
DISN Data Services Course

Revised December 1999

Prepared For:

DEFENSE INFORMATION SYSTEMS AGENCY

Deputy Director of Operations
DISN Operations
DISN Transmission Services
DISN Networks (D3124)
Reston, Virginia 22090

Prepared By:

**Science Applications
International Corporation
(SAIC)**
7990 Boeing Court
Vienna, Virginia 22183

TABLE OF CONTENTS

SESSION 1 - DISN OVERVIEW

DISN Overview.....	1-1
DISN Services.....	1-2
DISA Mission.....	1-3
Customer Access to DISA Network Services	1-4
DISN Data Services and the DISN WAN	1-5
DISA Network Services.....	1-6
DISN Data Services Networks	1-7
DDN to DISN Network Transitions	1-8
Benefits of DISN Backbone Network	1-9
Benefits of DISN IP Router Networks	1-10
Evolution of Data Services	1-11
DISN Networking.....	1-12
Communications in DISN Data Services Networks	1-13
General Uses of DoD Networks.....	1-14
Reachable Networks from DISN.....	1-15
NIPRNET Network Components.....	1-16
The Internet.....	1-17
NIPRNET Connectivity to the Internet.....	1-18

SESSION 2 - DISN NETWORKING

DISN Networking.....	2-1
DISN Physical Components.....	2-2
NIPRNET	2-3
SIPRNET.....	2-4
Physical Media	2-5
LANs in DISN Data Services Networks.....	2-6
DISA and Premises Router Hierarchy.....	2-7
Local Area Network Components	2-8
Common Types of LANs.....	2-9
Host Components	2-10
Repeaters and Bridges	2-11
Routers.....	2-12
“Gateway” Routers	2-13
Army Circuit Bundling Initiative.....	2-14
Co-located Customer Premises Routers	2-15
Open Systems Interconnection (OSI) Reference Model.....	2-16
Bridge, Router, and Gateway Capabilities	2-17
Integrated Tactical-Strategic Data Network (ITSDN).....	2-18
Standard Tactical Entry Point (STEP) Site.....	2-19
Standard Tactical Entry Point (STEP) Locations	2-20
Defense Messaging System	2-21
X.400 and X.500 Recommendations	2-22

Table of Contents	1
-------------------------	---

TABLE OF CONTENTS

SESSION 2 - DISN NETWORKING (CONTINUED)

DMS Components.....	2-23
FORTEZZA Card	2-24

SESSION 3 - DISN WAN

DISN WAN	3-1
Wide Area Networks	3-2
WANs in DISN Data Services Networks	3-3
DISA Wide Area Network Carriers.....	3-4
DISN Wide Area Network	3-5
DISN WAN Redundant Paths	3-6
IDNX Multiplexer	3-7
Subchannel Management	3-8
DISN Backbone Virtual Routing	3-9
Data/Voice Integration.....	3-10
DISN Backbone Evolution.....	3-11
Original NIPRNET Infrastructure.....	3-12
Regionalized DISA Routers.....	3-13
NIPRNET Core Routers	3-14
Reorganized CONUS NIPRNET	3-15
Joint Interconnection Service (JIS)	3-16
NIPRNET Loading.....	3-17
NIPRNET Re-design	3-18
Regional Architecture	3-19
NIPRNET Re-design Benefits	3-20
ATM Backbone.....	3-21
Classified ATM Network.....	3-22
ATM Switch Connections	3-23
DISN Backbone Traffic Load	3-24

SESSION 4 - PROTOCOLS AND ARCHITECTURES

Protocols and Architectures	4-1
DISN Protocol TCP/IP Architecture.....	4-2
Natural Layering of Network Functions	4-3
Data Flow	4-4
Primary Layers of the Protocol Architecture.....	4-5
Standard Applications	4-6
Telnet	4-7
File Transfer Protocol (FTP)	4-8
Simple Mail Transfer Protocol (SMTP)	4-9
SMTP and POP3 Protocols.....	4-10
HyperText Transfer Protocol (HTTP)	4-11
Transmission Control Protocol (TCP)	4-12

Table of Contents	2
-------------------------	---

TABLE OF CONTENTS

SESSION 4 - PROTOCOLS & ARCHITECTURES (CONTINUED)

TCP Header Format.....	4-13
Three-Way Handshake.....	4-14
Internet Protocol (IP).....	4-15
Internet Control Message Protocol (ICMP).....	4-16
IP Datagram Header Format.....	4-17
IP Addressing.....	4-18
Class A IP Addresses.....	4-19
Class B IP Addresses.....	4-20
Class C IP Addresses.....	4-21
DISA Network Addresses.....	4-22
IP Address Resolution.....	4-23
Domain Name Service (DNS).....	4-24
DNS Name Resolution.....	4-25
Tiered DNS.....	4-26
Domain Naming Hierarchy.....	4-27
Address Resolution Protocol (ARP).....	4-28
Network-Level Protocols.....	4-29
DISN Internet Packet Format.....	4-30

SESSION 5 - INTEGRATING ATM

Integrating ATM.....	5-1
Circuit Switching.....	5-2
Packet Switching.....	5-3
Packet Switching Networks - X.25.....	5-4
Packet Switching Networks - IP Routers.....	5-5
Packet Switching Networks - Frame Relay.....	5-6
Cell Switching Networks - ATM.....	5-7
ATM Network.....	5-8
IP and ATM Routing.....	5-9
IP and ATM Interfaces.....	5-10
ATM Virtual Circuits.....	5-11
Service Delivery Node (SDN) Components.....	5-12
Bandwidth Manager.....	5-13
SDN Consolidation.....	5-14
DISN ATM Evolution.....	5-15
High-Bandwidth Services.....	5-16
Native ATM Interface.....	5-17
ATM ELANs.....	5-18
NIPRNET ELANs.....	5-19
DISN Global ATM Connectivity.....	5-20

Table of Contents.....	3
------------------------	---

TABLE OF CONTENTS

SESSION 6 - SUPPORT

Support.....	6-1
Subscriber Support	6-2
Resolving Network Problems	6-3
RNOSC Network Management System	6-4
Problem Reporting Steps.....	6-5
DISA Communications Servers	6-6
SIPRNET Dial-Up Access.....	6-7
Dial-In Access to RAS.....	6-8
Connecting to Comm Server.....	6-9
E-mail Assistance.....	6-10
NIPRNET and SIPRNET Registration.....	6-11
NIC Help Desk	6-12
SIPRNET Support Center	6-13
DoD Web Pages	6-14

SESSION 7 - ROUTING AND CONTROL

Routing and Control	7-1
Router Functions.....	7-2
Router Configuration Responsibilities	7-3
Cisco Router Types.....	7-4
Router and ATM Throughput Comparison.....	7-5
Router Addresses	7-6
Router IP Address Assignments	7-7
Routing Configuration	7-8
IP Address Evaluation by Router	7-9
Routing Table Views	7-10
Routing Table Updates	7-11
Routing Hierarchy.....	7-12
Default Gateway.....	7-13
Mixing Different Routers.....	7-14
Gateway Protocols	7-15
NIPRNET - SIPRNET Separation	7-16
Autonomous Systems	7-17
Routing Arbiter	7-18
CIDR Address Allocation.....	7-19
CIDR Routing Table Consolidation	7-20

SESSION 8 - NETWORK SECURITY

Network Security	8-1
------------------------	-----

Table of Contents	4
-------------------------	---

TABLE OF CONTENTS

Confidentiality vs. Availability	8-2
Countering the Threat	8-3
Security Responsibilities	8-4
DISA Security Programs	8-5
ASSIST Program.....	8-6
Compliance Assessment (VAAP)	8-7
Compliance Assessment or ASSIST Requests	8-8
Computer Emergency Response Team (CERT)	8-9
Comm Server Access Control System (NIPRNET)	8-10
Comm Server Access Control System (SIPRNET)	8-11
Comm Server Card Usage Monitoring.....	8-12
Host User Accounts and Passwords.....	8-13
New Security Measures	8-14
DoD Internet Connection Policy	8-15
SIPRNET Accreditation Process.....	8-16
Data Security.....	8-17
Single Level Security.....	8-18
Link vs. Host-to-Host Encryption.....	8-19
Network Encryption	8-20
Types of KG Encryption Devices	8-21
FASTLANE Encryption.....	8-22
Firewalls	8-23
Firewall Functions	8-24
Firewall Positioning	8-25
Firewall Components	8-26
Firewall Rulesets.....	8-27
Firewall Configuration	8-28
Intrusion Detection Systems (IDS).....	8-29
Air Force CITS Site	8-30
Additional Security Measures.....	8-31

SESSION 9 - ON-SITE RESPONSIBILITIES

On-Site Responsibilities	9-1
NIPRNET Router Node	9-2
SIPRNET Router Node	9-3
DISA Node Rack.....	9-4
Node Site Coordinator Responsibilities.....	9-5
Node Site Coordinator Responsibilities: Node Site POC	9-6
Node Site Coordinator Responsibilities: Installation & Maintenance Liaison	9-7
Node Site Coordinator Responsibilities: Node Site Access Control.....	9-8
Node Site Coordinator Responsibilities: Assist RNOSC	9-9
Node Site Coordinators' Conference	9-10

Table of Contents	5
-------------------------	---

TABLE OF CONTENTS

SESSION 10 - SUBSCRIBER INTEGRATION

Subscriber Integration	10-1
Subscriber Integration Responsibilities	10-2
DISA Subscriber Integration Process.....	10-3
DISA Network Services Provisioning Policy.....	10-4
DISA Network Management Systems.....	10-5
Network Monitoring	10-6
Areas of Responsibility.....	10-7
DDN Billing	10-8
DISN Billing	10-9
FY 00 DISN Data Services Network Charges.....	10-10
FY 00 DISN Data Services Network Charges.....	10-11
Organization Comm Server Cards.....	10-12

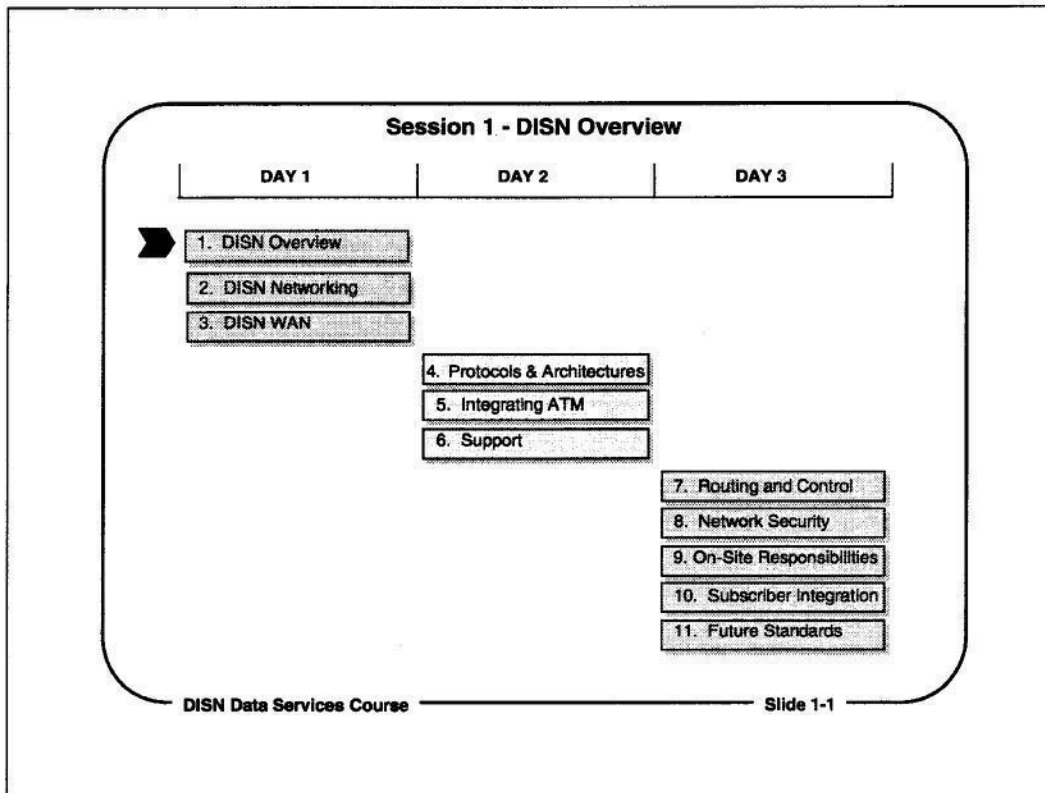
SESSION 11 - FUTURE STANDARDS

Future Standards	11-1
The Role of Standards	11-2
The World of Standards	11-3
U.S. DoD Input into International Standards.....	11-4
Open Systems Interconnection (OSI) Reference Model.....	11-5
DISN Services.....	11-6

APPENDICES

MAPS

NIPRNET - CONUS	
NIPRNET - Europe	
NIPRNET – Pacific	
NIPRNET – Southwest Asia	
SIPRNET – CONUS	
SIPRNET - Europe	
SIPRNET – Pacific	
SIPRNET – Southwest Asia	
DISN CONUS	
ATM Europe	
DISN Pacific	
Joint Interconnection Service (JIS)	

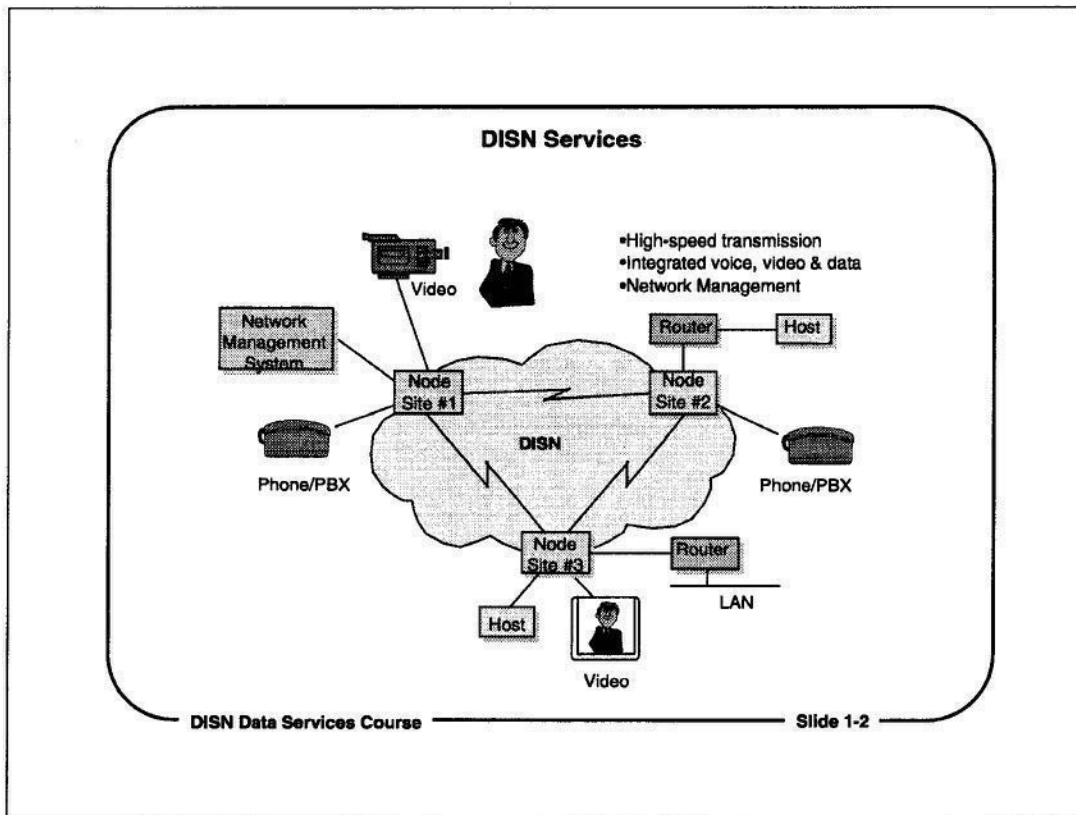


Session 1 - DISN Overview

Upon completion of this module, the students will be able to describe the evolution of the Defense Information Services Network (DISN), the components of the DISN Data Services networks, and the functions of the DISN network components.

This session will focus on:

1. Describing the components and objectives of the DISN Data Services networks
2. Specifying the benefits of the services provided on the DISN Data Services networks
3. Distinguishing between the DISN backbone and the DISN Data Services networks
4. Describing the other networks that interconnect with the DISN Data Services networks
5. Identifying the Internet services accessible from the DISN Data Services networks




DISN Services

The DISN Data Services networks are digital communications networks that the Defense Information Systems Agency (DISA) sponsors and maintains. The goal of DISA in operating the DISN Data Services networks is to:

- Provide reliable high-quality data communications services for DoD subscribers
- Create a high-speed backbone transmission network that will support a number of applications
- Integrate communications for a variety of applications, including data, voice, and video, over a single backbone network
- Manage the backbone network and the data services carried on the network for an economical, efficient operation.

The DISN backbone will support data traffic primarily. Eventually, both voice and video services will be carried on the network.

DISA Mission



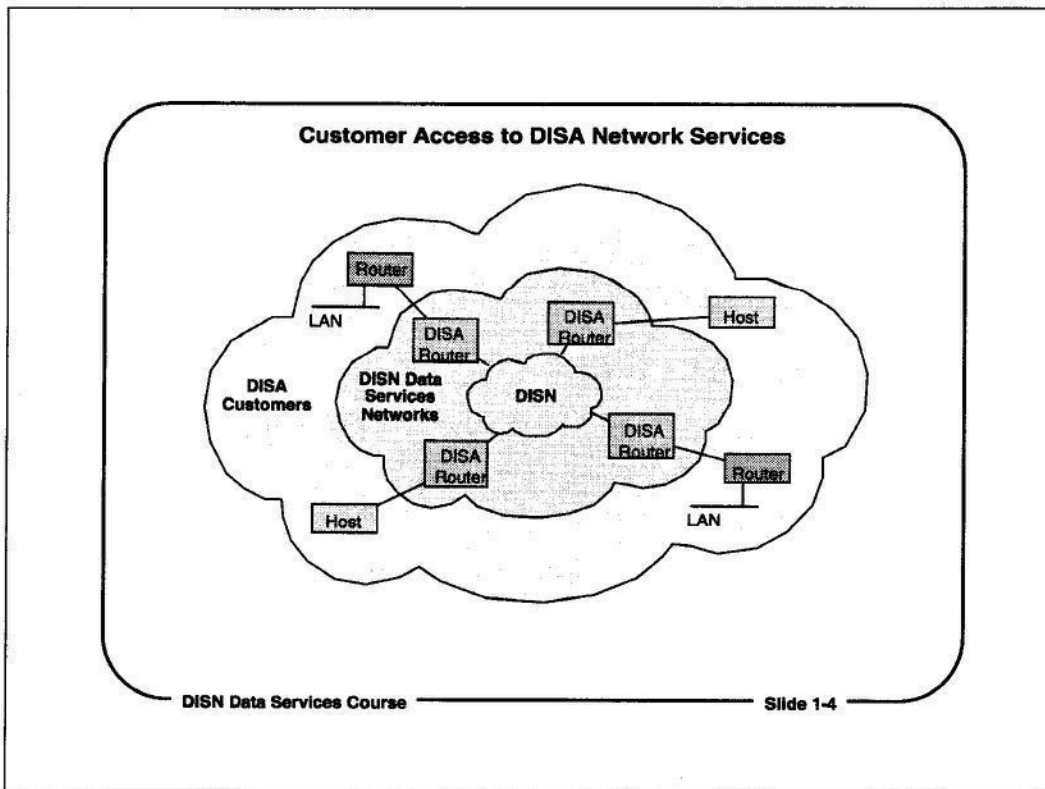
Provide communications to support and sustain the Warfighter

DISN Data Services Course Slide 1-3

DISA Mission

By building the DISN Data Services networks, DISA is carrying out its mission, which is to support the Warfighter. DISA's additional responsibilities include:

- Plan, manage, and engineer the Defense Information Infrastructure (DII)
- Provide automated data processing (ADP) and technical support to OJCS (Office of the Joint Chiefs of Staff) and OSD (Office of the Secretary of Defense)
- Provide systems engineering support for the National Military Command System and the Strategic Forces
- Provide engineering and technical support for the Global Command and Control System (GCCS)
- Provide systems architecture for current and future MILSATCOM
- Provide leased communications for DoD and other government agencies
- Ensure interoperability of tactical command, control, and communications (C3) systems.

