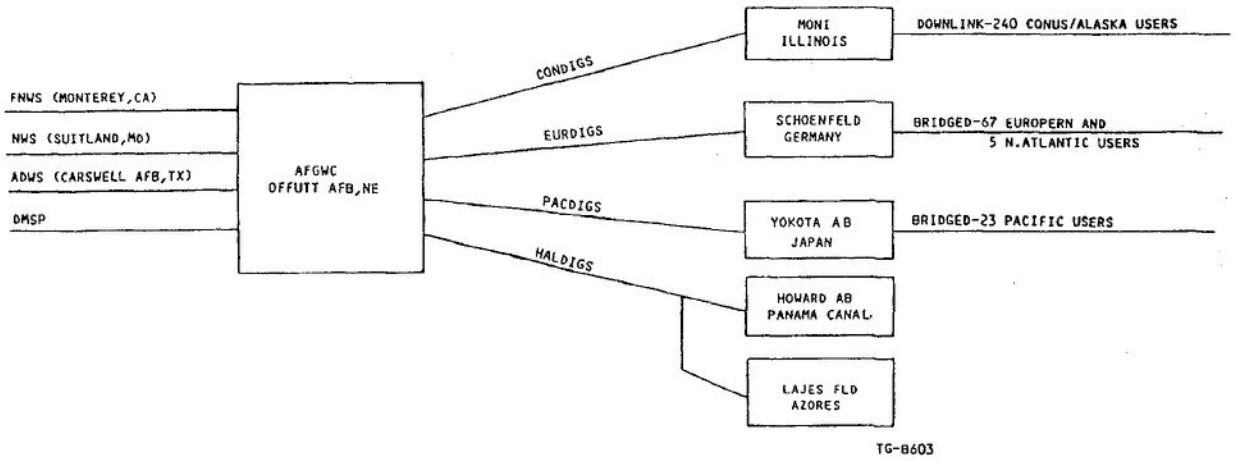


Figure 2-20. AFDIGS operational configuration.

photographs of specific geographic areas. Within a brief period of time, these photographs are printed out on a special imagery reception device located within the AFGWC facility. The photographs are then either analyzed or graphically reproduced and transmitted over AFDIGS circuitry.

AFDIGS Weather Data Dissemination. AFGWC processes and transmits data to locations worldwide. There are four AFDIGS systems.

CONUS digital graphics system (CONDIGS). Weather data leaving AFGWC on the CONDIGS circuit travels over a commercial path to the ALDEN satellite transmission facility in Moni, Illinois. ALDEN transmits data in footprints to areas in the CONUS and Alaska where 240 users, using passive receive systems, receive it on 6-foot satellite dishes.

European digital graphics system (EURDIGS). This circuit connects AFGWC to 67 users throughout Europe and 5 in the North Atlantic. The circuit is routed through commercial and military paths to Schoenfeld, Germany, where it is bridged to the various European users. Each of the circuits to the individual users has its own CCSD.

Pacific digital graphics system (PACDIGS). PACDIGS is routed from the Defense Satellite Communications System (DSCS) facility at Offutt to the DSCS at Zama, Japan, through DSCS facilities at Wahiawa, Hawaii, and Anderson AFB, Guam. From Zama, the circuit goes to Yokota AB, Japan, on a military microwave system and is then bridged to 23 users, all with separate CCSDs, throughout the Pacific.

Howard/Lajes digital graphics system (HALDIGS). HALDIGS connects AFGWC to Howard AB, Panama Canal Zone; Norfolk, Virginia; and Lajes Field, Azores. The circuit is routed commercially through Washington DC; Andrews AFB, Maryland; and Ft. Detrick, Maryland.

224. Signal flow of AFDIGS traffic

Within AFGWC, message traffic flows through the Weather Facsimile Switching Center (WFSC) and the Patch and Test Facility (PTF), which uses a spectron patch panel as an interface and testing point for all AFDIGS circuitry. Use figure 2-21 as we follow the signal flow through each of these facilities and on to the end user equipment.

AFGWC Forecast Service. As mentioned earlier, AFGWC derives data from several different sources. Personnel in forecast services have the difficult task of analyzing the data and producing weather forecasts for transmission over AFDIGS circuitry. Forecast service turns out products in two forms.

Hand-drawn maps. These are scanned by ALDEN digital graphics scanners in the WFSC at a rate of 720 scans per minute. The maps are scanned from left to right, one line at a time, producing serial data from the black and white information within that line. In one scanned line, there are 3,600 black and white elements. The white areas are represented by positive voltages, and the black areas by negative voltages. Both areas are input to the Interdata-50 (ID-50) computer.

The scanner also inserts a mode or method message selection (MOMMS) code. This MOMMS code serves as a map identification number and is inserted at the beginning and end of each map.

Magnetic tape. Computer-generated maps are stored on magnetic tape. These are read onto the I-50 from a magnetic tape drive in the WFSC for transmission over AFDIGS circuitry.

FNWS. This data arrives through commercial lines as a 4800 baud analog facsimile signal. The analog signal is input to a CODEX LSI 9600 MODEM and then input to the ID-50.

NWS. As with FNWS data, NWS arrives at AFGWC in analog format over commercial lines in completed map form.

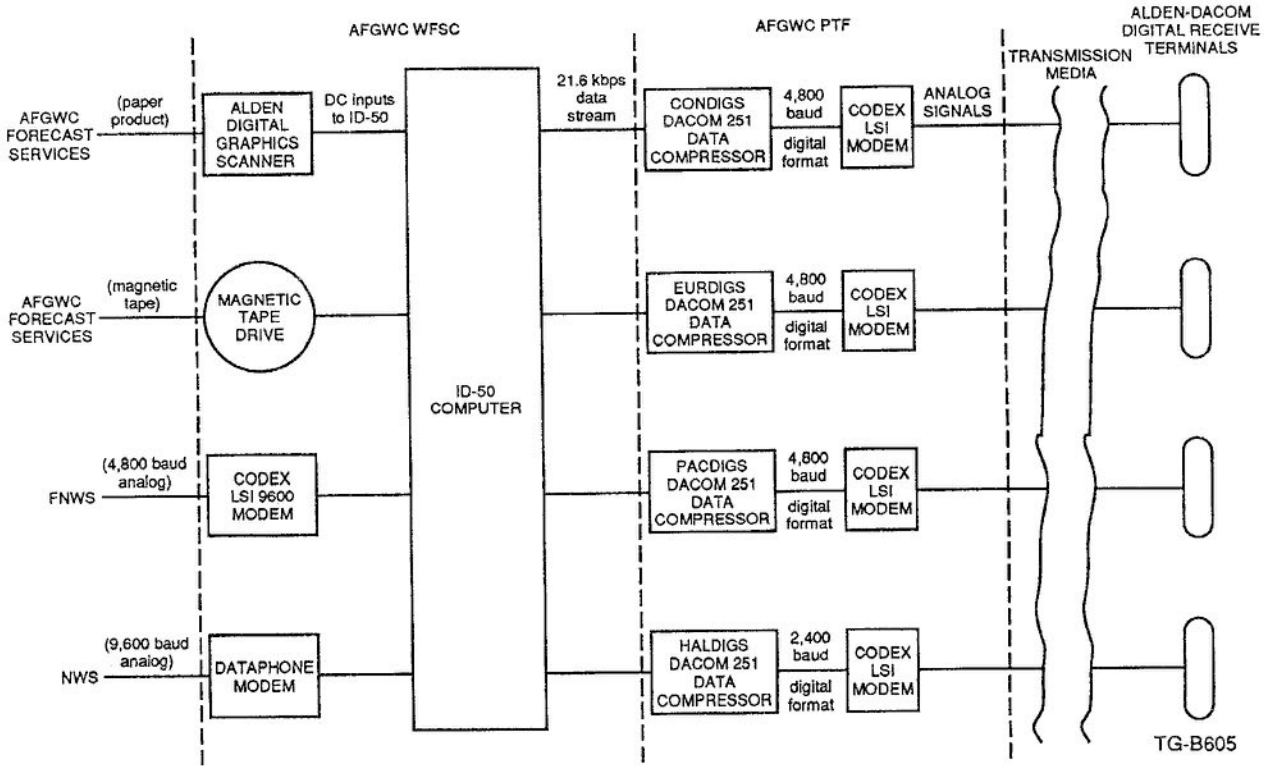


Figure 2-21. AFDIGS signal flow.

This 9600-baud signal is input to the ID-50 through a dataphone MODEM.

Interda-50 Computer. Data is input to the ID-50 in the form of positive and negative DC voltages. As noted earlier, positive voltages indicate white areas, and negative voltages indicate black. The ID-50 converts the data to digital format and provides a 21.6 kbps data stream output to the AFDIGS circuitry. The ID-50 also converts the MOMMS codes to a format that can be recognized by end-user equipment.

DACOM 251 Data Compressor. The DACOM 251 accepts the 21.6 kbps output of the ID-50 and compresses it the right baud rate for the AFDIGS circuits. CONDIGS, EURDIGS, and PACDIGS all operate at 4800 baud, while HALDIGS is a 2400 baud circuit.

CODEX LSI MODEMs. The CODEX MODEMs convert the output of the DACOM 251s to analog signals for transmission over VF systems.

Alden DACOM Digital Receive Terminal. When a signal is received, it is first demodulated and then sent to the user's digital receive terminal. This terminal, or facsimile recorder, is composed of three sections.

Message logic selection unit. This unit permits the selection of charts on a numeric basis (by MOMMS code) by the needs of the individual user. The user must have the unit "pinned" for the maps he or she wishes to receive.

DACOM 250-02 reconstructor. The reconstructor is a module within the terminal that recomposes the compressed data from either 2400 or 4800 baud to video data of 42,200 bps. This data is then passed on to the recorder section of the terminal.

Digital weather chart recorder. The recorder uses a moist electrolytic, current-sensitive paper that provides clean, crisp odorless recordings. Weather maps are reproduced in a quality almost identical to the original product.

If a user fails to receive a map for some reason, or the quality of the product is unacceptable, a request for retransmission from the WFSC at AFGWC may be sent, using the proper MOMMS code, through the user's ADWS circuitry. The request will be routed through the ADWS at Carswell AFB, Texas, to the WFSC, and the map will be retransmitted.

225. The automatic digital weather switch

Purpose of the Automatic Digital Weather Switch (ADWS). The ADWS, located at Carswell AFB, Texas, acts as a switching center for weather forecast and dissemination centers throughout the world. The ADWS uses a UNIVAC 1170 computer to control the switching of data among hundreds of weather stations, allowing them to interchange data readily.

Operational Configuration. The ADWS gathers data from many sources, as seen in figure 2-22, and makes it

possible for the users of one system to access data from any other system.

Receive only circuits. ADWS receives data from the National Weather Service (NWS), the Fleet Numerical Weather Service (FNWS), and the Federal Aviation Agency (FAA). NWS and FNWS are each 4600 baud analog circuits; FAA is a 2400 baud circuit.

Weather intercept control unit (WICU) circuits. The two WTCUs are located at RAF Croughton, England, and Hickam AFB, Hawaii. They are switching computers that gather and interchange data, as well as requests for retransmission of AFDIGS facsimile products between reporting stations throughout Europe and the Pacific. They each supply this data to the ADWS on 2400 baud analog circuitry, which is reformatted by Carswell's UNIVAC 1170 computer and shipped to AFGWC at Offutt AFB, Nebraska, on the 2400 baud circuits (primary and backup).

CONUS Meteorological Data System (COMEDS). COMEDS is a network of 20 switching stations that function in much the same way as the WICUs. These COMEDS switches gather data from 544 CONUS drops (weather stations) and interchange this data through the ADWS on 2400 baud analog circuits. The COMEDS drops also pass requests for retransmission of AFDIGS products to the ADWS. The UNIVAC 1170 reformats these requests and routes them to Offutt over the 2400 baud AFDIGS circuitry along with the WICU data from RAF Croughton and Hickam AFB.

226. The high-frequency regional broadcast system

Purpose of the High-Frequency Regional Broadcast Systems (HFRBS). HFRBS is the newest of the weather networks. There are two HFRBS sites in operation, one at Elkhorn, Nebraska, and the other at Elmendorf AFB, Alaska. There eventually will be eight sites, each broadcasting to a specific geographic region. The network is designed to provide operational field commanders with weather data products from both the AFDIGS and ADWS networks.

Operational Characteristics. HFRBS data is derived from two sources.

(1) Weather data from ADWS at Carswell is transmitted to the HFRBS sites in the form of 75 baud data transmissions.

(2) Facsimile transmissions selected from the outputs of each of the AFDIGS circuits.

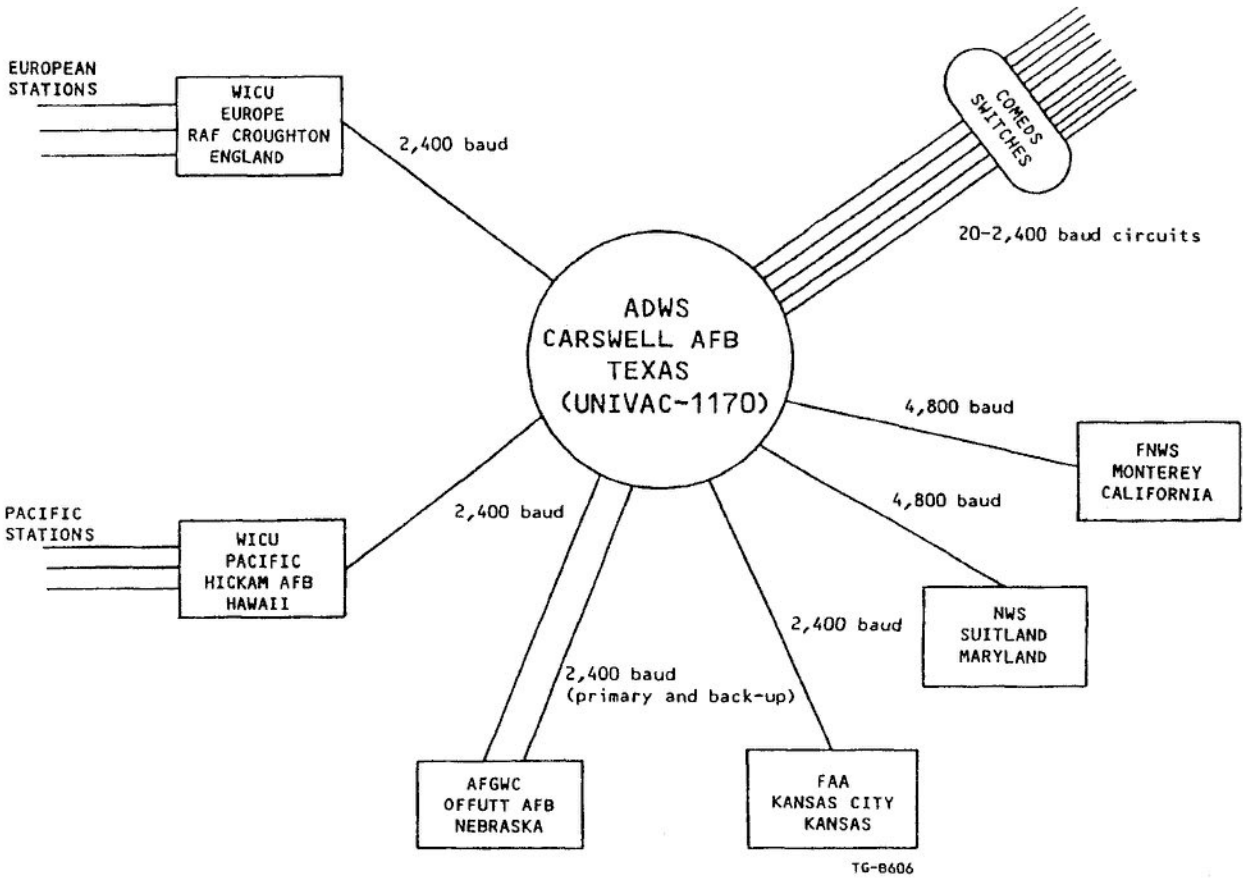


Figure 2-22. ADWS operational configuration.

54 These transmissions are converted from digital facsimile to analog format 120 scan per minute (spm) signals and routed to the HFRBS sites.

The ADWS and AFDIGS data are then transmitted by HF radio broadcast in footprints for the particular geographic region the HFRBS site covers. They can be received by any operational field commander who has the right communications receiver.

The HF broadcast is a two-channel transmission. The 75-baud ADWS traffic is on channel 1, and the 120 spm AFDIGS traffic is on channel 2.

Please write your response to unit self-test questions and then check the text answers at the end of the unit.

SELF-TEST QUESTIONS

223. The Air Force digital graphics system

1. What is the purpose of AFDIGS?
   weather forcasts for operational commanders
2. Name three sources of weather data used in AFDIGS.
   FNWS, NWS, ADWS
3. What are the four AFDIGS systems?
   CONDIGS
   EURDIGS
   PACDIGS
   HALDIGS

224. Signal flow of AFDIGS traffic

1. What are the four sources of input to the ID-50?
   Maps, forecast services
2. What is the output of the ID-50?
   21.6 Kbps data stream to either 2400 or 4800 baud for TX
3. What does the DACOM 251 do?
   compresses 21.6 Kbps to either 2400 or 4800 baud
4. How does a user select which maps he wishes to receive? must be "pinned"

225. The automatic digital weather switch

1. What is the purpose of the ADWS?
   act as a switching center
2. How do the two WICU circuits support the ADWS program? serving as an interface between Pac & Europe
3. What is COMEDS?
   network of 20 switches that interface data between conus drops.

226. The high-frequency regional broadcast system

1. What is the purpose of HFRBS?
provides commanders with weather reports

2. What is on each channel of an HFRBS transmission?
channel 1 is 75 baud ADDS data & channel 2 is 120 SPM AFDIGS Traffic.

ANSWERS TO SELF-TEST QUESTIONS

204

1. By interswitch trunk.
2. They provide for message protection in the event of complete ASC failure or saturation.
3. The AUTODIN matrix is the interconnectivity of all ASCs so that a failure or saturation of one ASC will not degrade the system too much.
4. A subscriber connected to only one switch or intermediate switch.
5. Subscriber mission and message priority.
6. Single-homed, dual-homed, and intermediate switch.
7. To provide a collecting point for message traffic and to interface the ASC at much higher speeds than the subscribers operate. Also, it is a more cost-effective way of providing service to several low-speed users.

205

1. Message switching, hybrid AUTODIN red patch service, query response, guaranteed sequential delivery, and AUTODIN limited privacy service.
2. Message switching, message processing, and message protection and bookkeeping.
3. Message programming.
4. Query/response service allows Q/R terminals to access Q/R host computers through the AUTODIN system.
5. This allows bulk data messages to be transmitted and received in sequential order.
6. A manual patch in the AUTODIN PTF provides direct user-to-user service.
7. The store-and-forward system keeps a record of each message on a history tape for recovery purposes. ALPS does not.

206

1. Block-by-block must receive an acknowledgement on the preceding block before another is transmitted. Continuous operation allows transmission of line blocks without interruption; however, an acknowledgement for a block must be received by the 83rd character of the next line block.
2. Mode I, mode II, and mode V.
3. Mode II can operate full- or half-duplex, and there is no automatic error or channel control. Mode V can operate full-duplex, and it uses control characters for channel control.
4. Mode I operation allows independent and simultaneous two-way operation with automatic error and channel controls.
5. Mode II has no automatic error detection or channel control. Mode V has only partial channel control, and message accountability is maintained through the use of channel sequence numbers.

207

1. Master station clock.
2. The detection is accomplished by a phase comparator that beats the output of each oscillator against the other two oscillators' outputs. If a count exceeds seven in a 2-minute period, it will alarm and switch to another oscillator.
3. MODEM.

4. They provide electrical isolation of clear text traffic from black areas to red areas to prevent security violations.
5. To convert a DC signal from high- to low-level polar.

208

1. Manual.
2. Audioterminating and patching facilities.
3. DCA ACOC.
4. Primary TCF or commercial test board.

209

1. Shield point isolators.
2. To convert high-level polar signals to low-level polar signals and vice versa.
3. It provides the central point for the control and supervision of the PTF.
4. A red or black switch allows only one type of circuit to be brought up at a time.
5. Oscilloscope, data analyzer, and intercom panel.
6. Reroute and restoral.
7. Loss of crypto synchronization.
8. The CAU.
9. To provide electrical isolation between the encrypted and unencrypted areas.
10. To interrupt traffic flow to and from the ASC.
11. To maintain the required separation between R and Y community traffic.

210

1. It links the tech control with the ICCDP.
2. An LTU and a PDP 11/84.
3. By exchanging idle, control, and framing characters with the TCUs for the terminal stations.

211

1. It performs the message switching function of the ASC.
2. Gathers line blocks of messages, determines routing of messages, stores messages on the EMSS, retrieves messages from memory, and performs checking functions to guarantee complete and accurate transmission.
3. High-speed memory, basic-processing unit, and transfer channels.
4. Operators console, high-speed paper tape reader, and monitor printer.

212

1. Systems console.
2. As the monitoring and control devices.
3. The ASC service section handles requests for message transmission, tracer action, and duplicate transmissions. The service section gets a printout of incoming messages which are not formatted properly. Also used to originate and terminate message traffic for various staff elements of the center.
4. Card and paper tape.
5. Provides for the transmission and reception of messages in paper tape format at speeds of 75 baud.

213

1. A shield point isolator.
2. Red/black isolator.
3. Serial (bit-by-bit).
4. To ICCDP.
5. ATC.
6. High-speed memory.
7. It is not forwarded beyond that point.
8. An alarm will be activated at the systems console.

214

1. ARPANET technology.
2. The information stream is subdivided into small packets which are routed as separate messages through a network of packet switching nodes (PSN).
3. When a PSN receives a packet, it checks for errors. If none are found, the packet is forwarded to another PSN or delivered to the addressee. If errors are found, the node will request retransmission until an error-free packet is received.
4. Portions of the network which are congested or damaged are bypassed.

215

1. All are protected by KG-84A encryption devices.
2. The ISTs and host access lines are protected by KG-84As, and the terminal access lines by low-cost encryption and authentication devices (LEAD).
3. Both link and end-to-end encryption are employed. Physical and procedural security measures are used.

216

1. The ability to transfer meaningful information between equipment produced by different vendors.
2. X.25, TCP/IP, Telnet, FTP, and SMTP.
3. Military standard protocols and Government Open Systems Interconnection Profile (GOSIP).

217

1. A 16-bit CRC is used.
2. Error detection and correction hardware.
3. 99 percent for single-homed and 99.95 percent for dual-homed subscribers.
4. Category I (flash and flash override).
5. Through the use of five prepositioned mobile reconstitution nodes equipped with an NMC capability.

218

1. To store and forward message traffic between host users, other PSNs, or network gateways.
2. An interface message processor (IMP).
3. 9600 to 56,000 bps.
4. Only when directed to do so by the MC.

219

1. Either by direct lines at speeds of 110 to 9600 bps, or by dial-up lines at speeds of 110 to 2400 bps.
2. TCP.
3. The ability of the TAC to determine the terminal's input and output rate.
4. By using XON/XOFF protocol and RS-232 connectors.

220

1. Mini-TAC, HFEP, and TEP.
2. The input protocol to an HFEP is compatible with that of the hosts' terminals while the HFEP's output uses DDN protocol.
3. Statistical multiplexers and modems are used to connect terminal users to a remote mini-TAC over voice grade communications lines.
4. An internet gateway.

221

1. The CODEX 6510 IXP (an X.25 packet switch), and the Cisco Systems MGS Gateway Server.
2. 20 x.25 ports.
3. The Cisco Systems MGS Gateway Server.

222

1. To provide local site assistance to the network.
2. A 2-hour response time.
3. Hardware and software accountability, site access control and security, maintenance and installation coordination, and general administration and coordination responsibilities.

223

1. To provide weather forecasts to operational commanders.
2. FNWS, NWS, and ADWS.
3. CONDIGS, EURDIGS, PACDIGS, and HALDIGS.

224

1. Hand-drawn and computer-generated maps from AFGWC forecast services and analog formatted maps from FNWS and NWS.
2. A 21.6 kbps digital facsimile data stream.
3. It compresses the 21.6 kbps data stream to either 2400 or 4800 baud for transmission over VF channels.
4. They must be "pinned" in the message logic selection unit.

225

1. The ADWS acts as a switching center for weather stations around the world.
2. By serving as a data interface between reporting station throughout Europe and Pacific.
3. A network of 20 switches that gather and interchange data between CONUS drops.

226

1. It provides operational field commanders with ADWS and AFDIGS weather products.
2. Channel 1 is 75-baud ADWS data and channel 2 is 120-spm AFDIGS traffic.

Do the Unit Review Exercises (URE) before going to the next unit. ➡

UNIT REVIEW EXERCISES

Note to Student: Consider all choices carefully, select the *best* answer to each question, and *circle* the corresponding letter.

7. (204) Redundant connectivity between AUTODIN switching centers (ASC) provides which of the following?

   a. Message protection only in the event of an ASC failure.
   b. Message protection in the event of ASC saturation or failure.
   c. An alternative path in case of preempt.
   d. More gateway protection for ASCs.

8. (204) Which of the following statements is true?

   a. CONUS AUTODIN switching centers are connected via military lines.
   b. Overseas AUTODIN switching centers are connected via leased lines.
   c. CONUS AUTODIN switching centers may use either military or leased lines.
   d. Overseas AUTODIN switching centers may use either military or leased lines.

9. (204) How do overseas interswitch trunks (IST) operate?

   a. In either 1200 or 2400 baud single-channel operation.
   b. In either 1200 or 2400 baud dual-channel operation.
   c. In 1200 baud single-channel operation.
   d. In 2400 baud dual-channel operation.

10. (205) Of the three functions performed by the AUTODIN switching centers, which ensures reliable delivery of a message once it has entered the system?

    a. Message switching.
    b. Message processing.
    c. Message protection and bookkeeping.
    d. All of the above.

11. (205) Which AUTODIN service provides direct user-to-user service without using the message switching capability of the AUTODIN switching centers?

    a. Hybrid AUTODIN red patch service (HARPS).
    b. Query/response.
    c. Sequential delivery.
    d. AUTODIN limited privacy system (ALPS).

12. (206) Which mode(s) is a duplex operation with automatic error and channel control?

    a. Mode I.
    b. Mode II.
    c. Mode V.
    d. Mode I and V.

13. (206) Which mode(s) uses continuous transmission only?

    a. Mode I.
    b. Mode II.
    c. Mode V.
    d. Modes I and V.

14. (206) Which mode(s) uses channel sequence numbers for message accountability?

    a. Modes I.
    b. Modes I and II.
    c. Modes II and V.
    d. Modes I and V.

15. (207) All timing pulses within an AUTODIN switching center are generated by

    a. a modulation oscillator.
    b. the master character supply.
    c. synchronous oscillators.
    d. a master station clock.

16. (207) The equipment that converts high- to low-level polar DC signals for processing by the AUTODIN switching center is the

    a. shield point isolator.
    b. DC signal converter.
    c. modem.
    d. crypto.

17. (208) In a CONUS configuration, the analog terminating and patching facilities are part of the modem area. From this statement, what can you conclude about the Patch and Test Facilities (PTF)?

    a. The modem area is part of the PTF.
    b. No DC lines are routed into the PTF.
    c. The PTF operates DC only.
    d. The modem area is DC only.

18. (208) An AUTODIN Patch and Test Facility (PTF) performs all of the following functions *except*

2-6
a. providing manual rerouting of circuits.
b. replacing defective equipment parts.
c. reporting equipment faults to maintenance.
d. maintaining a facility log of all circuit outages.

19. (209) All low-level DC signals entering and leaving the AUTODIN switching center must pass through which patching facility?

2-7
a. Black DC patch bay.
b. Subscriber test board.
c. Secondary test board.
d. Audio primary patch bay.

20. (209) What is used to examine circuit outages in an AUTODIN switching center (ASC)?

a. The ASC data base.
2-7 b. The protocol display for the circuit.
c. The station circuit outage log.
d. The traffic analysis display.

21. (209) At the red traffic patch bays of an AUTODIN switching center, what prevents a tech controller from patching circuits between communities of interest?

2-7 a. The physical separation of red and black areas.
b. The physical separation of the communities of interest.
c. The different type patch jacks of the communities of interest.
d. The incompatibility of signals of the communities of interest.

22. (210) What is the function of an AUTODIN terminal concentrator (ATC) switch?

2-8 a. It determines which ATC is on-line at a given time.
b. It switches all circuitry within an AUTODIN facility.
c. It switches traffic from the line termination unit (LTU) to the PDP 11/84 (processor component).
d. It switches traffic from the ATC to the integrated circuit communications data processor (ICCDP).

23. (210) What component is the termination point for all data channels in an AUTODIN facility?

a. The line termination unit (LTU).
2-8 b. The PDP 11/84 (processor component).
c. The integrated circuit communications data processor (ICCDP).
d. The fixed-head disk (FHD).

24. (210) What component in the AUTODIN switching center performs code conversion of message traffic, adds framing characters, and transfers the data to the integrated circuit communications data processor (ICCDP)?

2-8
a. The line termination unit (LTU).
b. The PDP 11/84 (processor component).
c. The ATC switch.
d. The fixed-head disk (FHD).

25. (211) What component in the AUTODIN switching center performs the actual message switching function?

a. The AUTODIN terminal concentrator (ATC).
2-9 b. The AUTODIN terminal concentrator (ATC) switch.
c. The integrated circuit communications data processor (ICCDP).
d. The PDP 11/84 (processor component).

26. (212) Which console provides an interface between the AUTODIN switching center operator and the on-line program?

a. The crypto console.
2-10 b. The integrated circuit communications data processor (ICCDP) console.
c. The systems console.
d. The master console.

27. (212) The systems console of the AUTODIN switching center is essentially a

2-10 a. monitor and control device.
b. maintenance alarm system.
c. focal point of off-line systems operation.
d. systems training console.

28. (212) Which of the following functions is *not* performed by the service section of the AUTODIN switching center?

a. Answers message queries from subscribers.
b. Provides courtesy copies of messages generated by the integrated circuit communications data processor (ICCDP).
c. Generates a service message when an incoming message is not correctly formatted.
d. Requests message retransmission and message acknowledgement.

29. (212) What component of the AUTODIN switching center processes originating and terminating message traffic for the various staff elements of the center?

a. The integrated circuit communications data processor (ICCDP).
b. The AUTODIN terminal concentrator (ATC).
c. The systems console.
d. The service section.

30. (213) The signal flow from a subscriber to its first appearance in an AUTODIN PTF is

a. subscriber, modem, path, modem, audiopatch bay.
b. subscriber, modem, path, shield point isolator, modem, black digital patch bay.
c. subscriber, modem, shield point isolator, audiopatch bay.
d. subscriber, modem, shield point isolator, MDF, black patch bay.

31. (214) How do switching nodes handle subscriber message traffic?

a. Information is subdivided into small packets and each packet is then handled as though it were a separate message.
b. Messages are formatted into packets and each packet is transmitted on a first-in, first-out basis.
c. Messages are separated into packets by priority and classification and are then transmitted separately by priority.
d. Messages are separated into packets by priority and are then transmitted separately by priority.

32. (214) How are packets routed in the Defense Data Network (DDN)?

a. Using predetermined paths.
b. Using the fastest route possible.
c. Using the shortest route possible.
d. Using adaptive routing methods.

33. (214) What feature enhances the survivability of Defense Data Network (DDN) packet switching node (PSN)?

a. They use advanced message security methods.
b. They use diverse message routing methods.
c. They can be installed in large quantities.
d. They are highly portable switching devices.

34. (215) What are the two segments of the Defense Data Network (DDN)?

a. Classified and unclassified.
b. Military Network (MILNET) and SECRET.
c. Massachusetts institute network (MINET) and SECRET.
d. SECRET and unclassified.

35. (215) Once combined, what will DSNET1, DSNET2, AND DSNET3 form?

a. Advanced Research Projects Agency Network (ARPANET).
b. Military Network (MILNET).
c. DDN Integrated Secure Network (DISNET).
d. Sensitive Compartmented Information Network (SCINET).

36. (215) Besides the use of physical and procedural security measures, how is message traffic safeguarded in the Defense Data Network (DDN)?

a. By bulk encryption.
b. By link and end-to-end encryption.
c. By separation of all message traffic.
d. By limitation of user connectivity.

37. (216) Which of the following protocols is the standard network access protocol for DDN?

a. X.25.
b. TCP/IP.
c. Telnet.
d. FTP.

38. (216) Why does DDN provide more services for the Military Standard protocols than it does for the Government Open Systems Interconnection Profile (GOSIP) protocols?

a. There are more military standard protocols.
b. There are more GOSIP protocols.
c. GOSIP does not provide a full set of protocols.
d. DDN provides an equal number of services for both protocol suites.

39. (217) What determines the total Defense Data Network (DDN) user-to-user undetected bit error rate?