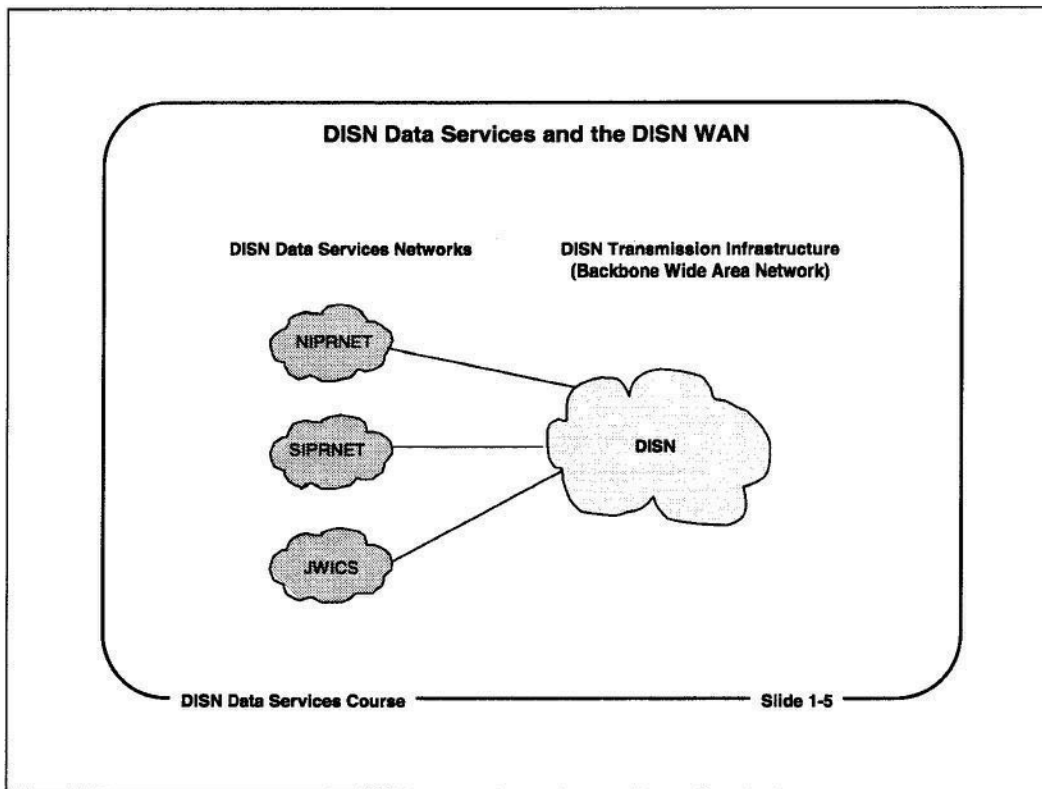


Customer Access to DISA Network Services

DISA provides long-haul transmission services for DoD customers' data applications. It is the designated, primary supplier of long-haul transmission services for DoD users.

DISA also provides IP router networks, referred to as the DISN Data Services networks, to give DoD customers access points into DISA's long-haul transmission network.

DISA's data customers access the long-haul network through DISA's access networks, which are the DISN Data Services networks.



DISN Data Services and the DISN WAN

The Defense Information Systems Network (DISN) is the backbone transmission network. The networks that use the DISN for long-haul, wide area transmission are Internet protocol (IP) router networks.

The IP router networks that DISA maintains are referred to as the DISN Data Services networks. The IP router networks provide data services that are carried over the DISN backbone network.

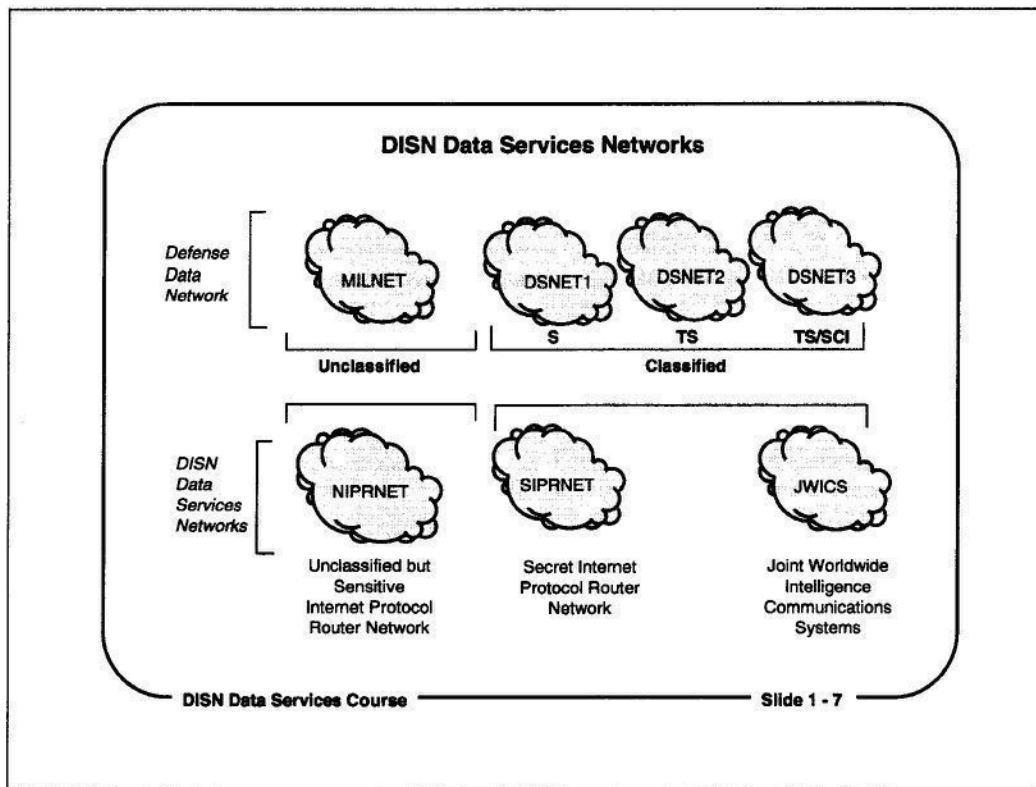
DISA Network Services		
User Requirement	DISA Service	Network Transport
Data	<ul style="list-style-type: none"> • NIPRNET • SIPRNET • JWICS 	<ul style="list-style-type: none"> • ATM • Frame relay
Voice	<ul style="list-style-type: none"> • DSN 	<ul style="list-style-type: none"> • IDNX
Video	<ul style="list-style-type: none"> • DVS-G • Special arrangement 	<ul style="list-style-type: none"> • Point-to-point • Dial-up
Messaging	<ul style="list-style-type: none"> • DMS 	<ul style="list-style-type: none"> • Commercial services

DISN Data Services Course Slide 1-6

DISA Network Services

DISA can provide a number of network services to its customers, in order to meet a wide variety of customer applications and needs. For example, DISA customers who have applications that require data transmission, such as host access, file transfer, and Web server access, can be served by the NIPRNET or SIPRNET. The choice depends on the customer's security requirements and the customer's applications.

In order to provide the service the customer needs on the NIPRNET or SIPRNET, DISA may elect to route the customer's traffic over a variety of network transport methods. These may include point-to-point leased lines, ATM, IDNX links, or commercial services.

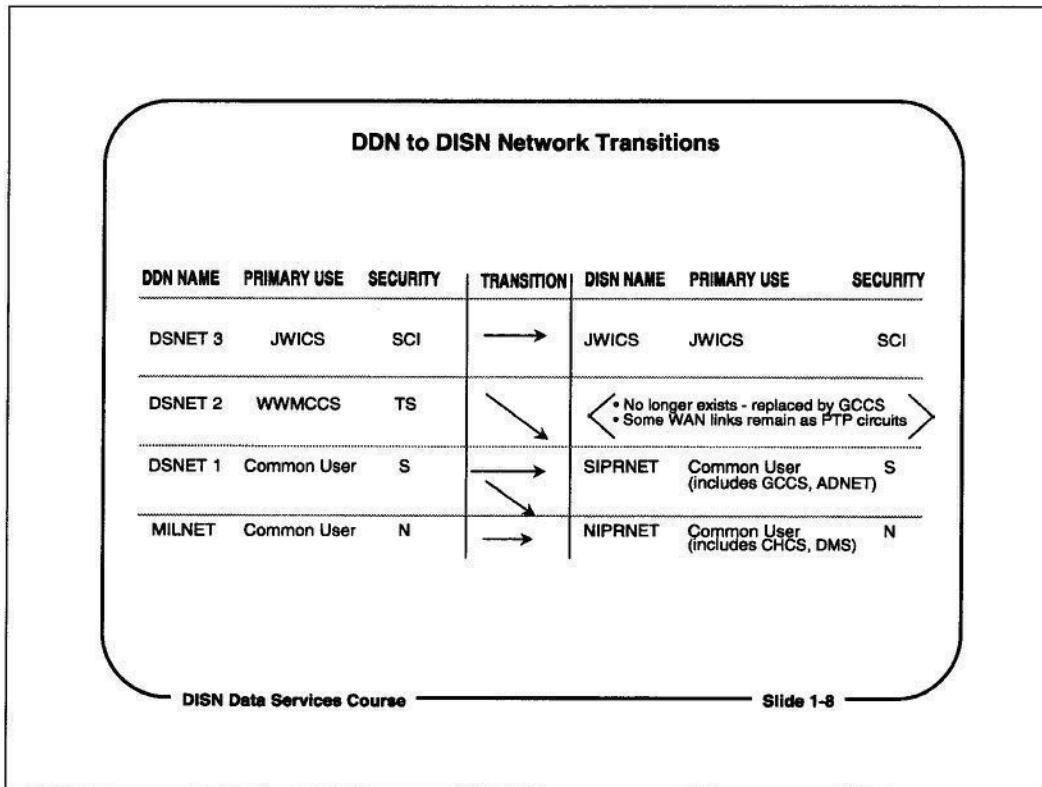


DISN Data Services Networks

The four separate networks that comprised the old Defense Data Network (DDN) were transitioned to three DISN Data Services networks. In most cases, the internal structure and operation of the old and new networks have been transparent to DISN Data Services network customers.

The three networks in the DISN Data Services networks are:

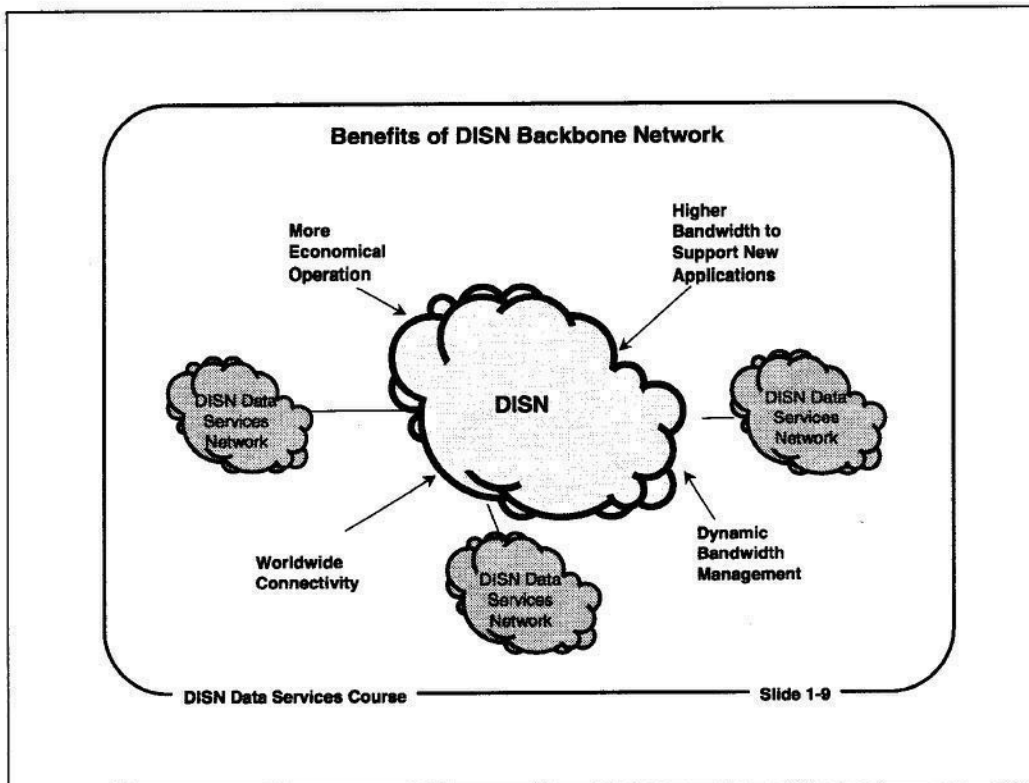
- The Unclassified but Sensitive Internet Protocol Router Network (NIPRNET)
- The Secret Internet Protocol Router Network (SIPRNET)
- The Joint Worldwide Intelligence Communications System (JWICS)



DDN to DISN Network Transitions

The four DDN networks, each of which had its own backbone network, were collapsed into three IP router networks in the DISN Data Services network structure. The older DDN networks were transitioned to the following DISN Data Services networks:

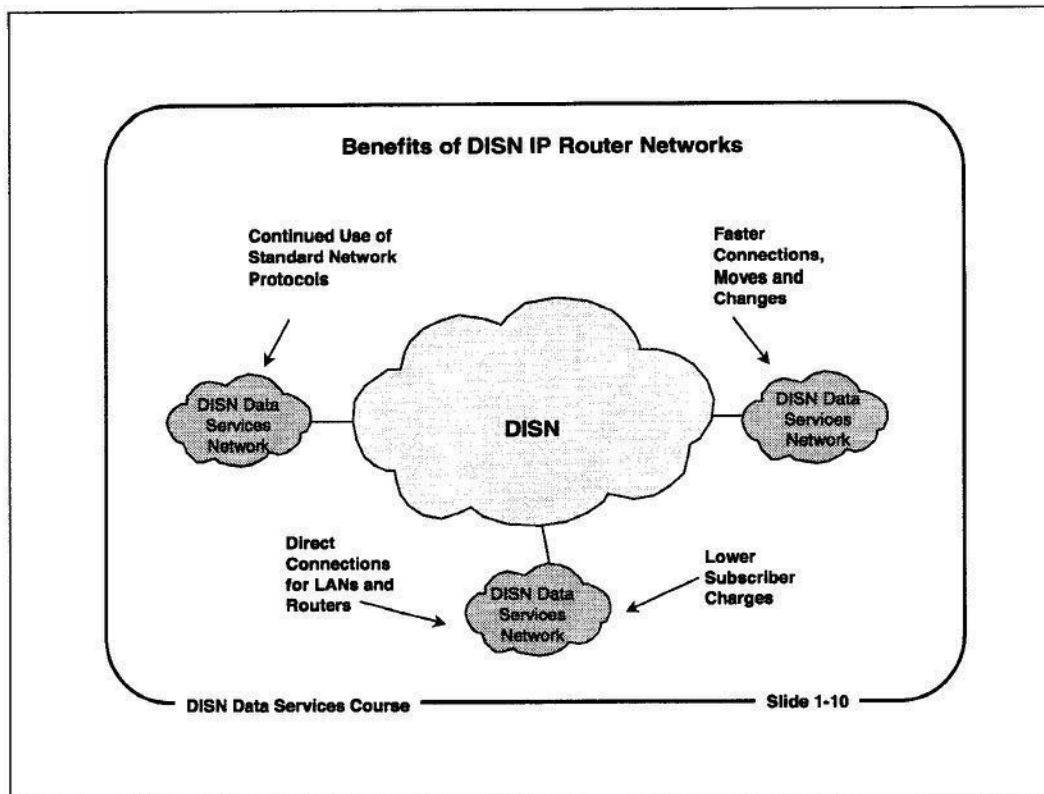
- Except for becoming a router network, DSNET3 was virtually unchanged. It still has a Top Secret/SCI security classification.
- DSNET2 ceased to exist after WWMCCS was replaced by the Global Command and Control System (GCCS). GCCS runs on the secret IP router network, SIPRNET.
- Most DSNET1 users were migrated to SIPRNET.
- Unclassified traffic on the old MILNET was moved to the unclassified IP router network, NIPRNET.



Benefits of DISN Backbone Network

The benefits of the DISN backbone transmission infrastructure are:

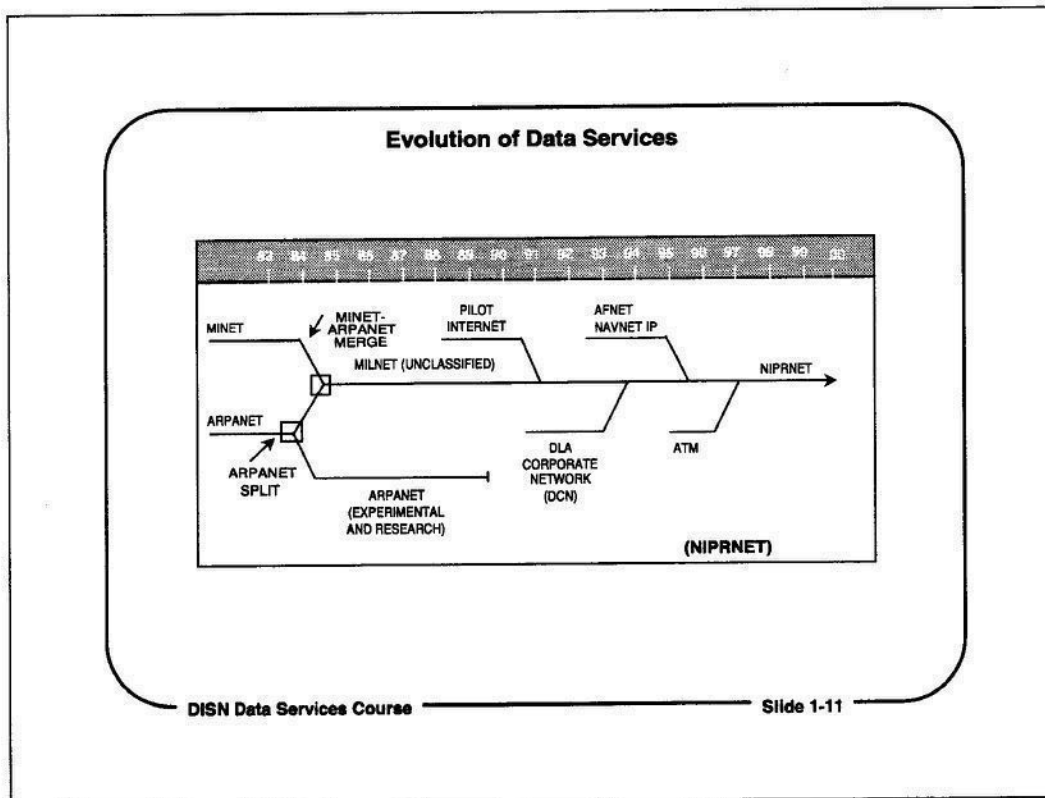
- **More economical operation** - The network is more economical for DISA to operate, because the backbone will be composed of high-speed, high-capacity shared trunks, instead of lower-bandwidth circuits assigned to specific networks.
- **Higher bandwidth** - The bandwidth of the network backbone is in the multi-megabit, rather than the kilobit range, which will provide faster transmission and more network capacity for new users and new applications.
- **Dynamic bandwidth management** - The bandwidth on the DISN backbone can be managed closely, so that demands for bandwidth on the backbone can be adjusted dynamically.
- **Worldwide connectivity** - The DISN backbone connects DoD systems around the world. It also connects DoD systems to the Internet.



Benefits of DISN IP Router Networks

The benefits of the DISN IP router networks are:

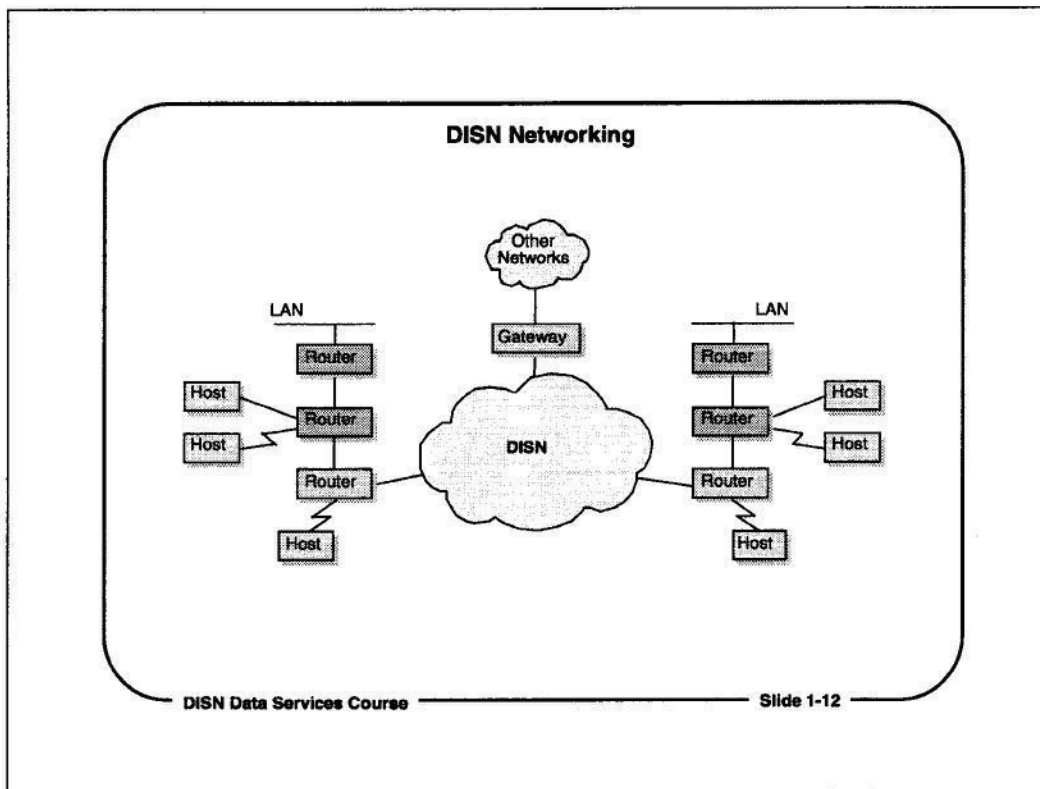
- Lower user connection charges - Average costs for user connections to the DISN are lower than they were under the old DDN rate structure.
- Faster connections, moves, and changes - Connections to DISN will be controlled more closely by local users, so new hosts and networks can be added and moved faster and more easily.
- Direct connections for LANs and routers - Customer connections to the DISN Data Services networks from customer LANs and routers interface directly to IP routers.
- Continued use of standard protocols - The IP router networks use the standard TCP/IP protocols, eliminating problems with re-training users and revising host and application software.



Evolution of Data Services

The DISN Data Services networks have evolved from several older networks. Some milestone events in the evolution of the DISN Data Services networks are:

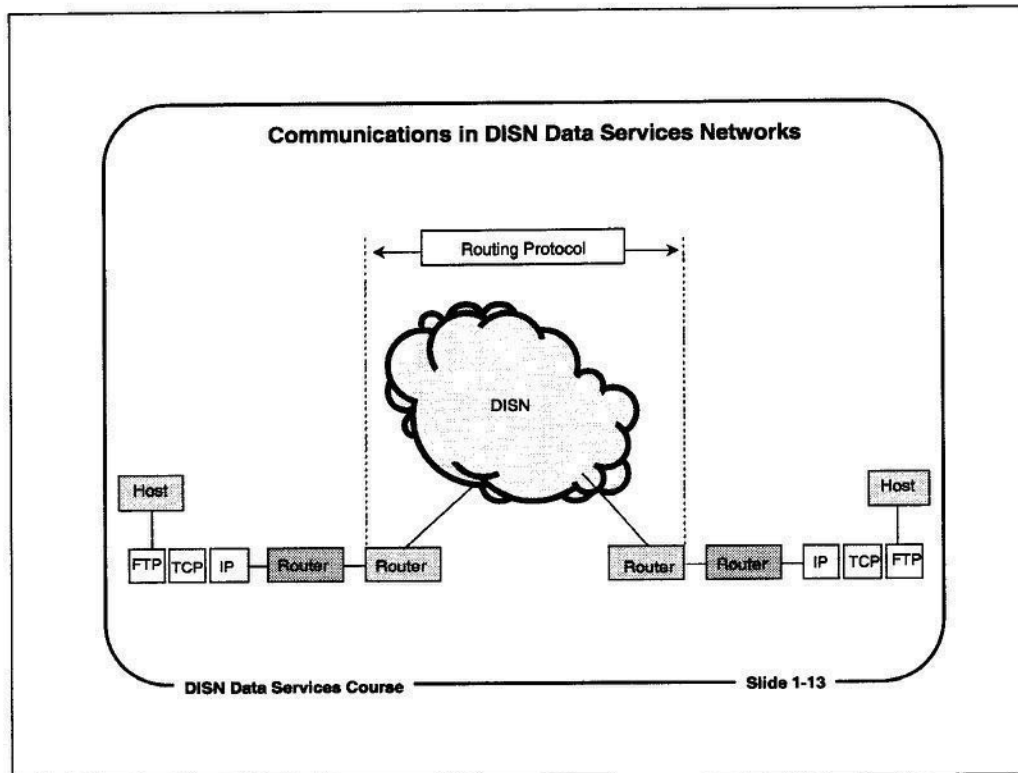
- 1983** ARPANET split into military and non-military parts; the existing DoD network, MINET, is merged into a new military communications network, the Defense Data Network (DDN).
- 1990** ARPANET discontinued, and its traffic moved to other networks.
- 1991** DISN Pilot Internet project started.
- 1992** Near-term transition to experimental IP router network begun.
- 1993** Transition of DDN to IP routers and DISN Data Services networks started
- 1996** DDN transition to DISN Data Services networks completed.
- 1997** Transition to ATM services begins. (NIPRNET)
- 1998** Integrate classified ATM (SIPRNET) into the unclassified infrastructure.
- 2000** Expand the ATM infrastructure worldwide.



DISN Networking

When the migration to the DISN Data Services networks was completed, all systems were moved to one of the DISN Data Services networks behind DISA IP routers. In addition, traffic from all of the DISN Data Services networks was moved to the DISN backbone.

Today, most customer networks are workstations and servers on LANs that are connected to the DISA router nodes..



Communications in DISN Data Services Networks

Some of the characteristics of the DISN software architecture are:

- Routers use the IP protocol to route IP datagrams
- Routers use a proprietary Cisco routing protocol to exchange routing information; eventually, this will be replaced by an OSI router-to-router protocol
- Hosts use TCP/IP protocols, as well as the FTP, Telnet, HTTP, and SMTP protocols at the applications level
- Routers use special routing update protocols to pass network routing information to and from other routers.

General Uses of DoD Networks					
	E-Mail	Format Messaging	Data	Voice	Video
AUTODIN		X			
DSN				X	
DCTN				X	X
DISN Data Services	X	X*	X		X**
DISN/ATM	X	X	X	X	X
DVS-G					X

* With DMS ** Unique User Application

DISN Data Services Course Slide 1-14

General Uses of DoD Networks

The DISN Data Services networks are only a few of the networks supported by DISA. Some of the other networks DISA runs include:

AUTODIN - Store-and-forward switching system for transmitting messages.

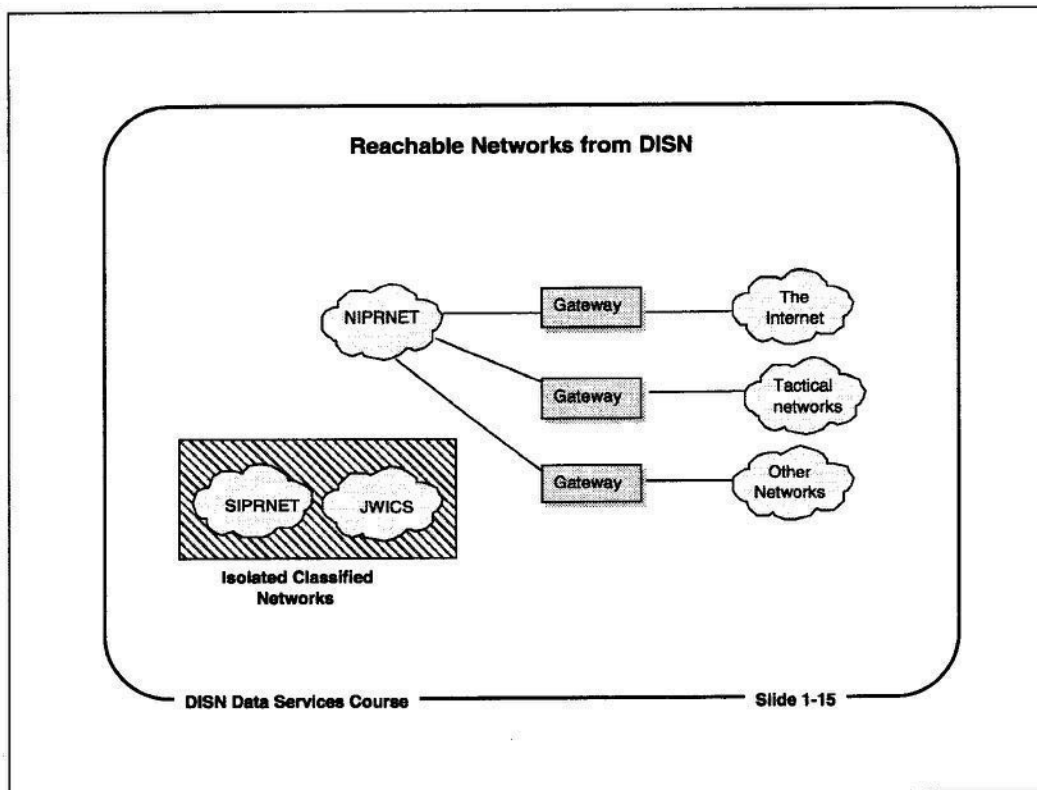
DISN Data Services networks - Managed bandwidth data networks, for classified and unclassified data applications.

DSN (Defense Switched Network) - Unclassified and classified voice networks.

DCTN - High-bandwidth digital network capable of supporting digital video and voice traffic; on-demand access with pay-by-use pricing and volume discounts.

DMS (Defense Message System) - Upgrade to AUTODIN; integrates secure messaging and unclassified e-mail systems in a single system, along with file encryption and authentication.

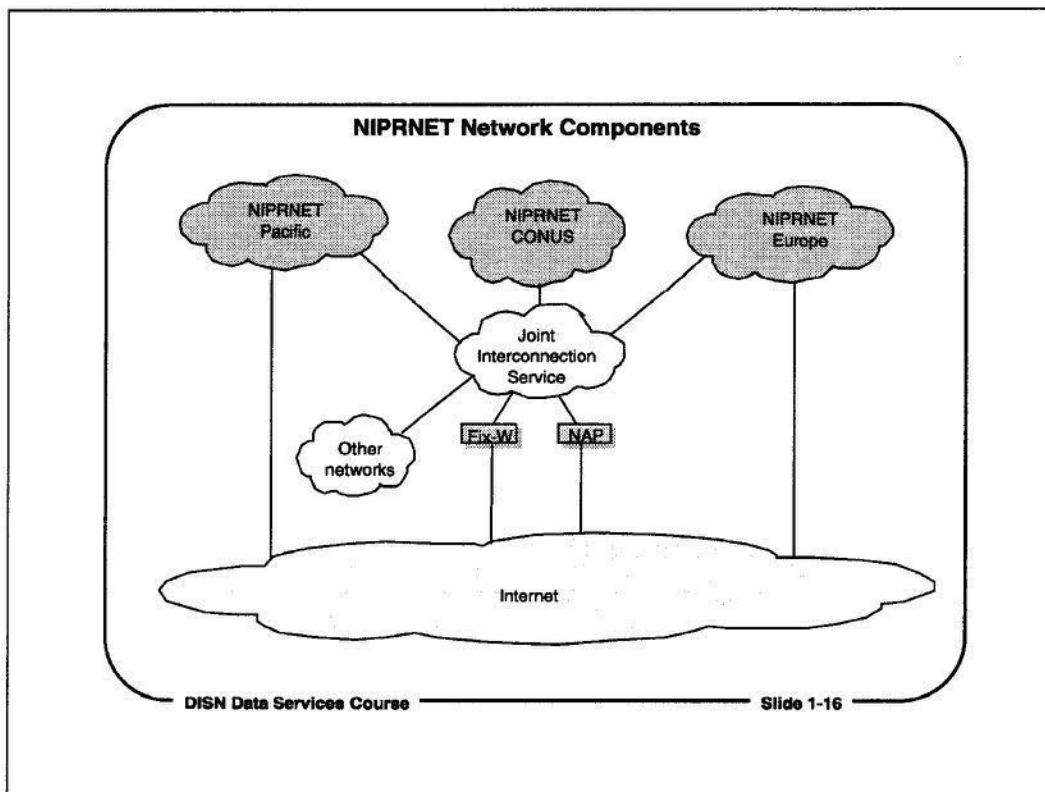
DVS-G (DISA Video Services-Global) - Provides worldwide videoconferencing and video transmission services



Reachable Networks from DISN

Other networks can be reached from devices on the DISN Data Services networks if there are physical connections between the two networks, and if the other networks are "known" to DISN gateways.

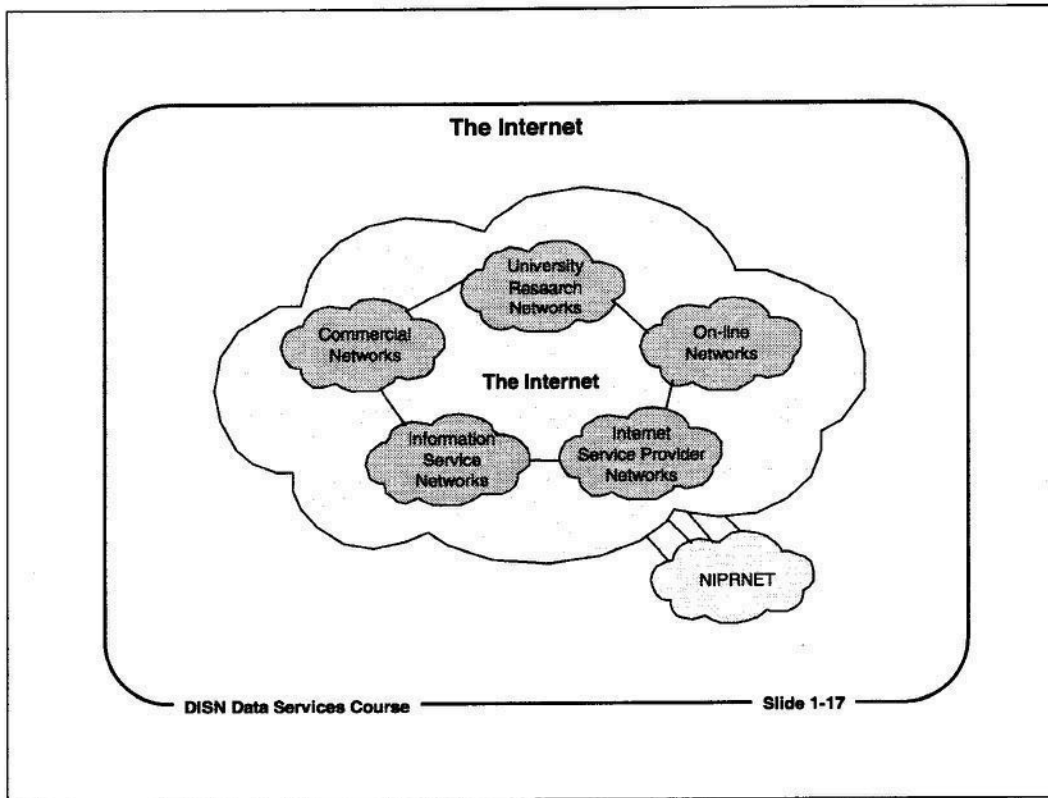
The networks in the Internet are reachable from the DISN Data Services networks. Gateways on the NIPRNET connect into the Internet. Internet hosts can be reached from the DISN Data Services networks because NIPRNET hosts and Internet hosts use the same protocols (TCP/IP), and because there is a physical connection between the two networks.



NIPRNET Network Components

The unclassified DISN Data Services network, NIPRNET, is composed of several networks that have been joined together to create a worldwide unclassified common user network for DoD users. The components of the NIPRNET are:

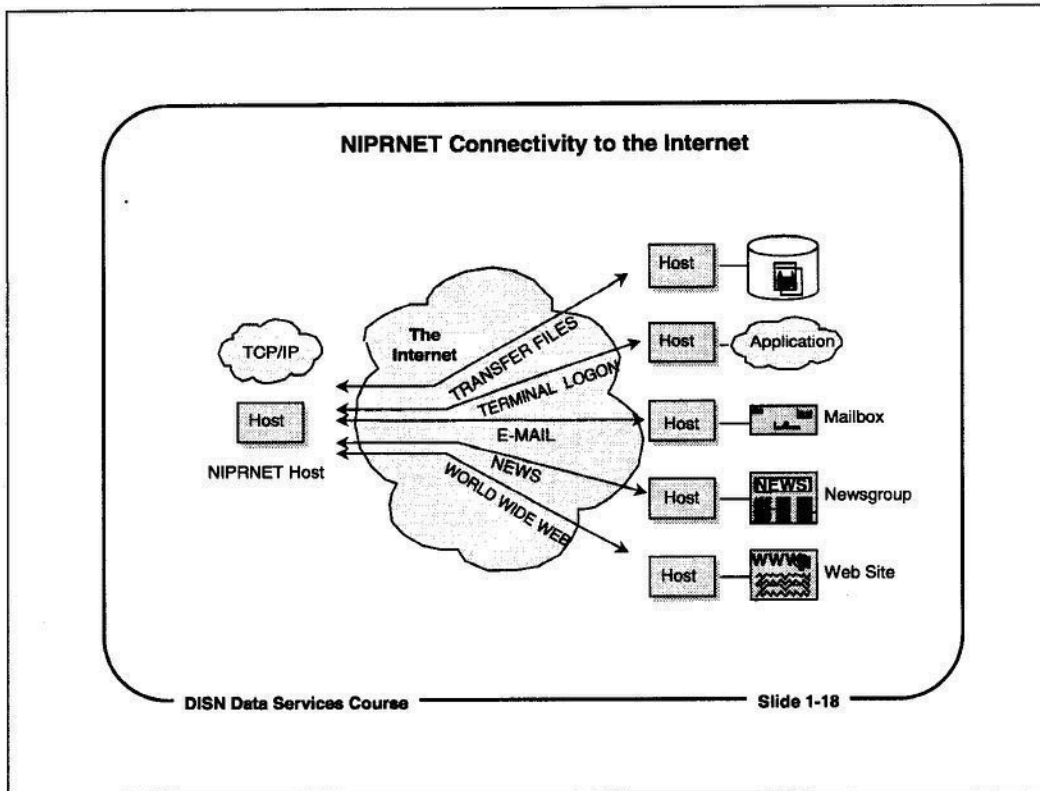
- JIS (Joint Interconnection Service) - These routers provide a network interconnection service, so that separate IP router networks, such as the Internet and the Pacific and European NIPRNET networks, can connect into the CONUS NIPRNET.
- The NIPRNET is connected to the Internet through the JIS network at nine Internet traffic exchange points, including the New York Network Access Point (NAP) gateway in Pennsauken, New Jersey, and the FIX-West gateway at Moffett Field, CA.



The Internet

NIPRNET hosts can connect to hosts on the network of commercial and research networks known as the Internet. The Internet is a set of worldwide networks that are interconnected, and use the same communications protocols. This allows all Internet hosts to communicate with each other.

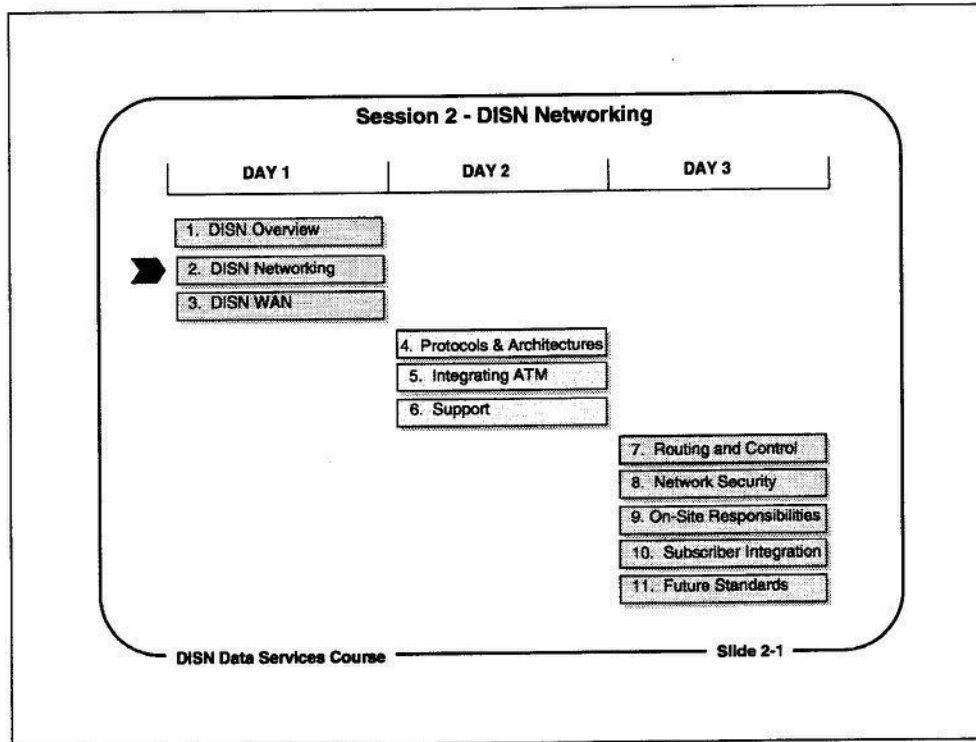
The NIPRNET is only one of the networks that form the Internet. Regional networks, university and academic networks, commercial networks, and networks run by Internet Service Providers (ISPs) are all connected together to form the Internet.



NIPRNET Connectivity to the Internet

NIPRNET users can connect to the Internet to access data that is available on other systems. They may also find other applications and Internet services that are not available on DoD systems, such as newsgroups and chat services.