2-19
a. The cyclical redundancy check (CRC) count of the circuit.
b. The checksumming count of the circuit.
c. The user's network protocol access scheme.
d. Both the CRC and the checksumming counts of the circuit.

40. (217) What is the network availability for Defense Data Network (DDN) single- and dual-homed users?

2-19
a. At least 95 and 95.9 percent, respectively.
b. At least 95.9 and 95 percent, respectively.
c. At least 99 and 99.95 percent, respectively.
d. At least 99.5 and 99 percent, respectively.

41. (217) How is message traffic handled when Defense Data Network (DDN) switches or trunks are congested, damaged, or destroyed?

a. Traffic is automatically routed around the problem area.
2-20
b. The sending switch buffers the data until the problem clears.
c. All message traffic is assigned both a primary and a secondary route.
d. All unacknowledged message traffic is automatically retransmitted.

42. (218) What are the transmission rates of Defense Data Network (DDN) interswitch trunks (IST)?

2-20
a. 110 to 2400 bps.
b. 110 to 9600 bps.
c. 2400 to 9600 bps.
d. 9600 to 56,000 bps.

43. (219) How many user inputs can be accommodated by a terminal access controller?

2-25
a. 15.
b. 16.
c. 63.
d. 64.

44. (219) At what transmission rate are terminals and hosts connected to terminal access controllers by dial-up lines?

2-25
a. 110 to 2400 bps.
b. 110 to 9600 bps.
c. 2400 to 9600 bps.
d. 9600 to 56,000 bps.

45. (220) Which of the following host-owned and host-supported Defense Data Network (DDN) interface devices provides an interface to DDN protocols?

2-27
a. Terminal access controller (TAC).
b. Terminal emulation processor (TEP).
c. Host front end processor (HFEP).
d. Miniterminal access controller (mini-TAC).

46. (220) What equipment component of the Defense Data Network (DDN) monitors the status of network components, measures network performance, and provides a limited fault isolation and diagnosis capability?

2-28
a. The terminal access controller (TAC).
b. The terminal emulation processor (TEP).
c. The host front end processor (HFEP).
d. The network monitoring center (NMC).

47. (221) What part of the Air Force concentrator is an internet protocol router (IPR)?

2-28
a. The Cisco Systems MGS Gateway Server.
b. The Codex 6510 IXP.
c. The multiplexer.
d. The RS-232 cables.

48. (221) When would the proper operation of the Air Force concentrator be viewed as mission essential?

a. When passing classified information.
2-28
b. When passing command and control messages.
c. When it is the base's primary method of connecting classified computer networks to Defense Data Network (DDN).
d. When it is the base's primary method of connecting unclassified computer networks to the DOD internet.

49. (222) What is the primary responsibility of a Defense Data Network (DDN) node site coordinator?

2-29
a. Local site assistance.
b. Site administration.
c. Site access control.
d. Maintenance coordination.

50. (223) The sources of information used by AFGWC for AFDIGS facsimile transmission are

2-33
a. CONDIGS, PACDIGS, EURDIGS, and HALDIGS.
b. ADWS, FNWS, and CONDIGS.
c. ADWS, FNWS, NWS, and DMSP.
d. FNWS, NWS, and CONDIGS.

51. (224) What determines which maps will be sent to users of the Air Force AFDIGS system?

    a. All maps are assigned message routing indicators before transmission.
    b. Users must pin their message logic selection unit for the maps they wish to receive.
    c. Users must request transmission of maps by mode or method message selection (MOMMS) code through Air Force Global Weather Central (AFGWC).
    d. Each map is assigned a mode or method message selection (MOMMS) code, which determines which users will receive it.

52. (225) What computer at the Automatic Digital Weather Switch (ADWS) controls the switching of data between weather stations?

    a. ID-50.
    b. UNIVAC 1170.
    c. CACOM 250-02.
    d. Weather intercept control unit (WICU).

53. (225) Automatic Digital Weather Switch (ADWS) takes data received from the weather intercept control units (WICU), reformats it, and transmits it

    a. to Air Force Global Weather Central (AFGWC).
    b. over the CONUS Meteorological Data System (COMEDS) network.
    c. over the Air Force Digital Graphics System (AFDIGS) network.
    d. to European weather stations.

54. (226) What is on channel two of a high-frequency regional broadcast systems (HFRBS) transmission?

    a. 75 baud Automatic Digital Weather Switch (ADWS) traffic.
    b. 75 baud Air Force Digital Graphics System (AFDIGS) traffic.
    c. 120 spm Automatic Digital Weather Switch (ADWS) traffic.
    d. 120 spm Air Force Digital Graphics System (AFDIGS) traffic.

Please read the topic page for Unit 3 and continue. ➡

DEFENSE SWITCHED NETWORKS

Page

Since the activation of DSN, there has been some confusion about the term Defense Switched Network (DSN). One day AUTOVON was here; the next day we had DSN. This implied to most people, and still does, that DSN simply took the place of AUTOVON. This is only partially correct, however, since DSN includes much more than just AUTOVON. DSN is the voice-switched network in the Defense Communications System and is composed of some of the following elements:

- DSN backbone.
- European Telephone System (ETS).
- Automatic voice secure network (AUTOSEVOCOM).
- Defense Commercial Telephone Network (DCTN).

The DSN mission is to provide long-haul, rapid, low-cost voice, data, TV, and secure-voice communications to users for routine and command and control purposes. It also provides worldwide voice communications services for the DOD and other authorized users. The technical control facility (TCF) will be provided remote access to the individual circuit paths and do fault isolation and rerouting. The network is divided into four geographical calling areas. Calls between these areas are routed through gateway switches, two of which are leased and two of which are Government-owned. Let's start by discussing the network most familiar to everyone, and that is the automatic voice network.

It should be noted that we are still in the transition period for DSN, and the technical data has not kept pace with these rapid changes. This unit is based on the most current information available to this point in the metamorphosis.

3-1. The Transition to DSN

This section will deal with the above-mentioned transition from AUTOVON to DSN. Even though DSN has now replaced AUTOVON as a system, some AUTOVON switches still exist in Europe. These switches are used primarily as backups and will eventually be phased-out.

The transition from AUTOVON to DSN has been a long and complex process—so complex that even the experts on the system have a difficult time keeping up with it all. To get some perspective of the transition, let's first look at the AUTOVON system and some of its design objectives.

227. Design objectives and switch connectivity of the AUTOVON system

Design Objectives. The AUTOVON system's switched networks had to meet the DODs design objectives of responsiveness, survivability, reliability, security, and reduced cost. The following paragraphs will explain these objectives.

Responsiveness. Commanders must be able to communicate within the necessary commands and other levels and be able to respond selectively to pertinent situations. Thus, a communications system had to be provided in which the command and control communications extended to operational areas is responsive to the reaction time of the forces involved. AUTOVON provided this in that a normal connection through the AUTOVON system took approximately 4 seconds.

Survivability. The communications system had to provide the requirements of a communications capability equal to the minimum demands of command control under all conditions. The voice of command must be survivable. AUTOVON provided survivability in that multiple communication paths existed in the event of a complete loss of capability from one country.

Reliability. The communications system had to be absolutely reliable for controlling operational forces. Reliability in a switched environment is contingent on equipment design, maintenance efficiency, and redundancy. All three of these factors had an economic impact that prevented the complete integration of dedicated networks into the Defense Communications System (DCS).

Security. The ultimate goal for the common user network was to provide secure communications among all subscribers. This security concept was applied to both digital and voice communications circuits and was used with the intent of denying unauthorized persons the content of transmission. Security was provided by secure voice terminals in instances where subscribers justify their use.

Cost. The total cost to the Government was to be reduced primarily by the removal of redundancy in the systems and by sharing of common equipment and facilities. Many leased AUTOVON switches provided service within the continental United States (CONUS) and Canada. US Government-owned switches provided service throughout the rest of the

world. Listed below are only some of the switches, most of which were converted to DSN switches.

ALCONBURY, UK	AF
COLTANO (LEGHORN), IT	A
DONNERSBERG, GE	A
FELDBERG, GE	AF
FAIRFORD, UK	AF
HILLINGDON (UXBRIDGE), UK	AF
LANGERKOPF, GE	AF
MARTLESHAM HEATH, UK	AF
MILDENHALL, UK	AF
MT. PATERAS, GR	AF
MT. VERGINE, IT	AF
SCHOENFELD, GE	AF
TORREJON, SP	AF
YOKOTA, JA	AF
OKINAWA (FT. BUCKNER)	A
GUAM (FINEGAYAN)	N
CLARK, PI	AF
WAHIAWA, HI	N LEASED
PANAMA, CZ	A
SHEPPARD AFB, TX	AF TRAINING
KOREA (OSAN)	A/AF

Switch Connectivity. The global AUTOVON system was divided into five major areas: Alaskan, CONUS, Caribbean, European, and Pacific. These areas were interconnected by the use of gateway centers (switches). Figure 3-1 shows the general layout of the global AUTOVON-gateway system. Units 4, 5, and 8 are the Alaskan system. Units 1, 2, 3, 6, and 7 make up the CONUS-PAC gateway system. Units 11, 12, and 13 are the CONUS-Caribbean system. Units 9, 10, 14, 15, 16, 17, 18, 19, 20, and 21 are the European-gateway system.

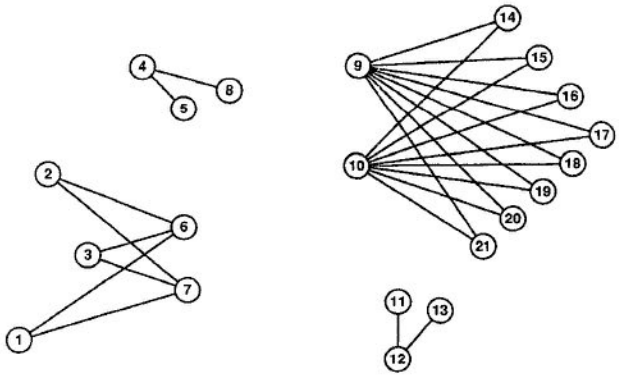


Figure 3-1. AUTOVON gateway system.

Figure 3-2 depicts the interswitch trunk configuration for the Pacific area. You can see that centers A, B, and C had to be connected to the CONUS through center 1, 2, or 3 or a combination of these centers. By the use of this trunk configuration, any switch had the advantage of multiple routes to reach the CONUS.

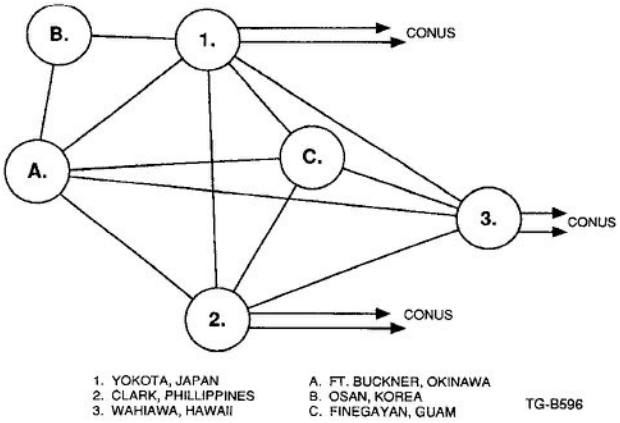


Figure 3-2. Pacific interswitch trunk configuration.

Figure 3-3 shows the interswitch trunk configuration for the European area. Multiple routes existed in this area, also, similar to those found in the Pacific area.

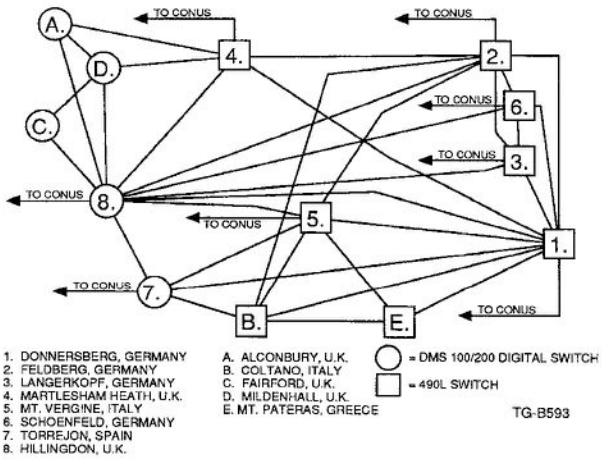


Figure 3-3. European interswitch trunk configuration.

Figure 3-4 depicts the major components that make up the global AUTOVON network. In this figure, the terms AUTOVON user, subscriber, access line, IST, and PABX are all used. To make the terms clear to you, they are defined as follows:

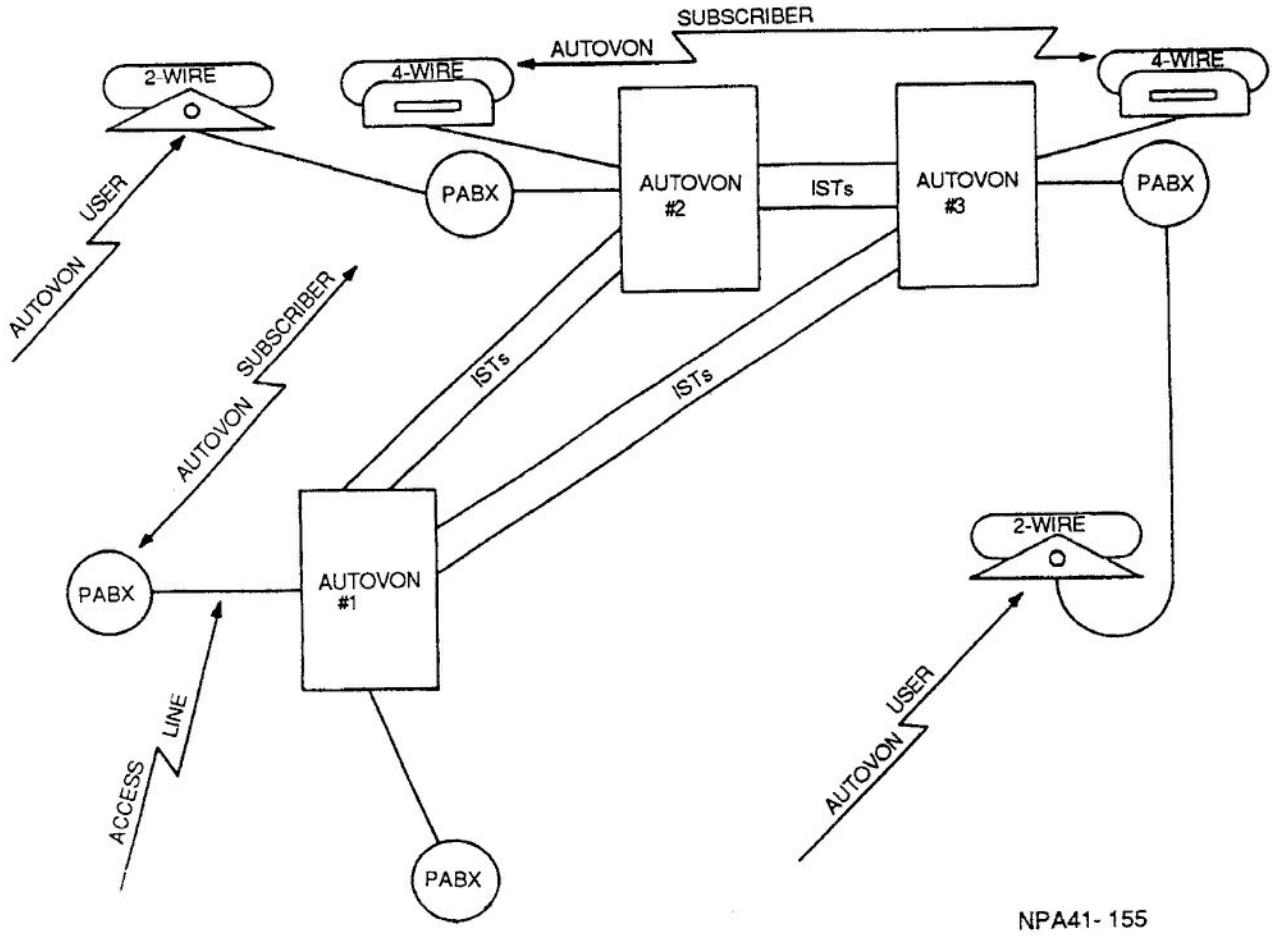


Figure 3-4. AUTOVON network components.

AUTOVON user. Any two-wire telephone that is capable of accessing the AUTOVON switch through a PABX is termed an AUTOVON user. AUTOVON users usually have to dial 8 to access AUTOVON.

AUTOVON subscriber. Any four-wire telephone with direct access to AUTOVON or PABX is referred to as an AUTOVON subscriber.

Access lines. The lines that connect an AUTOVON subscriber to an AUTOVON switch are called access lines.

Interswitch trunks. Lines that connect the AUTOVON switches to each other are known as interswitch trunks.

Private branch exchange (PBX). A private manual telephone switchboard that provides dial service on a subscriber's premises and serves only those stations with local and trunked communications. An on-base private branch exchange (PBX) user can also use the AUTOVON system, but only after calling the operator for help. At that time, if permission is granted, the operator will physically patch you into the system.

Private automatic branch exchange (PABX). A PABX has the same usage as a PBX except that calls within the system are completed automatically by dialing. An operator at the switchboard is required to route and complete incoming calls from the base dial central office (DCO). Depending on how the circuit is engineered, stations within the system are connected to the base DCO by dialing directly, or they are made to go through the operator

Although AUTOVON provided adequate service for many years, its technology has become antiquated. A new system had to be made to take advantage of today's digital technology. DSN was the answer.

228. Uses and capabilities of the Defense Switched Network

DSN System Uses. Effective military command and control requires a communication system capable of not only transmitting battle orders but coordinating personnel movements, ordering parts, and arranging the details essential to the success of any worldwide operation. DSN delivers these capabilities reliably and efficiently.

In the past, voice networks used analog technology almost exclusively. Today, the technology of digital equipment has

advanced to the point where entire networks can pass voice data digitally. Digital *data* technology has advanced rapidly in recent years as well. Logically, if voice traffic can be passed digitally, why not tie all these different systems (voice and data) together to have the good qualities from each network?

For example, a football team is made up of individuals, each with specific talents that, when used in concert, help make the team a strong unit. Most quarterbacks are gifted with an arm strong enough to pass the ball long distances. The receivers provide speed that helps the team advance the ball quickly. The linemen provide raw power and work together to help protect critical elements of the team from those who wish to interfere with the operation of their team. Running backs provide both power and speed. Working as individuals, the unit may function adequately, but it is only when these individuals work as a unit that their effectiveness is maximized.

This is the basic philosophy of DSN. Eventually, DSN will connect to virtually all DOD networks to provide a powerful, worldwide system with a variety of quick and efficient services. Some of these networks have already been linked to provide services, such as voice, data, video, teleconferencing, and facsimile.

Some users will have only a few needs for the system, but some will require much more than just voice connectivity. The two main categories of DSN users are command and control (C^2) users and operational support users.

Command and control users. The DSN is designed as a primary system of communication during periods of crisis, theater nonnuclear war, postattack, and peacetime readiness. The network assures connection to those key users who are assigned flash or flash-override precedence. These precedences will be covered in a later unit. Key users include members of the national command authority, the unified and specified commands, and the strategic and tactical subordinates of these commands.

Operational support users. The DSN provides telecommunications services for those engaged in logistics, personnel, engineering, and other activities that support command and control elements worldwide. This is the bulk of the traffic on DSN.

Worldwide Capabilities. The DSN will interconnect all military locations worldwide, providing terminal-to-terminal long-distance common-user and dedicated telephone, data, and video services. The DSN phase I network is already operational on a worldwide basis. Key survivability, responsiveness, and security enhancements are planned for DSN phase II. Eventually the network will provide long-distance replacement for direct distance dialing (DDD) and wide area telecommunications service (WATS).

Overseas DSN networks will have four times as many tandem nodes as AUTOVON did. The full-overseas DSN, including end offices (EO), will be 15 to 20 times larger than AUTOVON. The EO will be covered in a later lesson.

The DSN will provide transport services to the secure voice system, which includes secure telephone units (STU-IIIs) and red switches, the Defense Data Network (DDN), and the interservice/agency automated message processing exchange (I-S/A AMPE).

The Defense Communications Agency (DCA) is responsible for the design, acquisition, and single systems management of the network. The network will be upgraded gradually through a three-phase implementation schedule, incorporating new commercial technologies, such as those associated with the Integrated Services Digital Network (ISDN).

229. Design objectives of DSN

When DSN was being devised, certain needs became more important than others. After much consideration, it was decided that DSN would be implemented to achieve five key service objectives:

(1) Survivability.
(2) Responsiveness.
(3) Security.
(4) Cost effectiveness.
(5) Interoperability.

Survivability. DSN nodes are greater in number and more widely distributed than AUTOVON nodes. They are interconnected by a variety of transmission media and sophisticated routing. End offices will be multiple-homed and will interoperate with interfacing networks (allied military, DOD, public). This will add alternate reserve capacity to carry critical DSN traffic during emergencies.

Responsiveness. The DSN offers multilevel precedence/preemption (MLPP), and precedence access thresholding (PAT), which protects critical traffic from unnecessary preemptions and associated delays. High-speed digital technology and modern out-of-band signaling shortens call-establishment delays. Also, pushbutton telephones and off-hook and abbreviated dialing features reduce addressing delays.

Security. The DSN will provide transport and switching support for secure voice system (SVS) terminals that provide end-to-end encryption. The low-cost STU-III terminal will make end-to-end encryption available to many more users than previously possible. The DSN ultimately will provide bulk encryption for backbone and common-channel signaling circuits. The network also will provide service denial protection by proper guards against unauthorized manipulation of switching, transmission, ,signaling and network management controls.

Cost Effectiveness. DSN development costs are reduced by using commercial equipment and services wherever possible and by consolidation of DSN tandem and EO functions in single switches. New digital switching and transmission equipment is more reliable and will significantly reduce the

need for operations and maintenance staffing. This new technology results in savings in dollars as well as critical manpower billets overseas. Transmission costs are reduced with the elimination of long access lines. The DSN allows use of 12-button telephones, without operator assistance for precedence calls. Automatic collection of traffic data allows DCA engineers to maintain optimum network design continuously.

Interoperability. The DSN will extend its capabilities by making manual and automatic interfaces with various NATO, tactical, Federal agency, and public networks. Interoperability is enhanced by using national and international standards.

230. Major subsystems of DSN

The DSN consists of four major subsystems:

(1) Digital switching.
(2) Transmission.
(3) Timing and synchronization
(4) Administration/network management (A/NM).

Digital Switching. The digital switching subsystem includes the end office, the small end office (SMEO), the stand-alone switch (SAS), the multifunction switch (MFS), the remote switching unit (RSU), and commercially provided public switched networks (PSN). As part of the DSN, these switches will be interconnected to and supervised by the DSN A/NM subsystem and shall meet the required specifications. The private automatic branch exchange (PABX) or PBX may be interconnected to the DSN switching subsystem, but will not be an integral part of the subsystem. The primary difference in the switching subsystems are in the network applications and internal call processing features and functions. The switching subsystem incorporates a threshold control function to control network traffic overloads by using authorized precedence levels and maximum calling areas. This is known as the precedence access thresholder (PAT). The PBXs do not incorporate this ability, but are controlled by the host switch through access line protocol.

The DSN switch can provide two-wire service for remote concentrations of users/subscribers with the use of a remote switch unit (RSU). Certain switch types may also provide remote line modules (RLM), which provide service to added users remotely located from the RSU. High-priority users should not be terminated on an RSU or RLM, since the RSU or RLM can become isolated from the parent switch upon failure of transmission media.

The DSN will consist of network areas that differ in their makeup (digital and analog), timing arrangement, connectivity, and administration. However, all of the areas will form the global DSN, which will provide intercommunication to all its users. The DSN will be designed to allow for future, yet-to-be-defined, terminal, and network interfaces. The PAT, RSU, RLM, and other switch equipment can be seen in figures 3-5, 3-6, and 3-7. These figures illustrate the network elements for the Western Hemisphere, Pacific, and European geographical areas, respectively.

End office (EO). An EO is an integral part of the DSN. It provides switched call connections and all DSN service features to the user, including multilevel precedence and preemption. The EO will not serve as a tandem in the DSN. It may connect to another EO where direct traffic volume between the two EOs dictates. The EO provides long-distance services by interconnections with SASs and/or MFSs. Dial service attendant (DSA) assistance to all DSN users will be provided through selected EOs.

Switch design technology continues to reduce the need for DSA attendants. Routine tasks associated with older switches are now done by stored program/processor subsystems. Also, there is no longer a need for a separate group of attendants to serve the network and the end offices. A single attendant can service users located within a geographical area. The number of consoles, locations, and staffing levels are the responsibility of the Services.

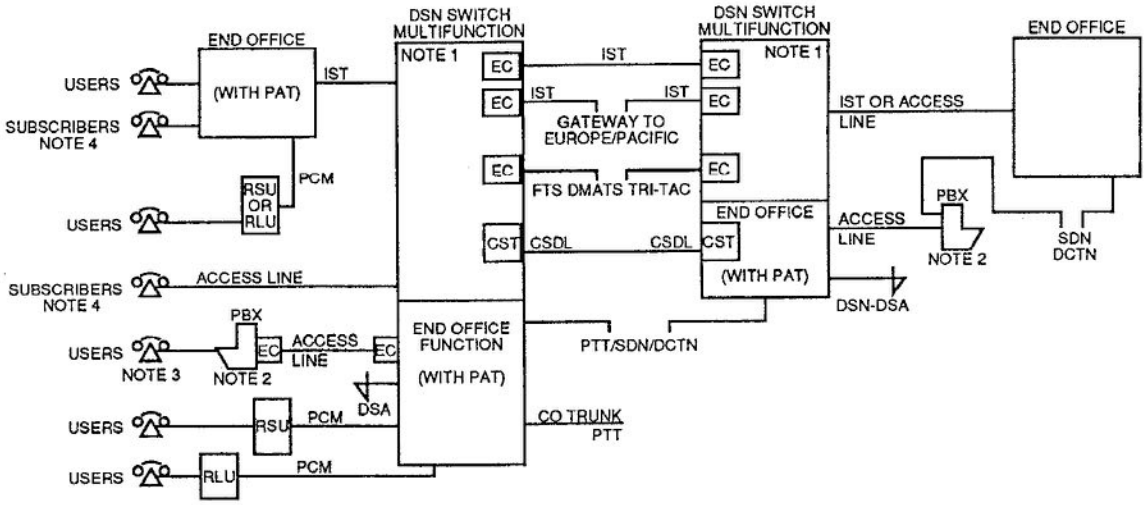
Small end office (SMEO). This digital switch is 1,000 terminations or less and serves as a dial central office and a terminating office in the DSN. The SMEO shall be equipped with access lines without precedence access threshold (PAT) ability to interface with the EO and MF nodal switch. The SMEO access line groups shall be classmarked for various combinations of maximum precedence levels and calling area. The SMEO equipment shall be configured to route ongoing calls to the SMEO access line groups to let C^2 users terminate on the SMEO.

Stand-alone switch (SAS). The SAS functions primarily as a tandem in the DSN and provides long-distance services through interconnections with MFSs and other SASs. As part of the DSN, SASs will be supervised and interconnected to the DSN A/NM subsystem.

Multifunction switch (MFS). This switch incorporates the combined functions of a stand alone switch and an end office switch. No physical division exists between the SAS and EO functions within the MFS, but a logical division exists.

Private branch exchange (PBX). A PBX is a telephone exchange serving a single organization or area, and it requires connection to another telephone exchange for long-distance service. A PBX, either manual or automatic, is customer premise equipment and is, therefore, not an integral part of the DSN. In the DSN, a PBX will be connected to and served by an EO or the EO side of a MFS. PBX subscribers may be offered indirect precedence originating ability through an EO attendant position. Because the PBX is behind the EO side of the DSN, full DSN features may not be available.

Transmission Subsystem. The DCS transmission subsystem consists of interswitch trunks and access lines. The line and trunk elements may consist of Government-owned/leased facilities that include cable, radio, fiber optic, and satellite transmission media. The subsystem initially will have both analog or digital transmission facilities but will

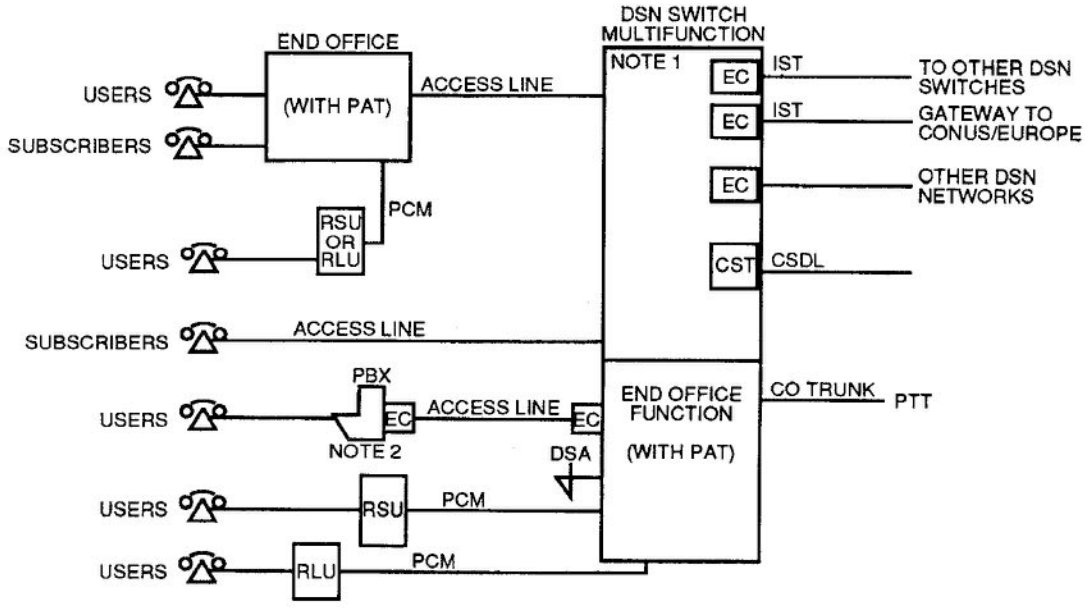


IST - INTERSWITCH TRUNK
PTT - POST TELEPHONE AND TELEGRAPH
DSA - DIAL SERVICE ASSISTANCE
CST - COMMON CHANNEL SIGNALING TERMINAL
EC - ECHO CANCELER
CSDL - CCS DATA LINK
SDN - SOFTWARE DEFINED NETWORK
DCTN - DEFENSE COMMERCIAL TELECOMMUNICATIONS NETWORK

1. TYPICAL MULTIFUNCTION DSN SWITCH
2. PBX'S ARE NOT ELEMENTS OF THE DSN
3. USER'S ACCESS TO THE DSN IS LIMITED TO A PAT OR CLASS MARKED
4. DSN SUBSCRIBERS HAVE DIRECT (UNRESTRICTED) ACCESS TO THE DSN
5. PAT = PRECEDENCE ACCESS THRESHOLD

NPA41-201

Figure 3-5. DSN network elements West Hem (U.S. and Canada).



IST - INTERSWITCH TRUNK
PTT - POST TELEPHONE AND TELEGRAPH
DSA - DIAL SERVICE ASSISTANCE
CST - COMMON CHANNEL SIGNALING TERMINAL
CSDL - CCS DATA LINK
PAT - PRECEDENCE ACCESS THRESHOLD

NOTE:
1. TYPICAL MULTIFUNCTION DSN SWITCH
2. PBX'S ARE NOT ELEMENTS OF THE DSN

NPA41-200

Figure 3-6. DSN network elements (Pacific).