NIPRNET users can send e-mail to other Internet users, because NIPRNET e-mail addresses are valid throughout the Internet, and Internet addresses are valid on the NIPRNET. A NIPRNET user who has access to a Web browser program can connect to Web sites on either the Internet or the NIPRNET. All other Internet facilities are available to NIPRNET users, subject to restrictions on Web access screening by base- or service-level firewalls.

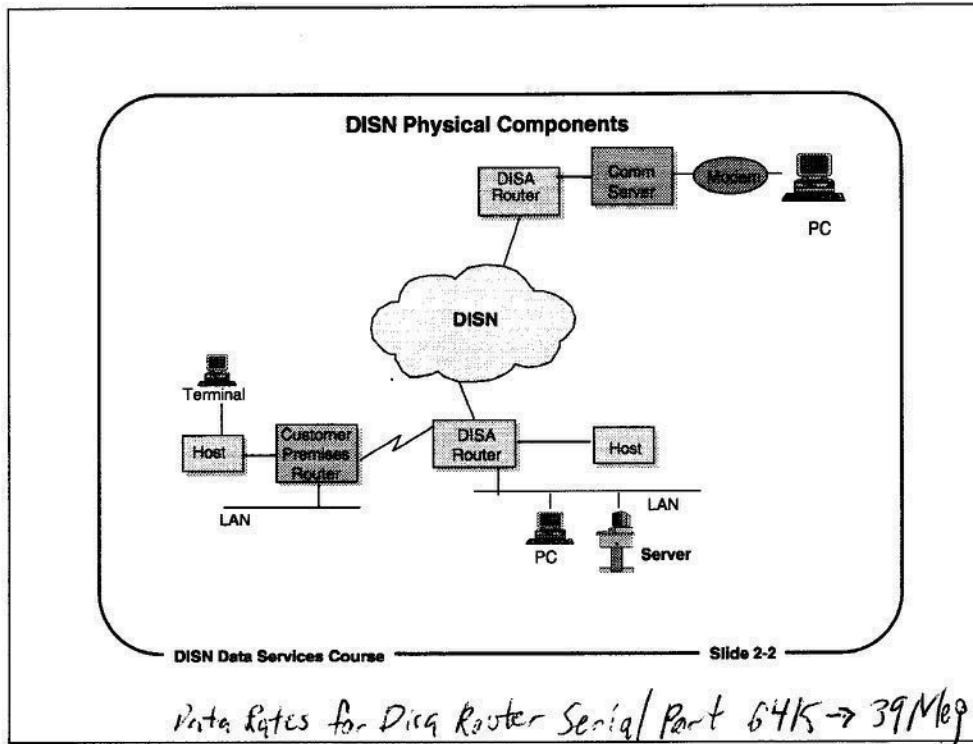


Session 2 - DISN Networking

Upon completion of this module, the students will be able to describe the components of the systems and networks that connect to the DISN data services networks, the role of the Defense Messaging System, and the integration of the ITSDN tactical networks into the DISN Data Services networks.

This session will focus on:

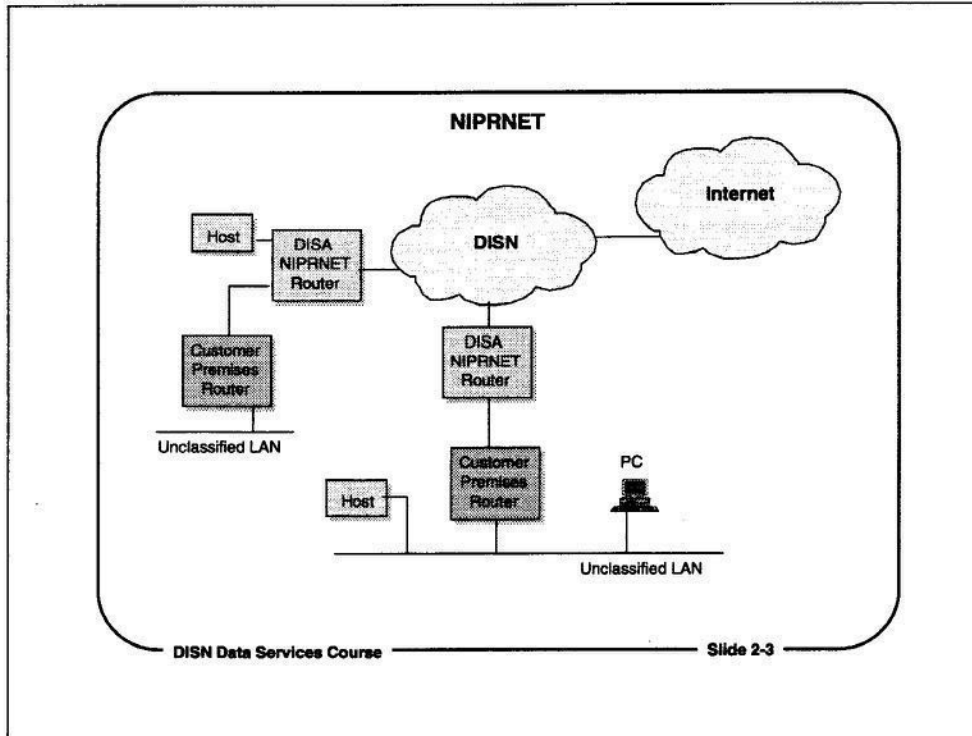
1. Describing the types of networks and systems that connect to the DISN data services networks
2. Describing the interface of the LANs connected to the DISN data services networks
3. Identifying the roles of DISA and customer premise routers
4. Distinguishing among repeaters, bridges, routers, and gateways
5. Understanding the functions of the Defense Messaging System (DMS) as an application on the DISN Data Services networks
6. Describing the integration of the ITSDN tactical networks into the DISN backbone and the DISN Data Services networks



DISN Physical Components

The hardware and transmission components of the DISN Data Services networks are:

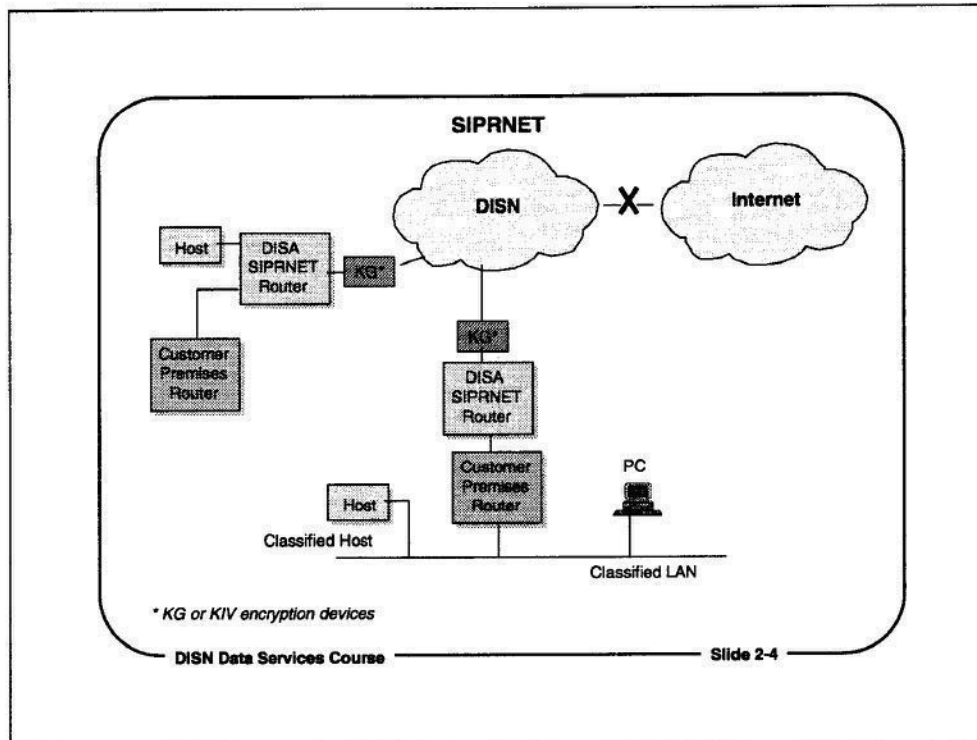
- Trunks - High-speed digital data communications circuits that carry traffic on the DISN.
- Host computers - Mainframes, minicomputers, and servers that provide applications for DISN Data Services network users.
- Terminals - Display or batch job entry devices attached to a host that users utilize to access the network.
- Local area networks (LANs) - Data communications networks for communications within an office or building, or on a military post, camp, base, or station.
- Routers - Special purpose communications devices that connect LANs to the DISN Data Services networks; may be called concentrators or gateways.
- PC and servers - Computers connected to LANs.
- Gateways - Special-purpose computers that connect DISN Data Services networks to other networks.
- Communications Server (Comm Server) - A special-purpose device that allows users to dial into the DISN Data Services networks.



NIPRNET

The NIPRNET, which is the DISA Unclassified but Sensitive Internet Protocol Router Network, is composed of its own set of dedicated routers. The NIPRNET routers are the access points through which NIPRNET customers connect to the NIPRNET and the DISA wide area network, DISN. The NIPRNET is DISA's general-purpose, common user data network.

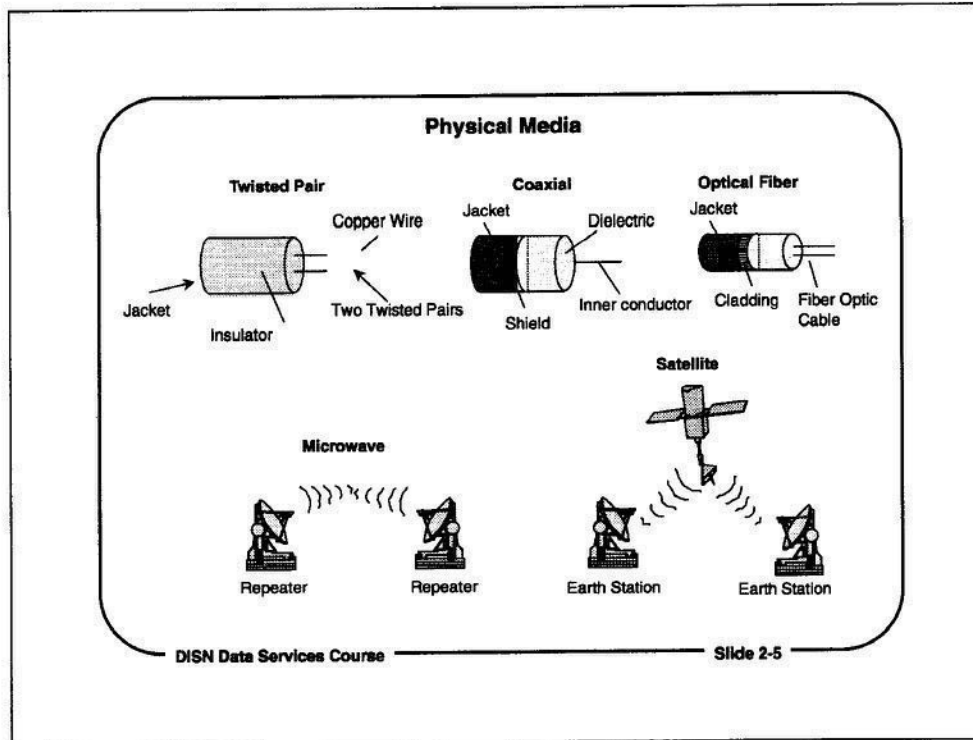
The NIPRNET also connects to the Internet through NIPRNET JIS routers that are positioned at Internet Network Access Points (NAPs) in the U.S.



SIPRNET

Like the NIPRNET, the SIPRNET, which is the DISA Secret Internet Protocol Router Network, is composed of its own set of dedicated routers. The SIPRNET routers are the access points through which SIPRNET customers connect to other SIPRNET users, and to the DISA wide area network, DISN. SIPRNET is DISA's general-purpose Secret data network. Only specially-authorized and accredited Secret systems may be connected to SIPRNET.

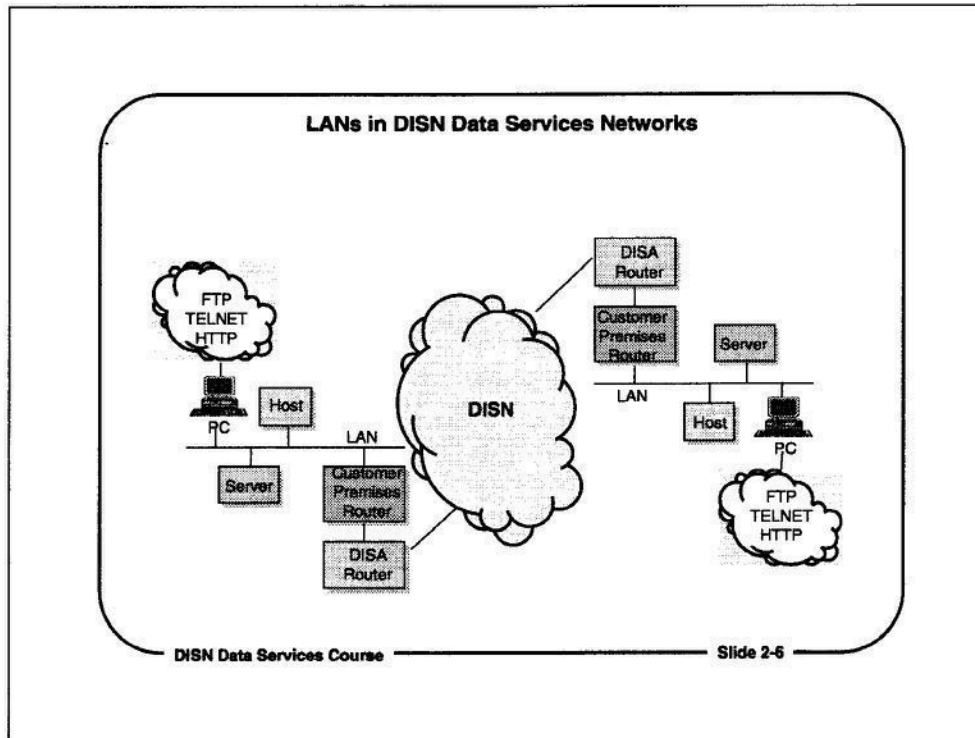
SIPRNET does not have a connection to the Internet. SIPRNET traffic is encrypted at both the host and the link level, to protect SIPRNET users and their data.



Physical Media

Various types of physical media make up the circuits in the DISN Data Services networks, including:

- Twisted pair - Two insulated wires twisted together; the pairs are bundled together into cables.
- Coaxial cable - A single copper conductor surrounded by insulation and an outer metal jacket, which is also a conductor.
- Fiber optic - Thin strands of glass or plastic that carry pulses of light, which are interpreted as digital data.
- Microwave - Terrestrial radio transmissions that use carrier frequencies in the microwave ranges for data transmission. Microwave repeater stations must have line-of-sight paths between them.
- Satellite - Radio transmission between terrestrial earth stations using a satellite orbiting around the earth; often uses the same frequency ranges as terrestrial microwave transmissions.

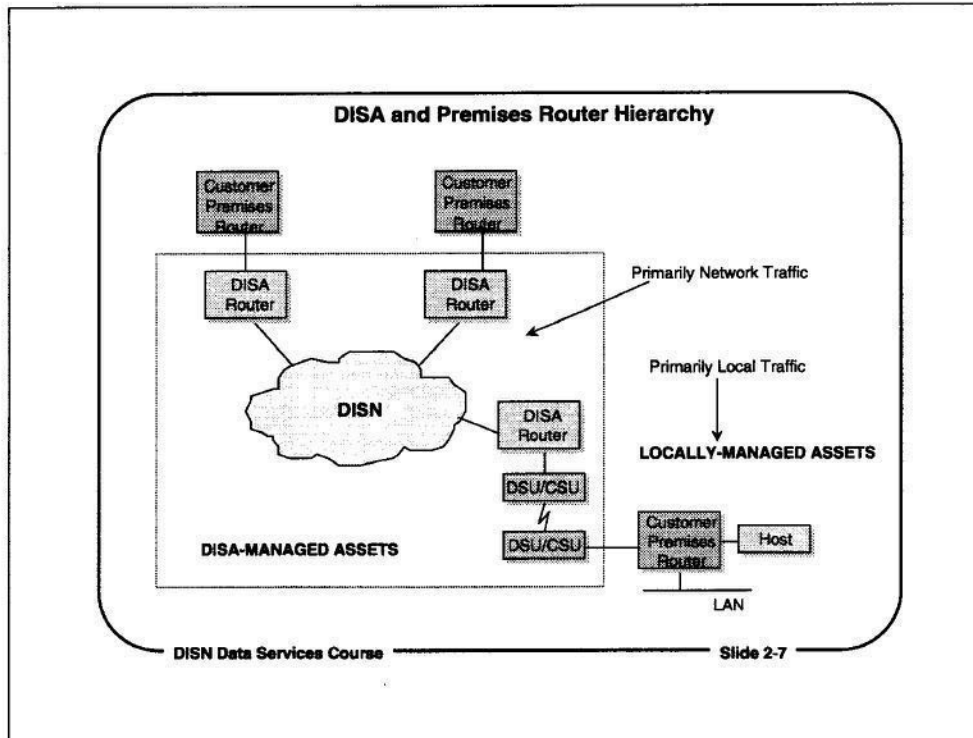


LANs in DISN Data Services Networks

Local Area Networks (LANs) are data communications networks for communications within an office, building, or on a military post or base. LANs connect PCs, servers, hosts, and other computers.

In the DISN Data Services networks, LANs connect to premise routers or to DISA routers that are connected directly into the DISN backbone.

Computers on LANs may use proprietary LAN network operating system protocols, such as Novell NetWare's IPX/SPX, in addition to TCP/IP. End-users on DISN Data Services customer networks use applications protocols and utility programs, such as FTP, HTTP, and Telnet.



DISA and Premises Router Hierarchy

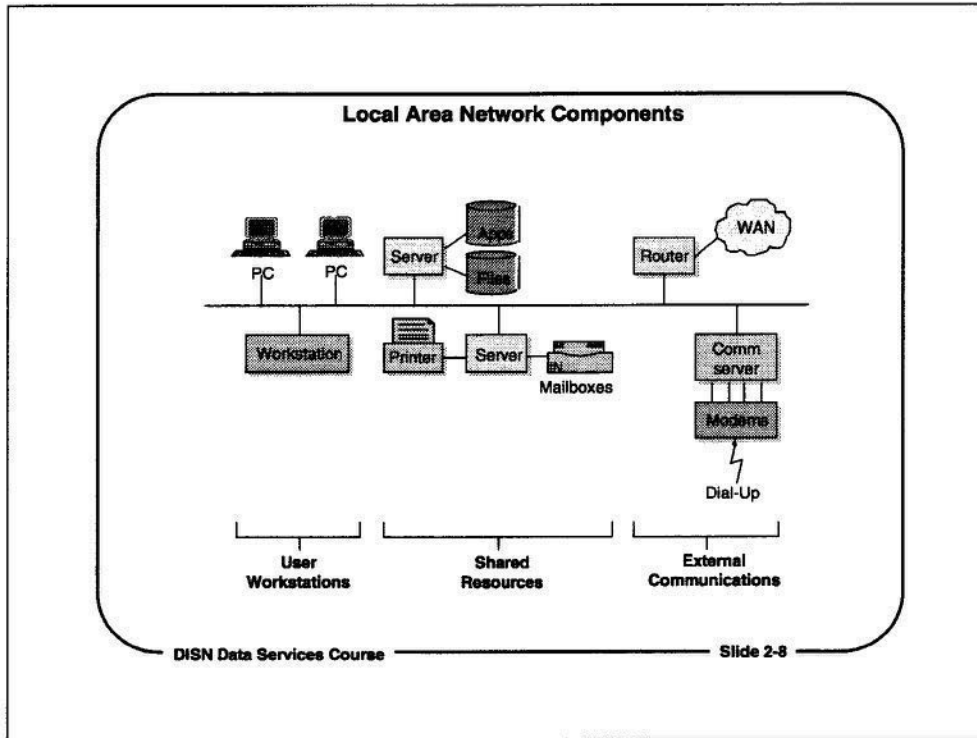
DISA routers and facilities belong to, and are the responsibility of DISA. Customer premise or “premise” routers that connect into DISA routers are the responsibility of the local base or post.

DISA owns or manages these parts of the network:

- DISN backbone trunks
- Routers directly connected to the DISN backbone
- Access circuits to routers
- Modems or DSU/CSUs on both ends of an access circuit
- Communications Servers for dial-up network access.
- KG Devices for classified networks

Local camp, post, or station authorities own and manage these parts of the network:

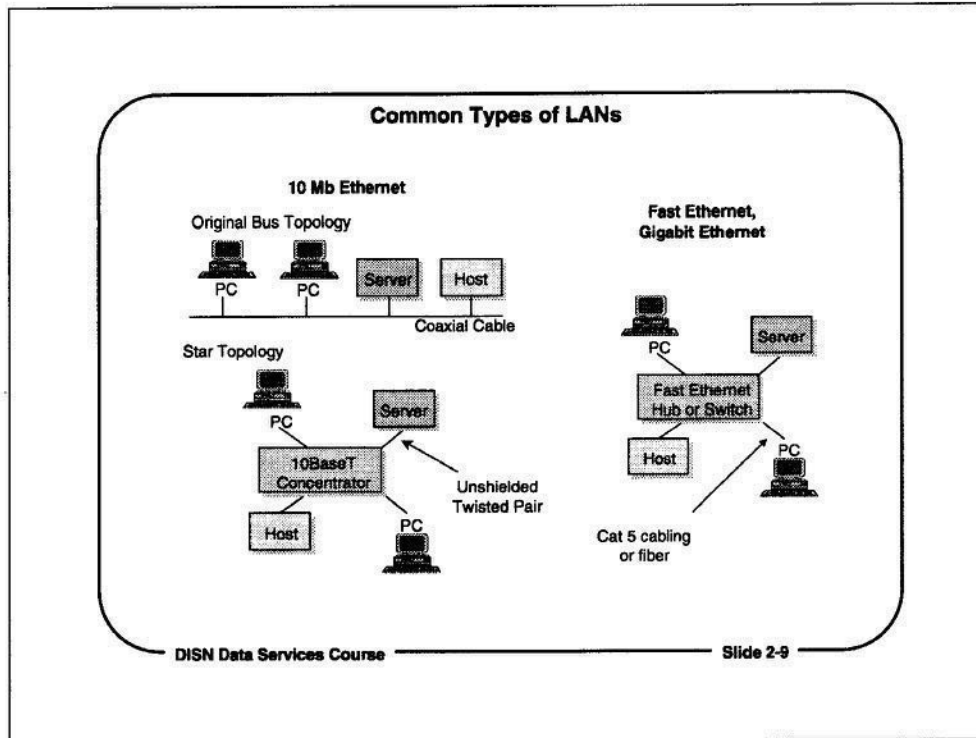
- Customer premise routers
- Hosts, PCs, and workstations
- LANs
- LAN cabling



Local Area Network Components

Local area networks (LANs) have three principal components. They are:

- **PCs and workstations** - These are end-user devices through which users access the LAN and its services. They can run their own standalone applications, or access shared network applications, such as e-mail.
- **Shared resources** - Hardware and/or software that are available to the users of the LAN. A server is a networked computer that provides network services, such as file, print, e-mail, and directory services.
- **External communications** - Routers and communications servers allow LAN users to communicate with other networks and with hosts that are not connected to the LAN. They may also support dial-in ports, so that remote users can access network services remotely, or logon to the network.

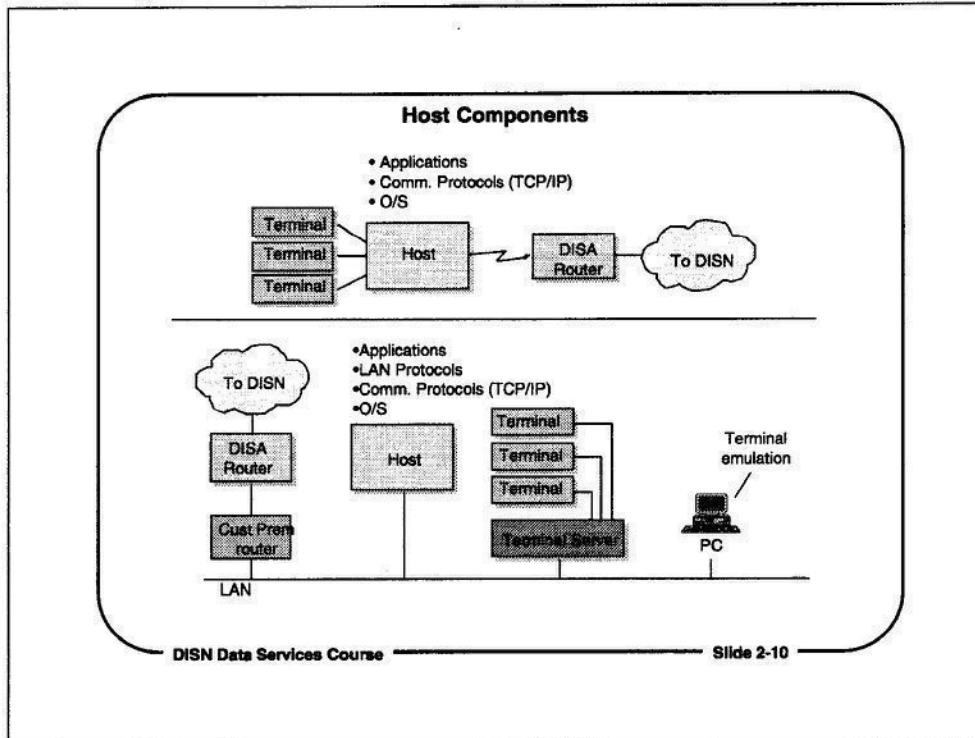


Common Types of LANs

Most LANs are Ethernet, conforming to one of the IEEE 802.x standards. The original Ethernet, specified in the IEEE 802.3 standard, used coaxial cable. Most coaxial cable Ethernet cabling has been replaced by twisted pair wiring, which is less expensive, and easier to install.

Ethernet LANs were originally broadcast networks, however, many new Ethernets are hubbed through LAN switches. The LAN switch emulates the LAN broadcast domain, but it maps Ethernet addresses to switch ports. The benefit of a LAN switch is that it can give two devices the full 10 Mb LAN bandwidth, instead of forcing them to share the network bandwidth with other devices.

Newer, higher-speed forms of Ethernet have been developed, such as 100 Mb Fast Ethernet, and 1,000 Mb Gigabit Ethernet.

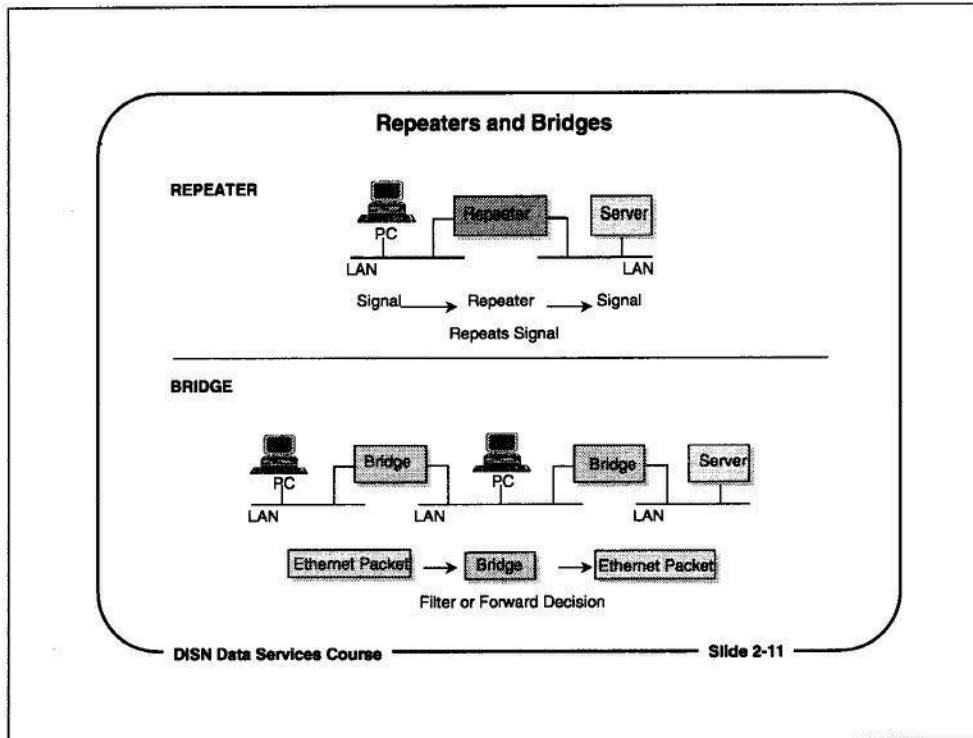


Host Components

Host computers are mainframes, minicomputers, or, in some cases, servers that may be connected to the DISN Data Services networks through a base LAN, or directly to a DISN Data Services router.

The components of a host connected to a DISN Data Services network are:

- Terminals - Users access host applications through directly- or remotely-connected terminals.
- LAN-attached terminals may also connect through a terminal server. PCs may use host applications by emulating a host terminal.
- Communications protocols - Protocols for LAN and WAN communications.
- Applications - End-user applications.

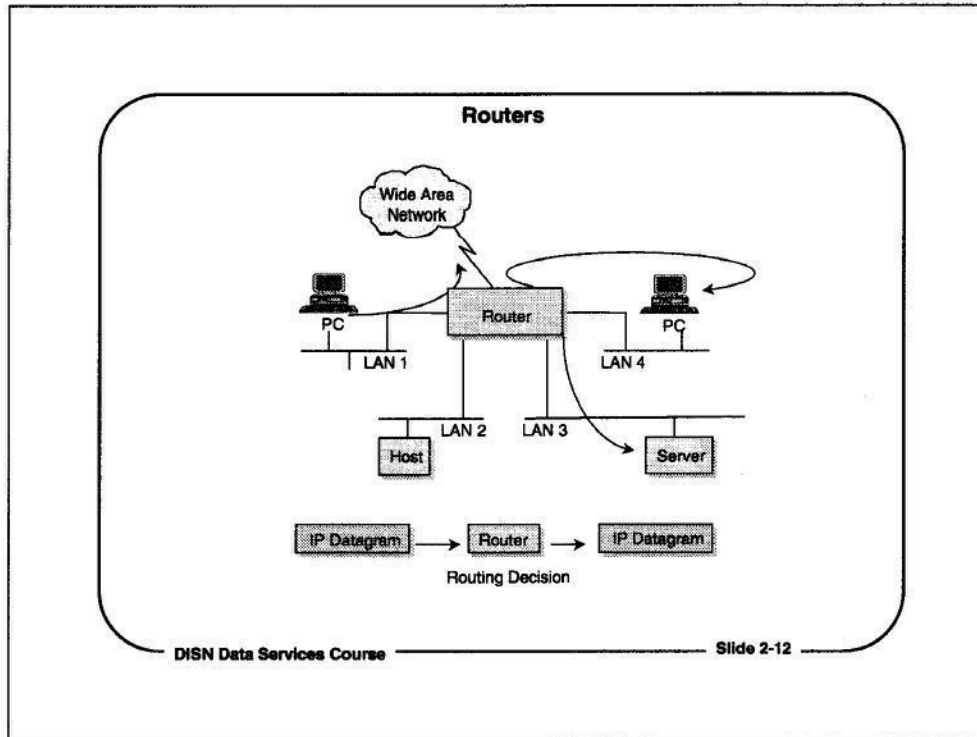


Repeaters and Bridges

Repeaters and bridges connect LAN segments together. They are used on LANs that are behind the routers or concentrators that connect LANs to DISN Data Services networks. Neither repeaters nor bridges are visible to a customer premise router or a DISN Data Services network. They are also invisible to other customer premises LANs.

A repeater is a special-purpose device that copies or repeats electrical or optical signals from one network to another. The result of adding a repeater is that the potential length of the overall network is increased.

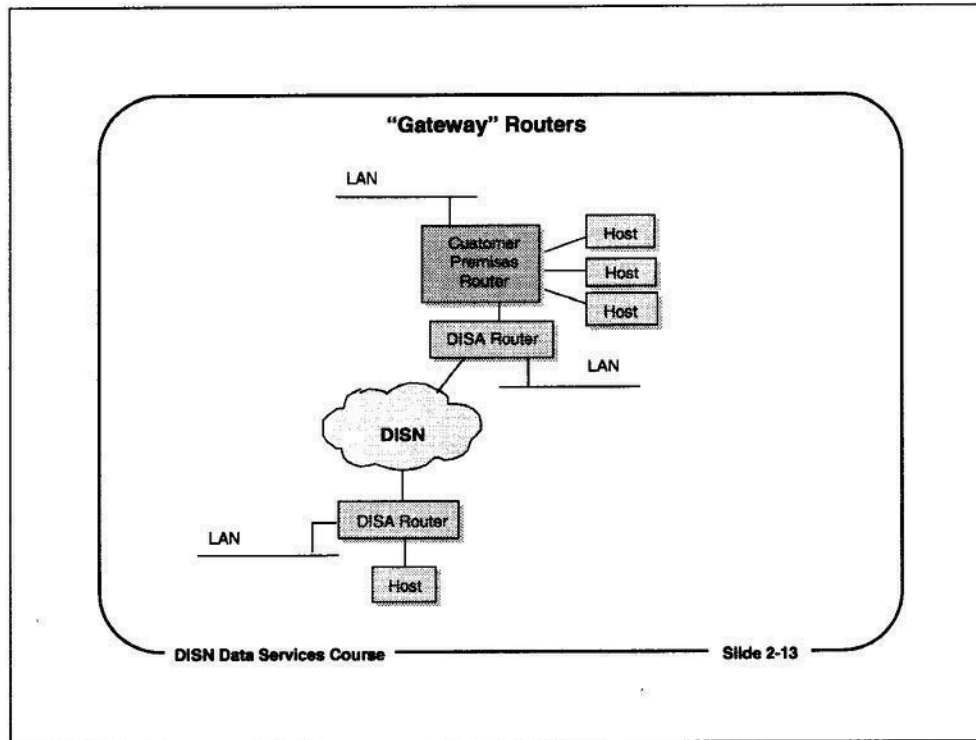
A bridge is a special-purpose computer that connects two networks at the data link level. Bridges store and forward network packets. They may examine the packet to determine if it should be forwarded to the next network segment, according to forwarding rules established by the bridge administrator. Bridges use LAN adapter addresses to make packet forwarding decisions.



Routers

A router is a special-purpose computer that is connected to two or more networks that use the same network addressing and delivery rules. Routers direct data packets to other routers for delivery to a final destination.

Routers direct transmissions from LANs onto DISN Data Services networks. They also connect LANs together, passing traffic destined for a device on one LAN to another router. In some DISN Data Services networks, routers may be referred to as concentrators when many LANs or hosts are connected to them. A concentrator routes traffic onto a single link into the DISN.

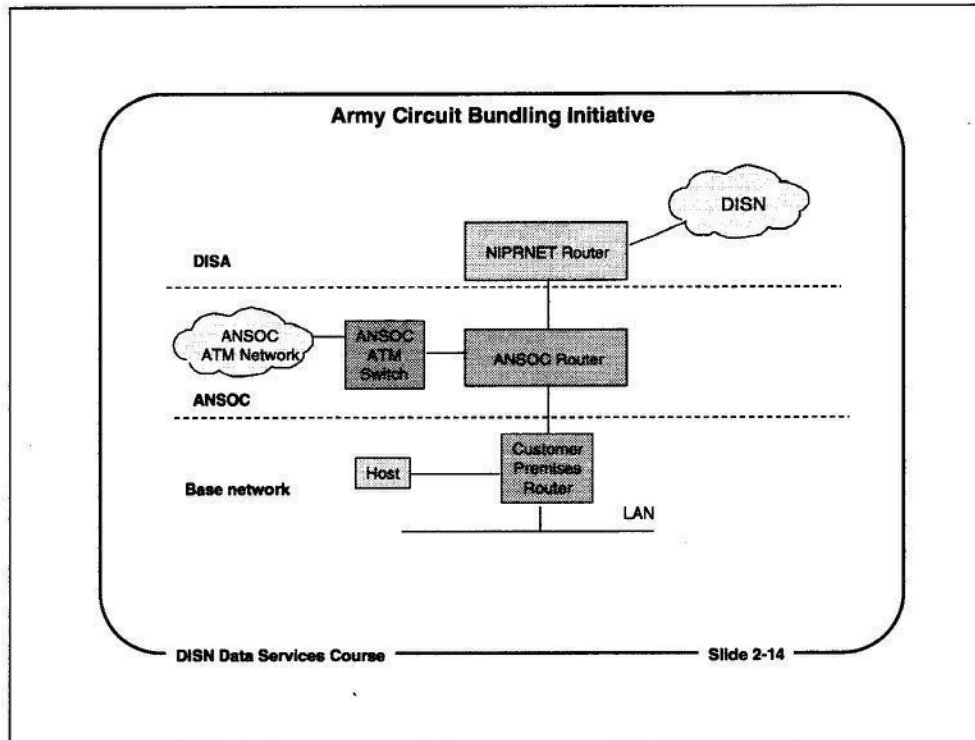


“Gateway” Routers

Gateway routers are routers that are also called “gateways” or “concentrators.” They connect LANs and hosts to DISN Data Services networks, and reduce the number of DISA router port connections required.

The benefits of gateway routers are:

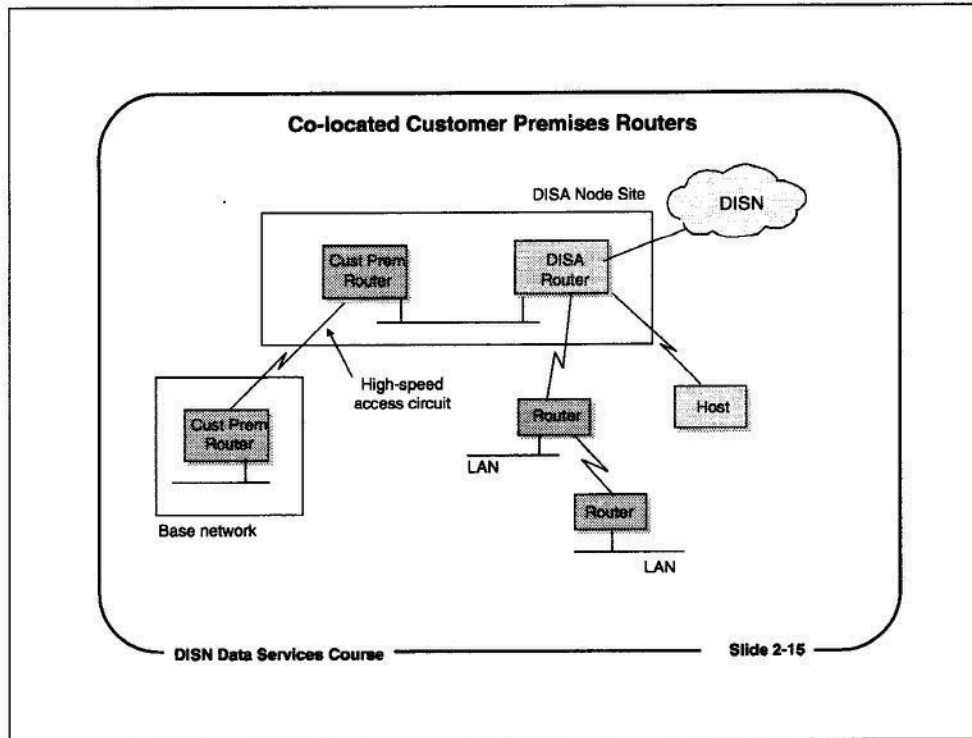
- Lower connection costs
- Greater connection capacity
- Lower connection cost per host or LAN.



Army Circuit Bundling Initiative (CBI)

The Army has developed its own network, called the Army Circuit Bundling Initiative (CBI) as a means to keep traffic destined for other Army units on an Army-operated network. The network is run by the Army's Network Systems Operations Command (ANSOC).

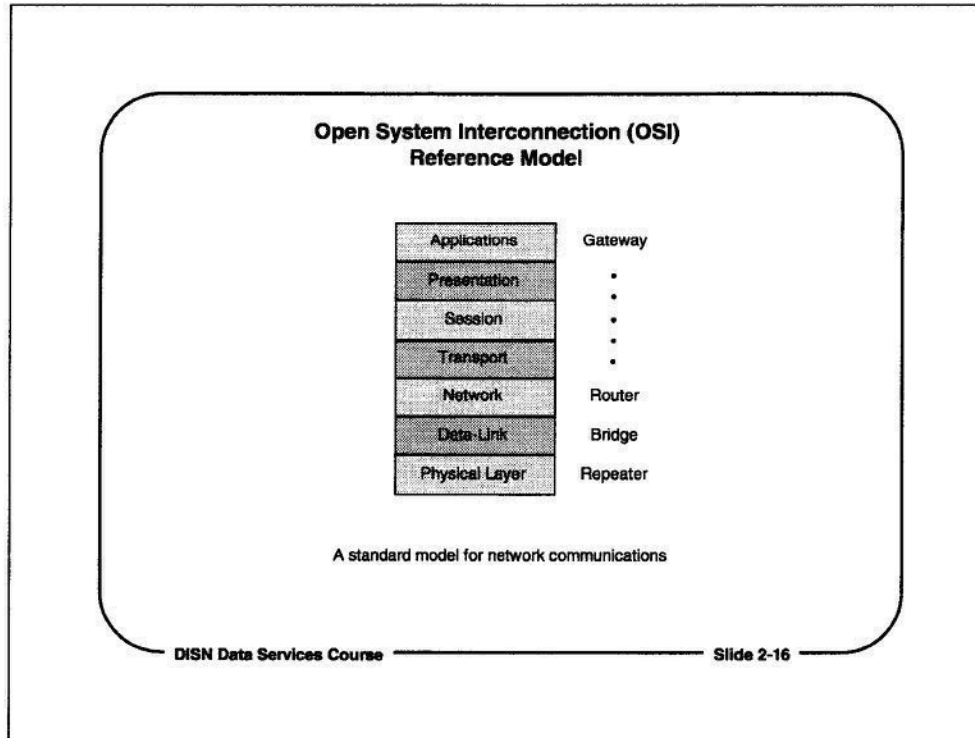
The ANSOC router, which is also called the Army security router, is part of a standard suite of security devices that protect the Army base networks. The CBI network connects the ANSOC routers to Army ATM switches, which carry traffic among Army units over an ATM backbone. Traffic for other services or agencies goes to the NIPRNET, as does Internet traffic.