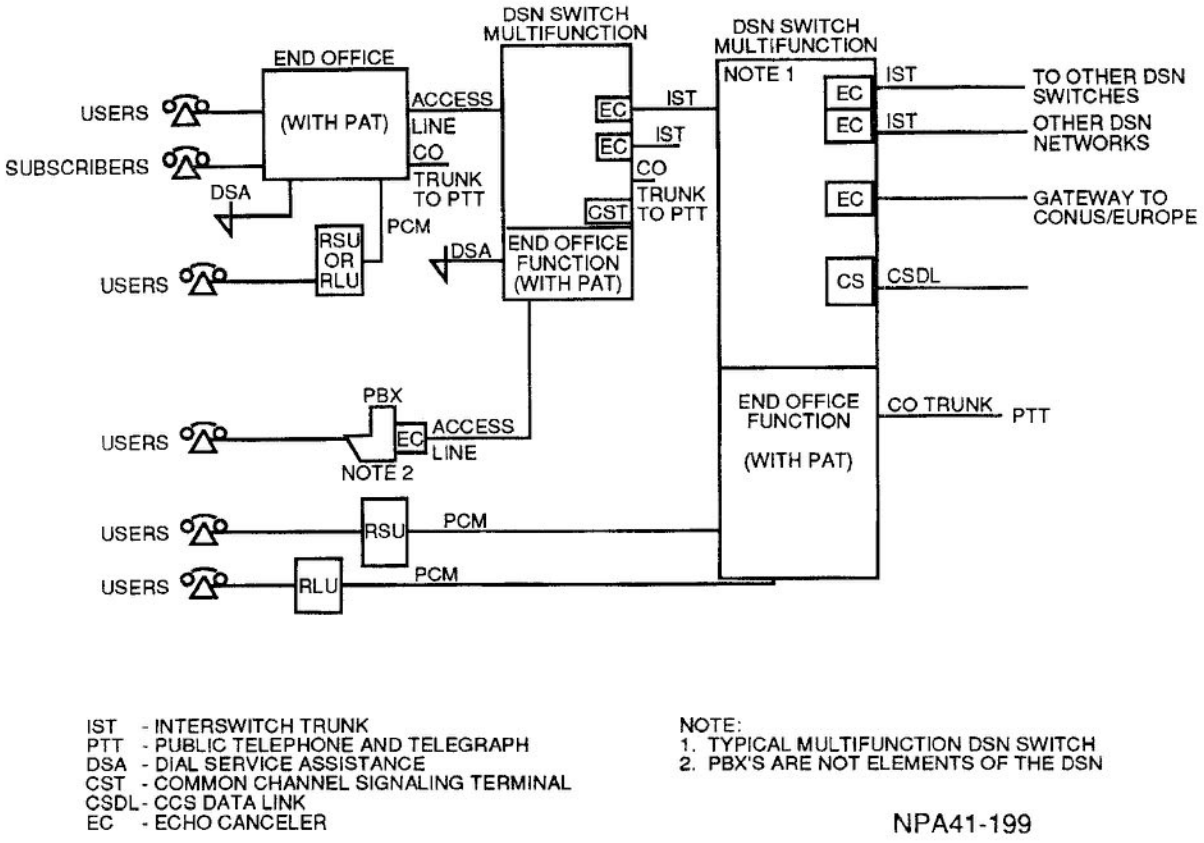


Figure 3-7. DSN network elements (Europe).

eventually use only digital facilities. A proper mix of various transmission facilities will be used to make sure of survivability and versatility of the network. There are three transmission subsystem elements.

Interswitch trunks (IST). A trunk is a single or multichannel connection between terminal facilities. In the DSN, ISTs are the transmission links between two DSN switches.

Access lines. Access lines are single or multichannel connections that allow user equipment to gain access to the network. The DSN will provide the opportunity to drop the individual four-wire subscriber lines, including the special interface equipment. Most of the four-wire voice lines will become two-wire user loops homed on the serving EO with improved service and capabilities.

Dual homing. Where economically feasible, the goal architecture of the DSN is to have all end office locations "dual homed" (the tandem portion of the network will be entered through two multifunction switches). All DSN switches that support "high priority" functions and facilities with an established mission requirement for survivability will be dual homed. Where possible, diverse DCS transmission paths will be used to support dual homing requirements.

Timing and Synchronization Subsystem (T&S). Synchronization refers to a method of operating digital switching and transmission systems at a common or synchronized clock rate. Improperly synchronized clock rates cause portions of the bit streams to be lost in transmission.

Because digital switching systems are directly interconnected by digital transmission facilities, the DSN requires synchronized clock rates. The timing and synchronization subsystem for the DSN is based on the use of a highly accurate frequency reference. This frequency is obtained from a station clock synchronized to the worldwide LORAN C navigation system, to the Department of Defense Global Positioning System (GPS) satellite, or to another highly accurate source such, as a cesium beam atomic clock. Because timing for DSN switches can be disseminated through the transmission hierarchy, clocks at minor nodes can be slaved through transmission links to timing systems at major nodes.

Administration/Network Management (A/NM). As a provider of worldwide communications for the armed forces, DCA will manage a large, geographically dispersed network. This network includes more than 200 US Government-owned switches in Europe and more than 60 US Government-owned switches in the Pacific, as well as leased switching and transmission services in the Western Hemisphere and Hawaii.

Comprehensive computer support that is survivable and secure will be required to maintain control of this large

network. This computer support will help with these network functions:

a. Monitoring and surveillance to detect performance abnormalities automatically.

b. Implementing real-time controls that prevent switch or network congestion.

c. Analyzing traffic data to permit continuous optimal operation of the network.

The A/NM system will have made contingency plans in advance that address expected outages. Also, computer aids that decrease personnel requirements will be used locally and from remote locations in administration, operations, maintenance, and network management of network elements.

A/NM will be implemented through a hierarchy of control centers. Traffic and call data from switching subregions, along with certain alarms, will be relayed by Subregional Control Facilities (SRCF) to the Area Communications Operations Centers (ACOC). SRCFs, which are run by the military departments, are responsible for administration and maintenance associated with subregional switches, while DCA-run ACOCs provide theater-wide administration and network management. Alternate ACOCs do a subset of the management functions and are ready to assume full control in the event the parent ACOC malfunctions. The DCA Operations Center in Arlington, Virginia, coordinates worldwide operations and handles operational reports from contracted A/NM facilities for the Western Hemisphere.

231. The functions and associated equipment of the digital multiplex switching system

Digital Multiplex Switching (DMS) Equipment. The DMS is a time-division multiplex central office switch that switches pulse code modulation (PCM) telephone traffic and directly interfaces with T-1 or equivalent lines. It is designed to be fully compatible and competitive with today's telephone networks and converts analog telephone traffic into PCM format, which is then switched at electronic speeds. There are three series, and each has its own specific use. The DMS-100 is designed to provide local customer telephone switching from 1,500 lines up to 100,000 lines. The DMS-200 is designed for toll operation servicing up to 60,000 trunks, and the DMS-300 is a toll machine designed specifically for international gateway operation. The DMS-100/200 is used for combined local/toll applications.

The system is partitioned into four major blocks, as illustrated in figure 3-8, and integrated into an efficient and versatile telephone switch to serve as a local switch, a toll switch, or a joint local/toll switch.

The broken line drawn between the peripheral modules and the network represent 30 channels of PCM encoded

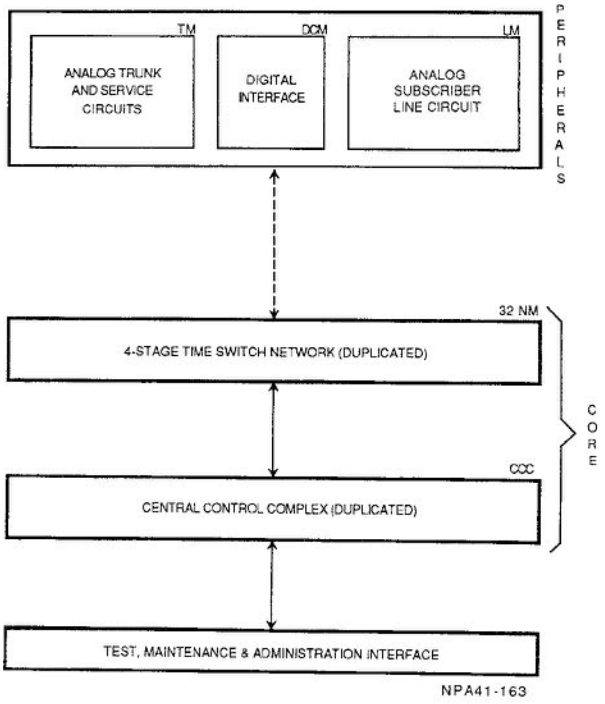


Figure 3-8. System partitioning for DMS.

speech, multiplexed in time with one synchronizing channel and one signaling channel. The resulting 30 + 2 channel digital speech link has a transmit appearance and a receive appearance on the network, thus giving a four-wire transmission characteristic to the digitized speech. The digital speech links can be assigned to trunk or line speech, thus providing a universal network for local and/or toll applications.

The analog line and trunk speech and signaling are encoded (or decoded) into (or from) the 30 + 2 channel PCM format by the line module and the trunk module, thus eliminating the need for external channel banks. The digital carrier module interfaces directly with T-1 carrier systems and provides a convenient point for synchronization, alarm interfacing, and extracting the trunk signaling information. The peripheral processors in the line modules, trunk modules, and digital carrier modules relieve the central processor unit (CPU) of time-consuming repetitive tasks such as digital collection and circuit supervision. The CPU concentrates on intelligent tasks, such as message handling, translation, and resource management.

Network. The entire network is physically partitioned into 32 fully duplicated network modules (NM) for economical startup and incremental growth. The following is a list of components that make up the network along with their functions.

Network message controller (NMC)—functions as a message center for messages between the peripheral processors and the CPU, as well as network control commands from the CPU to the network modules.

Trunk module—encodes and multiplexes incoming speech from a maximum of 30 analog trunks into 8-bit PCM format. It combines them with internal control signals as well as the trunk supervisory and address signals for transmission at 2.56 mps to a single input appearance on one of the duplicated network modules. The 30 digital speech signals and the two control channel signals received from the associated output appearance on the same network module are demultiplexed and decoded by the trunk module into three individual channels of combined analog speech and signaling.

Digital carrier module (DCM)—interfaces directly with the T-1 office repeater, which eliminates channel bank requirements. The DCM carries out synchronizing of and alarm interfacing with the T-1 digital carrier system. It extracts or inserts trunk signaling information for interface format of the switch.

Line module (LM)—is a single bay with a maximum capacity of 640 subscriber lines that access the network through two (minimum) or four (maximum) digital speech lines. The maximum number of digital speech channels available to a line module is 120; hence the line module is designed to operate as a concentrating stage.

Central control (CC)—consists of a synchronized pair of central processor units and a data store, which are accessible through separate program store and data store buses. Interfacing with the peripheral units is carried out by duplicated central message controllers. The central message controllers operate in a load-sharing mode and relieve the central processor units of the real-time load of communicating with the peripheral units and the network.

Input/output controller (IOC)—is a self-contained subsystem that interfaces input/output (I/O) devices such as magnetic tapes and terminals with the central message controller. It is made up of a message processor connected to some input/output device interface circuits by a bus. I/O terminals and magnetic tape units interface with the CMC and the CPU through the I/O device interface circuits. Up to six input/output controllers can be served by the central message controller at one time.

Call Processing. The DMS software system is basically a message-driven system. Messages between the peripheral processors and the central control convey events occurring at the peripherals and commands from the central control.

For example, on a dial pulse intraoffice call, a subscriber origination is reported to the central control by the line module peripheral processor through the network message controller. The central control sends a series of commands instructing the peripheral processor to assign a digital channel, send dial tone, receive digits, and report back to the central control after a predetermined number of digits have been received. When the central control determines the called subscriber line from the received digits, it sends a message to the originating peripheral processor to stop receiving digits, and another message to the right terminating peripheral processor to stop scanning and assign a digital channel.

The central control, on receiving acknowledgement messages from both peripheral processors, sends a message to the network monitor to setup the network connection. It then sends a message to the originating peripheral processor to send audible ringing tone and a message to the terminating peripheral processor to start ringing the called line. When the called subscriber answers, the event is detected by the originating peripheral processor and a message is sent to the central control. It in turn sends a message to the terminating peripheral processor to stop ringing and a message to the originating peripheral processor to remove ringing tone and to cut through.

If the calling line now goes ON-HOOK, the originating peripheral processor sends a message to the central control, which in turn commands the network monitor to release the network connection and sends a message to the originating peripheral processor to disconnect the digital channel and resume going ON-HOOK. The processing of other calls is done similarly by passing messages between the peripheral processor of each trunk module, digital carrier module or line module, and the central control.

Please write your response to unit self-test questions and then check the text answers at the end of the unit.

SELF-TEST QUESTIONS

227. Design objectives and switch connectivity of the AUTOVON system

1. Which design objective does redundant switch connectivity provide? survivability

2. Speed of operation meets which design objective? Responsiveness

3. How are AUTOVON switches connected?
Via interswitch trunks

4. What are access lines?
connect subscribers to a switch

5. Describe an AUTOVON subscriber.
4 wire phone with direct access to DSN.

228. Uses and capabilities of the Defense Switched Network

1. DSN users fit into what two categories?
command & control & users & support users

2. DSN will be how much larger than AUTOVON?
15 - 20 times

229. Design objectives of DSN

1. What are the five key objectives of DSN?
survivability, cost, reliability responsiveness, security

2. What will make end-to-end encryption available to many more users than previously possible?
STU - III

3. Why will DSN reduce manpower requirements?
New digital switching & TX equip & more reliable

230. Major subsystems of DSN

1. What are the major subsystems of DSN?
switching, TX, timing, SYNC,

2. What two elements make up the transmission subsystem? inter switched trunks & access lines

3. How will DSN maintain timing and synchronization? From a station clock sync. to the world wide loran c navagation system to the department of defense

4. What DCA element provides theater-wide administration and network management of DSN?
ACOC's

231. The functions and associated equipment of the digital multiplex switching system

1. What connects the peripheral modules and the network module in a DMS system? 30 channels of PCM encoded speech, mixed with on channel of sync & one of signaling
2. List the intelligent tasks that the central processor unit performs. message handling, translation & resource management
3. Which component is used to eliminate the channel bank requirement when interfacing to a T-1 carrier? PCM
4. The input/output controller interfaces magnetic tapes and terminals with what other unit? CMC central message controller
5. What must the central control unit receive before it can send the message to setup the network connection? acknowledgement messages, temporal processors

3-2. Automatic Secure Voice Communications (AUTOSEVOCOM)

The secure voice network is configured to give maximum service to the national command authorities, unified and specified commands, and other essential users both in and out of the Department of Defense.

The users of the secure voice network are broken into two categories: narrowband and wideband. The network as a whole is broken into three functional elements: (1) switching centers, (2) transmission facilities, and (3) subscriber terminals. Each element, together with the various subscriber equipment configurations, are covered in this section. This section will also discuss the operation of the secure voice network.

232. Elements of the secure voice network

Subscribers. As stated earlier, secure voice network subscribers will be referred to as either narrowband or wideband subscribers. You probably remember from technical school that the terms "narrowband" and "wideband" refer to the frequency bandwidth required to transmit a signal. This is true; a wideband signal is one that occupies 20 kHz or greater bandwidth, and narrowband signals occupy something less than 20 kHz. The wideband subscribers in the secure voice network transmit and receive signals in digital form at 50 kbps. Narrowband subscriber signals are also digital at 2.4 or 4.8 kbps.

The bandwidth required to transmit a wideband digital signal after it is converted to analog form is almost 48 kHz, which definitely exceeds the 20-kHz minimum standard in defining a wideband signal. Thus, these subscribers are termed wideband.

Digital signals of 2.4 or 4.8 kbps are also converted to analog form but require only approximately 4 kHz of bandwidth for transmission; hence the term "narrowband subscriber."

Narrowband terminals. Two similar types of narrowband subscriber terminals are used in the secure voice network. They are the type I terminals, for all classifications of conversations, and type II terminals, for sensitive, but unclassified, and privacy conversations.

Regardless of type, the terminal is capable of transmitting either clear (normal) or secure communications, in either the voice or data mode, at 2400 or 4800 bps. The built-in modem allows data communications through the data port (RS-449/232) over full- or half-duplex transmission in either synchronous or synchronous format.

Secure voice/data telephone terminal (STU-III). The STU-III is a small, easy-to-use telephone that can be used for clear or secure communications (fig. 3-9). A significant feature of all STU-IIIs, also known as the low cost terminal (LCT), is parallel in development, production, and interfacing of the models made by different companies. The terminal

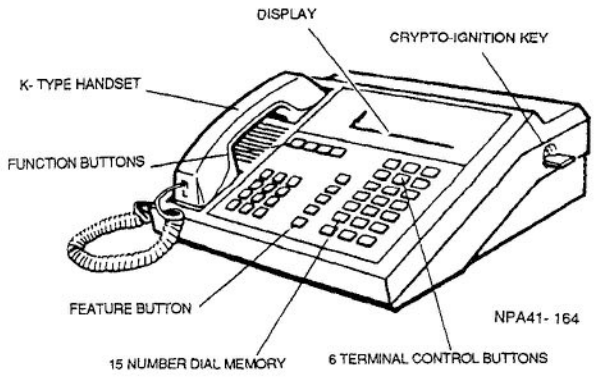


Figure 3-9. Secure voice/data telephone terminal (STU-III).

is easy to install and is plug compatible with standard modular or multiline (key system) connectors. It operates in the full-duplex mode over a single-telephone circuit using echo canceling MODEM technology. The primary operation of the unit is at 2400 bps, and some models also offer repertory or speed dial ability and custom PBX interfaces.

Setup involves simply plugging into the existing telephone wall outlet and commercial AC power. The terminal initiates its own diagnostics and is then ready for clear operation. The operation is similar to that of any "normal" telephone. The user picks up the receiver, gets a dial tone, and places a clear call. Transition from clear to secure is done simply by pressing the secure voice (or secure data) function button. Setup of the secure link requires less than 12 seconds and is done without any added user or outside operator involvement. The user can program the terminal for proper data transmission directly from the faceplate. The terminal control buttons are also used to initiate loading of the keys that "unlock" the COMSEC functions of the terminal and enable secure transmission (fig. 3-10).

The secure voice and data capabilities of the phone are "unlocked" through use of a crypto-ignition key (CIK). Added security is provided by displaying the identification of the called party on the terminal. This display includes the name associated with the called party, the level of security, and the mode of transmission (voice or data). Calls can be switched from secure back to clear or from secure voice to secure data without disconnecting communications.

Besides preventing the interception of communications, the STU-III is designed to prevent either external monitoring or compromise. The physical design of the terminal complies with TEMPEST requirements and offers added options such as push-to-talk handsets and high-altitude electromagnetic pulse (HEMP) protection. In the event the physical integrity of the terminal is compromised by authorized parties, all keying material held within the terminal is erased or zeroed.

The STU-III is designed with the flexibility to provide unmatched user accessibility and control. Control of COMSEC functions is provided through the CIK, and some units allow up to 32 CIKs to be programmed for access to each terminal. These CIKs are grouped into four key sets. Because each key set is completely independent, they can each operate in the terminal using different identifications and levels of security. Consequently, one terminal can provide secure communications, including positive identification, for up to four different groups or projects operating at up to four different levels of security.

This terminal does not limit an individual's CIK access to only one terminal. For people who work in several locations, it allows an individual's CIK to access up to four different terminals in different locations. The flexibility of the COMSEC control features makes sure that the terminal is both accessible and easy to use.

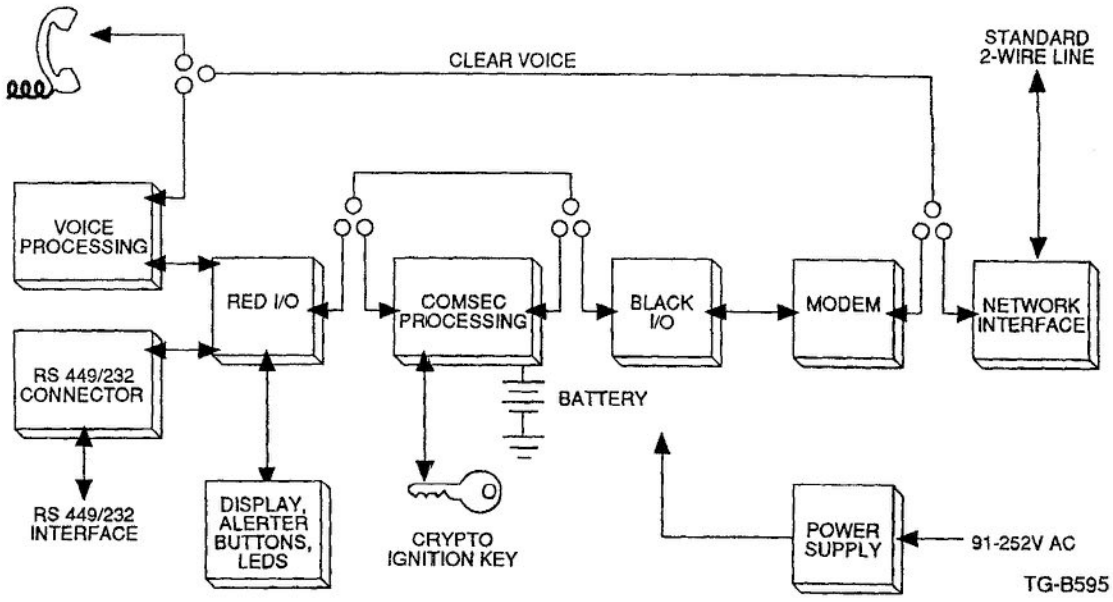


Figure 3-10. Components of the STU-III.

Secure voice/data cellular terminal (STU-III). The cellular telephone is a member of the STU-III family and is interoperable with all other versions of the STU-III. This telephone combines cellular mobile radio-telephone technology with advanced secure voice/data communications. The unit includes a message center, integrated with the standard cellular handset, that can be conveniently mounted inside a vehicle and provide all STU-III functions including an authentication/classification display. It is designed to operate in a mobile vehicle and in all CONUS cellular telephone systems and many of the foreign cellular telephone systems (fig. 3-11).

The cellular terminal provides a totally new concept in cellular radio communications security. It includes the following components:

a. Cellular radio—consists of a transceiver, handset, and hang-up cup.

b. Secure cellular terminal—provides users with the highest level of security commercially available today. When monitored over the cellular network or the public switched telephone network, the terminal's transmissions are totally unintelligible to an unauthorized listener.

c. Secure message center—displays call process and terminal authentication messages. The message center push-buttons control the clear, secure voice, and secure data operating modes. The message center can be mounted as a pan of the handset console or at any other preferred location.

d. Crypto ignition key—provides users the ability to activate the secure operating modes.

Since new STU-IIIs are coming on the market, from new vendors trying to get involved in this new technology, the terminal at your station may not be exactly the same as the one mentioned above. The operating principle is basically the same for all units, and this section should familiarize you with its general operation.

Wideband terminals. Wideband subscriber terminals (WBST) require a direct connection to a secure voice switch. This is due to the large frequency bandwidth required to transmit the signal. The switch facilities that serve the wideband terminals may be either automatic or manual, as you will see in the next section.

The equipment required for the wideband subscriber terminal is as follows:

a. DSN compatible desk set (four-wire telephone).

b. TSEC/KY-3 or similar ciphony equipment.

c. Modem (if a connection through a switch to a distant WB subscriber is required).

The DSN compatible desk set is nothing more than a standard four-wire telephone. The frequency output is in the voice-frequency range (approximately 300-3400 Hz). The terminal impedance for this equipment is 600 ohms.

The TSEC/KY-3 is housed in a steel cabinet within the subscriber's office or area. Its purpose is to convert the voice signal from the desk set into an encrypted 50-kbps signal. The 50-kbps signal is really a 478-kbps serial data stream representing voice input, with 2 kbps added by the KY-3 to maintain synchronization and control of the ciphony units. This 50-kbps data stream, though termed a digital stream, actually seems to be (and can be measured as) an isochronous, quasi-analog signal. The output of the KY-3 can be fed directly through a secure voice switch to any other WB subscriber homed on that same switch. For calls from one WB subscriber to another at a different location, the 50-kbps signal from the KY-3 must be converted to analog form by a modem. The output of a secure voice modem occupies a frequency bandwidth of approximately 60-108 or 48-kHz

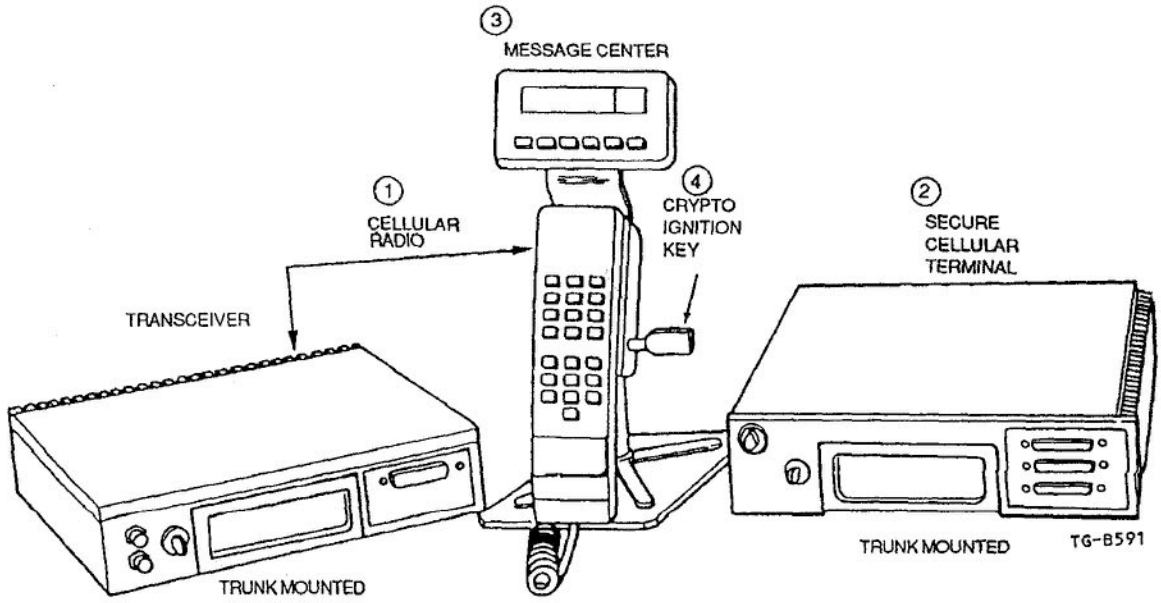


Figure 3-11. Secure vioce/data cellular terminal (STU-III).

total. As you can see, a WB secure voice circuit would occupy a complete group of an FDM system. Another method of transmission is through TDM systems. In this case, the 50-kbps signal is fed into a digital convener (like a CV-3034) to convert the isochronous 50-kbps signal into a 50-kbps synchronous signal that can be readily sampled and encoded by a time division multiplexer, such as the AN/FCC-98 terminals.

Secure Voice Switches. In the preceding paragraphs, we have talked around the secure voice switches. You probably have an idea already about the function of a secure voice switch. Here we will look at four types of secure voice switches in use in the secure voice network. The switches are the AN/FTC-31, WECO 758A, WECO 758C, and SECORD. We will discuss each switch separately and make comparisons as we do. Before we do, keep in mind that narrowband subscribers are widely dispersed and each can call another wideband subscriber without going through a secure voice switch. The wideband subscriber must go through a secure voice switch for all calls.

AN/FTC-31. The AN/FTC-31 is an automatic four-wire telephone switch. It is specifically designed for wideband secure voice communication. The switch is provided line terminations in 25-line increments; i.e., 25, 50, 100, etc. Subscriber terminations are in increments of 20; i.e., 20, 40, 60, etc. The AN/FTC-31 is capable of providing:

a. Automatic dial connection between local subscribers served by the same switch.

b. Automatic dial connection between local subscribers of an AN/FTC-31 switch and distant wideband subscribers of another AN/FTC-31 switch.

c. Access to manually established long-distance calls through narrowband facilities.

Operational capabilities of the FTC-31 switch include automatic preemption of calls and high-traffic capacity where up to 80 percent of its terminating lines can be interconnected before any blocking of calls will occur. Other capabilities include automatic fault isolation within the switch and class of service identification for each subscriber.

As stated in the preceding paragraph, the AN/FTC-31 is capable of providing its wideband subscribers with interface and access to narrowband lines and subscribers. This operation is carried out through the secure voice access console (SEVAC). Since the SEVAC is a very important unit in the secure voice operation of the AN/FTC-31, let's discuss its capabilities. The SEVAC, with associated ancillary equipment, will provide the following capabilities:

a. Interface with the AN/FTC-3 I for manual completion of long-haul calls originating and/or terminating at the associated AN/FTC-31.

b. Interface with DSN, JOSS, and other secure voice switches to manually complete incoming or outgoing calls over the NB lines.

c. Provide operator-controlled conferencing facilities to permit subscribers of the associated AN/FTC-31 switch to be conferenced in a local conference bridge with one NB connection. This lets a local conference be interconnected with a distant conference or a single NB secure voice subscriber over the NB line. One five-line conference bridge may be provided for each 25 lines of the associated AN/FTC-31. Each of the conferencing bridges may connect up to five local WB subscribers and one NB trunk. Two conference bridges may be interconnected by the operator to conference 10 local subscribers and one NB trunk if desired. The operator can preempt any conference.

d. Automatic disconnect of either WB trunks or NB access lines on call completion.

e. Automatic detection of either an DSN preempt tone or AN/FTC-31 preempt tone, with subsequent preempt tone notification automatically sent to either AN/FTC-31 or NB access line and disconnection of associated circuits.

f. Provide a patch and test facility for maintenance testing and cross-connection of circuits associated with the SEVAC and AN/FTC-31.

The SEVAC is a black facility, since all interconnections between WB and NB trunks are made on the encrypted side of the console's secure equipment. The conference equipment and portions of the NB interfaces are considered RED equipment, requiring installation by RED/BLACK criteria. The SEVAC operator uses a TSEC/KY-3 in the secure mode to setup calls to the AN/FTC-31, but the SEVAC operator cannot enter any established conversation or conference. See figure 3-12 for a typical AN/FTC-31 and SEVAC operation.

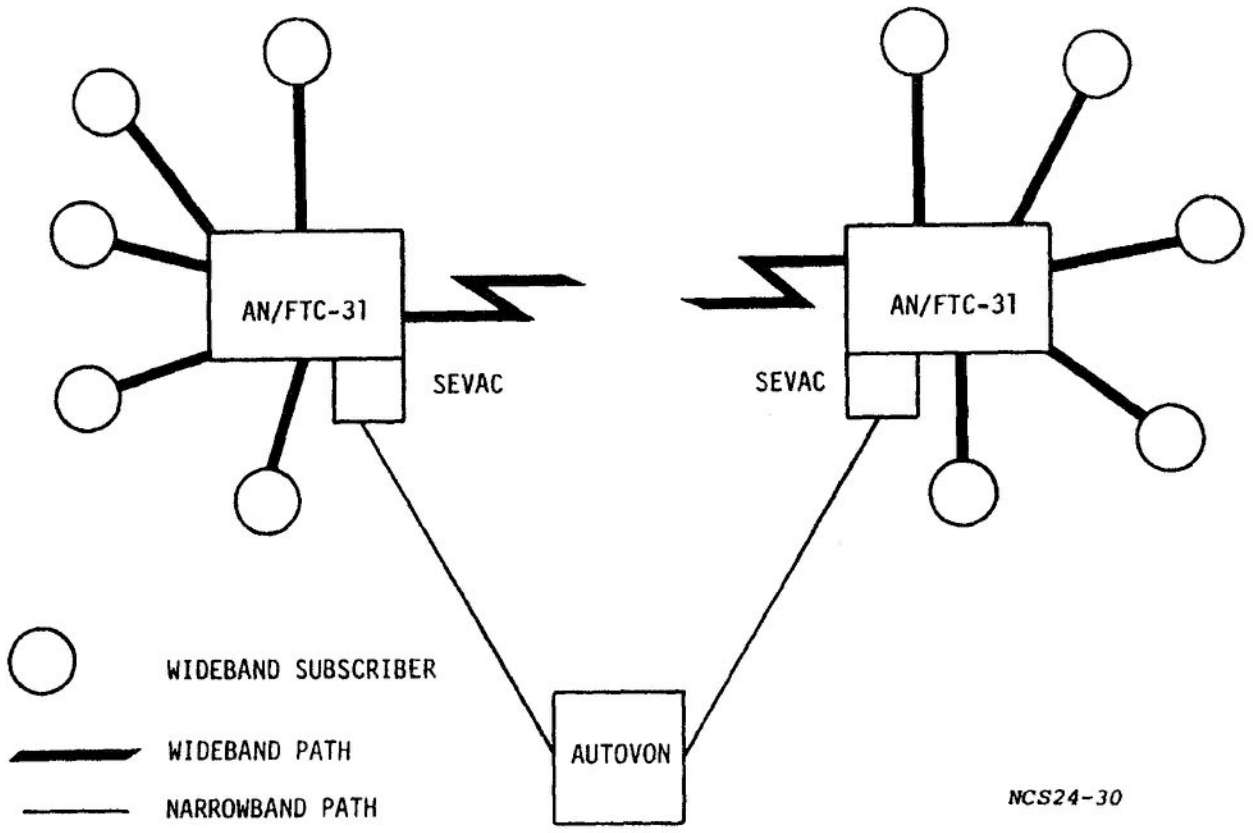


Figure 3-12. AN/FTC-31 switch with SEVAC.

62

WECO 758A. The Western Electric Company 758A used in secure voice operation is a manually operated, 40-line, wideband, four-wire secure voice switch. Secure voice subscribers served by the 758A have Government-furnished WB ciphony TSEC/KY-3 equipment. Subscribers of the 758A use end-to-end encryption through the TSEC/KY-3s; therefore, the 758A switch is designated as a BLACK switch. The following switching actions are done, supervised, and controlled by the WECO 758A operator:

a. Connection of calls between local switch subscribers.

b. Connection of calls between local switch subscribers and subscribers served by another secure voice facility.

c. Handling of preemption procedures during local and local/distant circuit operation.

d. Handling of service assistance requirements with the overall switch-operating responsibility.

e. Manual operation between the 758A and other WB and NB secure voice facilities will be provided. Interface to other WB facilities will be through conditioned WB trunks/circuits. Interface to NB facilities will be through conditioned NB trunks/circuits with WB-to-WB conversion equipment used at the 758A.