Co-located Customer Premises Routers

NIPRNET customers who want high-speed network access (3 Mb to 39 Mb) may have to co-locate a customer premises router at a DISA node site. Access to the node site from the military base or installation would be over a high-speed leased line.

At the DISA node site the connection between the DISA router and the customer premise router would be Fast Ethernet (100Mb). In most cases, the DISA router would connect to an ATM node, in order to get enough backbone bandwidth to deliver the high-speed access service.



Open Systems Interconnection (OSI) Reference Model

The seven-layer Open Systems Interconnect (OSI) Reference Model is a conceptual description of the functions that two systems perform when they communicate. The levels of the model describe generalized data transport, flow control, and data interpretation mechanisms. Communications devices, such as repeaters, bridges, routers, and gateways, operate at different levels of the OSI model.

Repeaters work at the physical level, because they are concerned with moving bits on physical media. Bridges operate at the data link level, because they use the protocols that govern how data is packaged for transmission on a data link, such as a LAN. Routers operate at the network level, because they use protocols that determine how to direct traffic to a destination. Gateways, which deal with the format of data, may operate at levels up to and including the Application level.

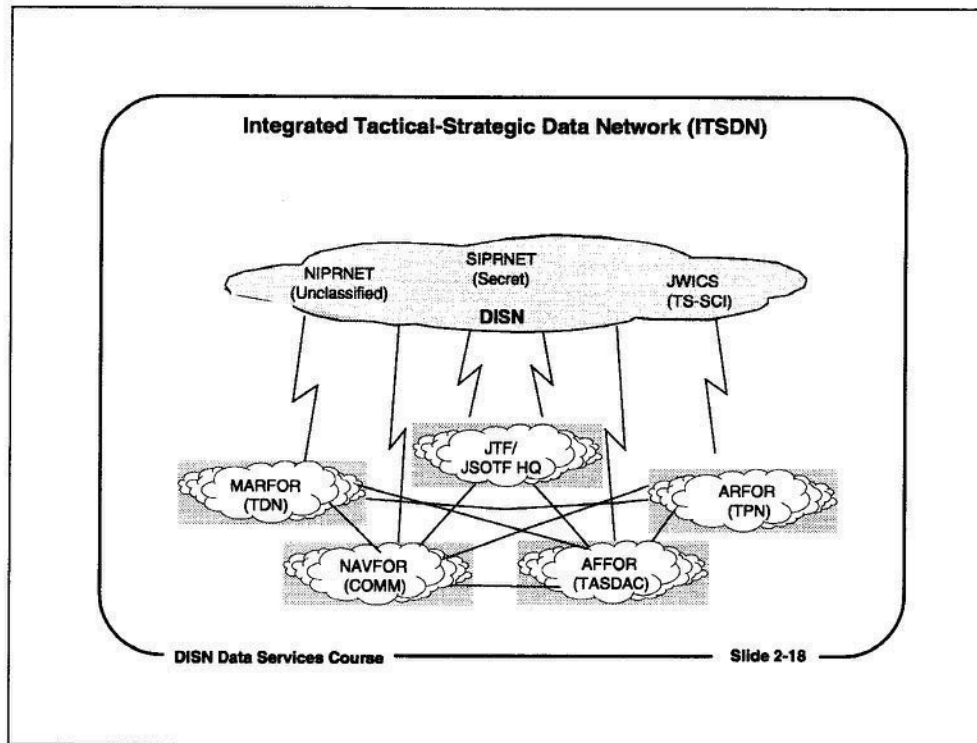
Bridge, Router, and Gateway Capabilities		
BRIDGE	ROUTER	GATEWAY
Extends LAN segments	Connects LANs/WANs to other LANs/WANs or to other networks.	Connects networks together Translates between different protocols or formats
Makes packet forwarding decisions on LAN addresses	Makes routing decisions on network addresses	Makes gateway decisions on network addresses or application being performed
Ignores higher-level protocols	Must understand specific network-level protocols	Must understand protocol at all levels
Operates at OSI level 2 (Data Link level)	Operates at OSI level 3 (Network level)	Operates at OSI levels 3 to 7 (Network thru Application)
Simple, fast device	More complex, slower device	Most complex, slowest device

DISN Data Services Course ————— Slide 2-17

Bridge, Router, and Gateway Capabilities

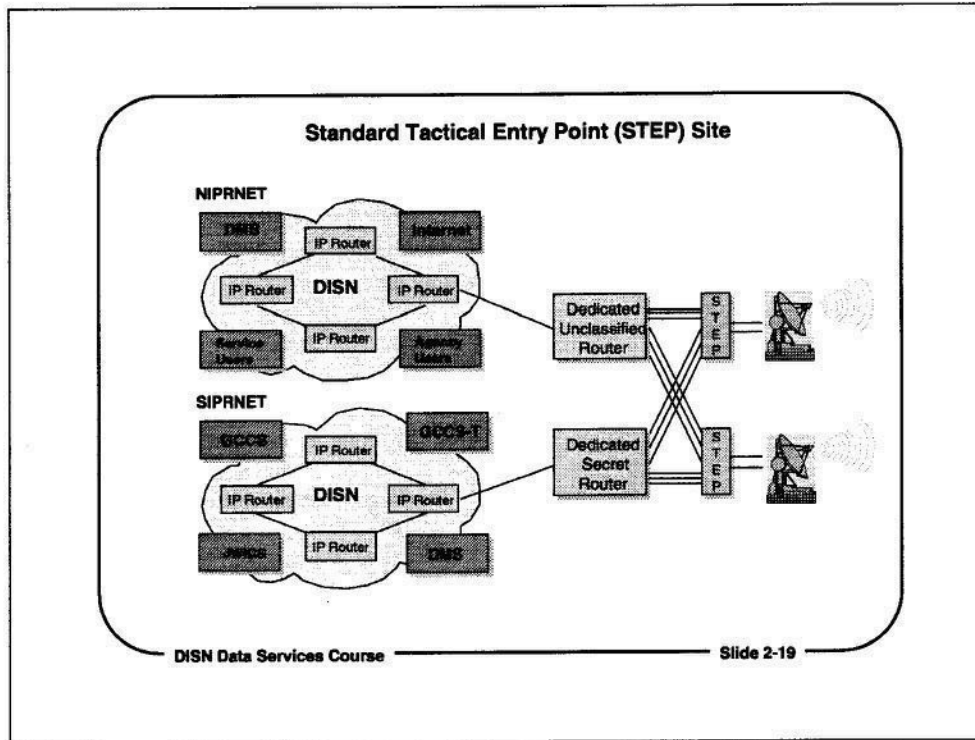
The complexity of the software of devices increases from bridges to routers to gateways, because of the increasing complexity of the operations and transformations each has to perform.

The speed of operation of these devices decreases from bridges to routers to gateways. Routers have more complicated decisions to make and more manipulations to perform than bridges. Gateway operations may be the most complex of all, so gateways are usually the slowest of all three devices.



Integrated Tactical-Strategic Data Network (ITSDN)

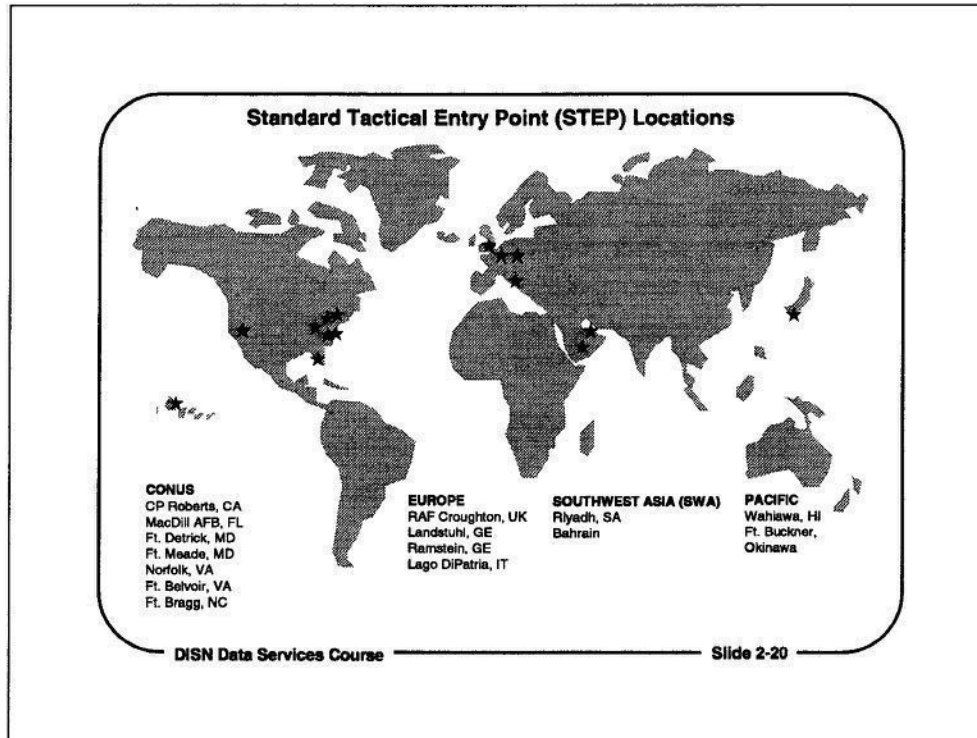
U.S. armed forces that have been deployed to the field can still access the DISN Data Services networks through the ITSDN tactical access networks. These router networks are connected back into the SIPRNET and NIPRNET networks through satellite earth stations, called STEP sites, at entry points around the world.



Standard Tactical Entry Point (STEP) Site

The entry points for ITSDN tactical networks into the DISN Data Services networks are located at satellite earth stations. The interface between the satellite earth station and the DISN Data Services networks is called the Standard Tactical Entry Point (STEP). A tactical network can connect through the STEP back to the DCS entry points, so that tactical networks deployed in the field can interconnect with the DISN Data Services networks.

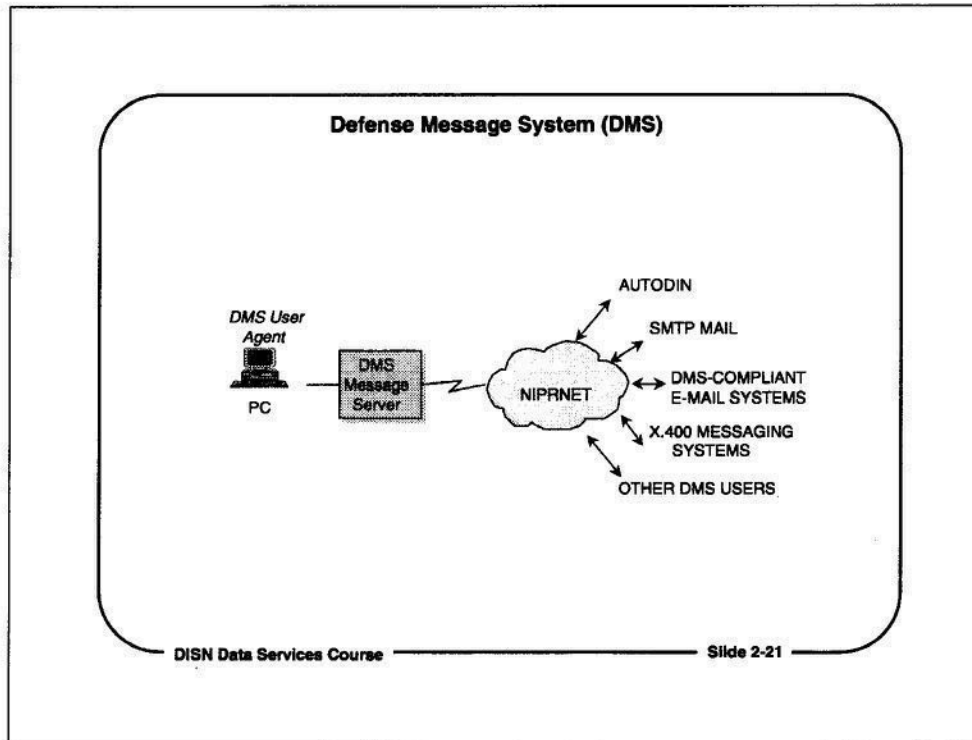
Both SIPRNET and NIPRNET are reachable from deployed units through the STEP site entry points and the ITSDN tactical networks. The JWICS network is accessible through specially-provisioned STEP sites.



Standard Tactical Entry Point (STEP) Locations

STEP earth stations have been deployed at fifteen locations worldwide. At least one of the locations can be reached from any location in the world.

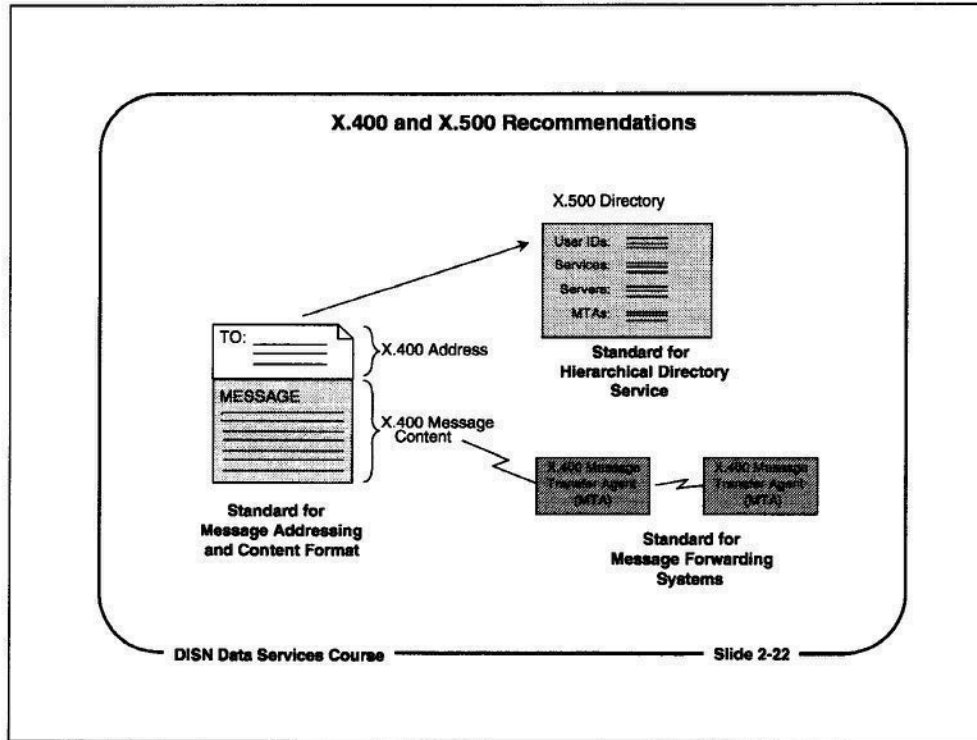
Each STEP location can access the NIPRNET, the Internet (through the NIPRNET), and the SIPRNET.



Defense Messaging System (DMS)

The Defense Messaging System (DMS) is a DoD messaging system that will integrate different e-mail and messaging systems into one, integrated system. The DMS will replace the AUTODIN message switching system. It will also incorporate e-mail capabilities.

DMS uses PCs and workstations on LANs as DMS hosts. It interfaces to LAN, host-based, and public e-mail systems. Messages may originate or be delivered to the DMS or to an e-mail system mailbox. DMS uses a DoD variation of X.400 addressing, and X.400 message transfer agents based on ACP (Allied Communications Publications) addressing.



X.400 and X.500 Recommendations

The core of the DMS architecture is based on the X.400 and X.500 standards. The X.400 and X.500 standards were established by the International Telecommunications Union (ITU). The X.400 standard specifies a message handling system architecture for messaging, addressing, and message content. It also specifies how systems that are Message Transfer Agents (MTA) store and forward messages. In practice, MTAs may be native X.400 e-mail systems, or e-mail systems that can handle X.400 messages.

X.500 is also an ITU standard for Directory Services. It defines the function and structure of a Directory Service for message systems that use the X.400 standards.

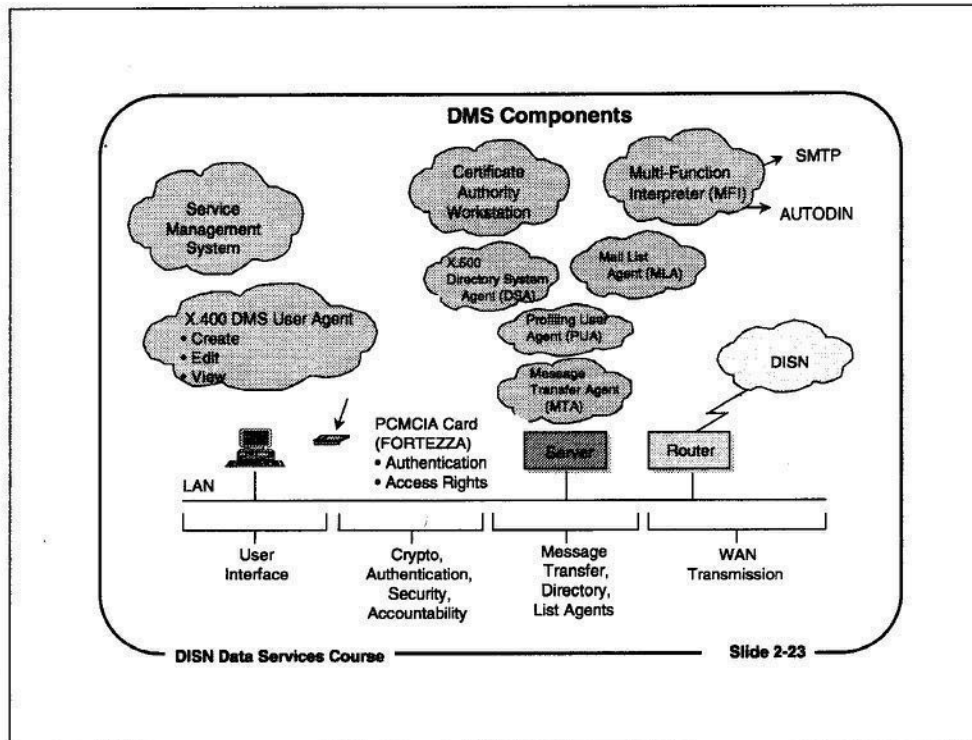
DMS architecture uses both X.400 and X.500 recommendations, with significant extensions and some variations. For example, DMS addresses are a DoD variation of ITU standard X.400 addresses. Several DMS components are designed and deployed as DMS-specific extensions to the X.400 and X.500 recommendations.

The principal components of a DMS address are:

C = Country
 A = Administrative Entity
 O = Organization
 OU = Organizational Unit
 PN = Personal Name

The X.400/DMS address of a user may look like this:

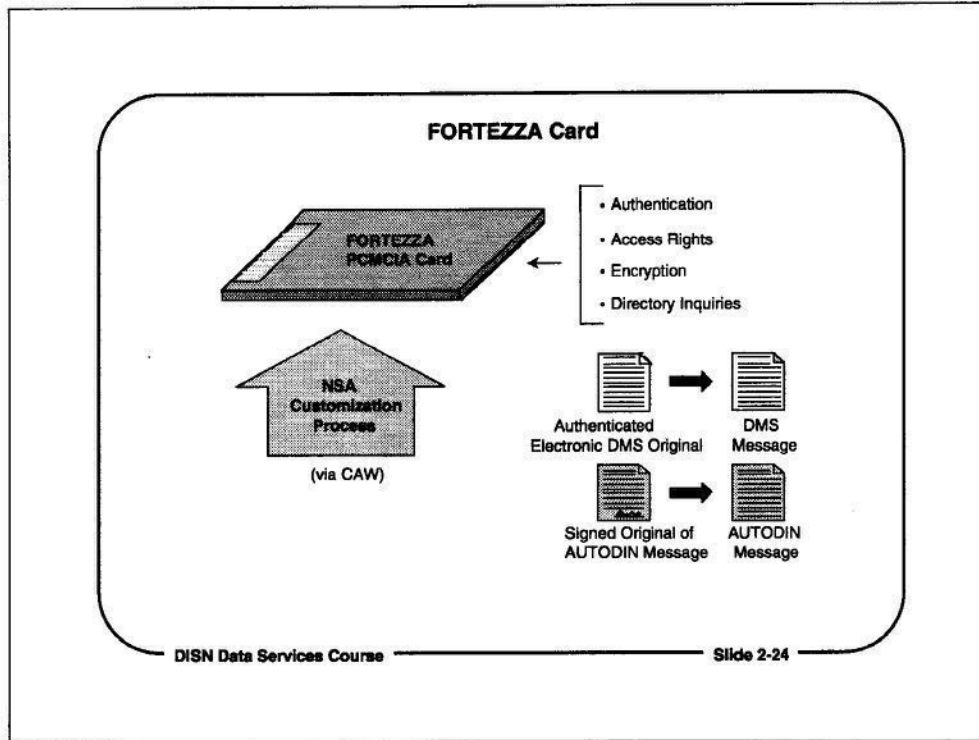
C=US/A=DMS/O=AR/OU=AZ+HUA/OU=2SIG/OU=HQ/PN=JJONES



DMS Components

The major components of the DMS system are:

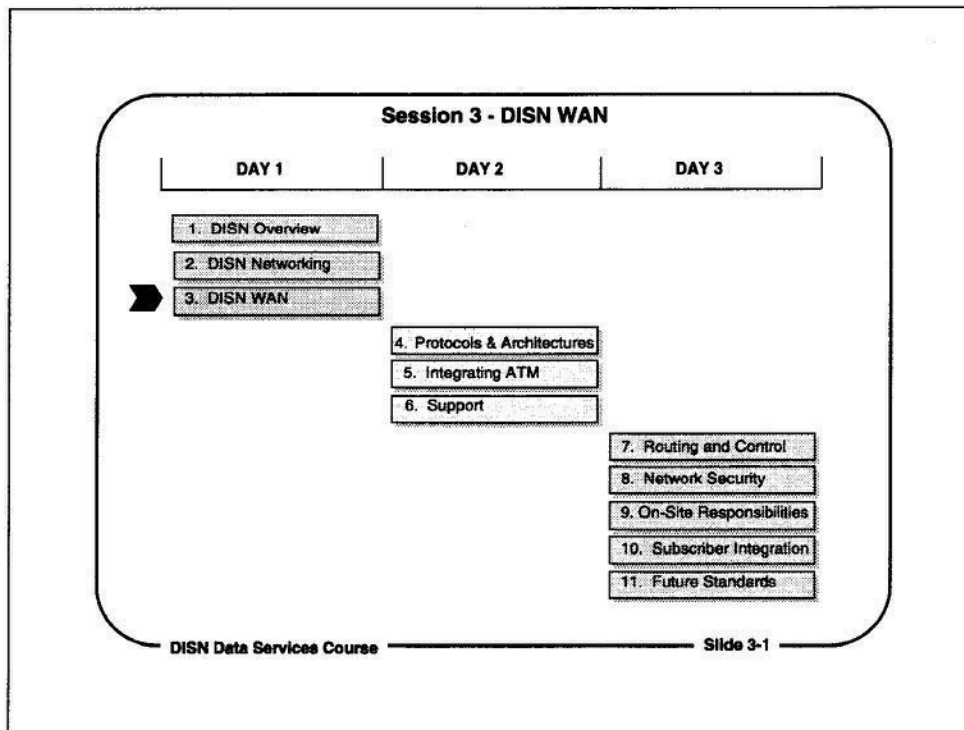
- **Service Management System (SMS)** - The SMS consists of components and policies established to manage the messaging and directory services of DMS.
- **X.400 User Agent (UA)** - The UA is a software application which provides the end user with the ability to compose and submit messages to the Message Transfer System.
- **Directory User Agents (DUA)** - DUAs contain software applications for accessing the directory, and cache directory information read from the directory.
- **Message Transfer Agent (MTA)** - The MTA stores and forwards messages through the Message Handling System (MHS).
- **Message Store (MS)** - The MS stores messages for UAs, much like a mailbox.
- **Directory System Agent (DSA)** - The DSA stores directory information on users, groups, network resources, or other items.
- **Mail List Agent (MLA)** - Messages created for distribution to a large number of recipients are addressed to a Mail List (ML), which is managed by the MLA..
- **Multi-Function Interpreter (MFI)** - Each MFI provides translation services from DMS messaging to AUTODIN, or to SMTP or X.400 domains.
- **Profiling User Agent (PUA)** - The PUA manages message distribution lists for the UAs.



FORTEZZA Card

A DMS system administrator uses a CAW (Certified Authority Workstation), defined by the National Security Agency (NSA), to embed personal information, message authentication, encryption, and directory inquiry rights code in each FORTEZZA PCMCIA card.

The FORTEZZA card is a Type 2 PCMCIA card that is keyed to a specific user's DMS access and usage rights and security clearance. Users must have access to a computer equipped with a PCMCIA interface adapter to use the FORTEZZA card. The card is about the size of a credit card, so DMS users can carry their DMS "rights" and identity with them wherever they go.

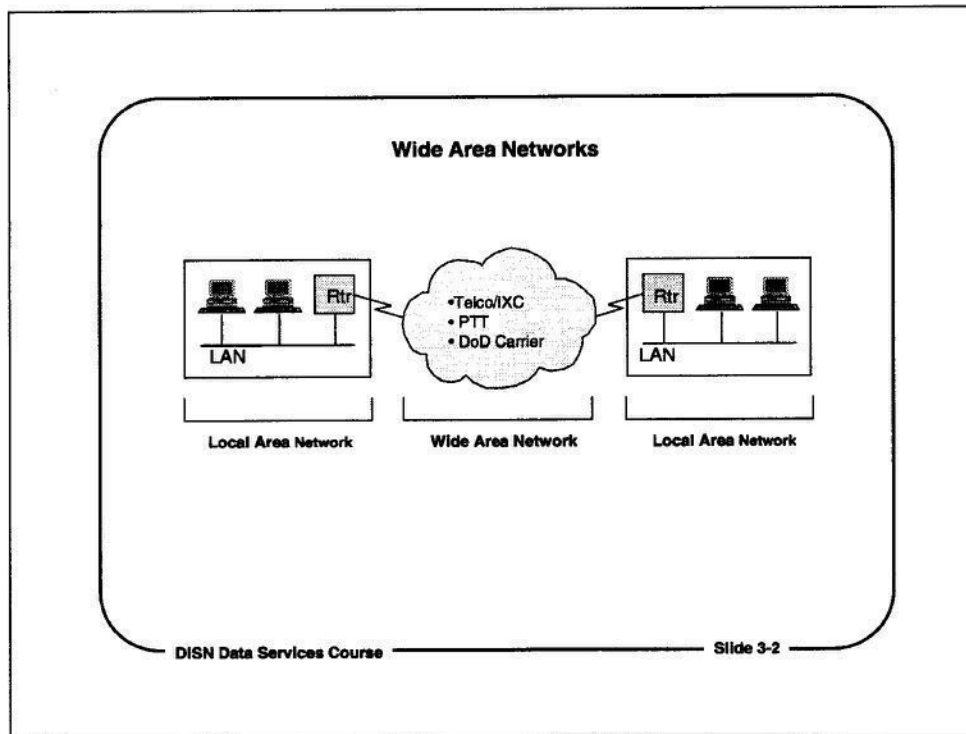


Session 3 - DISN WAN

Upon completion of this module, the students will be able to describe the role of the DISN wide area network (WAN), which is referred to as the Defense Information Services Network (DISN), and its role in long-haul backbone transmission for the DISN data services networks.

This session will focus on:

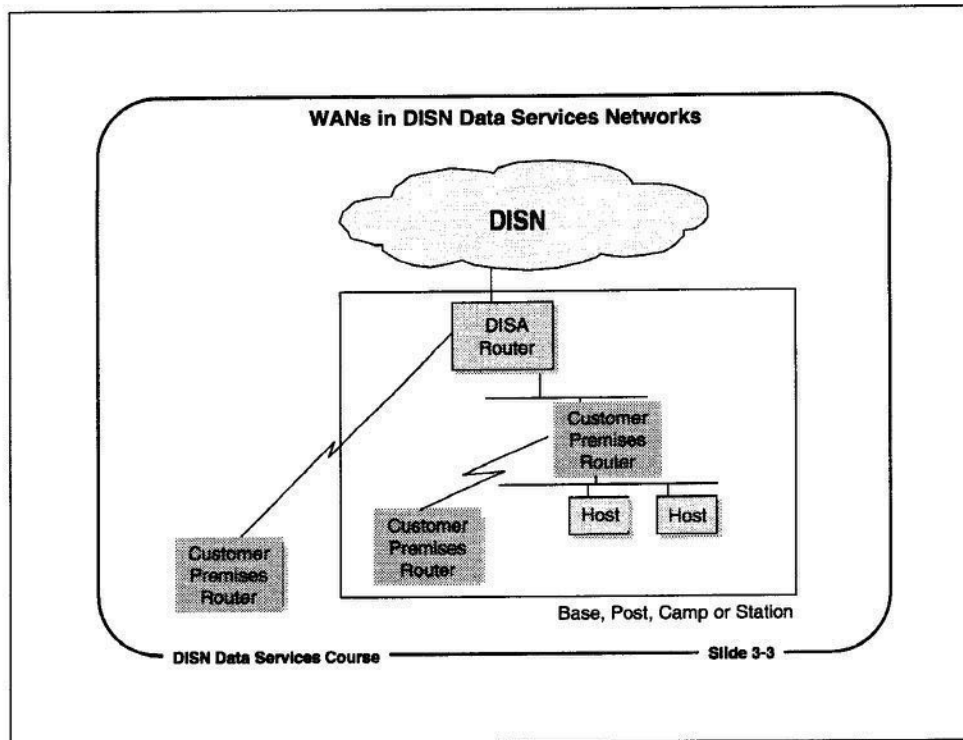
1. Differentiating the DISN WAN from other types of networks
2. Identifying the carriers that provide the circuits that comprise the DISN backbone
3. Describing the functions of the IDNX multiplexers in support of the DISN backbone
4. Describing the benefits of reorganizing the NIPRNET and SIPRNET backbones to incorporate ATM transmission services



Wide Area Networks

The Defense Information Systems Network (DISN) is a wide area network. It provides long-distance connectivity for the DISN Data Services networks. DISN connects other networks together, such as the local area networks that are behind customer premise routers. Like most other wide area networks, DISN uses commercial carriers (in addition to some DoD circuits) for long-distance communications.

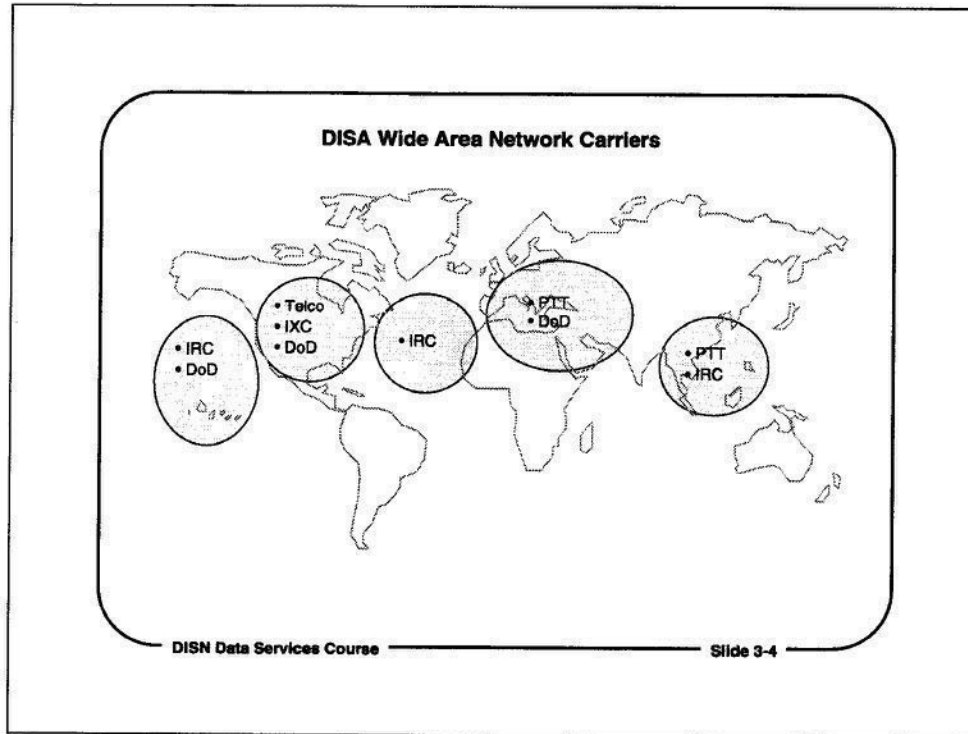
A wide area network, or WAN, connects smaller local networks together into an interconnected group of networks. An interconnected group of networks is sometimes called an internetwork, or an internet.



WANs in DISN Data Services Networks

DISA routers connect directly to the DISN backbone network. The DISA routers are the main interconnection points for wide area network connectivity for the DISN Data Services networks.

Customer premise routers see the DISN wide area network indirectly, through the DISA routers, but they have the same use of the DISN wide area network as hosts and networks directly connected to the DISA routers.

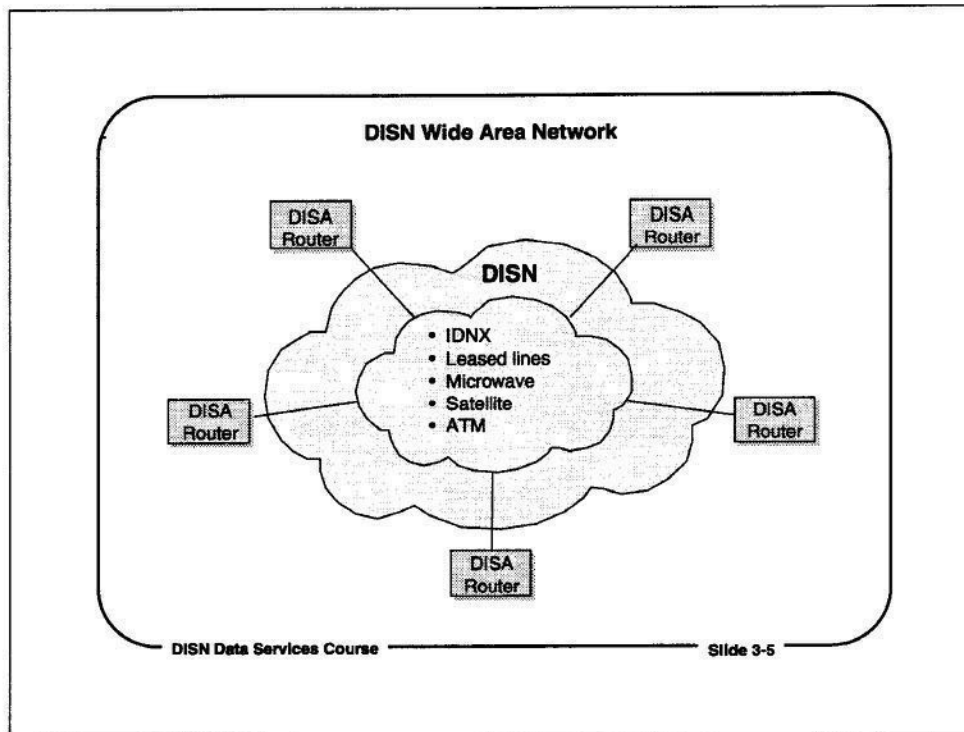


DISA Wide Area Network Carriers

DISN wide area network circuits are leased or wholly-owned circuits that are provided by a combination of commercial and military carriers. Local availability, cost, and operational requirements determine the selection of a carrier.

Within CONUS, most DISN circuits are leased from the local telephone companies and the long-distance carriers, which are called the Inter-exchange Carriers (IXCs). Across the Atlantic and the Pacific, DISA leases circuits from the International Record Carriers (IRC), but it also uses some DoD facilities.

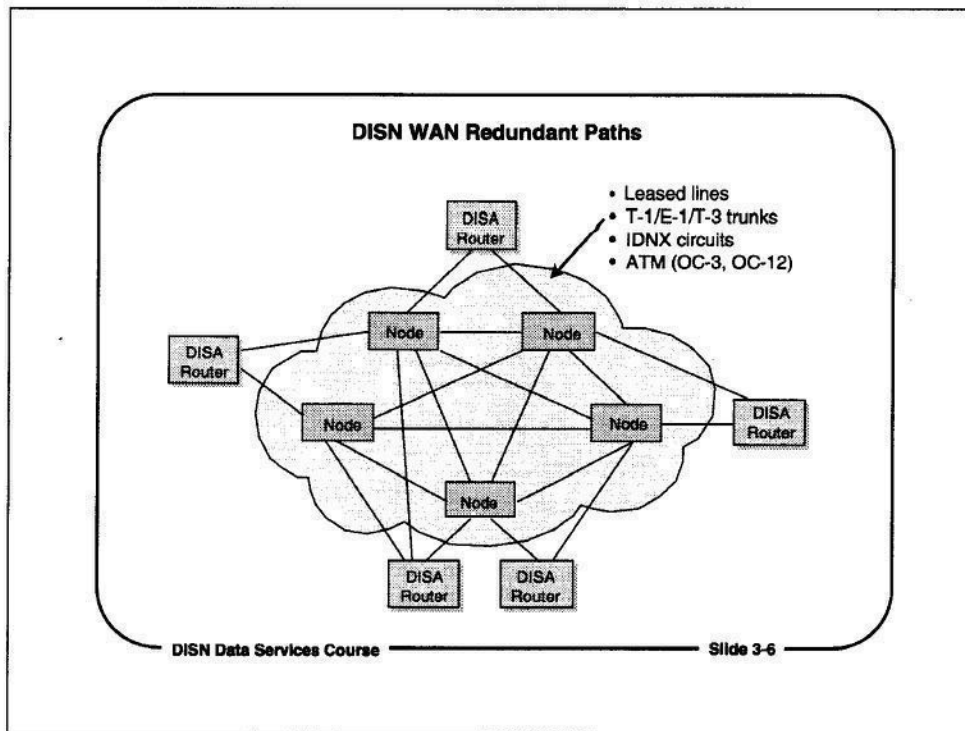
In the European and Pacific theaters, DISA uses DoD, IRC, and local postal telephone and telegraph (PTT) circuits. Much of the new ATM backbone network is being provisioned as a private network for DISA by commercial carriers.



DISN Wide Area Network

The DISN backbone connects the DISA routers for the NIPRNET and the SIPRNET into a worldwide wide area network.

The DISN is composed of a variety of physical media and circuit types, including terrestrial and satellite paths, copper twisted pairs, fiber optic cable, submarine cables, microwave, and satellite circuits, and ATM networks.

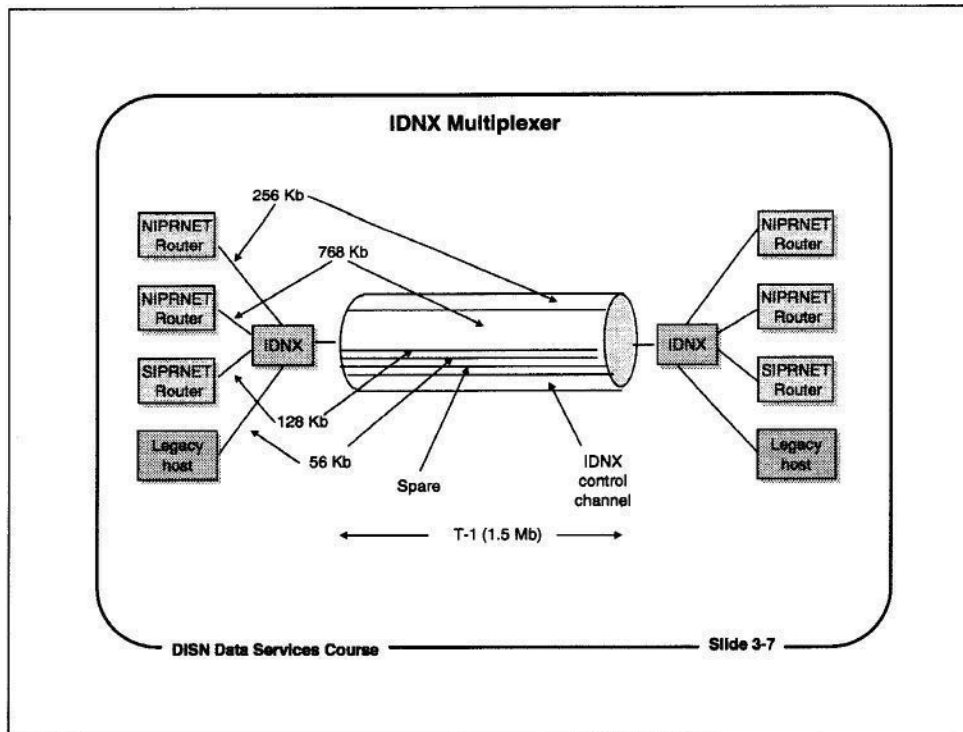


DISN WAN Redundant Paths

The DISN backbone network, which provides long-haul transmission services for the NIPRNET and SIPRNET routers, is composed of a variety of circuit types and transmission technologies. The circuits may be low speed (56 Kb to 256 Kb) leased lines, T-1, T-3, or E-1 trunks, point-to-point circuits connecting IDNX multiplexers, or the new DISN ATM (Asynchronous Transfer Mode) services.