WECO 758C. The Western Electric Company 758C is an automatic, four-wire, WB secure switch. The present size of switches used in the network varies from 60 to 250 termination lines and trunks. Secure voice subscribers served by the 758C have Government-furnished WB ciphony TSEC/KY-3 equipments. Subscribers of the 758C use end-to-end encryption through the TSEC/KY-3; therefore, the 758C is designated as a BLACK switch. An operator console is provided to take subscriber lines "out of service," to provide normal attendant functions for preemption, and to establish calls over NB access lines. The interface to NB facilities is done through wideband to narrowband conversion equipment located at the WECO 758C switch.

Secure voice cord board (SECORD). A SECORD is a four-wire, manual switchboard with associated control equipment to provide secure voice service for up to 15 TSEC/KY-3 subscribers. A SECORD operator can interconnect local subscribers or connect them to one of five NB access lines. A SECORD establishes calls in the clear voice mode. When a calling party is connected to a called party, a transfer is made to the secure mode by the subscribers on local calls. If an NB access line is involved, the operator makes the transfer to the secure mode. All traffic through the SECORD is in the secure mode. A SECORD console can be remotely located from associated switching equipment; it also can be desk mounted:

a. A SECORD provides an NB interface to DSN, JOSS, or other DCS NB facilities for WB TSEC/KY-3 subscribers.

b. A SECORD provides the following added capabilities:

(1) Operator preemption of local WB or NB access lines with tone notification.

(2) Tone notification to SECORD subscribers of DSN preemption through a switching control subsystem (SCS).

A typical configuration is shown in figure 3-13. As shown by this figure, the signaling rate is 50 kbps between the subscribers and the SECORD and between one subscriber and another. When a subscriber wishes to go long haul, however, the wideband signal often must be converted to a 2400-bps NB signal for transmission over standard DSN or other voice-frequency circuits.

Summary. The function of the secure voice switch, whether automatic or manual, is to establish a connection from a calling terminal, through the network, to the called terminal, and to disconnect the circuit when a call is completed. Figure 3-14 is a typical area arrangement for a secure voice network.

233. Operational elements of the secure voice network

Narrowband Operation. As you have already learned, it is not necessary for a narrowband subscriber to go through a secure voice switch to place secure calls. All that is required for one narrowband subscriber to talk secure to another narrowband subscriber is that they have compatible equipment and a communication path (i.e., DSN, FDM channel, etc.). However, the only way a narrowband subscriber can be connected to a wideband subscriber is through a secure voice switch.

Connections between narrowband subscribers are straightforward and simple. The calling terminal establishes voice contact with the called party. When the two parties are ready to go secure, the originating and terminating parties activate the switch control unit (by operator assistance or manually themselves). On completion of the call, both parties resume their original status by disconnecting the switch control unit.

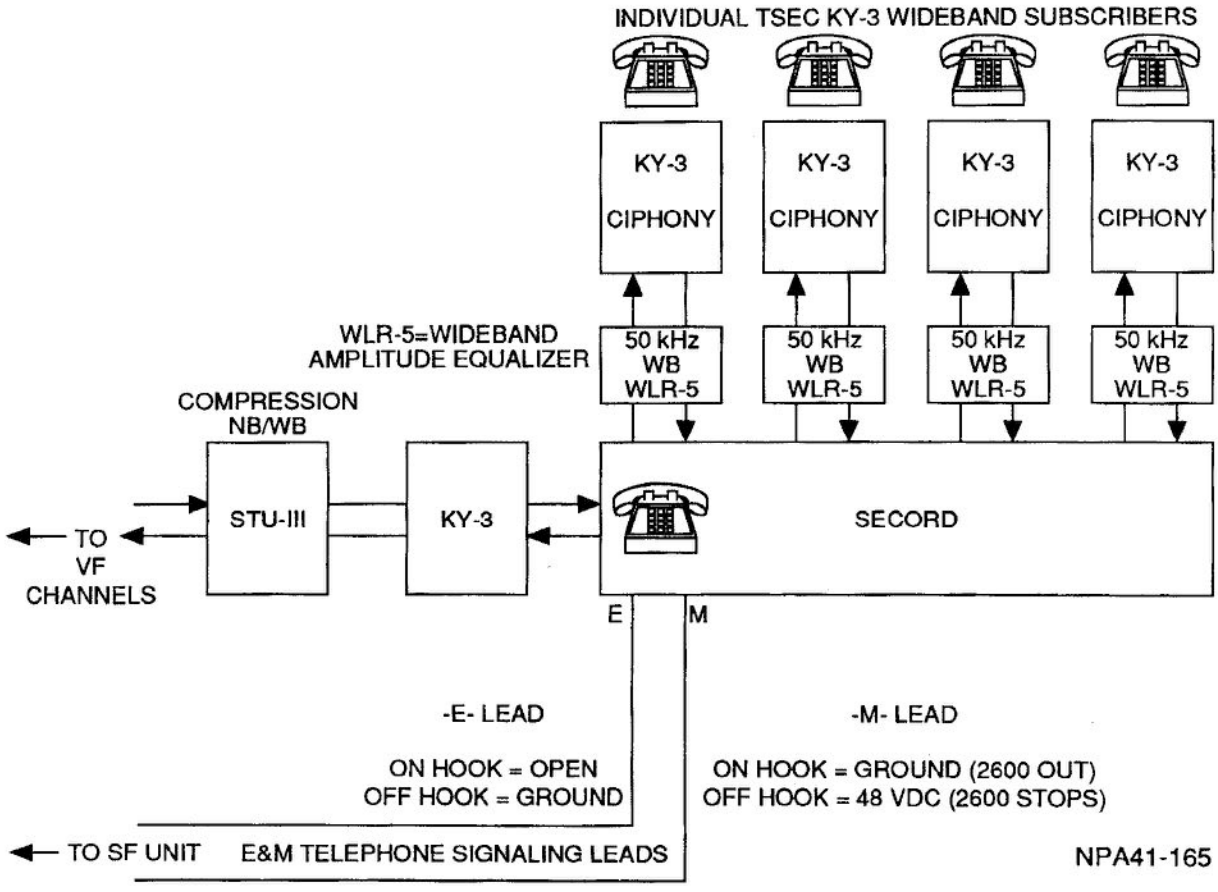


Figure 3-13. Typical SECORD terminal.

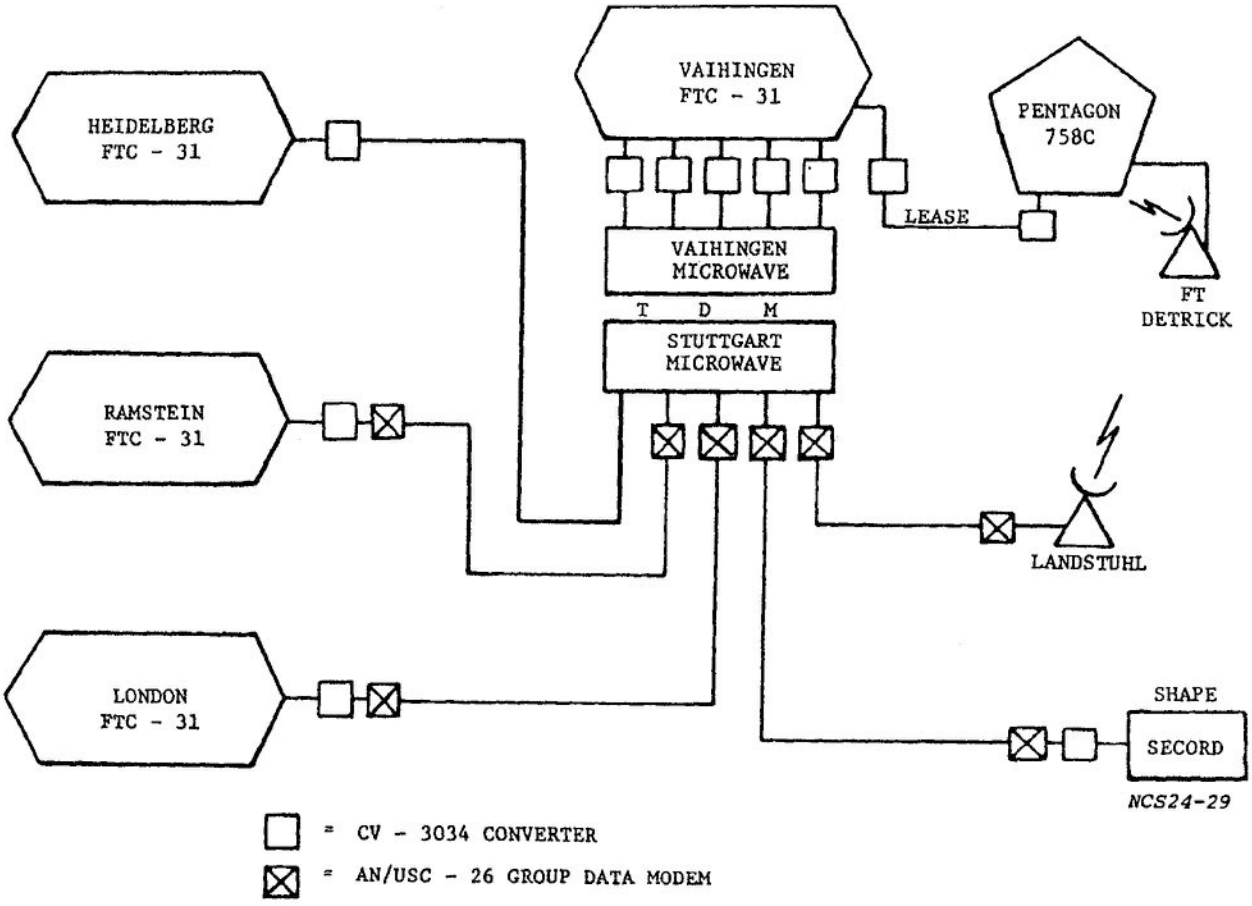


Figure 3-14. Secure voice network in European area.

Wideband Operation. The operational signal sequences used on wideband secure voice lines depends on the type of switch servicing the wideband subscriber. In the following paragraphs, we will discuss the various types of signals used to operate a wideband secure voice terminal. These signals are divided into two types: analog and digital. The analog signals are essentially the same as those used in the DSN system. They are used for circuit supervision, information, and control. Another form of analog signal used in wideband service is clear speech (voice). Voice signals on the wideband path are used in establishing calls.

When voice is used, the two parties on the call establish voice contact, then switch to the cipher mode. At this time, the signal is converted to an encrypted 50-kbps digital signal. Supervisory and control signals are used to establish connections through a wideband switch or switches much like a DSN call.

Two signaling sequences are covered later in this section. As stated earlier, the sequence of signals used is determined by the type of switch processing calls. The following examples are for calls made between subscribers connected to the same secure voice switch.

Supervisory and control sequence through an automatic switch. A wideband secure voice subscriber, using a TSEC/KY-3, has the following sequence of events for making and completing a secure voice call:

a. When the four-wire subset telephone is in an on-hook (idle) condition, a 2600-Hz tone is transmitted to the switch. The level of this tone is a –20 dBm0.

b. When the subset goes off-hook, the TSEC/KY-3 drops the 2600-Hz tone. Absence of the tone is detected by the secure voice switch. The switch, in turn, sends a dial tone (600/1200-Hz steady tone) back to the TSEC/KY-3. The dial tone indicates that the switch is ready to receive.

c. On receiving the dial tone, the subscriber then dials the right digits. The digits are convened (by the subset) to dial pulses and are transmitted. The dial pulses are really short bursts of 2600 Hz at a level of –9 dBm0.

d. The automatic switch receives the pulses, processes them, and selects the proper subscriber line. If the called subscriber is busy or disconnected, the switch will originate a busy signal of 600/1200 Hz (interrupted) and send it to the calling subscriber. If the called subscriber is on-hook and ready to receive, the switch will send a ringing tone (1000 Hz

interrupted, on 2 seconds and off 4 seconds) to both calling and called parties. At the called terminal, the ringing tone activates a 19-Hz power supply that rings the called subset.

e. As soon as the called subscriber goes off-hook, the terminal equipment automatically switches to the cipher mode and transmits a 50-kbps encrypted signal back through the automatic switch to the calling party. When the calling terminal equipment receives the 50-kbps signal, the TSEC/KY-3 switches to the cipher mode and starts transmitting a 50-kbps encrypted signal, also. Both terminals remain in the cipher mode as long as they are receiving the 50-kbps signal.

f. When the call is completed, both parties go on-hook. This causes each TSEC/KY-3 to stop transmitting the 50-kbps signal and transmit a disconnect signal of 2600 Hz at a level of –9 dBm0. After 260 milliseconds, the TSEC/KY-3 drops the level of the disconnect tone to –20 dBm0, the normal on-hook signal. The automatic switch recognizes the (–9 dBm0, 2600 Hz) disconnect tone and disconnects the path through the switch.

Supervisory and control sequence through a manual switch. The sequence of events used in completing calls through a manual switch is different from those described above. The following is an explanation of how a wideband subscriber places calls through a manual secure voice switch:

(1) The subscriber wishing to place a secure voice call goes off-hook with the telephone subset. This action removes the 2600-Hz tone (normal on-hook condition) from the line to the secure voice switch. The loss of the 2600-Hz tone activates a light and buzzer at the switchboard operator's position.

(2) The operator answers the call. At that time, the subscriber requests the desired subscriber. This exchange of information is in a clear text voice.

(3) The operator then rings the desired subscriber by placing a 1000-Hz tone on the called line.

(4) When the called subscriber answers, both terminals are switched to the cipher mode. This switch may be manual or automatic, depending on the wiring configuration of the subscriber and switch.

(5) When the call is completed, both terminals go on-hook. This signals the operator to disconnect the circuit path through the switch.

Keep in mind that these descriptions are very general. Actual operational sequences may vary from switch to switch and subscriber to subscriber.

Secure Voice Switch and Subscriber Connection. We have looked at two examples of subscriber and switch connections for wideband secure voice users. Here, we will discuss the circuits that connect the subscribers to other subscribers or to secure voice switches. We will also discuss the circuits used to connect the various secure voice switches together.

In technical school, you learned that the Defense Communications Agency (DCA) sets forth standards or parameters that circuits must meet to support specific types of traffic. Those parameters were for circuit characteristics such as frequency response, delay, noise, etc. The following are the parameter codes and explanations for circuits serving 50-kbps wideband subscribers and secure voice switches.

G1 circuit parameter code. This code applies to a circuit that interconnects two TSEC/KY-3 subscriber terminals. This code also applies to a circuit used to connect a TSEC/KY-3 terminal to an automatic switch that has internal equalizers. The AN/FTC-31 and WECO 758C both have equalizers on all receive lines connected to the switch. An example of a G1 circuit is shown in figure 3-15,A. The terminal equipment (TSEC/KY-3) has been designed to operate properly over a circuit that meets the specifications set forth in the DCS technical schedule for this parameter code.

G2 circuit parameter code. This code applies to circuits connecting a TSEC/KY-3 terminal to a SECORD or AUTOSEVOCOM switch that does not have internal equalizing equipment. An example of a G2 circuit is shown in figure 3-15,B.

G3 circuit parameter code. This code applies to a circuit connecting two switches in a local area; i.e., geographically close enough so that long-distance facilities, such as a carrier system, are not required. Equalization is required for this code, and repeater amplifiers may be required if level loss warrants them. Figure 3-15,C, shows a G3 circuit.

Z4 circuit parameter code. This code applies to circuits interconnecting wideband switches through long-distance facilities. Z4 also applies to a circuit used to connect a subscriber terminal to a secure voice switch through long distance facilities. Z4 circuits are often complicated and, in some cases, may involve changing modulation methods for different types of transmission facilities (e.g., FDM to PCM). Figure 3-16 shows examples of Z4 circuits. Notice that the circuits are different; however, they must both meet the same specifications from end to end. You should also see that, if a call is made from a wideband secure voice subscriber to another subscriber at a different geographical location, the call may traverse any combination of the parameter code circuits. Figure 3-17 is an example of G1, G2, G3, and Z4 circuits all being used for one secure voice call.

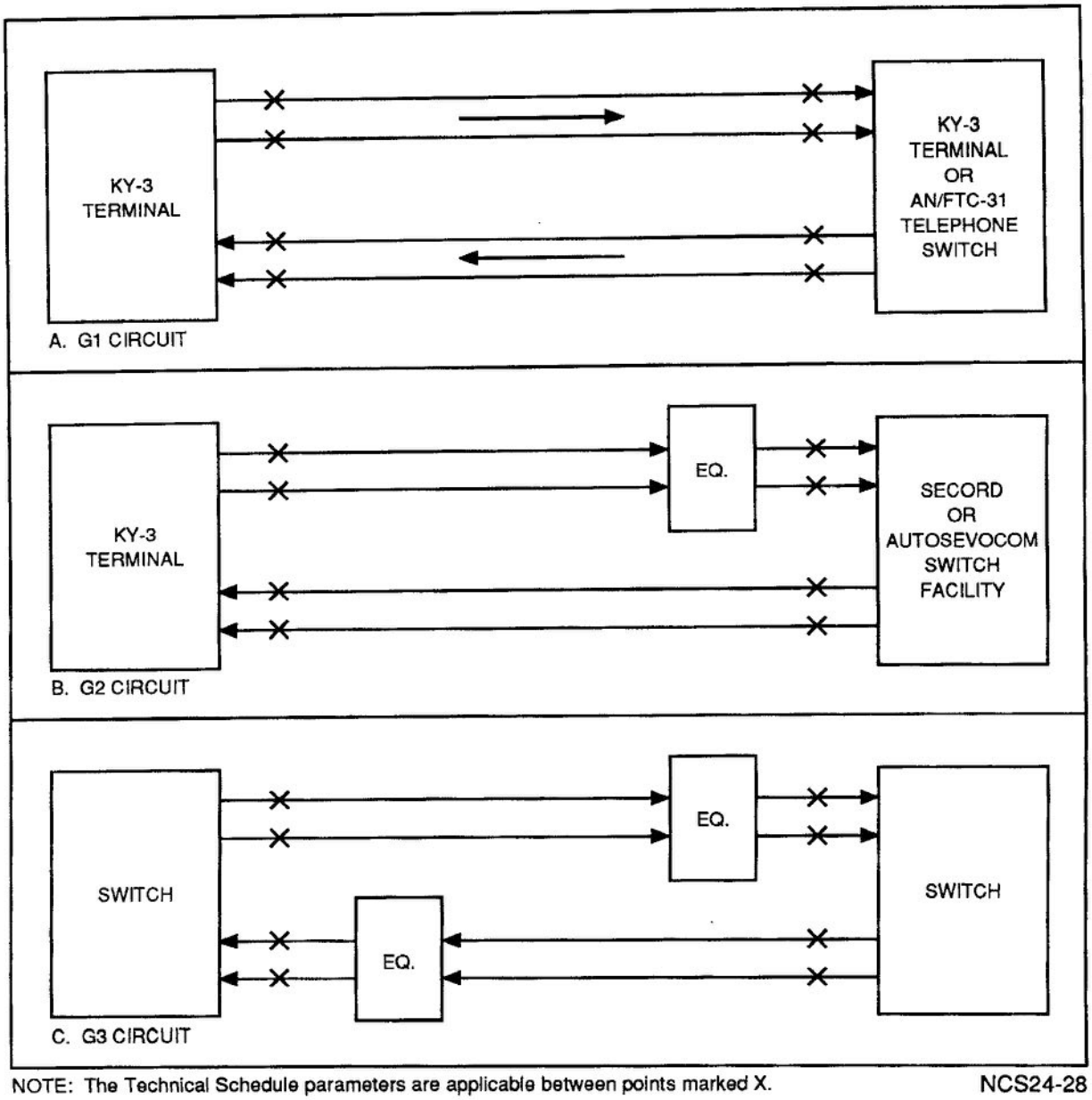


Figure 3-15. G1, G2, and G3 circuits.

234. Characteristics associated with AUTOSEVOCOM trouble isolation and testing

Signal Familiarity. The discussion in this part of the unit will provide you with some insight as to the types of signals that should be present at various points in a circuit. You should be familiar with these signals to decide whether they are normal. Let's discuss some of them in more detail.

First, we must keep in mind, when talking about AUTOSEVOCOM, that the circuit we will use must be able to pass both analog and digital signals. In a switch-to-switch trunk configuration, analog signals are converted to digital in a CV-3034. Normally, this conversion occurs at or near the switch where the analog tones originate. Until another CV-3034 reconverts these signals, at or near the distant switch, the original tones cannot be observed. Within the analog signal, there is a converted 50-kbps digital signal, now suitable for transmission over an analog channel (such as a 60-108-kHz group channel), but the original analog

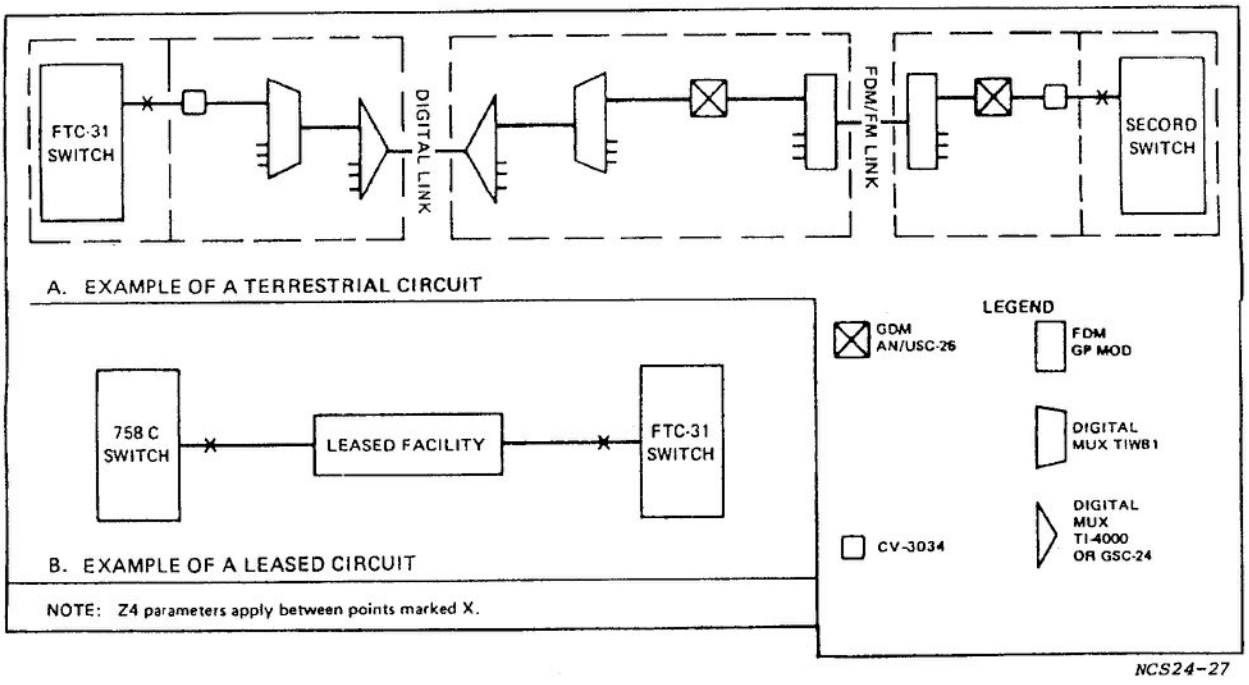


Figure 3-16. Examplesof Z4 circuits.

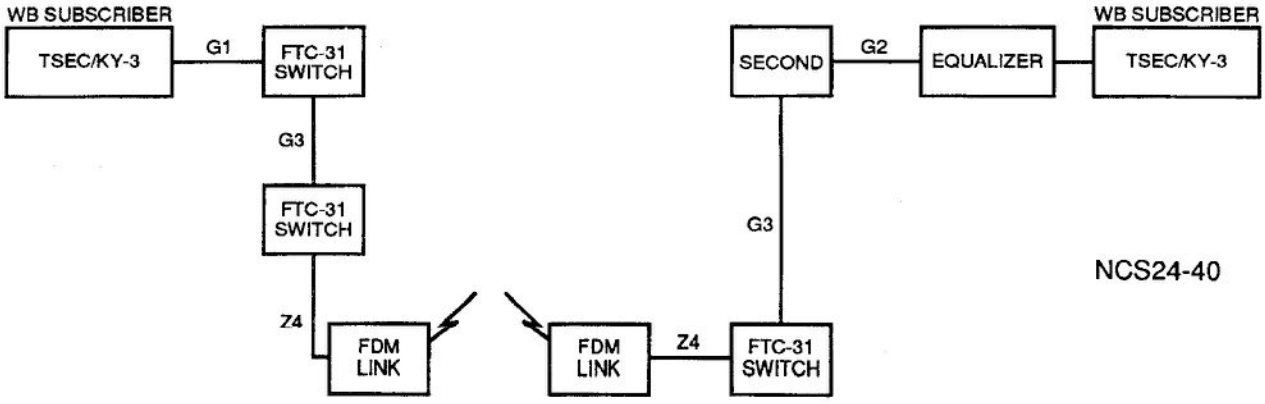


Figure 3-17. Multiparameter wideband connection.

tones from the switch will not appear and cannot be observed at this point.

The signals from the group data modem (GDM) appearing at the input/output of the group channel are in the 60-108-kHz frequency range. It is important that the levels of these signals be correct. The levels can be monitored by bridging a level measuring set across the channel at the GDM or input/output of the channel at the group. Alternately, the level can be checked by measuring the level of the carrier beacon with a frequency selective voltmeter. The carrier beacon that is transmitted from the GDM has a fixed relationship to the composite level. In the full-group mode, the carrier beacon is at 94.406 kHz and is 7 dB below the composite level. In the half group mode, the carrier beacon is 89.597 kHz and is 3 dB below the composite level. The normal group channel level is –5 dBm0 for the full group, and the carrier beacon level is –12 dBm0. In the half-group mode, the carrier beacon is –11 dBm0 (3 dB below the half-group composite level of –8 dBm0). Either level measurement method is valid, and the more convenient method should be used.

Digital signals that can be observed at the 50-kbps level will normally be in a nonreturn-to-zero (NRZ) format, a positive voltage for a logic one and a negative voltage for a logic zero. There may be some variation in the normal operating levels of these signals. The maintenance section or your in-station training program should be able to familiarize

you with the normal input/output levels of the equipment in your station. In some cases, the digital signals that are present will be in a different format, but these are usually at speeds higher than 50 kbps.

In general, locating a trouble is a matter of going through the circuit in a logical manner to isolate the problem to a progressively smaller segment of the circuit. Once the smaller segment is identified, troubleshooting may continue down to the particular equipment or circuit segment that is causing the trouble.

Obtain Information. The nature of the complaint (symptom) is one of the keys as to how to proceed. It is important first to get as much information as possible from the originator of a complaint. This can save you time and needless testing in many cases. Here are some cases you may encounter:

If a subscriber cannot establish a connection through the network, it is an indication that there is a problem in getting the supervisory and control signals through the circuit. If the subscriber complains of poor quality, it might indicate that the supervisory and control signals are getting through but that the error rate on the circuit is high. The exact problem (symptom) the subscriber is experiencing can provide valuable information and speed up fault location.

If a subscriber cannot establish a connection, it is important to know whether this applies only to certain connections. If a connection cannot be established to any other subscriber, including other subscribers on the same switch, then the problem is localized to the subscriber's circuit or equipment or the local switch. On the other hand, if local calls can be established but long-distance calls or calls to a particular area or subscriber cannot be established, the problem is probably in the trunk circuit, the distant switch, or maybe even in a distant subscriber's circuit or equipment. Normally, subscribers talk to certain other subscribers repeatedly. If they have a problem establishing a connection to those subscribers whom they normally call, they may complain that they "can't raise anybody." This is a natural reaction, but it does not provide a sufficiently specific symptom with which to isolate the problem. A few tactful questions may bring out added useful information.

Analyze the information. After all the available information has been collected, try to determine from analysis of the information, before any testing is tried, where the problem might be. You may need more information to reach a conclusion. Some tests may be indicated, or perhaps another inquiry with the subscriber may provide the answer.

Analysis of all available information should point to the other information needed and, therefore, to the type of test that may be required to provide this information. Suppose a subscriber can call local subscribers but cannot establish a connection to two subscribers in the same area. Both these problems indicate the possibility of interswitch trunk troubles. If, however, other subscribers are using these interswitch trunks, the problem may still be in the local switch. The next step, of course, is to determine whether the interswitch trunks are in fact being used by other subscribers. In a busy period, this might be easily determined by observing the signals on the trunks. In a nonbusy period, it may be necessary to make a test call through the interswitch trunk.

If the connections cannot be established through an interswitch trunk, you must know something about the circuit configuration. The first question is whether or not the supervisory and control signals are getting through the circuit. The analog signals that appear at the input to the CV-3034 that interfaces a AN/GSC-24 multiplexer do not appear again until the output of the CV-3034 at the distant switch. A logical step is to place the trunk in an idle condition. Now, you will be transmitting a 2600-Hz off-hook signal. Have the technical controller at the distant end check to see if the 2600-Hz signal is being received. If a 50-kbps digital signal, rather than the 2600-Hz signal, is being received, the problem may be that the CV-3034 is out of synchronization.

The next logical step is to find out whether the 50-kbps signal is good at the input to the CV-3034. If so, the CV-30344 should be checked on a loop-back basis to determine if it can synchronize and pass analog signals on a back-to-back basis. If not, then the problem is isolated. However, if it seems to be satisfactory, a similar loop-back should be made through the CV-3034 at the near end of the trunk. If both CV-3034s are satisfactory, the next step is to loop the circuit back at various points. The particular configuration and test points should be chosen initially on the basis of convenience; for example, at the digital interface of a group data modem rather than at the analog interface. The more inconvenient or more difficult tests should be done only if the problem has been isolated to a particular segment; as a final step, it is necessary to pinpoint the trouble.

Regardless of the cause of the impairment, some added analysis may save needless testing effort. Look at the routing of the circuit through several multichannel transmission links. If one of these links is out or is experiencing trouble, other channels in that multichannel link would also be adversely affected, and this trouble would probably be known. It would be useless to try to test the 50-kbps circuit until the link is restored.

Summary of Trouble Isolation Steps. Use the following steps as a general approach to trouble isolation:

(1) Learn the circuit configurations, the functions of the equipment involved, the types of signals at various points, the available built-in indicators, and convenient loop-back points that can be used. This will be a continuing process, but it will be worth the effort when troubles occur.

(2) When trouble occurs, find out from the person reporting the trouble all the information you can get as to the specific nature of the trouble (symptom).

(3) Analyze before proceeding with further tests. Do only those tests that will provide the information needed.

(4) If the trouble cannot be isolated without "breaking" the circuit into segments (for example, by looping back at

various points), do the more convenient loop-backs first. Proceed to the more difficult tests only if the need is indicated.

(5) Learn from each experience. Use such experience to advantage; it may provide shortcuts that save you time in examining the circuit. For instance, you may find that particular types of troubles are normally attributable to certain segments. Temper logic with experience. Document frequent problems in the circuit history folder for future reference.

Please write your response to unit self-test questions and then check the text answers at the end of the unit.

SELF-TEST QUESTIONS

232. Elements of the secure voice network

1. What are the two classes of secure voice subscriber terminals? How are they different? wideband & narrow terminals

2. What is the signaling rate for narrowband subscriber terminals? 2.4 - 4.8 kbps

3. What is used to unlock the secure voice and data capabilities of a STU-III? Crypto Ignition Key

4. List the components included in a secure voice/data cellular terminal. cell radio, secure terminal, secure message center, crypto key

5. When would a modem be used on a WBST? accessing another terminal

6. What is the purpose of the 2-kbps signal added by the ciphony unit of a WBST? maintain sync

7. What is the purpose of the secure voice access console of the AN/FTC-31 switch? It provides interface & access to narrow band subscriber lines

8. Describe the WECO 758A switch. manually operated 40 line wideband 4 wire secure voice switch

9. What is the primary difference between the WECO 758A and WECO 758C secure voice switches? WECO 758A is a manual switch, the WECO 758C is an automatic secure voice switch

10. What is the subscriber capacity of a SECORD? 15 wideband TSEC/KY-3 subscribers

11. If a WB SECORD subscriber wants to call a narrowband subscriber, what conversion is necessary prior to accessing an AUTOVON line? 50 kbps wideband signal converted to 2400 bps narrow band signal

233. Operational elements of the secure voice network

1. What is required for narrowband secure voice service? Compatible equipt. & path

2. Why would analog signals be present on a wideband secure voice circuit? supervision, control, info & clear voice

3. When a wideband subscriber is connected to an automatic secure voice switch, what frequency of signal and level is present during on-hook conditions? 2600hz -20dbm0

4. Describe the events that happen when a subscriber terminates (goes on-hook) a call through an automatic secure voice switch. ciphony signal stops, Tx 2600hz tone at -9, for 260msec the tone goes to -2 @ switch recognizes & then disconnects

5. How does a manual secure voice switch operator signal or ring a called terminal? ringing tone of 1000 Hz called the terminal

6. What notifies the manual secure voice switch that a subscriber wishes to make a call? equipt. stops Tx ring 2600 Hz on tone that activates light at switch

7. What parameter code would be given to a circuit that connects a wideband subscriber to a switch that does not have internal equalizers? 62

8. What parameter code would apply to a circuit connecting two wideband switches over long-distance mediums (tropo, M/W)? 24

234. Characteristics associated with AUTOSEVOCOM trouble isolation and testing

1. What types of signals must AUTOSEVOCOM circuits be able to carry? Analog & digital

2. What do you check to verify that a 50-kbps signal is at the proper level? What piece of equipment would you use to make this check? carrier beacon

3. What is the key that first determines how you will proceed to troubleshoot a problem? Nature of Complaint

4. After the subscriber advises you he was unable to complete a call to a distant party, what is your first check? call to check trunk

5. If the trouble on an AUTOSEVOCOM circuit cannot be isolated without breaking the circuit into segments, how would you proceed with troubleshooting? loopbacks

3-3. RED Switches

A RED switch is one of the three interoperable parts of the secure voice system (SVS). It will allow subscribers within a secure area to conduct unencrypted secure voice communications. The switches will provide improved command and control and crisis management capabilities and will interface with other elements of the SVS and tactical networks. It will initially interface with the AUTO- SEVOCOM network and will later replace the Worldwide Secure Voice Conferencing System (WWSVCS) in a nonnuclear environment. RED switches will be installed at the National Military Command Center (NMCC), the Alter- nate National Military Command Center (ANMCC), and the primary command centers of the unified and specified commands. This network will be established under Defense Communications System (DCS) control to interconnect these switches.

235. Components associated with the operation of the RED switch system

Operation. The RED switches were designed to provide a more accessible secure voice capability and very high quality, responsive, secure communications, including internal and external conferencing. They will provide an interface capability to all types of secure voice systems, including tactical networks. These RED switches will significantly improve the secure voice communications vital to command and control and crisis management. It will be operated at a system high level of SECRET and will be capable of simultaneous operation at higher levels, including sensitive compartmented information (SCI). Other secure devices or systems that interface with these RED switches must also be operated at SECRET or higher level.

The RED switch system consists of the RED switch and all associated remote switching units (RSU), interfaces, subscriber instruments, and command center consoles (fig. 3-18). The RED switch network consists of 11 switching systems and the transmission media to interconnect them. It is not the intent of the DOD RED switch program to provide a RED telephone for everyone assigned to the command centers. RED telephones are expected to be provided only to those persons/offices having a command and control function. With this tasking in mind, the engineers require that these switches be expandable to 1,500 ports (lines/trunks).

Terminals. The primary terminal for use within the SVS will be the STU-III/low cost terminal, type I. A version of the

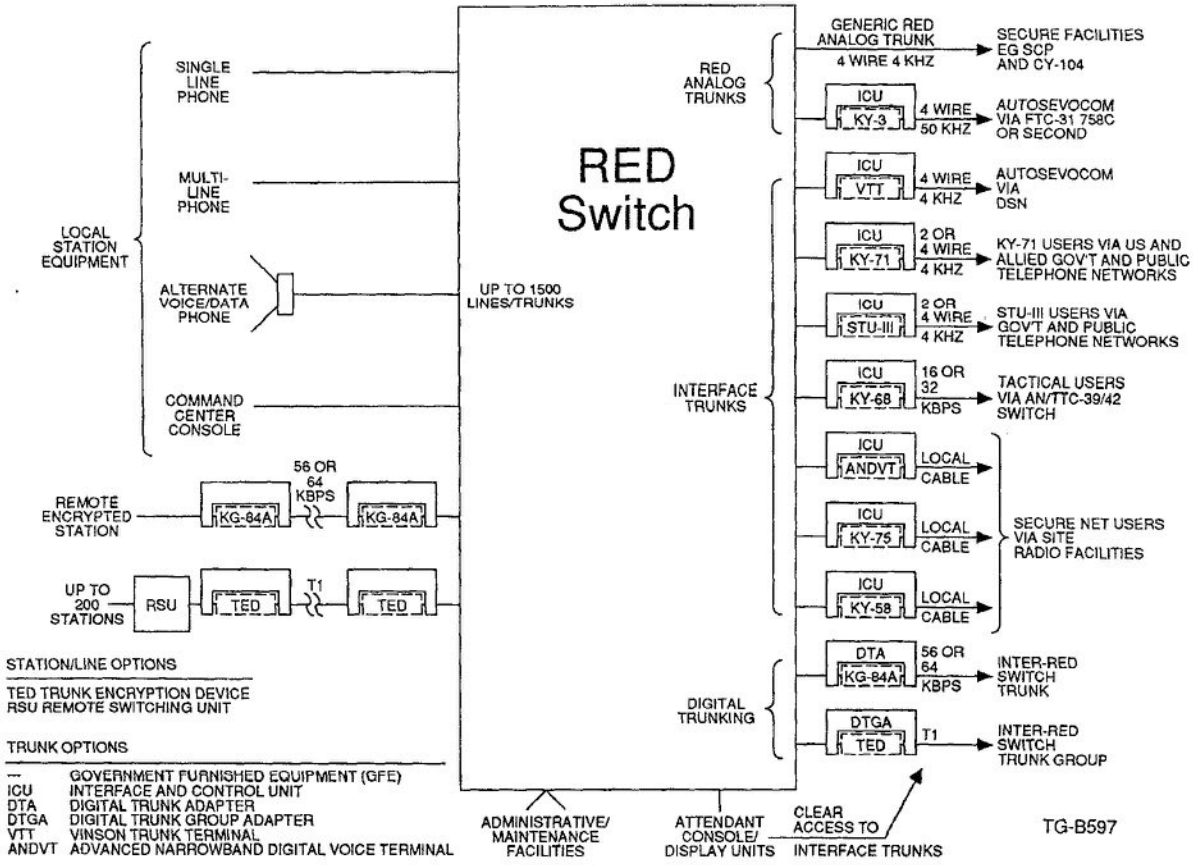


Figure 3-18. RED telephone switching system.

STU-III LCT is the RED interface terminal (RIT), which provides remotable RED audio, control, and status inputs/outputs. The RIT will be integrated into the RED switches, radio wireline interfaces (RWI), and the DSN general-purpose conferencing subsystem (GPCS) to provide the interface for STU-III terminals:

a. LCT type I terminals—provide state of the art cryptographic protection and can be used for all security classifications up to TOP SECRET sensitive compartmented information. When unkeyed, or in the nonsecure mode, it functions as any ordinary telephone. A small display is built into the STU-III that identifies the connected remote terminal and the highest common security level of the two terminals.

b. STU-II terminal—is a fully integrated microcomputer-based equipment that includes voice processing, cryptologic, control, and telephone line modem functions in a single chassis. It can accommodate up to six desk sets with junction boxes (each up to 1,000 feet away from the terminal) and was purposely designed with separate desk sets to give the user flexibility in the areas of procurement and installation.

Secure Conferencing. The RED switch has the function for secure conferencing. Its objective is to improve the capability for informed rapid response to developing crisis situations in support of command levels from the NCA to the executing commander. This function will also provide worldwide secure voice and secure graphics (teleprinter and facsimile) conferencing capabilities between the NCA, the Commander in Chief, and subordinate commanders. The secure conferencing nodes are directly interconnected to collated RED switches and use the jam resistant secure communications (JRSC) links of the Defense Satellite Communications System (DSCS) to complete their long-haul connections with distant end terminals.

236. Features of the system and user station in the secure digital switch system

System Features. The secure digital switch is designed as a modular, expandable, high-isolation, redundant, nonblocking switch with emphasis on reliability and interface flexibility. The switching system provides intra/intercommunications among subscriber lines, attendant consoles, trunks, and data ports. It features extremely high crosstalk isolation, unlimited digital conferencing, multilevel precedence and preemption call processing (to subscriber level), and full-electronic PABX service capabilities. The switch can interface with the KY-3, KY-71/72, KY-57/58, KY-68/78, and STU III cryptographic devices as well as T1 bulk encryption equipment that permits circuit access to AUTOSEVOCOM, DSN, and commercial networks.

This system offers direct digital data switching with standard data rates of up to 64 kbps for synchronous data and 19.2 kbps for asynchronous data. It also can interface directly (via bulk encrypted T1 span lines) with other secure digital switch systems such as remote switching units and secure portable switches.

User Station Features. The station feature operation is simple and straightforward, designed with the user in mind. A multiline phone is used as both a single and multiline instrument and has the features and capabilities of modem digital telephone switches. The phone has 19 special feature keys that can be expanded by use of a "second" function key. It can accommodate up to 48 station lines, in groups of 12, which may be programmed for station directory numbers, direct access (hot-line) service, or intercom lines to permit executive call screening.

Some more of the user station features include abbreviated dialing, automatic local call-back/call-forwarding (including busy, no answer), call pickup, call transfer, conferencing, consultation add-on consultation hold, and station enable/disable. There is an LCD (liquid crystal display) that has two lines of 16 characters and displays the number dialed, level of security accessed, time, day, date, and preprogrammed messages. A built-in speaker is provided for the ringer and for speaker phone usage.

Each station (or line key) can be assigned unique class marks to allow/deny activation of any feature. Class marks are also provided to allow station to trunk, station to attendant, maximum calling area, and maximum precedence authorization restrictions. Class marks are software controlled and assignable through data base update through the system administrative console.

237. Interfaces used by the RED switch

The RED switch is designed to have the interface capabilities listed below, but the quantities at your station are site-dependent.

Trunk Circuits. The switching system will have the inherent ability to interface with the central office, PABX, and tandem trunking/tie line arrangements generally accepted within the telephone industry. Class of service marks are provided to define the service needs, capabilities, and limitations of individual trunks and trunk groups.

Generic RED Analog Trunk Circuits. The switch provides RED analog trunk circuits to accommodate connection to existing and future government secure voice systems and facilities. Trunks are capable of providing any combination of automatic and manual incoming and outgoing service.

KY-3 Trunk Circuits. These trunk circuits provide automatic and manual incoming and outgoing access to/from wideband (KY-3) users and interfaces of the AUTOSEVOCOM network.

VTT Trunk Circuits. An interface and control unit (ICU) is used to adapt a VINSON trunk terminal (VVT) to provide secure RED switch access (both full-duplex and half-duplex) to/from users of VINSON subscriber terminals (VST) and facilities interfaced through a VTT. All incoming and outgoing VTT calls are processed through the attendant, who makes the key variable and rate selections. Calls are initially processed in the clear mode and controlled to the secure mode after coordination with the distant party. The extension of calls within the RED switch is possible only after the VTT has entered the secure mode.

STU-II Trunk Circuits. An ICU is used to adapt a KY-7 I STU-II to provide secure RED switch access to/from STU-II equipped secure voice users and facilities. These trunk circuits provide interface options to meet the requirements for direct connection to the commercial telephone networks (domestic and foreign), DSN, and military PABXs. They are capable of automatic and manual incoming and outgoing service. These trunk circuits can interoperate with STU-II terminals using the full-duplex, half-duplex VOX, and push-to-talk secure transmission modes. They also provide alternate voice/date service.

STU-III Trunk Circuits. An ICU is used with a type I STU-III terminal to provide secure RED switch access (both full-duplex and half-duplex VOX) to/from properly cleared STU-III equipped secure voice users and facilities. The trunk circuits include features to deny RED switch access whenever the distant STU-III is cleared for less than the SECRET level. These trunk circuits provide interface options meeting the requirements for direct connection to the commercial telephone networks (domestic and foreign), DSN, and military PABXs. They are capable of automatic and manual incoming and outgoing service. Alternate voice/data capability is provided.

DSVT Trunk Circuits. An ICU is used to adapt a KY-68 digital subscriber voice terminal (DSVT) to provide secure RED switch access (both full-duplex and half-duplex push-to-talk modes) to/from DSVT compatible tactical terminal users. These trunk circuits will have interface options meeting the requirements for direct digital loop or trunk connection to tactical digital channels (both 16 and 32 kbps) accessing an SB-3865 switchboard and an AN/TTC-39 or AN/TTC-42 switch. They are capable of automatic and manual incoming and outgoing service. DSVT trunk circuits let RED switch users/attendants establish preset and progressive conferences using the conference bridging capabilities of the connected tactical switch. These trunks also provide alternate voice/data capability.

ANDVT Radio Access Circuits. An ICU is used to adapt advanced narrowband digital voice terminal (ANDVT) to provide secure connectivity to/from ANDVT users accessed through local-site radio facilities. All incoming and outgoing ANDVT calls are processed by the attendant. Calls are initially processed in the clear mode and controlled to the secure mode after coordination with the distant party. The attendant selects the ANDVT key variable and either net broadcast or point-to-point transmission modes. Alternate voice/data capability is available.

PARKHILL Radio Access Circuits. An ICU is used to adapt KY-75 PARKHILL equipment to provide secure connectivity to/from PARKHILL users accessed through the local site radio attendant. Calls are initially processed in the clear mode and controlled to the secure mode after coordination with the distant party.

VINSON Radio Access Circuits. These circuits use an ICU to adapt a KY-58 VINSON terminal to provide secure connectivity to/from VINSON users accessed through the local site radio facilities. All incoming and outgoing calls are processed by the attendant. Calls are initially processed in the clear mode and controlled to the secure mode after coordination with the distant party. The attendant selects the key variable and makes the rate selection.

Digital Trunk Circuits. These circuits provide single-channel digital interswitch trunking service between RED switches. These 56/64 kbps circuits are secured with KG-84A link encryption devices.

Digital Trunk Group Circuits. These circuits provide 24-channel digital interswitch trunk group service (1.544 mbps) between RED switches and also provide for the connection of RSUs to the RED switch. These trunk groups will be secured with KG-81 or KG-94 trunk encryption devices.

Cryptographic Interfaces. The secure digital switch, to achieve connectivity with distant RED subscribers, must interface with COMSEC cryptographic devices. There are two basic types of interfaces: those that require a RED/BLACK interface device to pass network signaling and those that do not.

Interface Ancillary Device (IAD). The IAD is a RED/BLACK interfacing device that allows a secure digital switch to interface with a crypto device and achieves automatic network inward/outward dialing over nonsecure transmission media. The IAD passes supervisory and address signaling in setting up a secure call, assures that the crypto in question has achieved sync and gone secure before passing RED audio signals, and monitors said crypto throughout the call for alarm conditions or status changes. The IAD is modular and flexible, allowing RED and BLACK sides to be independently configured for particular systems, networks, and cryptos.

Noninterface Ancillary Device. Under certain circumstances, network signaling is either unnecessary or impossible. Some of these devices are T1 span lines, satellite links, narrowband radio links, and dedicated trunks. In such cases, an IAD is not required, but interfaces are made to handle this problem.

Please write your response to unit self-test questions and then check the text answers at the end of the unit.

SELF-TEST QUESTIONS

235. Components associated with the operation of the RED switch system

1. What is the system high level of security for operation of the RED switch? Secret

2. What components make up the RED switch system? remote switch units, interfaces, subscriber instruments, & consoles

3. Which terminal will accommodate more than one desk set? STU-III

236. Features of the system and user station in the secure digital switch system

1. For which standard data rates will the RED switch offer direct switching? 64K sync. 19.2K a sync.

2. How many station lines can the multiline phone accommodate? 4/1

3. What is assigned to each user station to allow or deny activation of any multiline phone function? class mark

237. Interfaces used by the RED switch

1. On what type interfacing would you encounter class of service marks? Why are they used? Trunk ckts.

2. What component is used by the STU-II and III trunk circuits to provide secure RED switch access? ICU

3. How does a user access radio circuits to achieve secure connectivity? local site radio facility

4. What must a secure digital switch do in order to achieve connectivity with distant RED subscribers? interface COMSEC crypto device

5. What is the function of the interface ancillary device when setting up a secure call? passes the supervisory & address signaling

3-4. Defense Commercial Telecommunications Network (DCTN) Configuration

Since the withdrawal of the AT&T interstate telecommunications package (TELPAK) tariff in May 1981, the cost of telephone and data services used by the Department of Defense has increased significantly and seems to have a consistent increasing trend. The government is the biggest private line network user, using 1.5 billion call minutes a year to more than 1.3 million users in all 50 states. The old long-distance network, which is both obsolete and too expensive, brought about the development of the DCTN.

238. Principles associated with the Defense Commercial Telecommunications Network

History. The CONUS government agencies are in need of services that provide electronic and voice mail, full-motion color video, and access to management information on a real-time basis. Since the current analog switches cannot support this requirement, a new network had to be made. Further studies showed that the system needed is essentially a data network onto which voice will be overlaid. While data will now account for only 15 percent of the networks traffic, it is growing at about 20 percent a year, compared to 5 percent for voice. Through research it was found that a switch to the new technologies could drive down costs by at least 20 percent.

The solution was a network based on packetized technology and support software. Packet-switching was selected for three reasons: interoperability, buffering and flow control, and cost. A later examination of the terrestrial and domestic satellite (DOMSAT) carrier's tariffs showed that a combined satellite and terrestrial network can provide a variety of voice, data, and video services at an effective cost. By consolidating requirements with a single contractor (as compared to procurements on an individual basis), overall cost savings can be obtained. As a result, the DCTN evolved to a leased, satellite-based communications system to carry DOD traffic at a price lower than is being paid now, satisfying new wideband requirements, such as video teleconferencing and bulk data transfer.

Function. As a subsystem of DSN, DCTN has, along with other independent networks, become a major element of the overall digital switching network. An important service provided by the DCTN contractor is the subcontracting of elements needed to complete the network if they are not available from the contractor's own resources. This relieves DCA of the task of obtaining competitive quotations for services from multiple vendors and integrating them into the network. Also, DCA is provided with a single point of responsibility for network administration.

The DCTN is a communications network leased by DCA/Defense Commercial Communications Office (DECCO). It connects various CONUS bases through voice and data circuits, and it provides both general-purpose and dedicated services. It also provides a transmission path over terrestrial and satellite links for a nonprecedence switched voice network. The network consists of Earth terminals and terrestrial feeder networks that encompass a 50-mile (telephone line) local area near each Earth terminal. DCTN is designed for administrative traffic. Command and control traffic can also be carried, but not with DCTN as the sole medium. A portion of the routine CONUS DSN traffic is carried by DCTN, but precedence traffic is excluded.

Existing circuits with voice grade services can be transferred to DCTN without changing the users' equipment. Besides the services used for voice and quasi-analog transmission, DCTN will provide data channels having digital interfaces and services comparable to our present wideband and high-speed data rate transmission circuits. A typical DCTN link is shown in figure 3-19. The interface between the equipment, which is the responsibility of the contractor, is called the demarcation line. Exact demarcation lines will be established by mutual agreement during the service order process.

239. Mission and objectives of the DCTN

Mission. The DCTN will be used by the Air Force for peacetime operations in a manner that provides engineered systems at the lowest possible cost, meets the users' needs, provides timely and flexible service, and allows for an orderly growth of services. New services will be introduced by economically sharing satellite capacity resources at a reduced charge, compared to changes for separate individual satellite leases. Management of the overall system is designed to reduce the charges for leased services by rerouting portions of long-haul terrestrial communications through satellite systems to provide service consistent with the National Communications System (NCS) restoration priority (RP) system.

Objectives. The major objectives of the DCTN are to enhance the services available from satellite-based leased commercial communications, to reduce the cost of the otherwise increasing DCA management role, and to reduce the cost of services as compared to present procurement methods. Other objectives are to consolidate requirements, to acquire a system that will evolve with future DOD networks, and to provide systems management to make sure of user-to-user services.

The military objectives of the DCTN are:

a. To provide more economical CONUS communications services. Initially, the system will provide connectivity for CONUS users.

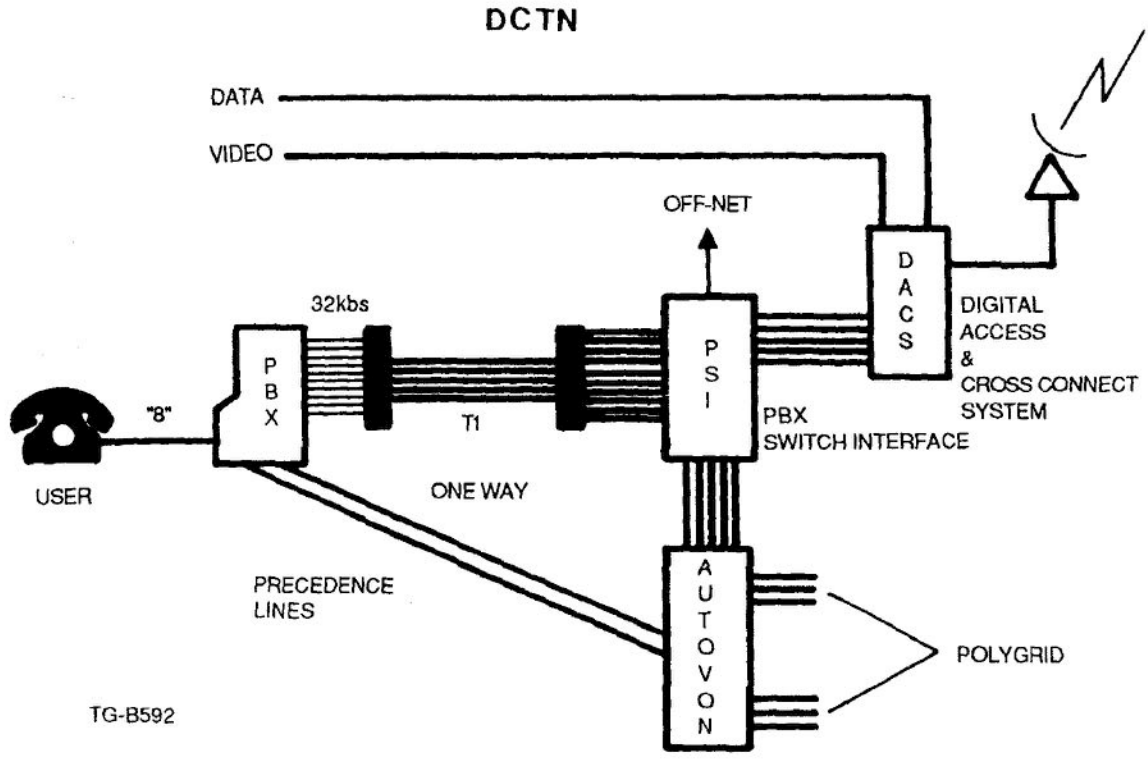


Figure 3-19. Typical DCTN link.

b. To lease satellite transmission capacity and interconnecting wideband terrestrial capacity that can be rapidly and flexibly allocated to meet the needs of the NCA, the DOD, and the military departments.

c. To establish military access to commercial satellite systems in support of National Security Directive 97.

d. Flexible allocation of transmission capacity.

e. Diversity of communications media.

f. Bulk encryption on satellite paths.

g. Options:

(1) Contingency transportable Earth stations.

(2) Tracking, telemetry, and command (TT&C) protection on future satellites.

(3) Electric magnetic pulse (EMP) protection on Earth terminals.

The operating and maintenance agency for the DCTN will be provided by AT&T by contract. Their duties and responsibilities are governed by a contract with DECCO. The contractor, AT&T, is responsible for furnishing DCTN leased services to the Government on a turnkey basis. The DCTN system includes all communication facilities as required to provide transmission media between users. The contractor will provide terrestrial trunks for circuits not competitive in cost when implemented by satellite transmission, unless specifically directed to the contrary by DCA. The contractor will manage the overall DCTN system under the direction and control of the DCTN program management office (PMO).

DCTN voice-only services are the commercial equal of "toll quality" circuits. The specific characteristics provided are described in DCS operating maintenance electrical performance standards for digital circuits under DCS schedules V1 and V2. Many current subscribers using quasi-analog data services will require conditioned channels, and they will provide their own modems. DCTN will provide full-period channels, with characteristics equal to that provided by PCM, 64 kilobit/second mu-255 format. Now, DCA is also offering an economical asynchronous service by multiplexing teletype channels into voice frequency carrier telegraphs over voice channels. DCTN will provide a more economical arrangement for these services over satellite.

240. Services associated with the DCTN

PBX Tie Trunk. The PBX tie trunk DCTN service will not transverse more than one satellite hop. The DCTN contractor is responsible to provide all signaling, supervision, and routing interface characteristics up to the user's PBX. The service provides users with economical alternatives to wide-area telephone service (WATS) lines, direct distance

dialing (DDD) lines, and foreign exchange (FX) lines, particularly over transcontinental distances.

Off-Net Dialing. One service provided is off-net dialing, which is based on offerings being made available by the commercial marketplace. The effective use of DCTN transmission capacity dictates that the PBX switch interface (PSI) have a function that will sort traffic from a larger volume of traffic than really intended to be carried by the DCTN. Therefore, any proposed system will include this PSI function to sort all routine DSN traffic originated at each PBX. For authorized DOD users, off-net dialing services are provided through PBX trunks, where the user dials a number in the following format: "8" + a 10-digit DDD number.

All off-net services will enter and exit the DCTN network at the distant end switch concentrator. DCTN will be used to satisfy the needs for administrative type traffic and, also, to provide diverse routing for command and control traffic. Routine CONUS general-purpose voice traffic will be carried by DCTN; precedence traffic will be excluded. A maximum of 50 percent of all routine circuits at a single location can transverse through DCTN. The use of DCTN for precedence traffic may be done during crisis conditions. Besides satisfying the needs for voice and quasi-analog transmissions, DCTN will provide data channels having digital interfaces and services on wideband high-data-rate transmission circuits. Many of these services are presently not economically available through existing terrestrial facilities but can be readily implemented by use of satellite transmission.

The DCTN contract will allow Air Force users to request a wide variety of services. The new service applications for digital ports include:

a. Near full-motion video telebroadcast.
b. Near full-motion video teleseminar.
c. Near full-motion video teleconferencing.
d. Full-motion video telebroadcast.
e. Voice and graphics teleconferencing.
f. Electronic document distribution.
g. Bulk data transfer.
h. Word processing.
i. Wideband telemetry.
j. High-resolution graphics.
k. PBX tie trunk service.

DCTN will provide full-period (24 hours per day) scheduled service (dedicated service in specified time increments) and switched scheduled service (general-purpose switched connections for economy and conservation of satellite capacity).

Please write your response to unit self-test questions and then check the text answers at the end of the unit.

SELF-TEST QUESTIONS

238. Principles associated with the Defense Commercial Telecommunications Network

1. List the reasons that packet-switching was selected to support the DCTN. interoperability flow & cost

2. The DCTN is designed for what type traffic? admin. traffic & command and control traffic

3. What is the contractor interface between the users' equipment and DCTN links called? demarcation line

239. Mission and objectives of the DCTN

1. What is the overall management goal of the DCTN system? minimize changes by rerouting
2. What are the major objectives of DCTN? enhance services available
3. Who has overall direction and control of the DCTN system? DCTN program management

240. Services associated with the DCTN

1. What is the DCTN contractor responsible for providing on a PBX tie trunk? signaling supervision trunking
2. What is the function of the PBX switch interface in DCTN? sort traffic to utilize DCTN capacity
3. Which piece of equipment provides the entrance and exit points for DCTN systems off-net service? switch concentrator
4. A single facility can route what percent of the total number of routine circuits via DCTN? 50%

3-5. Integrated Services Digital Network (ISDN)

Although an Integrated Services Digital Network (ISDN) has not yet become a part of the military environment, it is vital that you understand the basic concept and realize that ISDN *is* coming. ISDN will have a major impact on the communications services offered to users at all levels of networking.

241. Preparing for an integrated services digital network architecture

Concept Development. ISDN is a concept that went into formal planning and development in the early 1970s. The first set of ISDN standards, upon which all initial product development is based, was defined by the International Telegraph and Telephone Consultative Committee (CCITT) and ratified at its plenary assembly in October 1984. These standards form the basis for all work that is ongoing in the civilian sector to bring ISDN to realization, but there are many issues yet to be resolved. The resolution of these standards issues is essential to speedup the availability of key ISDN components, such as line termination equipment and low-cost silicon devices for use in terminals. Standards for signaling procedures and protocols are also essential for digital connectivity and for the implementation of voice and data services across network boundaries.

A System Overview. ISDN makes use of digital techniques for the simultaneous transmission of voice, data, facsimile, and video signals on a single line. Unlike analog signals, which have to be encoded to be sent over phone lines (thereby increasing the likelihood of errors and resulting in slower data rates), digital transmission sends data in its original form. This integrated transmission is achieved through the use of separate *channels*.

The CCITT architecture permits the separation of user access functions from core network functions through an *access* node. Access nodes are a critical element in the implementation of ISDN. They provide the means for users to obtain services from existing networks at early ISDN

implementation stages, and they form the basis for the evolution of the core network to a fully integrated network.

Service Interfaces. Customers will be able to choose from two service interfaces: basic access and primary access.

Basic access. Basic access (144 kbps) consists of two 64 kbps ***B*** channels and one 16 kbps ***D*** channel. This interface arrangement is known as ***2B+D*** access. The B channels are used for bidirectional digital voice and data traffic, while the D channel carries signals that handle call clearing, call setup, packet switching, and other similar functions. 2B+D access is used to support single subscriber terminals.

Primary access. The primary access interface (1.544 mbps) offers customers even higher data rates. It consists of 23 B channels (64 kbps each) and one 64 kbps D channel. This interface arrangement, known as *23B+D* access, can be used by those customers who wish to interconnect PBXs, premise-based LANs, and other concentrated traffic systems. Primary access uses the same bandwidth as existing T-carrier systems (1.54 mbps), with even higher bandwidths planned for the future.

The Benefits. From the users' point of view, ISDN is a standard method for interfacing with, and tying together, various digital public and/or private networks so that all network services are accessed in the same way. These advantages translate to increased and improved services and cost effectiveness. From the carriers' point of view, the advantages of converting to an all digital environment are many, both in simplicity of maintenance and cost factors (profit factors for the commercial folks). Some of the benefits to consider are listed below.

High-speed digital connectivity. A network user may not really care whether transmission is through an analog or digital technique as long as product quality and reliability are kept high. But the user will realize a savings as a result of the benefit of being able to send *all* of his or her services on one transmission line as opposed to paying for separate transmission lines.

High-quality transmission. The transmission of services in a digital format reduces the possibility of errors. It also permits transmission at higher data rates than using an analog format.

Worldwide standard interfaces. As mentioned earlier, CCITT, an international organization, determined the interface standards for the integration of ISDN. These standards are being used by all countries as ISDN becomes a reality. This, of course, reduces production costs and system integration expenses.

Simplified maintenance. One major feature is the minimization of inside wiring and the simplification of add-ons, moves, and changes. New data and telephone wiring will not have to be continually installed and rerouted. Universal wiring and programmable switches will help cut ongoing labor costs.

New/enhanced services. ISDN makes possible the integration of voice, data, facsimile, and video products as user services. Imagine being able to talk over a telephone, transmit message traffic, send graphic reproductions of maps or other materials, and take part in a video teleconference, all from one location. Eventually, all from one desktop unit.

Migration Strategy. There will be two victims, in both the civilian and military communications communities, of our migration to an ISDN architecture: those large users with a large equipment base, and the local telephone exchanges. The migration will require equipment replacement, or at least augmentation, to provide the necessary adaptation to existing physical plants. Many of these problems were forecast long before the start of ISDN. The conversion of telecommunications networks from analog to digital has long been viewed as the wave of the future.

Most network managers have known for years that there would come a necessity to replace or upgrade switching equipment, replace analog modems or multiplexers with digital interface units and channel banks, and completely rethink networking philosophies. Many users, though, view this as a forced migration to ISDN and find it less than palatable since their existing networks were designed to increase security, reduce costs, and increase user access. The fact is, without user acceptance and support, the already extended development cycle of ISDN is likely to stretch out even more.

Please write your response to unit self-test questions and then check the text answers at the end of the unit.

SELF-TEST QUESTIONS

241. Preparing for an integrated services digital network architecture

1. What are the primary services provided by ISDN?
voice data fax & video in digital format

2. What provides users access to existing ISDN networks? ISDN access nodes

3. Explain the channel arrangements for 2B+D and 23B+D access interfaces.
2 B+D 144 Kbps consists of two 64 Kbps B-channels & one 16 Kbps D channel.

4. Name five benefits of ISDN.
- High speed digital connectivity
- high quality TX
- world wide access

ANSWERS TO SELF-TEST QUESTIONS

227

1. Survivability.
2. Responsiveness.
3. Via interswitch trunks.
4. Lines that connect subscribers to a switch.
5. Any four-wire telephone with direct access to DSN, including PABX.

228

1. Command and Control (C^2) Users and Operational Support users.
2. 15 to 20 times.

229

1. Survivability, Responsiveness, Security, Cost Effectiveness and Interoperability.
2. Low cost STU-III terminal.
3. New digital switching and transmission equipment is more reliable.

230

1. Digital switching, transmission, timing and synchronization, and administration/network management (A/NM).
2. Interswitch trunks and access lines.
3. From a station clock synchronized to the world-wide LORAN C navigation system, to the Department of Defense Global Positioning System (GPS) satellite, or to another highly accurate source, such as a cesium beam atomic clock.
4. The ACOCs.

231

1. 30 channels of PCM encoded speech, multiplexed with one synchronizing channel and one signaling channel.
2. Message handling, translation, and resource management.
3. Digital carrier module (DCM).
4. The central message controller.
5. Acknowledgement messages from both peripheral processors trying to establish the network.

232

1. Wideband and narrowband terminals. They differ by equipment required, operating speed, bandwidth, and ability and method of accessing other terminals.
2. 2.4 or 4.8 kbps.
3. Crypto-ignition key.
4. Cellular radio, secure cellular terminal, secure message center, and crypto-ignition key.
5. When accessing another terminal not connected to the same secure voice switch.
6. Maintain synchronization and control functions of each terminal's ciphony equipment.
7. It provides interface and access to narrowband subscriber lines from wideband subscribers.
8. It is a manually operated, 40-line, wideband, four-wire, secure voice switch.
9. The WECO 758A is a manual switch; the WECO 758C is an automatic secure voice switch.
10. Up to 15-wideband TSEC/KY-3 subscribers.
11. The 50-kbps wideband signal must be converted to a 2400-bps narrowband signal.

233

1. Compatible equipment and a communication path.
2. Supervision, control, information and clear voice.
3. 2600 Hz, –20 dBm0.
4. 50-kbps ciphony signal stops and TSEC/KY-3 transmits a 2600-Hz tone at –9 dBm0 for 260 milliseconds and then drops the level of the tone to –20 dBm0 (normal on-hook). The automatic switch recognizes the –9 dBm0, 2600-Hz tone as a disconnect and breaks path through the switch.
5. By sending a ringing tone of 1000 Hz to the called terminal.
6. The subscriber terminal equipment stops transmitting the 2600-Hz on-hook tone, which activates a buzzer and light at the switchboard.
7. G2.
8. Z4.

234

1. Analog and digital.
2. Carrier beacon; frequency selective voltmeter.
3. Nature of the user complaint.
4. Check the interswitch trunk circuit being used to get to the distant end switch by placing a call on it yourself.
5. Perform the more convenient loop-backs first.

235

1. Secret.
2. Associated remote switching units, interfaces, subscriber instruments, and command center consoles.
3. STU-II.

236

1. Up to 64 kbps for synchronous; 19.2 kbps for asynchronous.
2. 48.
3. A class mark.

237

1. Trunk circuits. To define the service requirements, capabilities, and limitations of trunks and trunk groups.
2. An ICU.
3. Via the local-site radio facility.
4. Interface with a COMSEC cryptographic device.
5. Passes the supervisory and address signaling.

238

1. Interoperability, buffering and flow control, and cost.
2. Administrative traffic and command and control traffic, as long as DCTN is not its sole medium.
3. Demarcation line.

239

1. To minimize the changes for leased services by rerouting communications via satellite.
2. To enhance the services available on commercial-leased satellite communications and reduce the cost of services.
3. DCTN program management office.

240

1. Signaling, supervision, and routing interface characteristics up to the user's PBX.
2. To sort traffic to utilize the DCTN to capacity.
3. Switch concentrator.
4. 50 percent.

241

1. Voice, data, facsimile, and video in a digital format.
2. ISDN access nodes.
3. 2B+D (144 kbps) consists of two 64-kbps B-channels and one 16-kbps D-channel. 23B+D (1.544 mbps) consists of 23 64-kbps B-channels and one 64-kbps D-channel.
4. High-speed digital connectivity, high-quality transmission, worldwide standard interfaces, simplified maintenance, and new and enhanced services.

Do the Unit Review Exercises (URE) before going to the next unit. ➡

UNIT REVIEW EXERCISES

Note to Student: Consider all choices carefully, select the *best* answer to each question, and *circle* the corresponding letter.

55. (228) When compared to AUTOVON, how much larger will the overseas Defense Switched Network (DSN) eventually become?

3-5
a. 5 to 10 times larger than AUTOVON.
b. 10 to 15 times larger than AUTOVON.
c. 15 to 20 times larger than AUTOVON.
d. 20 to 25 times larger than AUTOVON.

56. (229) Why is Defense Switched Network (DSN) more survivable than AUTOVON?

3-5
a. DSN is a larger network.
b. DSN has more nodes.
c. DSN requires less maintenance than AUTOVON.
d. DSN uses adaptive routing of traffic.

57. (230) An end office would be considered part of what subsystem of Defense Switched Network (DSN)?

3-6
a. Transmission.
b. Timing and synchronization.
c. Administration/network management (A/NM).
d. Digital switching.

58. (230) What are single- or multichannel connections that allow user equipment to gain access to the network?

3-8
a. Interswitch trunks.
b. On-base cables.
c. Access lines.
d. Connection lines.

59. (231) In a digital multiplex switching system, what appears between the peripheral module and the network in addition to the 30 channels of encoded speech?

3-9
a. Orderwire channel and timing channel.
b. Sync channel and alarm channel.
c. Sync channel and signaling channel.
d. Supervisory channel and alarm channel.

60. (232) What is used to provide access control of the COMSEC functions in a STU narrowband terminal?

3-13
a. Crypto key cards.
b. Crypto pin blocks.
c. Crypto ignition key.
d. Crypto sync switch.

61. (232) Wideband secure voice subscribers homed on an AN/FTC-31 switch may access a narrowband subscriber through which unit?

3-15
a. Secure voice cord board (SECORD).
b. Secure voice access console (SEVAC).
c. Switch control subsystem.
d. Switch control subsystem and secure voice cord board (SECORD).

62. (232) What is the difference between the WECO (Western Electric Company) 758A and the WECO 758C secure voice switches?

3-16
a. 40-line manual vs. 60-line automatic operation.
b. 250-line automatic vs. 40-line manual operation.
c. There is no difference, both switches operate manually.
d. There is no difference, both switches operate automatically.

63. (233) Upon receiving short bursts of a 2600-Hz tone at –9 dBm0 from a subscriber, the proper response from an automatic secure voice switch is to

3-19
a. transmit a busy tone (1000-Hz interrupted).
b. disconnect the line it received the tone from.
c. transmit a dial tone to the subscriber.
d. connect that line to the proper subscriber line.

64. (233) Circuits that connect two wideband secure voice switches over long-distance mediums fall into which parameter code group?

3-19
a. G1.
b. G2.
c. G3.
d. Z4.

65. (234) An AUTOSEVOCOM circuit, being operated in the half-group mode, is measured at the input of the group modulator and the composite level is –13 dBm0. What level should the beacon carrier be?

a. –7 dBm0.
b. –10 dBm0.
c. –13 dBm0.
d. –16 dBm0.

66. (234) When you receive a call from the subscriber advising you his or her AUTOSEVOCOM circuit is inoperative, what should you do first?

a. Try placing a call on the circuit yourself.
b. Obtain information on the nature of the complaint.
c. Give the subscriber a loop-back for in station checks.
d. Check the level of the circuit and start testing.

67. (235) Red switch phones are provided

a. only to persons/offices having a command and control function.
b. only to persons/offices having security clearances of SECRET or higher.
c. to anyone assigned to a command center.
d. to anyone assigned to a command center with a security clearance of SECRET or higher.

68. (236) A secure digital switch phone can accommodate up to how many station lines?

a. 12.
b. 48.
c. 60.
d. 100.

69. (236) While you are using the RED switch, what feature can ensure that you have dialed the correct number at the proper level of security?

a. Recorded voice message.
b. Punched paper tape.
c. Punched computer cards.
d. Liquid crystal display.

70. (237) In a RED switch system, the maximum rate a 24-channel digital interswitch trunk group can operate at is

a. 19.2 kbps.
b. 64 kbps.
c. 1.544 mbps.
d. 4.8 mbps.

71. (237) What interface provides the RED switch 24-channel digital interswitch trunk group service at 1.544 mbps?

a. STU-III trunk circuits.
b. DSVT trunk circuits.
c. Digital trunk group circuits.
d. Digital trunk circuits.

72. (238) What type of transmission media has the Defense Commercial Telecommunications Network evolved to for an overall cost savings factor?

a. Tropospheric scatter.
b. Satellite.
c. High frequency.
d. Microwave.

73. (238) The Defense Commercial Telecommunications Network (DCTN) was designed to handle what type of traffic as its sole medium?

a. Administrative.
b. Command and control.
c. Routine CONUS AUTOVON.
d. Precedence CONUS AUTOVON.

74. (239) Which of the following is a major objective of the Defense Commercial Telecommunications Network (DCTN)?

a. To reduce the workload assigned to the military network.
b. To replace all the current communications media.
c. To improve the leased commercial satellite communication services.
d. To provide commercial contractor access to the military satellite network.

75. (240) What component of the Defense Commercial Telecommunications Network (DCTN) ensures full-system utilization and sorts the large volume of traffic the network carries?

a. Switch concentrator.
b. PBX switch interface.
c. Bulk data transfer.
d. Digital access and cross-connect.

76. (240) What is the *maximum* amount of routine traffic, from a single location, that can travel via the Defense Commercial Telecommunications Network (DCTN) at any given time?

a. 100 percent.
b. 75 percent.
c. 50 percent.
d. 25 percent.

77. (241) What are the basic and primary access interfaces used in Integrated Services Digital Network (ISDN)?

a. 2B+D and 23B+D.
b. 16B+D and 23B+D.
c. 2B+D and 64B+D.
d. 16B+D and 64B+D.

Please read the topic page for Unit 4 and continue. ➡

STUDENT WORK SPACE

DEFENSE SATELLITE COMMUNICATIONS SYSTEM

In the last volume, we discussed satellites as a transmission media. You will now see that it's the only system to have its own office within DCA. The system is so vast and has so many variables that it requires the management and supervision of a separate organization charged with the responsibility of ensuring that timely and correct decisions be made for control of the various aspects of the DODs satellite programs.

In this unit, we will look at the Defense Satellite Communications System (DSCS), one of its programs, the ground mobile forces (GMF) network, and an integral part of the DSCS, the Air Force Satellite Control Facility. We will also discuss the Air Force Satellite Communications System (AFSCS).

4-1. Operations

With the launching of new satellites and the modification of terminals, the Initial Defense Communications Satellite Program (IDCSP) entered a new phase and was renamed the Defense Satellite Communications System. This is a triservice program under the direction and operational control of DCA. As you read the following sections describing the DSCS, you may wish to refer back to Volume 1 of this course for a refresher on the operational characteristics of satellites.

242. The purpose and operational objectives of the DSCS

Purpose. The DSCS was developed to support unique and vital global communications networks for the DOD. The DSCS is an integral part of the DCS and normally supports:

a. Needs of the Worldwide Military Command and Control System (WWMCCS).

b. Establishment, extension, and upgrading of communications in direct support of combat forces.

c. Wideband communications requirements to remote locations not adequately served by other means.

d. Navy ship-to-ship, ground mobile forces, and other authorized DCS user requirements.

e. Other uses as directed by the Joint Chiefs of Staff (JCS) and/or Secretary of Defense.

A unique feature of DSCS is its ability to extend communications services to remote locations not adequately served by other means, to support Navy ship-shore-ship communications, the GMF of the Army, Marine Corps, and Air Force, and the Diplomatic Telecommunications System (DTS) of the Department of State (fig. 4-1).

Operational Objectives. The primary operational objective of the DSCS is to provide continuous high-quality communications to each validated user. In stressful environments, including trans- and postattack periods, the objective is to preserve the critical communication needs of the WWMCCS.

Operational objectives are achieved by supporting the DSCS performance criteria and its operational priority system. These objectives are met by ensuring that critical subscribers and systems maintain connectivity with the DCS; that sustained quality service is maintained through timely, effective testing and analysis in both normal and stress environments; and that efficiency is increased in the DSCS. Also, the system should remain flexible to serve the maximum number of potential users and to be tactically adaptable.

243. Characteristics and limitations of the DSCS

Characteristics. Due to the importance of defense satellite systems, they must have high reliability along with the basic characteristics that allow them to perform effectively. All communications systems must conform to certain basic requirements, some of which are listed below.

Reliability. Two types of reliability are of interest. The first is propagation reliability. The high-frequency (HF) band has always been subject to the irregularities of the ionospheric layers that surround the Earth. Thus, only a portion of the HF band is actually usable at any given time over a particular path.

Also, the multipath effects of ionospheric propagation seriously limit the amount of information that can be transmitted over a given channel. Added to these limitations are the "blackouts" that may result from ionospheric disturbances caused by sunspot activity. High-altitude nuclear explosions can introduce similar disturbances.

One is forced to conclude, and rightly so, that using HF frequencies and the ionosphere as a propagation medium yields less than desirable results. By contrast, a communications satellite of the active-type using line-of-sight (LOS) transmission at microwave frequencies is extremely reliable from a propagation standpoint.

A communications satellite introduces a second type of reliability problem—that of reliable unattended operation for long periods in orbit. Systems engineers have shown that a reliable communications satellite can be made with operational life expectancies of more than 1 year if the following practices are used:

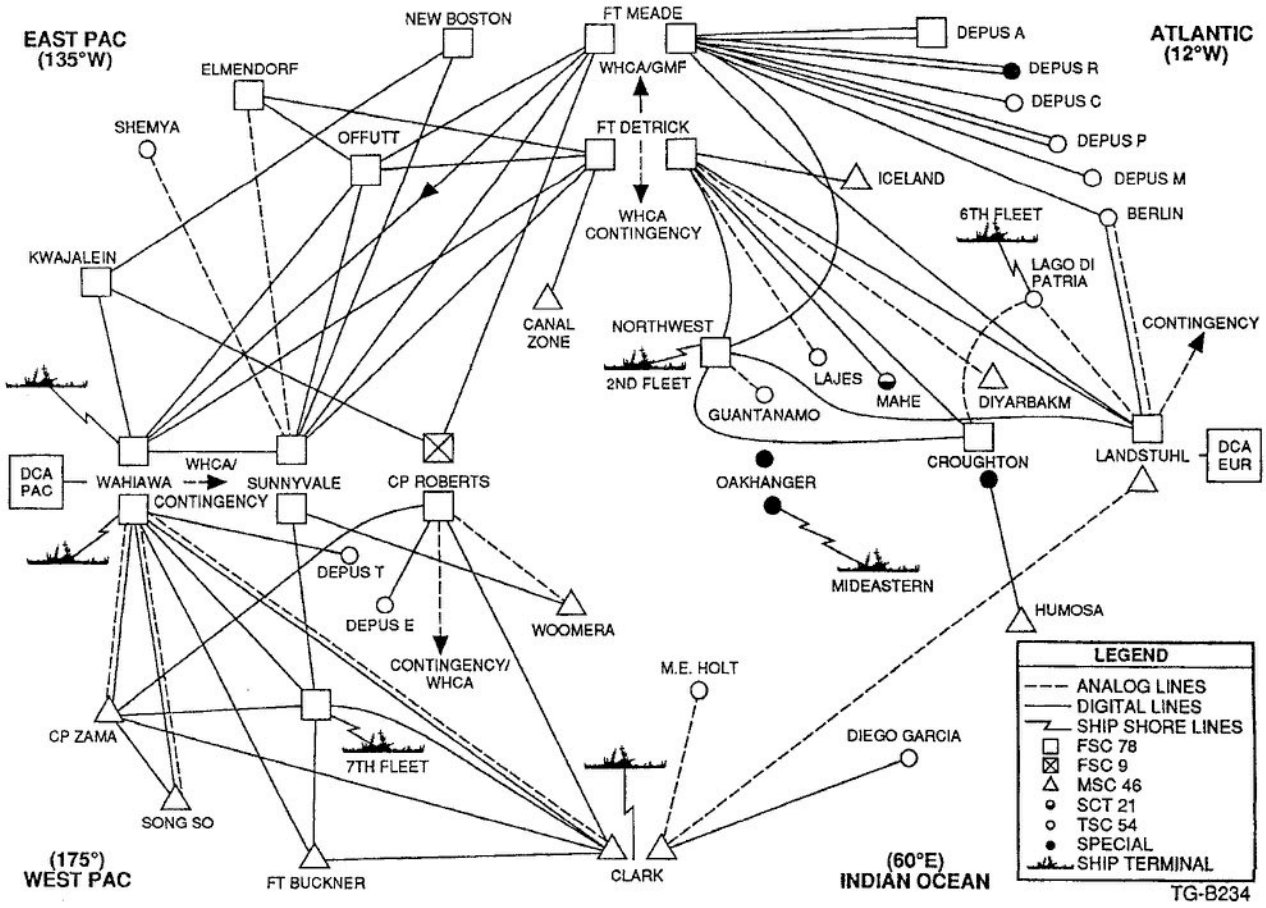


Figure 4-1. Defense Satellite Communications System (DSCS).

- Components of proven reliability are selected.
- All components are operated within their ratings.
- The satellite design provides adequate protection during launch and while in the space environment.
- Adequate use is made of redundancy to further increase the chance of successful operation.

Capacity. Through the years, people have become dependent, almost exclusively, on frequencies in the 5- to 30-MHz range for long-range global communications. These frequencies are shared among all countries and must support both military and civilian applications. This narrow range of frequencies and the propagation characteristics discussed previously seriously limit total communications capacity.

It is not surprising that a great interest exists in techniques that open more areas of the frequency spectrum to long-range communications (e.g., ionospheric and tropospheric scatter propagation). Communications satellites use the complete range of frequencies to 10,000 MHz and higher for long-range communications, thus providing more than 1,000 times the spectrum available in the HF band.

Flexibility. One need is to provide sufficient flexibility in systems so that new or changing demands can be satisfied without major overhaul or replacement of facilities. A disadvantage of submarine cable, for instance, is lack of flexibility because it is a fixed-plant facility. Limitations on the flexibility of other systems include the physical size of equipment, criticality of the troposphere, and microwave antenna aiming points and power needs. Satellite communications systems provide a high-degree of flexibility for several reasons:

(1) They have wide bandwidths that allow versatility in traffic handling capabilities.

(2) They are flexible in positioning or location because of their compact size.

(3) By providing wide bandwidths and essentially global coverage, they place minimum restraints on the number and location of ground stations served and the volume of communications sent to each.

Also, the use of solid-state devices and modular construction places minimum power requirements on systems. Usually, all terminal power can be supplied by small, mobile

power generator plants, an advantage that further broadens system flexibility.

Delay. Speed of communications is a must. All too frequently, delays are caused by poor propagation conditions. Weather, solar flares, and other atmospheric phenomena can totally disrupt normal communications links. When compounded by congested facilities, they cause delays in the transmission of urgent message.

Satellite systems designs have done much toward overcoming delay problems. Wide bandwidths have relieved traffic congestion by providing the capacity for many users simultaneously. The use of microwave frequencies and LOS principles have negated propagation problems. The ability to locate systems at sites convenient to users has ended or greatly reduced delivery delays.

Limitations. To understand the capabilities of space communications more fully, we must consider certain constraints and design limitations.

Natural constraints. The natural constraints that must be considered in space communications systems are listed below:

a. Path profile. An LOS path must be established between the transmitter and receiver.

b. Free space loss. Power radiated from a transmitting antenna is distributed over an everexpanding portion of the Earth's spherical surface. The resulting decrease in power density (power per unit area) reduces the energy "captured" by the receiving antenna and is known as free space loss. This is the most serious loss in satellite communications.

c. Noise. Noise is introduced at each stage of the communications process. The most significant contributions are from the medium through which communications are sent and from within the receiver itself. Noise reduces the ability of a receiver to detect weak signals.

Design limitations. Some design limitations that must be considered are as follows:

a. Transmitter power. This is a measure of the minimum signal strength with which a receiver can be gainfully operated.

b. Receiver noise figure. The inherent noise injected into a system by the receiver itself constitutes a basic limit on the minimum detectable signal.

c. Bandwith. The bandwidth of a system is limited by many considerations, most important of which is the capacity of a system to transmit data directly proportional to its usable bandwidth.

d. Data processing. Transmitting data into space does not necessarily mean that effective communication will be the result because all data does not represent information. One can find out the effective capacity of a system only by measuring how well transmitted data represents information. In other words, if data is transmitted with errors, there will be wasted energy, therefore, the system will not work as efficiently as it should.

e. Modulation. The effectiveness of a communications system varies greatly with the modulation technique used.

Please write your response to unit self-test questions and then check the text answers at the end of the unit.

SELF-TEST QUESTIONS

242. The purpose and operational objectives of the DSCS

1. What is the purpose of the DSCS?
   support global comm.

2. What is the primary operational objective of the DSCS? provide quality comm, to the users.

3. How does this objective change during times of stress? The DSCS strives to preserve the comm. needs of the WJMCCS.

243. Characteristics and limitations of the DSCS

1. What form of propagation is used by satellite systems? LOS in Microwave

2. What two types of reliability are important characteristics of a satellite system? Propagation reliability &

3. What are two ways satellite systems offer greater flexibility than other transmission systems? wideband offering greater wideband traffic handling capabilities

4. What two types of limitations apply to satellite systems? Natural constraints & design limitations.

4-2. Systems Control and Terminal Equipment

There are several types of terminals in use in the DSCS, each with its own operational characteristics, but they all must adhere to certain operational guidelines. In this section, we will discuss the operational control of the DSCS, the control system of the DSCS, and then take a look at the various terminals the system uses.

244. Control elements of the DSCS operations control system

DOCS is the system of operational control used in the DSCS. This control system is exercised by the DCA satellite operations division, the area communications operations centers, the DSCS operations centers, technical control facilities, and DSCS Earth terminals. This structure can be seen in figure 4-2.

DCA Satellite Operations Division (Code B440). B440 is the operations manager of the DSCS within the DCA directorate. One of their responsibilities is to develop and manage a control system (DOCS) that makes sure the DSCS mission and operational objectives are met. The DSCS control authority goes from B440 through the control hierarchy of the NCS/DCAOC and ACOCs to the DSCS operations centers.

DSCS Operations Center (DSCSOC). The DSCSOCs, colocated with dual-headed Earth terminals, perform satellite communications (SATCOM) network and satellite control. They conduct the daily operation and control of networks associated with chosen satellites under the authority of their ACOC. The DSCSOCs also provide operational direction of Earth terminals and satellite payloads by using DOCS equipment to maintain correct network parameters.

DSCS Earth Terminals. Earth terminals, or network control terminals (NCT), are operated and maintained by the military departments (MILDEP) and are a key element in the control process. NCT personnel perform the DOCS function by monitoring, measuring, and maintaining performance standards of terminal equipment, and by reconfiguring and adjusting operating parameters in response to direction from the DSCSOCs. Execution of all terminal operations is coordinated with the local TCF and/or the DSCSOC, as appropriate.

Technical Control Facility. TCFs support the DOCS by coordinating with NCTs and the DSCSOCs for channel fault isolation, corrective action, and channel activation or deactivation.

245. DSCS systems control

DSCS Systems Control. DSCS system control is an inherent part of the DCS control structure (fig. 4-2). Systems control will be exercised at the lowest level consistent with authority and resources. It is the means by which DSCS assets are used to maintain and restore maximum DSCS performance under changing traffic conditions, natural or manmade stresses, disturbances, and equipment disruptions.

The basic aspects of systems control include the timely acquisition of systems performance data, facility and satellite load status, and service quality indications. It also includes rapid analysis and processing and display of information to include real-time data base management. Decisionmaking and control execution are a major emphasis of systems control. It takes into consideration the support of long-range systems management and engineering objectives.

Planned and Reactive Changes. The DSCS has two methods for making changes to the systems it manages: planned and reactive. Planned changes are caused by

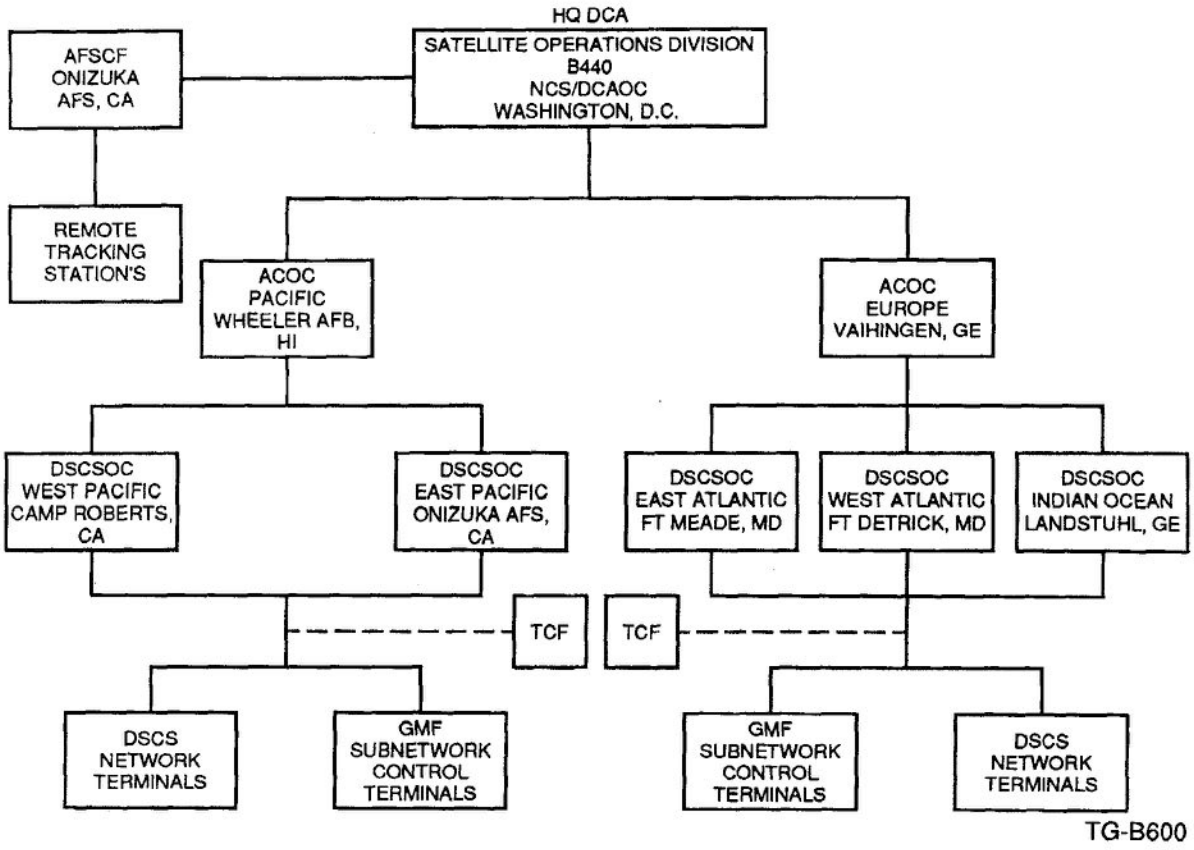


Figure 4-2. DSCS Operations Control System (DOCS).

management decisions on reconfiguration of DSCS subsystems and are based on a variety of engineering factors or on operational performance analysis indicators. Reactive changes are in response to disturbances, such as equipment failures, system outages, circuit degradation, or unusual traffic demands.

The systems control design supports DCA and the MILDEPs in the performance of their DSCS activities. Also, it builds on the inherent monitoring and control features of major satellite facilities to help DCA in the execution of its network administration and management activities.

Systems Control Objectives. The primary objectives for DSCS systems control are to:

a. Make sure of critical subscriber and system connectivity.

b. Make sure that systems control reacts quickly and flexibly, but in such a way as to impose no operational constraints on the system.

c. Incorporate a level of control and systems management survivability consistent with the survivability of the DSCS.

d. Make sure of sustained quality service through timely, effective testing and analysis in both normal and stressed environments.

e. Make sure of interoperability or compatibility with the control systems associated with other communications systems.

f. Increase DSCS efficiency.

g. Improve management visibility of availability status, quality of service, and performance of the DSCS.

h. Make operation and maintenance activities easier at DSCS stations.

i. Decrease manpower resources and support information required for control.

246. The Air Force satellite control facility

Air Force Satellite Control Facility (AFSCF). The Air Force has responsibility for launching DSCS satellites and, as mentioned in Volume 1 of this course, the AFSCF is under the operational direction of the Department of the Air Force and performs telemetry, tracking, and control of all satellites in the DSCS. It has the responsibility of keeping satellites in their assigned orbital positions, maintaining the prescribed altitude relative to Earth, and supporting the housekeeping functions necessary to make sure of optimum operations.

Though the AFSCF is not really a part of the DSCS control structure, it must coordinate all of its actions with the right DSCSOCs, as well as with B440. As you can see in figure 4-2, the AFSCF has a worldwide network of remote tracking stations (RTS), which supply a constant status of all DSCS satellites. The AFSCF is located in Onizuka AFS, California.

247. Terminals used in the DSCS

At present, four types of terminals are used in the DSCS:

(1) AN/FSC-9.
(2) AN/MSC-46.
(3) AN/FSC-78.
(4) AN/GSC-39.

AN/FCS-9. The AN/FSC-9 is a fixed terminal maintained by the Army. There is one located at Ft. Dix, New Jersey, and one at Camp Roberts, California. They are the primary entry points to the continental United States for the Pacific and European satellite communications links. They are both nodal stations.

AN/MSC-46. The AN/MSC-46 has a misleading nomenclature. It is a heavy air transportable terminal, not a mobile terminal as the "M" (in MSC-46) would lead you to believe. This system is an SHF system with most of its equipment sheltered in vans. Five vans make up the system (fig. 4-3):

(1) Operations control van (OCV).
(2) Maintenance van.
(3) Transmitter van.
(4) Storage van.
(5) Multiplexer van.

The antenna is transportable on an antenna trailer, often called a "bogey." Most installations have a radome surrounding the antenna to protect it from the weather.

Frequency range. The terminal has two power amplifiers. The high-power amplifier is a klystron with a maximum power output of 10kW (70 dBm). The low-power amplifier uses a traveling wave tube (TWT) and has a maximum power output of 2.5kW. Only one may be selected at a time.

Antenna system. The AN/MSC-46 uses a 40-foot paraboloid reflector for its antenna. Gain is approximately 57 dB at 8 GHz.

Tracking. This system tracks satellites manually, through the use of elevation and/or azimuth handwheels, or automatically. In the manual method, the operator/maintenance technician uses inputs to a servosystem to adjust the antenna position for maximum signal strength from the satellite. In the "autotrack" (automatic tracking) mode, the terminal will use the satellite's beacon frequency to fine-tune the antenna position.

Link and channel capability. AN/MSC-46 terminals consist of a maximum of 9 uplinks (transmit) and 15 downlinks (receive). They were originally configured to be either nodal or nonnodal systems with different FDM multiplexer vans; however, most have been reconfigured to use a digital subsystem van.

There are several MSC-46 terminals located around the world being operated and maintained by the using service. Presently, the Air Force has MSC-46 terminals at Diyabakir, Turkey; Humosa, Spain; and Misawa, Japan. These can be used in either a nodal or nonodal configuration, depending on the requirements of the communications link.

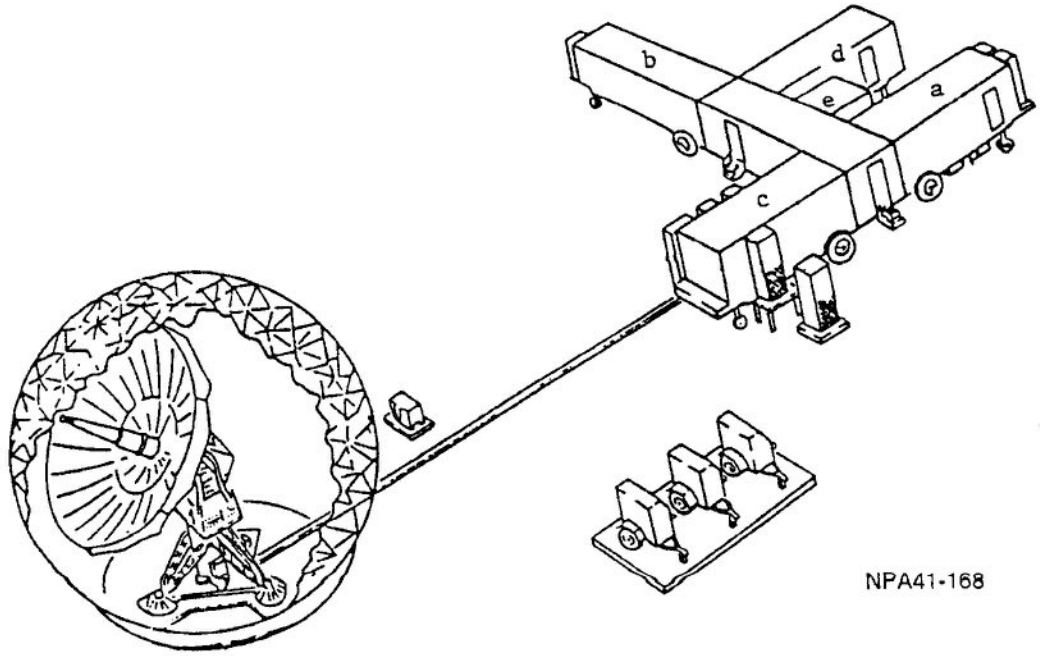


Figure 4-3. AN/MSC-46.

AN/FSC-78. AN/FSC-78 terminals are an updated version of the AN/MSC-46. It is a fixed SHF system using phase II and III satellite repeaters.

A typical layout of an AN/FSC-78 consists of an antenna group, a

communication/transmitter (C/T) equipment building, and an interfacility line trench connecting the two structures.

Frequency range. The frequency range of the AN/FSC-78 terminal is identical to that of the AN/MSC-46: receive frequencies are 7.25 to 7.75 GHz, and transmit frequencies are from 7.9 to 8.4 GHz.

Output power. The terminal has two 5kW TWT power amplifiers.

Antenna system. The AN/FSC-78 has a 60-foot parabolic reflector that works with a 7-foot hyperbolic reflector to form a Cassegrain feed system. Gain is approximately 60 dB at 8 GHz.

Tracking. Satellites may be tracked manually, through the use of elevation and/or azimuth handwheels, or automatically. In the manual mode, the operator/maintenance technician uses the inputs to a servo system to adjust antenna position for maximum signal strength from the satellite. In the autotrack mode, the terminal uses a satellite beacon frequency to fine tune antenna position.

Link and channel capability. AN/FSC-78 terminals consist of a maximum of 9 uplinks (transmit) and 15 downlinks (receive).

These terminals are located at the following sites:

a. RAF Croughton, England.

b. Elmendorf AFB, Alaska.

c. New Boston, New Hampshire.

d. Onizuka AFS, California.

e. Offutt AFB, Nebraska.

AN/GSC-39. The AN/GSC-39 is a medium-traffic, fixed terminal. It is made up to two major equipment groups: an antenna group and a communications equipment group. The communications equipment group is contained in two vans, the transmitter and operations vans that, along with a maintenance and supply van, provide all terminal support.

Frequency range. Frequency range for this system is the same as for the MSC-46 and FSC-78.

Output power. This terminal has two 5kW TWT power amplifiers.

Antenna system. A 38-foot parabolic main reflector provides high-gain, narrow-beam radiation of RF energy.

Tracking. The antenna has an autotrack capability that enables it to move from –2.5 to +92° in elevation.

All terminals in the DSCS have spread spectrum and antijam capabilities. Multiple access of satellites is done using frequency division techniques.

Please write your response to unit self-test questions and then check the text answers at the end of the unit.

SELF-TEST QUESTIONS

244. Control elements of the DSCS operations control system

1. What is the DOCS?
   systems operational control for DSCS

2. Who is responsible for managing the DOCS?
   DSCS satellite operations Division

3. What are the functions of the DSCSOCs?
   conduct daily operations of satellite

4. What does an NCT do?
   performs control functions for all DSCS satellites.

245. DSCS systems control

1. What conditions will the DSCS control system encounter while trying to maintain and restore maximum performance? changing traffic conditions, natural or manmade stresses, & equipt. disruptions.

2. Name the two methods the DSCS has of making changes to a system and briefly explain each.
planned changes occur as a result of management decisions.

246. The Air Force satellite control facility

1. What is the primary function of the AFSCF?
telemetry, tracking, & control of satellites

2. How does the AFSCF receive status on DSCS satellites? network of remote tracking

247. Terminals used in the DSCS

1. What four satellite terminals are used in the DSCS?
AN/FSC 9, 46, 78, & 39

2. Which terminal is air transportable?
AN/MSC 46

3. What is the frequency range of DSCS terminals?
~~AN/FSC 94~~ 7.25 - 8.4 GHz

4-3. Associated Networks

There are many networks that use the satellites of the DSCS. Some of them are under the direct control and operational direction of DCA, and others are operated by the military departments. We will discuss two of these, the ground mobile forces network and the Air Force Satellite Communications System.

248. Ground mobile forces

Purpose and Applicability of Ground Mobile Forces. The US Army first made satellite terminals for its GMF to provide access into the DSCS. As the name implies, GMF terminals were designed specifically for military use in tactical communications. These terminals are capable of entry into the DCS during crises through a network of DSCS gateways. They augment other mobile communications systems and provide the quick reaction ability needed to support tactical mission.

Gateway Station. Gateway stations provide the deployed tactical community with the ability to extend their communications capabilities from a point-to-point mode to an intratheater or intertheater mode. There are 15-gateway stations.

Terminals. All GMF terminals operate in the same frequency range as the four DSCS terminals, and all include an automatic tracking 8-foot diameter antenna mounted as an integral part of the equipment enclosure. They are completely self-contained and designed to provide a full communications ability within 20 minutes of arrival at a deployed location. There are two terminals being used by the Air Force: the AN/TSC-94 and the AN/TSC-100.

AN/TSC-94. The AN/TSC-94 has all equipment necessary for the reception, transmission, and processing of multiplexed voice channels. It is used for point-to-point operation in tactical communications systems and is capable of simultaneous transmission and reception of a single high-rate

carrier. The terminal consists of receive, transmit, antenna, power, and distribution groups. Also, it has an environmental control unit (heating and air-conditioning) for personnel comfort.

The AN/TSC-94s 8-foot dish must be built on-arrival at the deployed location. It can then manually track satellites using switches on the antenna control panel, or track automatically through a method known as random step scan. This terminal can track either the satellite beacon or the communications signal. However, because the autotrack system can adjust the antenna only +12.5°, antenna movement is limited.

There is an output power capability of 500 watts through one klystron. The terminal has a single uplink and downlink, providing a total of 12-voice channels and 1-voice orderwire.

AN/TSC-100. The AN/TSC-100 is picked for single- or multiple-carrier service with single- or dual-tracking antenna. The terminal is composed of three major components (fig. 4-4). They include an S-280-type shelter, housing all of the terminal electronics except for the receiver low-noise front end, an 8-foot ground-mounted parabolic antenna system, and a diesel-powered generator and associated switch gear to provide primary power. The terminal can also operate with a 20-foot antenna.

249. The Air Force Satellite Communications System

The AFSCS provides a record communications capability to satisfy high-priority Air Force requirements for its operational command, control, and communications on a worldwide basis. It consists of a space segment and a terminal segment.

Space Segment. The space segment includes a communications capability designed into other satellite programs, and Air Force transponders are carried "piggyback" on other satellites. Air Force satellite communications

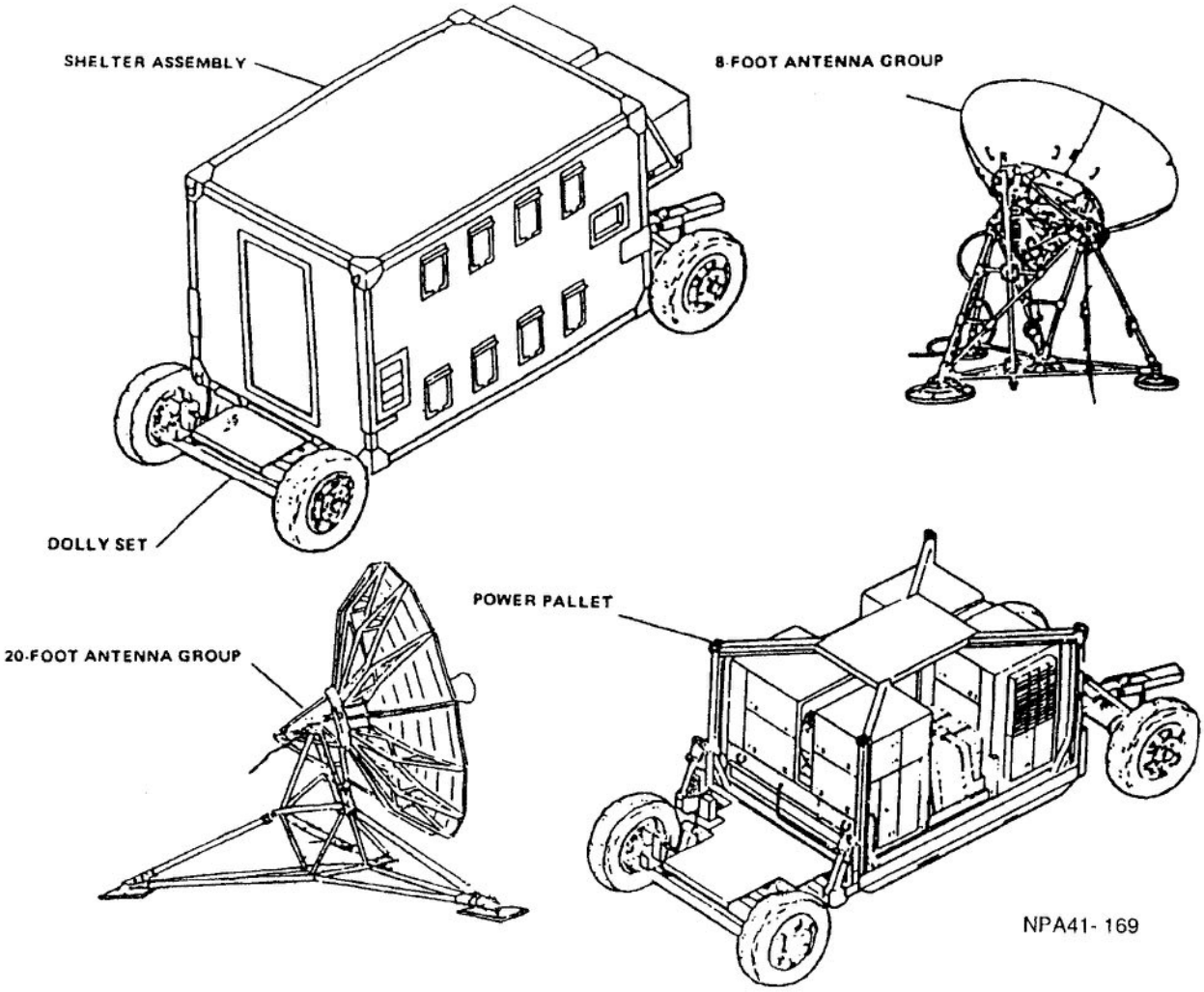


Figure 4-4. AN/TSC-100.

(AFSATCOM is a term used interchangeably with AFSCS) equipment is designed into each of the Navy Fleet Satellite Communications (FLTSATCOM) system satellites in geosynchronous equatorial orbit to provide overlapping Earth coverage in all areas except the polar regions. Polar coverage is provided by the Satellite Data System (SDS) satellites placed in highly inclined elliptical orbits.

Terminal segment. All AFSCS terminals provide two-way record communications (teletypewrite) over standard UHF radio channels using frequency shift keying (FSK) modulation at a 75 bps transmission rate in serial bit form. The terminals operate in four modes on the narrowband FSK channels: random access, roll-call polling, and two modes of time-access polling. Also, some terminals can transmit and receive two channels of wideband FSK signals.

AFSCS terminals are directed and operationally controlled by the Air Force and its personnel. There are three types of ground terminals and many types of airborne terminals all operating in the 240- to 400-MHz range. Multiple access of a satellite is done by frequency and time-division methods.

Please write your response to unit self-test questions and then check the text answers at the end of the unit.

SELF-TEST QUESTIONS

248. Ground mobile forces

1. How do GMF terminals enter the DSCS?
   set of DSCS gateway
2. What capability does the concept of GMF terminals' being self-contained provide? full comm. capability within 20 min timeframe
3. What two GMF terminals are used by the Air Force?
   AN/TSC 94 & AN/TSC 100

249. The Air Force satellite communications system

1. What is the purpose of the AMFSCS?
   provides records
2. What are the two segments of the AFSCS?
   space & Terminal
3. In what frequency range do AFSCS terminals operate? 240 to 400 mhz

ANSWERS TO SELF-TEST QUESTIONS

242

1. To support the global communications networks of DOD.
2. To provide quality communications service to its users.
3. The DSCS then strives to preserve the communications needs of the WWMCCS.

243

1. Line-of-sight transmission in the microwave frequency range.
2. Propagation reliability and reliable unattended operation for extended periods of time.
3. Wide bandwidths offer greater traffic handling capabilities, and their compact size makes positioning easier.
4. Natural constraints and design limitations.

244

1. It is the system of operational control for the DSCS.
2. The DSCS satellite operations division.
3. They conduct the daily operation of satellite networks and provide operational direction to their NCTs.
4. It performs control functions for all DSCS satellites.

245

1. Changing traffic conditions, natural or manmade stresses, disturbances, and equipment disruptions.
2. Planned changes occur as a result of management decisions to reconfigure subsystems. Reactive changes occur as the result of system disruptions.

246

1. It performs telemetry, tracking, and control of DSCS satellites.
2. Through a network of remote tracking stations.

247

1. The AN/FSC-9, AN/MSC-46, AN/FSC-78, and AN/GSC-39.
2. The AN/MSC-46.
3. 7.25 to 8.4 GHz.

248

1. Via a set of DSCS gateways.
2. The ability to provide a full-communications capability within 20 minutes of arrival at a deployed location.
3. The AN/TSC-94 and AN/TSC-100.

249

1. It provides record communications for high-priority Air Force command, control, and communications requirements.
2. The space segment and terminal segment.
3. From 240 to 400 MHz.

Do the Unit Review Exercises (URE) before going to the next unit. ➡

UNIT REVIEW EXERCISES

Note to Student: Consider all choices carefully, select the *best* answer to each question, and *circle* the corresponding letter.

78. (242) What is a unique feature of the Defense Satellite Communications System (DSCS)?

    a. Its capability to extend communications to remote locations.
    b. Its capability to transmit in the SHF frequency range.
    c. Its broad bandwidth and freedom from outside noise disturbances.
    d. Its freedom from solar bursts and other disturbances.

79. (242) During trans- and postattack periods, what is the primary objective of the Defense Satellite Communications System (DSCS)?

    a. To supplement other major communications networks.
    b. To preserve the communications needs of the WWMCCS.
    c. To provide a communications capability for the JCS.
    d. To provide a communications capability to remote locations.

80. (243) What areas are of concern when considering Defense Satellite Communications System (DSCS) system limitations?

    a. Free space loss and frequency reliability.
    b. Free space loss and natural constraints.
    c. Frequency reliability and design limitations.
    d. Natural constraints and design limitations.

81. (244) Who actually performs the DSCS Operations Control System (DOCS) function?

    a. DSCS operations center (DSCSOC) personnel.
    b. Code B440.
    c. ACOC/RCF personnel.
    d. Network control terminal (NCT) personnel.

82. (245) What are the two methods for making changes to Defense Satellite Communications System (DSCS) systems?

    a. Current and reactive.
    b. Planned and reactive.
    c. Planned and current.
    d. Planned and concurrent.

83. (245) What type changes are made to Defense Satellite Communications System (DSCS) systems in response to disturbances, such as equipment failures, system outages, circuit degradation, or unusual traffic conditions?

    a. Current.
    b. Reactive.
    c. Planned.
    d. Concurrent.

84. (246) Who performs telemetry, tracking, and control of the Defense Satellite Communications System (DSCS) satellites?

    a. The Air Force Satellite Control Facility (AFSCF).
    b. The DSCS operations center (DSCSOC).
    c. Code B440.
    d. The NCTs.

85. (246) How does the Air Force Satellite Control Facility (AFSCF) receive status of its satellites?

    a. Through status control channels from each of the Defense Satellite Communications System (DSCS) satellites.
    b. Through status reports from the DSCS operations center (DSCSOC).
    c. Through status reports from the remote tracking stations (RTS).
    d. Through status reports from code B440.

86. (247) What type terminal serves as the primary entry point to the CONUS for satellites in the European and Pacific communications links?

    a. AN/FSC-78.
    b. AN/MSC-46.
    c. AN/TSC-62.
    d. AN/FSC-9.

87. (247) What is the operating frequency range of the AN/MSC-46?

    a. 7.25 to 7.75 GHz.
    b. 7.75 to 8.4 GHz.
    c. 7.25 to 8.4 GHz.
    d. 7.9 to 8.4 GHz.

88. (247) All terminals in the Defense Satellite Communications System (DSCS) have

a. autotrack capability.
b. spread spectrum and antijam capabilities.
c. two 5kW TWT power amplifiers.
d. a 38-foot parabolic antenna.

89. (248) Which satellite program is designed to support tactical missions using Defense Satellite Communications System (DSCS) assets?

a. Air Force Satellite Communications System (AFSCS).
b. Navy Fleet Satellite Communications (FLTSATCOM).
c. Air Force Satellite Control Facility (AFSCF).
d. Ground mobile forces (GMF).

90. (248) How does the deployed tactical community extend its satellite communications capability to an intertheater mode?

a. Through the systems inherent ability to reach remote locations.
b. Through the use of a network of satellite relay facilities.
c. Through the use of a network of gateway stations.
d. Through interfacing circuitry with other communications networks.

91. (248) What two GMF terminals are being used by the Air Force?

a. AN/TSC-94 and AN/TSC-100.
b. AN/TSC-62 and AN/TSC-100.
c. AN/FSC-9 and AN/TSC-62A.
d. AN/MSC-46 and AN/TSC-62.

92. (249) What are the two segments of the Air Force Satellite Communications System (AFSCS)?

a. Classified and unclassified.
b. Space and control.
c. Unclassified and SECRET.
d. Space and terminal.

Please read the topic page for Unit 5 and continue. ➡

LOCAL AREA NETWORK

Local area networking (LAN) has emerged from its infancy into a healthy brawling adolescence. A few basic technologies have taken hold; commercial vendors are beginning to offer high-level functions, and standards committees in both Europe and America are publishing new specifications. The need to integrate personal computers into corporate environment has led to merging backend, general purpose, and personal networks. Our main focus here is to discuss the types of media used by the local area network, the types of topology and protocol, and the access interface devices.

5-1. Transmission Media

For several years, after the LAN was first introduced, technicians focused on the media, protocol, topology, and media access. These four parameters together describe LAN technology, which is defined as the method used to transmit information packets between stations. So let's start by discussing the different types of media we have available for this network.

250. Media used by the local area network

Three media are practical for local area networking: twisted pairs of copper wire, coaxial cable, and optical fiber. Each of the three serves certain applications better than others. Each supports certain transmission techniques and has its own cost and performance benefits.

Twisted Copper Wire. This type is also called twisted pair and is otherwise known as common telephone cord. Ranging in price from 5 to 25 cents per foot, it is the least expensive medium available for LAN installations. It is also the easiest to install; a user can string it along a baseboard in minutes. Further, twisted pair is the most readily available of all LAN media, since it is in constant, high-volume production for voice telephone use.

However, twisted copper wire has several disadvantages for data transmission. It is extremely susceptible to electrical interference or noise from outside sources (such as typewriters and air-conditioners). Such noise has very little effect, if any at all, with an analog voice signal, but it causes two interrelated problems for data transmission. First, it limits the speed at which data can travel, since a burst of noise that would garble only a few bits of low-speed data will destroy many bits of high-speed data. In other words, the higher the data speed, the more data will be lost if a "line hit" occurs.

Second, it limits the distance that a data signal can travel. A signal grows weaker, or attenuates, as it travels farther. Signals attenuate on all media, but a twisted pair's vulnerability to noise adds another factor. A length of twisted pair acts as an antenna; the longer it gets, the more noise it gathers. After a given distance, the increased noise obliterates the attenuated signal.

Two techniques are used to reduce this vulnerability: shielding and repeating. Shielding makes the medium less vulnerable to electrical noise but adds significantly to the cost of the wire. The use of active repeaters increases the distance a signal can travel. Repeaters are devices that receive a signal and retransmit it into another length of wire or cable. Repeaters are expensive and thus increase the cost of running twisted pair over a distance.

Twisted pair is best for low-cost, short-distance, local area networks, especially for small networks linking personal computers. It can carry data at rates up to 1-million bits per second over distances up to several hundred feet without repeaters.

Coaxial Cable. This type is the most widely used medium for local area networking. It comes in several forms, and each form suits itself to a different kind of application. All forms of coaxial cable have the same general structure: a central conductor, the part of the cable that carries the signal, is surrounded by a dielectric, or nonconducting insulator; then by a solid or woven metal shielding layer; and finally by some protective outer coating. All of these layers are concentric (centered) around a common axis, thus the term "coaxial." Since coaxial cable is a shielded medium by definition, it is largely immune to electrical noise and can carry data at higher rates over longer distances than can twisted pair. There are two general types of coaxial cable, named for transmission techniques they support.

Baseband cables. Baseband coaxial cable carries one signal at a time. Since signals on baseband cable travel at rates from 1- to 10-million bits per second, many signals can be time-division multiplexed over baseband cable. For local area networking, baseband signals are always digital, with the presence of a specified voltage representing the ON condition, and the absence of a voltage representing an OFF condition.

Broadband cables. Broadband coaxial cable can carry many signals at a time, with each signal occupying a different

frequency band on the cable. While data rates that are practical on any one channel of a broadband network are somewhat lower than those available with baseband transmission (between 1- and 5-million bits per second), the availability of between 20 and 30 such channels on a single cable greatly increases the amount of data the medium can carry. Of course, many signals can be time-division multiplexed over each single channel.

Signals on a broadband network are always analog, and bits of information are represented by variations in the strength or frequency of a carrier signal. The data channels of a broadband LAN can share the same cable with other analog signals, such as cable television (CATV) channels operating at different frequencies. Indeed, the actual cable used for broadband networking is the same type cable commonly used for CATV transmission.

A baseband signal is broadcast in both directions along a cable away from the sending station. Broadband signals are effectively unidirectional, due to the nature of the coupling and amplifying hardware necessary to carry the radio-frequency signal. To enable a station to send and receive such unidirectional signals, broadband networks use a frequency separation technique. In this technique, a station sends on one frequency in a *transmit* direction to a frequency translator at the head-end of the cable. The frequency translator then resends the signal at a higher frequency in the *receive* direction. Signals in one direction cannot interfere with signals in the other. Some single-cable systems use different *band split,* or differences in frequency between a given forward channel and its associated reverse channel.

The other technique for handling unidirectional signals in broadband network uses a dual cable. The cable is looped at the head-end so that it passes each station twice. Each station has a transmitter on the *transmit* length of cable and a receiver on the *receive* length. Dual-cable configurations offer twice the bandwidth, hence twice the number of channels, as single-cable configurations, since their stations transmit and receive at the same frequency but on different lengths of cable. On the other hand, dual-cable configurations also require twice as much cable to be purchased and installed.

Since broadband transmissions are analog, they require modems to propagate the digital signal on the radiofrequency carrier. These radiofrequency (RF) modems are available in two types: fixed frequency and frequency-agile. Fixed-frequency RF modems, as the name implies, transmits on only one frequency and receives on only one. Frequency-agile modems are able to transmit and receive on any of several pairs of frequencies; users can select these frequencies in software on most systems and, thus, can select from a range of available data channels.

While coaxial cable remains the medium of choice for most LAN applications, there has been much controversy over the choice between baseband and broadband transmission techniques. Actually, the two techniques serve quite different applications. The physical baseband cable is much more expensive than broadband cable depending on type. Baseband cable costs from 50 cents to 3 dollars per foot, while standard broadband cable costs between 35 cents and 1 dollar per foot. Baseband cable may require a hard conduit to comply with fire regulations. Broadband cable is already clad in rigid aluminum. Baseband cable cannot extend beyond a few thousand feet without expensive digital repeaters; broadband cable can stretch for many kilometers using only inexpensive amplifiers.

On the other hand, baseband cable is easy to install and requires almost no maintenance. A broadband data network requires a careful process of physical design. Its components must be tuned carefully to handle specific ranges of frequencies, and both cable and connecting hardware are very sensitive to changes in temperature and humidity. Broadband networking requires a staff of trained RF technicians, both for design and for everyday maintenance.

Baseband networks fit best in a small-to-medium data processing or office automation environment. They work well within a single building, although a single-baseband network can span across a small base. With current technology, baseband networks can handle only data traffic. Broadband networks work most effectively in large configurations, where economies of scale can justify maintenance costs. A broadband network can cover a large base with many buildings or even a good-sized city. Broadband networks can carry voice and video traffic as well as data.

For large applications, hybrid broadband and baseband configurations are beginning to appear. In such configurations, a broadband trunk carries data among several local baseband subnetworks along with such applications as local videoconferencing. Hybrid networks make best use of the advantages of both technologies, allowing simple baseband transmission to handle most of the data traffic, while the crankier but more powerful broadband systems provide a backbone for a multiservice network. Such a system reduces the number of connections; thus it reduces the number of components to be maintained on the broadband portion of the network.

Optical Fiber. Optical fiber is the newest medium in the commercial LAN market. In the long run, it has the most potential; but, for the present, it is the most limited. Right now, fiber-optic LAN transmission is limited to a single band per cable, the equal of baseband coax. Technologies, now commercially impractical, but experimentally proven, will allow fiber optics to carry many times the bandwidth of

CATV cable. Right now, fiber-optic cable is the most expensive medium available for LANs; in the future, as it comes into wider use for telephone applications, it will become the cheapest. Copper is a scarce resource; silicon, from which optical fibers are made, is the most abundant element on the surface of the Earth.

The principal advantages of fiber optics with present-day transmission technology are sturdiness and security. Optical fiber is immune to both the physical and electrical influences of the environment. Copper corrodes, glass does not. Copper conducts electricity, glass does not. Fiber optic cable is almost impossible to tap secretly with current military technology; operators can isolate a break or even a significant movement in a fiber optic cable to a single inch over a mile or more of cable.

The principal disadvantages of fiber optics for present day LANs are cost and difficulty of connections. As a new technology, fiber has yet to realize economies of scale; it remains expensive. The very property of fiber optics that makes it ideal for security makes it impractical for LAN use; fiber optic cable is extremely difficult to tap. With coaxial cable, one must be sure that only the conductor from the tap touches the conductor from the cable and that the connection remains adequately shielded. With optical fiber cable, one must align each fiber (of hundreds or thousands) to make sure of a continuous connection. New technologies have simplified the problem of connection to a fiber-optic trunk, and future technologies may simplify it further, but coaxial cable remains an easier medium to handle and work with.

Table 5-1 compares the transmission media available for local area networking.

TABLE 5-1
COMPARISON OF TRANSMISSION MEDIA

	TWISTED PAIR WIRE	BASEBAND COAXIAL CABLE	BROADBAND COAXIAL CABLE	FIBER OPTIC CABLE
Topologies supported	ring, star, bus, tree	bus,tree, ring	bus, tree	ring, star, tree
Max # of nodes per network	up to 1024	up to 1024	up to about 25,000	up to 1024
Max geographical	3 kilometers	10 kilometers	50 kilometers	10 kilometers
Type of signal	single channel: unidirectional; analog or digital depending on type of modulation used; half- or full-duplex	single channel; bidirectional, digital, half-duplex	multi-channel; unidirectional; RF analog; half-duplex (full-duplex can be achieved by using two channels)	one single channel, unidirectional, half-duplex signal-encoded lightbeam per fiber; multiple fibers per cable; full duplex can be achieved by using two fibers
Max bandwidth	up to 1Mbps	up to 10Mbps	up to 400 MHz (aggregate total)	up to 50Mbps in 10 kilometer range; up to 1 Gbps in expewrimental tests
Major advantages	low cost; may be an existing plant with no rewiring needed;very easy to install	low maintenance cost; simple to install and tap	supports voice, data, and video applications simultaneously; better immunity to noise and interference than baseband; more flexable topology (branching tree); rugged, durable equipment; needs no conduit; tolerates 100% bandwidth loading; uses off-the-shelf industry standard CATV components	supports voice, date and video applications simultaneously; immunity to noise, cross-talk, and electrical interference; very high bandwidth; highly secure; low signal loss; low weight/diameter; can be installed in small spaces; durable under adverse temperature, chemical, and radiation conditions
Major disadvantages	high error rates at higher speeds; limited bandwidth; low imunity to noise and crosstalk; difficult to maintain and troubleshoot; lacks physical ruggedness; requires conduits,trenches or ducts	lower noise immunity than broadband (can be improved by the use of filters,special cables and other means); bandwidth can only carry about 40% load to remain stable; limited distance and topology; conduit required for hostile environments; not highly secure	high maintenance cost; more difficult to install and tap than baseband; RF modems required at each user station; modems are expensive and limit the user device's transmission rate	very high cost (but declining);requires skill installation and maintenance personnel; experimental technology; limited commercial availability; taps not perfected; currently limited to point-to-point connections

Please write your response to unit self-test questions and then check the text answers at the end of the unit.

SELF-TEST QUESTIONS

250. Media used by the local area network

1. What are the four parameters that describe LAN technology? media, protocol, topology, & media access.

2. What are the three types of media used in LANs? twisted pair, coax, & fiber

3. What techniques do LANs use to reduce the vulnerability on twisted wire media? shielding & repeating

4. Name the two types of coaxial cable media used in LANs. Baseband & broadband

5. List the advantages and disadvantages of using fiber optics as a LANs transmission media.
adv. - sturdy & secure
disadv. - high cost & difficulty

5-2. Topology

A network's topology is the physical and logical arrangement of its stations in relation to one another. For local area networking, we use the term "stations" rather than the more traditional "nodes." A node in a traditional data communications network sits at the intersection of two or more transmission paths and switches traffic among those paths. On most local area networks, a station attaches to a single transmission trunk at one point, catching signals addressed to it, and transmitting signals along the single path to other similar stations. There are a variety of topologies available to LANs, and we will describe them in the following text.

251. The topology used in LANs

There are three basic LAN topologies: linear bus, ring, and star (fig. 5-1).

Linear Bus. In a linear bus, the stations are arranged along a single length of cable so that it can be extended on at least one end. A tree, also shown in figure 5-1, is a complex linear bus in which the cable branches at either or both ends, but offers only one transmission path between any two stations. All broadband networks, and many baseband networks, use a bus, or tree topology.

Ring. In a ring topology, the stations are arranged along the transmission path so that a signal passes through one station at a time before returning to its originating station; the stations form a closed circle. A loop network is a ring network in which one master station controls transmissions.

Star. A star network has a central node that connects to each station by a single, point-to-point link. Any communication between one station and another must pass through the central node. Right now, in the United States, bus and tree technologies are the most common. In Europe, ring architectures are more common, since much of the pioneering work in ring networking occurred at European universities.

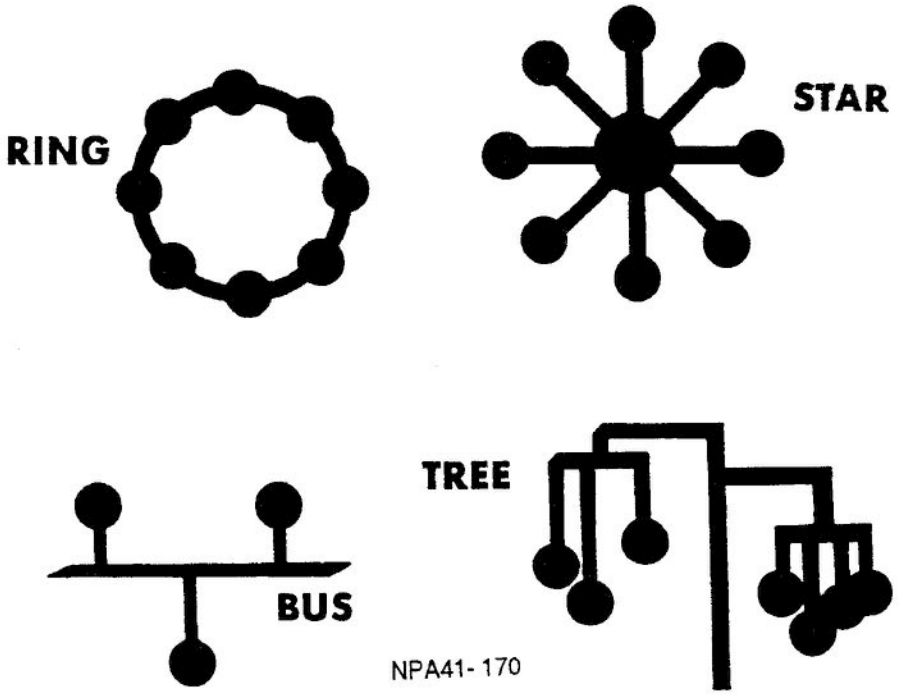


Figure 5-1. Types of topology.

In bus and ring networks, all transmissions are broadcast. Any signal transmitted on the network passes all the network's stations. The receiving intelligence in each station recognizes its address on a given signal and copies only its own signals. In star networks, signals sent through the central node are circuit-switched to the proper receiving station over a permanently or temporarily dedicated physical path.

Each topology has its strengths and weaknesses. In choosing a topology, look at such performance issues as delay, throughput, reliability, and robustness (robustness is the network's ability to continue through or to recover after failure of one or more of its stations). Also, consider such physical constraints as the circuit speed (or raw data rate), maximum operating distance, maximum number of stations, channel error rate, and overall system costs. Tables 5-2 and 5-3 compare the three basic topologies according to constraint and performance considerations.

TABLE 5-2
COMPARISON OF BASIC TOPOLOGIES (PERFORMANCE CONSIDERATIONS)

PERFORMANCE CONSIDERATIONS			
	LINEAR BUS	**RING**	**STAR**
DELAY	In token bus networks it is a fixed function dependent on the number of nodes. In contention bus networks it is variable dependent on current traffic. Delay distortion (jitter) is possible.	A fixed function dependent on the number of nodes in the network.	In heavy traffic conditions requests for service may be blocked at the switch in a PBX.
THROUGHPUT	decreases in token bus networks with each node added. In contention networks it is best in light, bursty traffic conditions and decreases in high-volume, steady traffic environments.	Decreases with each added node.	Dependent on internal bus capacity of central node.
RELIABILITY	Failure of one station will not affect the rest of the network. A break in a cable may affect only part of the network.	If one station fails the whole network fails unless bypass circuitry has been implemented in each interface or node. If loop is severed the whole network fails unless redundancy features have been implemented. Potentially low reliability can be compensated for by high quality engineering design.	Failure of one station does not affect the rest of the network. If central node fails the whole network fails.
ROBUSTNESS	Relationship between stations is peer-to-peer. Network is difficult to monitor. In contention networks the difference between nose and collisions may be difficult to distinguish.	Nodes are easy to understand, construct and maintain. May require custom designed, device-dependent interface. Communications control overhead is generally high. If network fails, recovery may be difficult, and may require complex logic and processing.	Readily available network monitoring and control software. High overhead for communications control. Corresponds well to applications in hierarchial (master/slave) networks.

TABLE 5-3
COMPARISON OF BASIC TOPOLOGIES (CONSTRAINT CONSIDERATIONS)

CONSTRAINT CONSIDERATIONS			
	LINEAR BUS	**RING**	**STAR**
CIRCUIT SPEED	Varies up to 50 Mbps.	Varies up to 10 Mbps.	Varies considerably depending on medium.
DISTANCE	Generally unlimited by topology.	Limitations are imposed on both total distance and distance between nodes.	Limitations are imposed on distance between central node and any user station.
MAX # OF NODES	In token bus networks user stations may be added or deleted without reconfiguring the networks. Addition of each station directly affects performance.	May be a fixed parameter dependent on command station capacity. Addition of each station directly affects performance.	Expansion limitations are dependent on capacity of central node. Difficult to reconfigure.
ERROR RATE	Bit errors are lowest when fiber optic cable transmission is medium, low when coax is used, and higher when twisted pair is used.	Twisted pair wire is vulnerable to transient errors. Fiber optics has very low error rate.	Twisted pair is vulnerable to transient errors.
COST	Generally lower cost per user station than star networks and higher than ring networks.	Generally lower cost per station than other topologies.	High initial cost. Low incremental cost thereafter.

Please write your response to unit self-test questions and then check the text answers at the end of the unit.

SELF-TEST QUESTIONS

251. Topology used in LANs

1. List the three basic topologies used in LANs.
   star
   bus
   ring
2. What type of topology is used by all broadband networks?
   bus of tree top.
3. How does a loop network differ from a ring network?
   loop has one master station

5-3. Access Interface Devices

A network's access method is the technique by which the network distributes the right to transmit among its participating stations. The right to transmit is an issue only in broadcast topologies, where several stations share a single main data channel on which all stations receive and on which any station can transmit. The access method is the network's way of controlling traffic.

252. Access methods used in LAN

Access control in a local area network can be centralized or distributed. Most conventional networks of computer terminals use central access control, with a mainframe, or its front-end processor, polling the terminals in sequence for their transmission. Most LANs use distributed access methods in which each station participates equally in controlling the network. There are two general classes of distributed access: random and deterministic. With a random access method, any station can initiate a transmission at any time. With a deterministic access method, each station must wait its turn to transmit.

The most common random access method on today's LANs is carrier sense multiple access (CSMA). In a CSMA network, all stations have the ability to sense traffic on the network. When a station wishes to transmit, it *listens* on the main data channel for the sort of electrical activity it recognizes as traffic; it *senses carrier.* If the station senses traffic, it defers its transmission for a random interval and then resumes listening. When the station senses no traffic on the channel, it transmits. One weakness in CSMA access is that two stations may sense a clear channel at the same time and transmit simultaneously. The result is a "collision," in which the signals from simultaneously transmitting stations interfere with one another. Many CSMA networks implement a mechanism for collision detection (CSMA/CD), which allows stations to recognize a collision, stop transmitting imme- diately, and resume transmission after a random wait to reduce the chance that any two stations will transmit at the same time.

The most widely used deterministic access method today is *token passing*. In a token passing network, stations distribute the right to transmit on the channel by circulating a *token*, a special bit pattern that assigns the right to transmit to the station that receives it. A station that wishes to transmit waits until it receives the token from the previous station in the token passing order. When the station receives the token, it transmits its data and then passes the token to the next station. Token passing is a form of distributed polling; each station on the network polls the next station in line for its transmission. Token passing networks require a slightly greater effort to configure than do contention networks, since each station must have not only a logical address but also a logical place in the token passing sequence.

CSMA and CSMA/CD are most often found in bus and tree networks; token passing is most often found in bus and ring networks. A third access method, *slotted access*, is found exclusively in ring networks. Slotted access is a deterministic access method similar to token passing. Instead of a token, the stations circulate an empty data frame that a station may fill whenever it receives a frame in its turn. Slotted access is even more deterministic than token passing, since the technique dictates not only when a station may transmit but exactly how much data a station may send each time it transmits.

A network's access method is the most important factor in determining its performance. Each access method functions differently under different kinds of traffic and on networks of different sizes. CSMA networks perform better with sporadic or *bursty* traffic patterns in which some stations transmit a great deal of data at a time or transmit very often, while others transmit a smaller amount of data less frequently. Performance on a CSMA network degrades as the likelihood of a collision increases. The chance of a collision increases with the number of stations likely to transmit and the physical length of the network's main cable, since the time a signal takes to reach the station farthest from the transmitting station affects the likelihood of that station's sensing carrier in time to withhold its transmission. Another factor in CSMA networks is the length of individual transmissions. A CSMA network operates more efficiently when stations transmit long individual messages than when they transmit a large number of short messages.

Deterministic access methods perform better under uniform, heavy traffic than do CSMA networks. The number of participating stations is the most important factor affecting performance in token passing and slotted networks, since the right to transmit must circulate through every station in turn before a given station may transmit after it has already passed the right. Under any loading conditions, performance is easier to predict for deterministic access methods than for random access methods.

253. Intelligent connector units

Intelligent Connector Unit (ICU). The local area network has a distinct system that works in tandem to allow the sharing of electronic resources. The ICU, which is one of these resources, provides the active system with a unit that interprets and monitors the data traffic across the network. The ICU is a flexible, microprocessor-controlled device that can communicate with other devices on the network. The hardware comprising an ICU consists of a series of integrated circuits and a radiofrequency transmitter and receiver.

Three different types of ICUs are available for use: (1) a dual-port ICU, which has two ports for connection to user devices; (2) a four-port ICU designed to support up to four

resources; and (3) a multiport ICU that provides as many as 32 ports and is designed specifically for multiport resources such as minicomputers and mainframes.

Operations. The communication process begins when a user issues a command to the ICU to call a resource with a particular name. The ICU responds by sending out a message on the network, called a query packet, indicating that it is looking for the address of an ICU with a particular name. All of the ICUs on the network read this packet, and each ICU with the proper name sends back a response.

In its response to the query, each ICU identifies itself by its synchronous data link control (SDLC address). The modified SDLC address used by some ICUs is the 16-bit physical address that uniquely identifies each ICU on the network. Once the ICU that originated the transmission knows the exact address of the ICU it is seeking, it proceeds to send a connect request packet directly to the address. The receiving ICU responds with a connection confirmation packet. At this time, a virtual connection, also called a link, has been established between the two serial resources.

All the necessary tables are immediately set up by the ICUs to handle flow control and duplicate packet detection. Flow control is the method that the ICU uses to match the sender's transmission rate with the receiver's ability to accept data. Duplicate packet detection assures data is neither lost nor duplicated. With these critical activities completed, the ICU tells the user that the link has been established by displaying a message on the user's terminal. If the ICU located the proper resource but found that it was already occupied and so not available for a link, a message indicating the resource is busy is displayed on the user's terminal.

The user who was informed that a link to a serial resource was completed, operates as though his or her terminal is connected directly to the remote device. If the user wishes to issue a new instruction to the ICU, he or she simply issues the proper link escape sequence. At this time, the link is suspended and the ICU prompt is once again displayed on the terminal, indicating that the ICU is available for the user's next command.

When you no longer have a need for a link, the first step toward disconnecting permanently is always to suspend the link by using the escape sequence (used to suspend a link and tell the ICU that you are no longer talking to the connected resource and that you wish to issue a new command). You can do all of these basic activities by using your terminal and typing simple commands that tell the ICU what action you would like to take.

Please write your response to unit self-test questions and then check the text answers at the end of the unit.

SELF-TEST QUESTIONS

252. Access methods used in LAN

1. What are the two classes of distributed access used in LANs? Define each. Random - any station can initiate TX Deterministic - each station must wait its turn

2. Which access method uses CSMA? Token passing?
Random & Deterministic

3. On a CSMA network, what would cause the probability of a collision to increase?
increase number of stations & length

4. What is the most important factor that affects the performance in token passing and slotted networks?
number of participating stations

253. Intelligent connector units

1. What is the purpose of the intelligent connector unit in LANs? interprets + monitors data on network

2. The intelligent connector unit is made up of what hardware? integrated CKTs, RF TXer, + RF RX'er.

3. What is used to identify each intelligent connector unit on a network during the communications process? SDLC address

ANSWERS TO SELF-TEST QUESTIONS

250

1. Media, protocol, topology, and media access.
2. Twisted pair wire, coaxial cable, and optical fiber.
3. Shielding and repeating.
4. Baseband and broadband.
5. Advantages: It is sturdy and secure. Disadvantages: High cost and difficulty of connection.

251

1. Linear bus, ring, and star.
2. Bus of tree topology.
3. A loop network has one master station that controls all transmissions.

252

1. Random and deterministic. Random—any station has the ability to initiate a transmission at any time. Deterministic—each station must wait its turn to transmit.
2. Random. Deterministic.
3. Increasing the number of stations on the network and physical length of the network.
4. The number of participating stations.

253

1. It interprets and monitors the data traffic on a network.
2. Integrated circuits, RF transmitter, and RF receiver.
3. SDLC address.

Do the Unit Review Exercises (URE) then complete ECI Form 34, Field Scoring Answer Sheet. ➡

UNIT REVIEW EXERCISES

Note to Student: Consider all choices carefully, select the *best* answer to each question, and *circle* the corresponding letter. When you have completed all unit review exercises, transfer your answers to ECI Form 34, Field Scoring Answer Sheet. **DO NOT RETURN YOUR ANSWER SHEET TO ECI.**

93. (250) Of the media types available for local area networks (LAN), which one is the least expensive and easiest to install for short distances?

    a. Twisted pair.
    b. Baseband cable.
    c. Broadband cable.
    d. Optical fiber.

94. (250) What is the principal advantage of using fiber optic cable on a local area network (LAN) system?

    a. Its cost effectiveness.
    b. Its sturdiness and security.
    c. Its life expectancy.
    d. Its ease of installation.

95. (251) What type of local area network (LAN) topology is being used when stations are arranged along a single length of cable so that it can be extended on at least one end?

    a. Ring.
    b. Star.
    c. Ring/star.
    d. Linear bus.

96. (251) What type of local area network (LAN) topology has a central node that connects each station by a single point-to-point link?

    a. Ring.
    b. Star.
    c. Ring/star.
    d. Linear bus.

97. (252) What access method do most LANs use?

    a. Central.
    b. Random.
    c. Distributed.
    d. Distributed random.

98. (252) Which of the following is a general class of the distributed access method?

    a. Central.
    b. Random.
    c. Distributed random.
    d. Carrier.

99. (252) What is the most widely used deterministic access method?

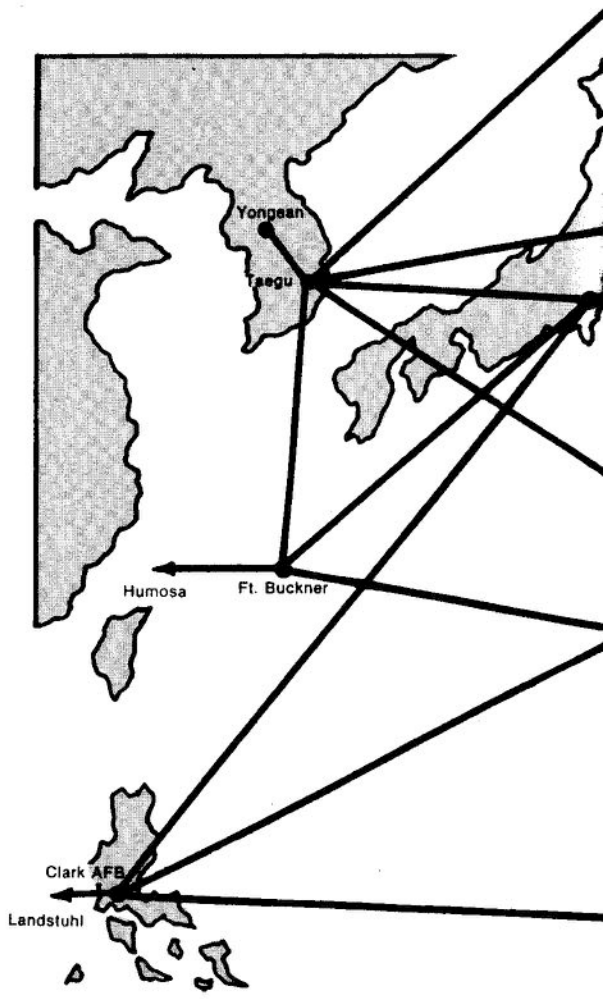
    a. Central.
    b. Token passing.
    c. Random.
    d. Carrier.

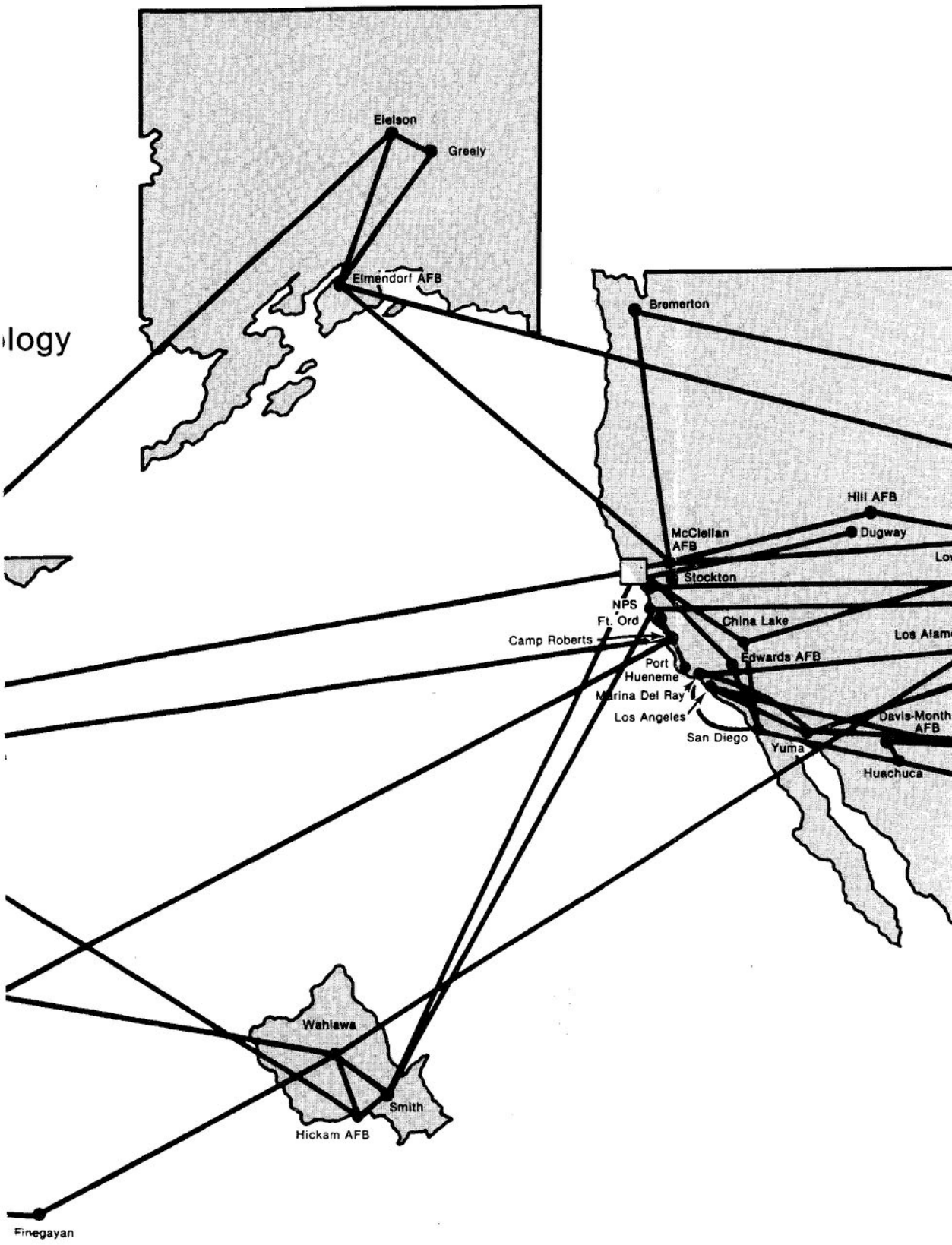
100. (253) What is the maximum number of ports a multiport ICU can have?

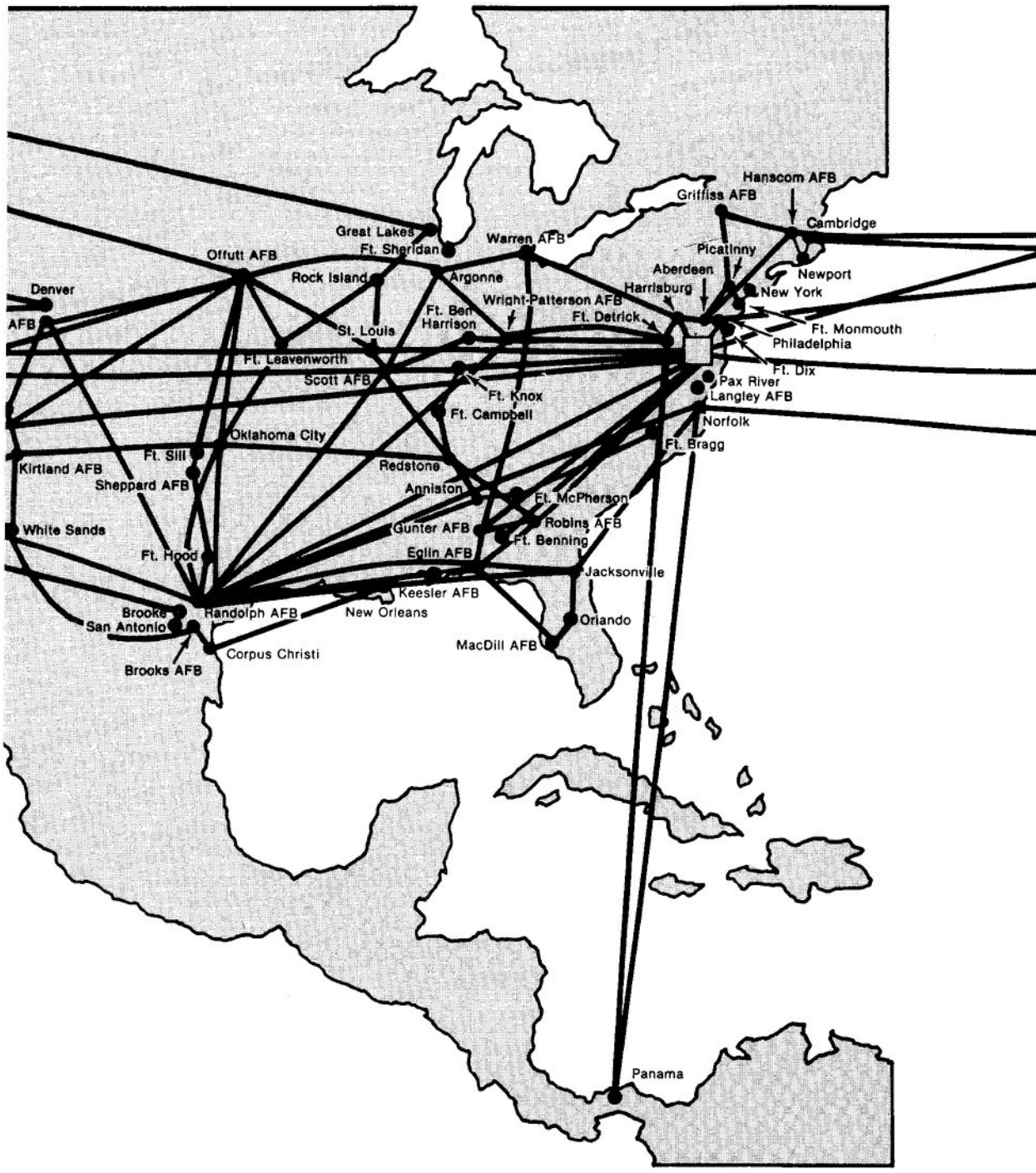
    a. 2.
    b. 4.
    c. 24.
    d. 32.

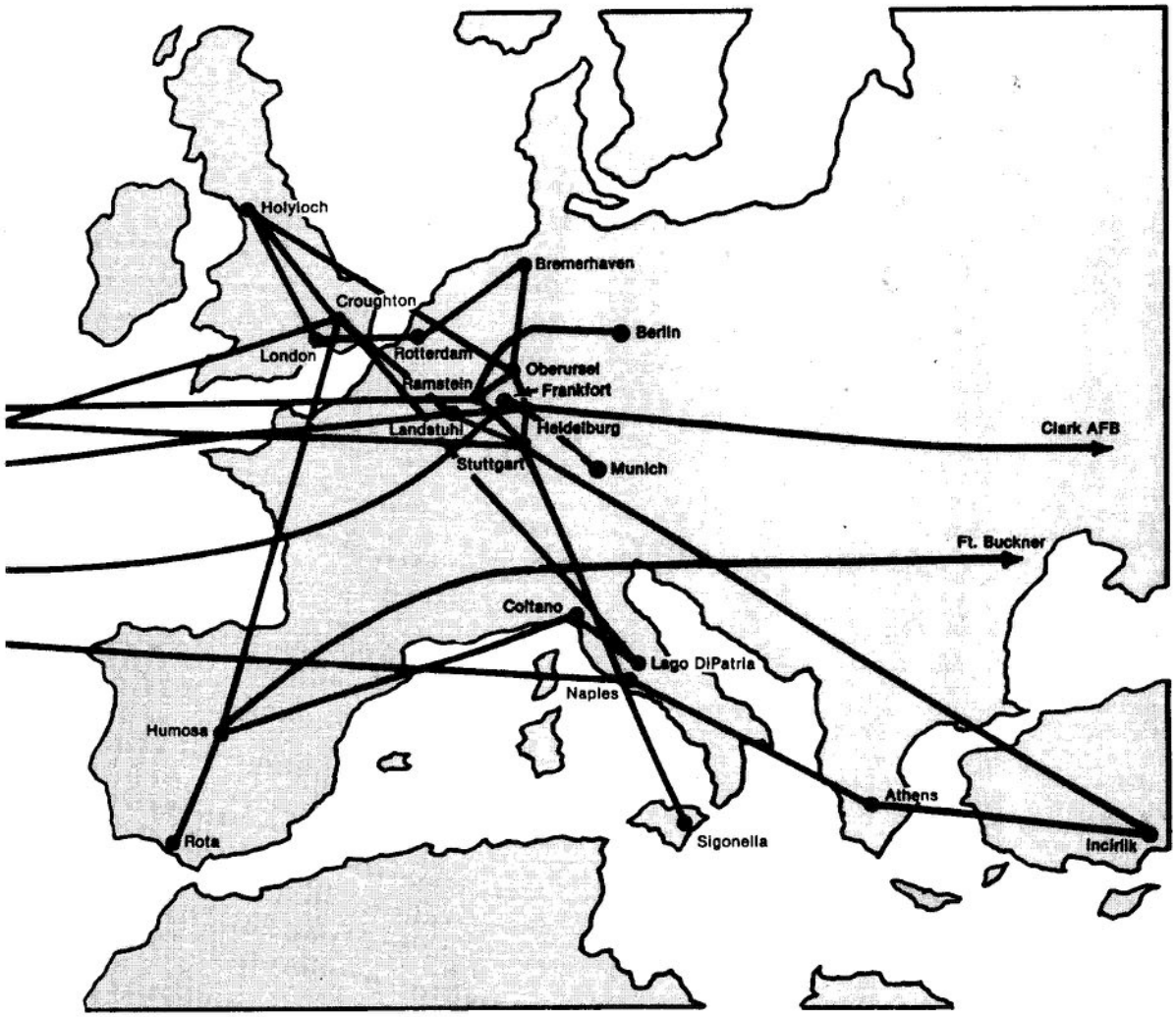
STUDENT WORK SPACE

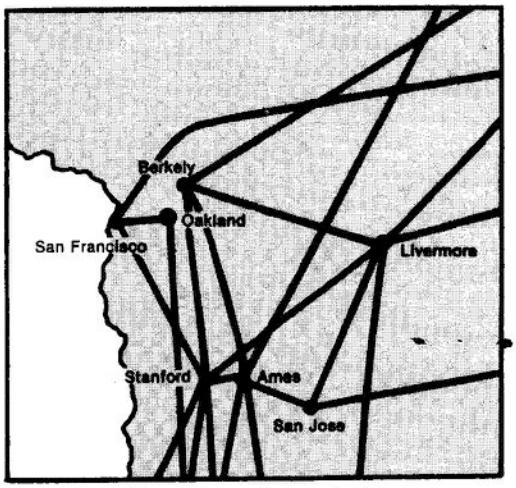
MILNET World To



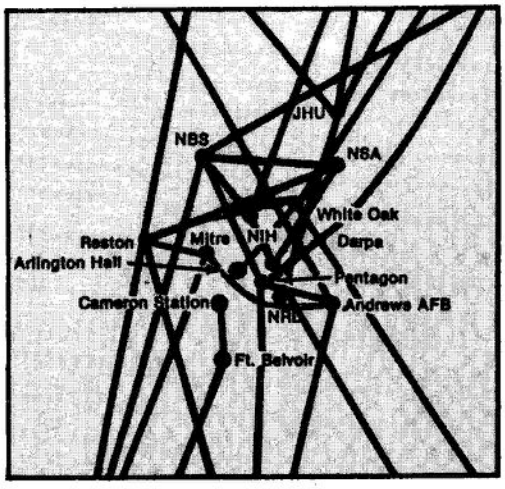

Eielson
Greely
Elmendorf AFB
Bremerton
Hill AFB
Dugway
McClellan AFB
Stockton
NPS
Ft. Ord
Camp Roberts
China Lake
Edwards AFB
Port Hueneme
Marina Del Ray
Los Angeles
San Diego
Yuma
Huachuca
Davis-Monthan AFB
Wahiawa
Smith
Hickam AFB
Finegayan


Hanscom AFB
Griffiss AFB
Cambridge
Great Lakes
Ft. Sheridan
Warren AFB
Offutt AFB
Picatinny
Aberdeen
Newport
Rock Island
Argonne
Harrisburg
New York
Denver
Wright-Patterson AFB
Ft. Ben Harrison
Ft. Detrick
AFB
St. Louis
Ft. Monmouth
Philadelphia
Ft. Leavenworth
Ft. Dix
Scott AFB
Pax River
Ft. Knox
Langley AFB
Ft. Campbell
Norfolk
Oklahoma City
Ft. Bragg
Ft. Sill
Kirtland AFB
Redstone
Sheppard AFB
Anniston
Ft. McPherson
White Sands
Gunter AFB
Robins AFB
Ft. Benning
Ft. Hood
Eglin AFB
Jacksonville
Keesler AFB
Brooke
Randolph AFB
New Orleans
Orlando
San Antonio
MacDill AFB
Corpus Christi
Brooks AFB
Panama





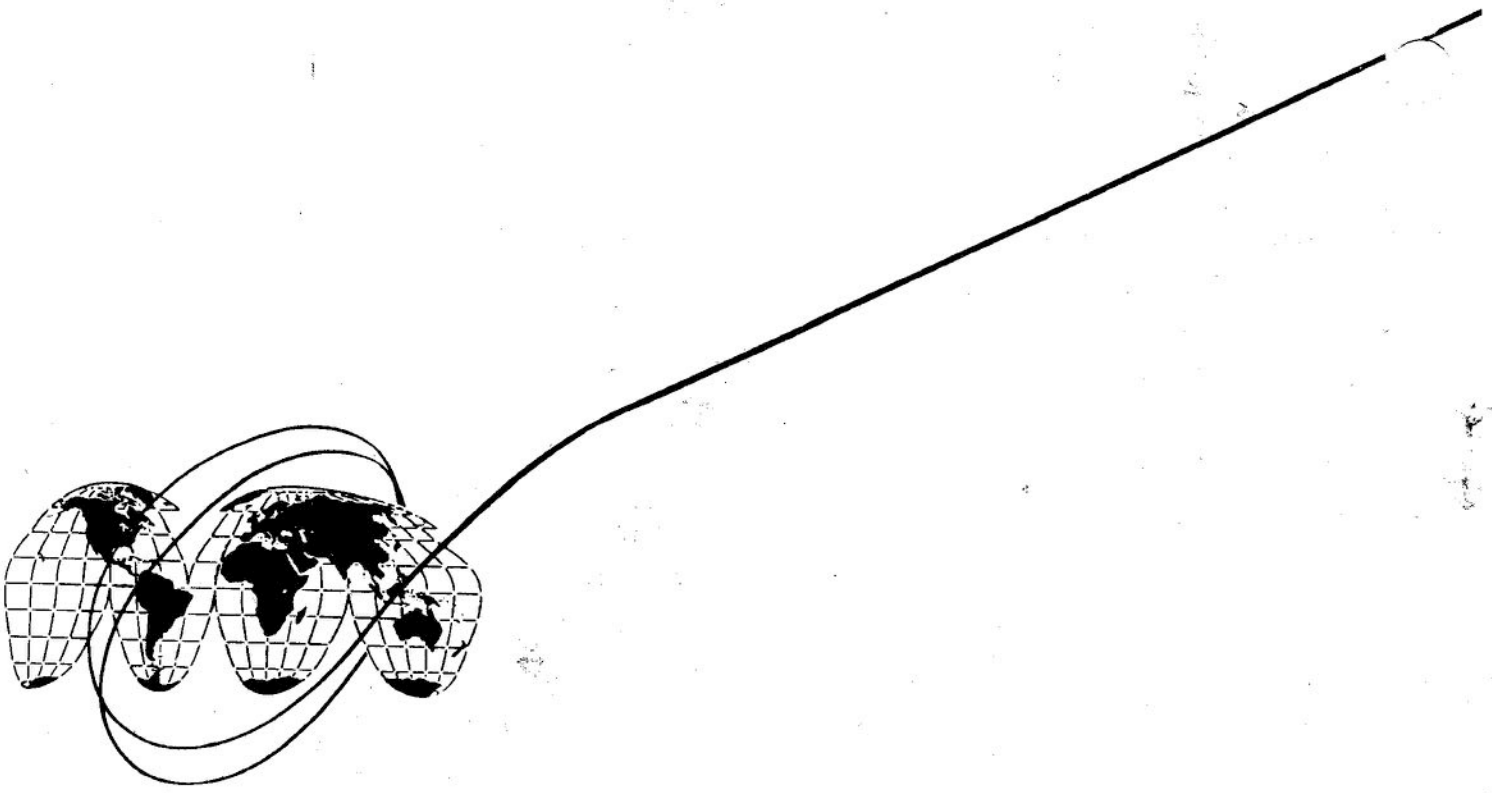
San Francisco Area



Washington Area

Foldout 1
MILNET World Topology

TG-249



AFSC 3C251
49350B 02 9111
EDIT CODE 02

95F 0554