In most cases, the DISA routers see the DISN backbone as a point-to-point circuit. In reality, most DISN routers connect to multiplexers or to ATM edge devices located at DISA node sites that act as multiplexers. A multiplexer combines several different lower-speed circuits into a single higher-speed circuit.

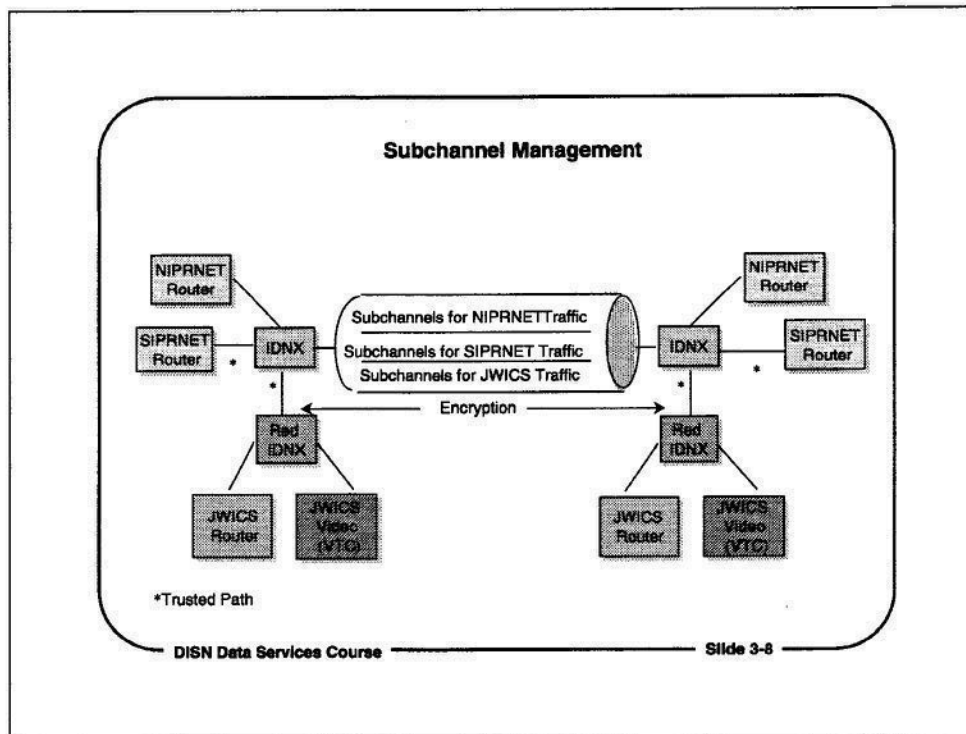
DISA routers are connected to the DISN backbone through at least two circuits, so that NIPRNET and SIPRNET routers won't be cut off if a single link from a router to the network backbone fails.



IDNX Multiplexer

The IDNX multiplexer, produced by N.E.T. Technologies, is widely used in the DISN backbone. Until the introduction of ATM, circuits between IDNX multiplexers (as well as multiplexers from other vendors) formed most of the DISN backbone network. Most of the IDNX multiplexers are used in the DISN backbone, but some are also used on access circuits from customer premises routers.

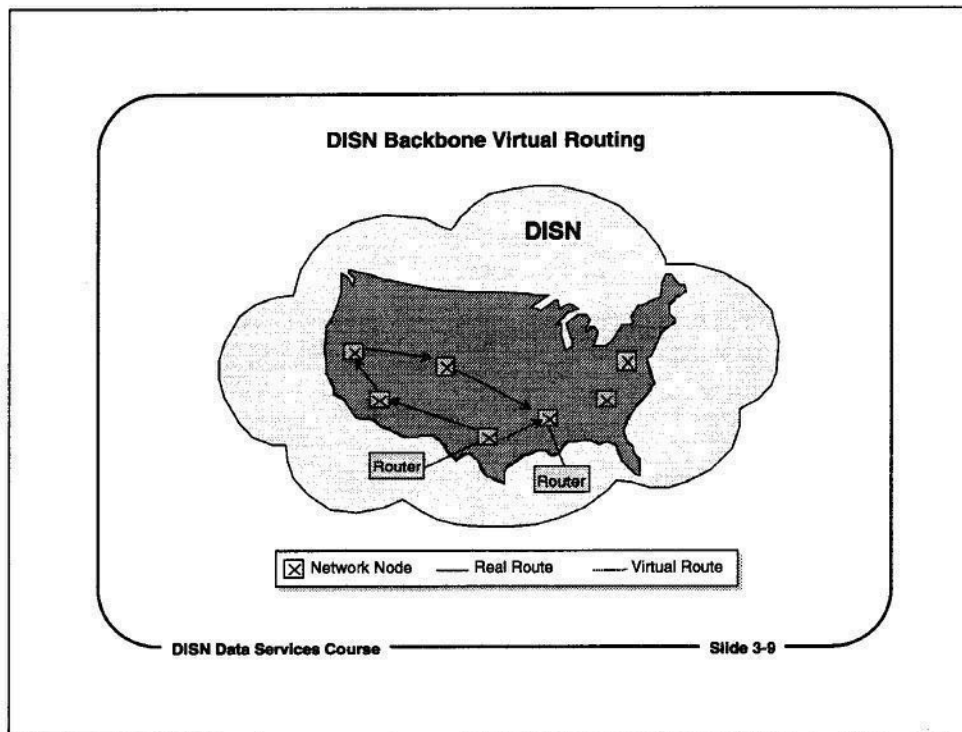
The IDNX is a time-division multiplexer, combining the lower-speed data streams from NIPRNET and SIPRNET routers and legacy host systems over a single, high-speed trunk circuit, such as a T-1 or T-3 circuit. The IDNX multiplexers assign the data from incoming sources to time-multiplexed channels on the circuit. The multiplexers on either side of the circuit coordinate their operations over an in-band control channel.



Subchannel Management

Traffic for each of the DISN Data Services networks is separated from other traffic because the DISN maintains logically separated subchannels for each network across each link. This concept can be implemented through the IDNX as shown in the above figure or through the bandwidth managers on the ATM network.

The JWICS network operates its own set of IDNX multiplexers, which connect into the DISN backbone. JWICS routers and equipment are behind the JWICS IDNX muxes. All of the JWICS equipment is controlled by the Defense Intelligence Agency (DIA), not by DISA. So, DISA provides backbone connectivity for the JWICS network, but DIA controls the JWICS network, its applications, and its interface to the DISN.

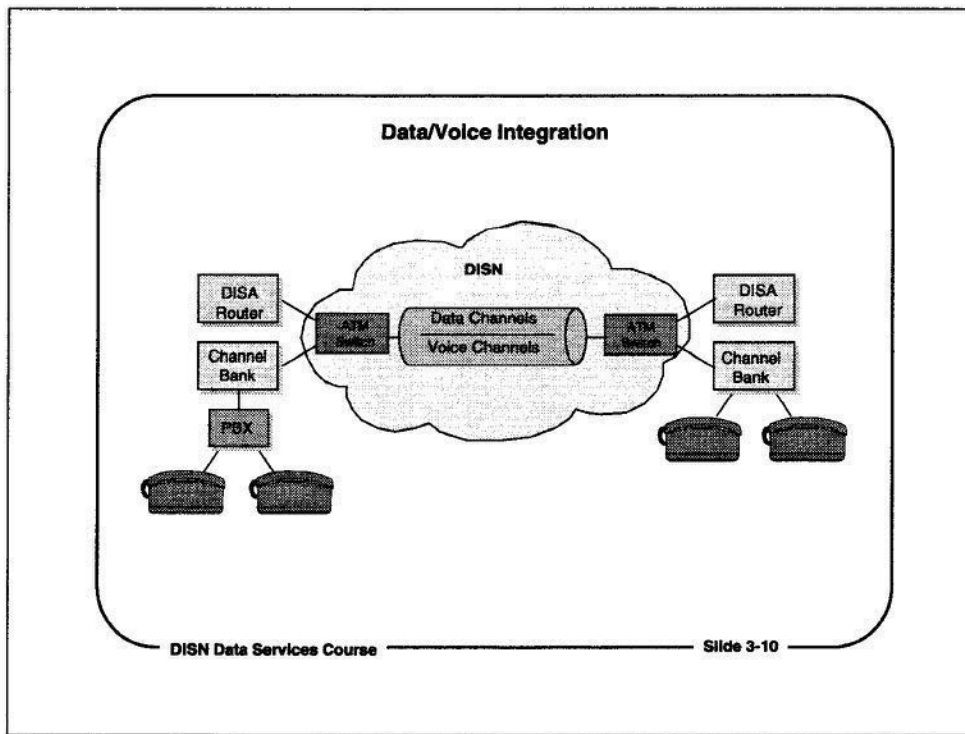


DISN Backbone Virtual Routing

The DISN backbone nodes have dedicated circuits that link them forming the DISN backbone, but the network manages the pathways to determine the best route traffic should take.

For example, even though a direct physical path may exist between two nodes, the network may route traffic through other nodes to get to its destination. The network makes this decision based on circuit bandwidth availability, network delay, cost, network congestion, and other factors.

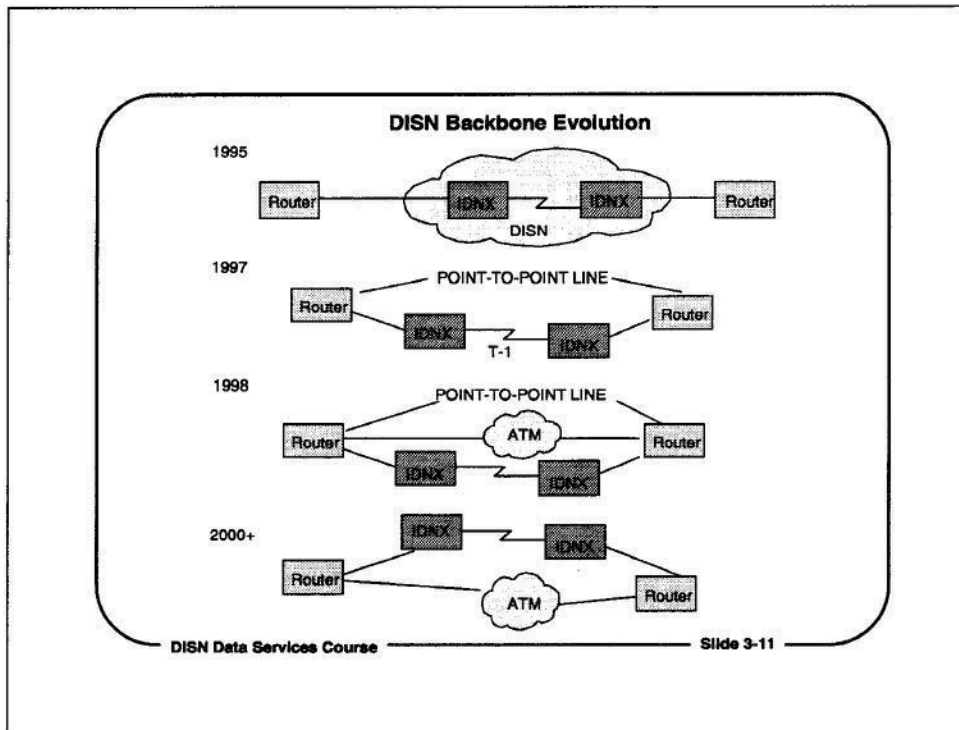
Network routing decisions made by the DISN backbone devices are completely independent of, and transparent to, the routing decisions made by the IP routers.



Data/Voice Integration

The DISN backbone can be used for a variety of applications. DISA subscribers use the DISN digital backbone for voice, video and data applications. Either the IDNX multiplexer network or the new ATM backbone network can carry data, voice, and video services, because the network carries any type of information in digital format.

In CONUS, the DISN ATM backbone carries data and video traffic. In Europe and in the Pacific, the ATM backbone carries both data and voice traffic.



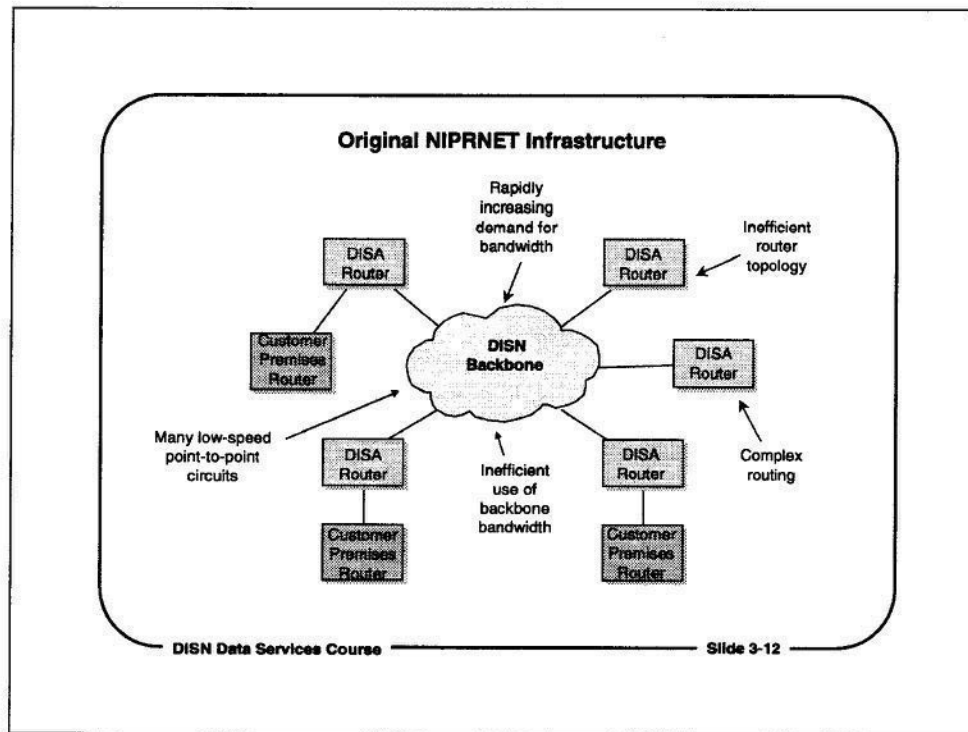
DISN Backbone Evolution

The DISN backbone has evolved in the past few years from a network based on IDNX multiplexer circuits to its present composition as a mixed network of IDNX multiplexers, point-to-point circuits, and an ATM network.

The IDNX network was originally the AFnet IDNX backbone. DISA capitalized the AFnet IDNX network when it started the transition from the old Defense Data Network (DDN).

In 1995, DISA installed a number of point-to-point circuits to augment the IDNX network, and to provide high-bandwidth connectivity between high-volume DISN Data Services network subscribers. Today, the DISN backbone still has a number of IDNX multiplexers. However, parts of the IDNX multiplexer network has been replaced by high-speed point-to-point circuits, or by the new ATM backbone network.

DISA is in the process of transitioning the DISN backbone so that it relies primarily on ATM, but the full transition will take several years.



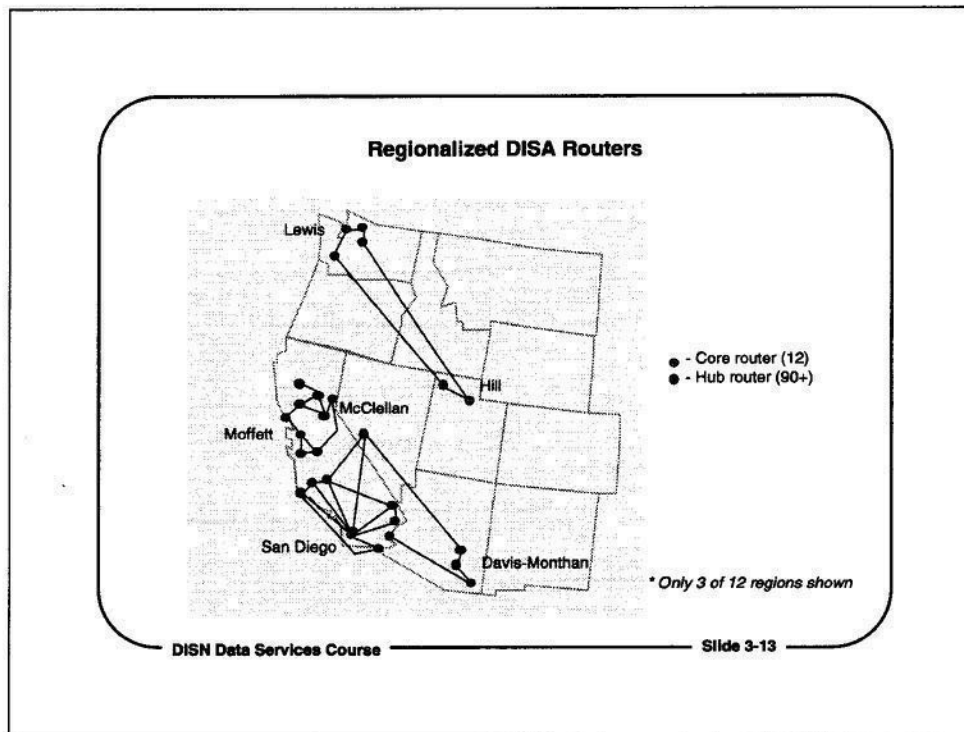
Original NIPRNET Infrastructure

The infrastructure of the original NIPRNET has proved to be inadequate to meet the needs of NIPRNET customers. To improve service to its subscribers, DISA is reorganizing the topology of the DISN Data Services networks and the structure of the DISN backbone network. When this change is completed, much of the DISA router topology will be reorganized, and the DISN backbone will include ATM.

In undertaking this change, DISA is trying to solve the following problems:

- Inadequate backbone bandwidth
- Inefficient router topology
- Complex routing paths
- Many low-speed point-to-point backbone circuits

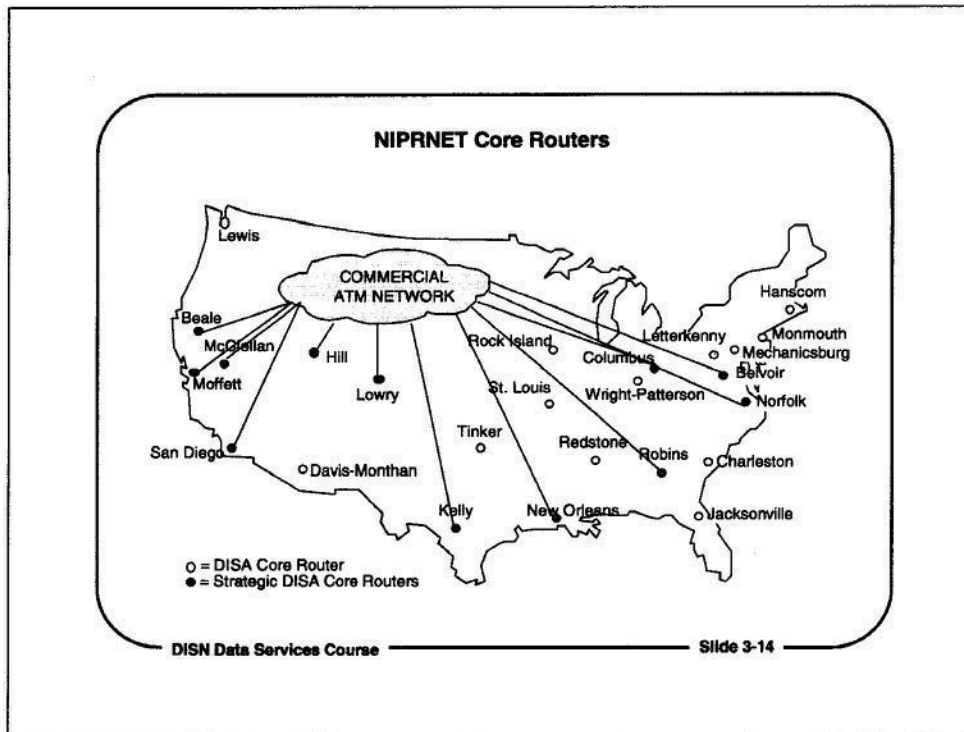
Initially, these changes will affect the CONUS NIPRNET only. In the future, the same changes will be made to the NIPRNET in Europe and the Pacific, as well as to the SIPRNET.



Regionalized DISA Routers

To make the topology of the NIPRNET routers more efficient, DISA re-organized the DISA NIPRNET routers in CONUS into twelve regions. Each region serves DoD installations in a specific geographic area. Each region has two routers designated as Core routers. The other DISA routers have been designated Hub routers.

Customer premise routers, hosts, and other networks connect to Hub routers. The Hub routers connect to both Core routers in the region through dedicated, high-speed circuits.

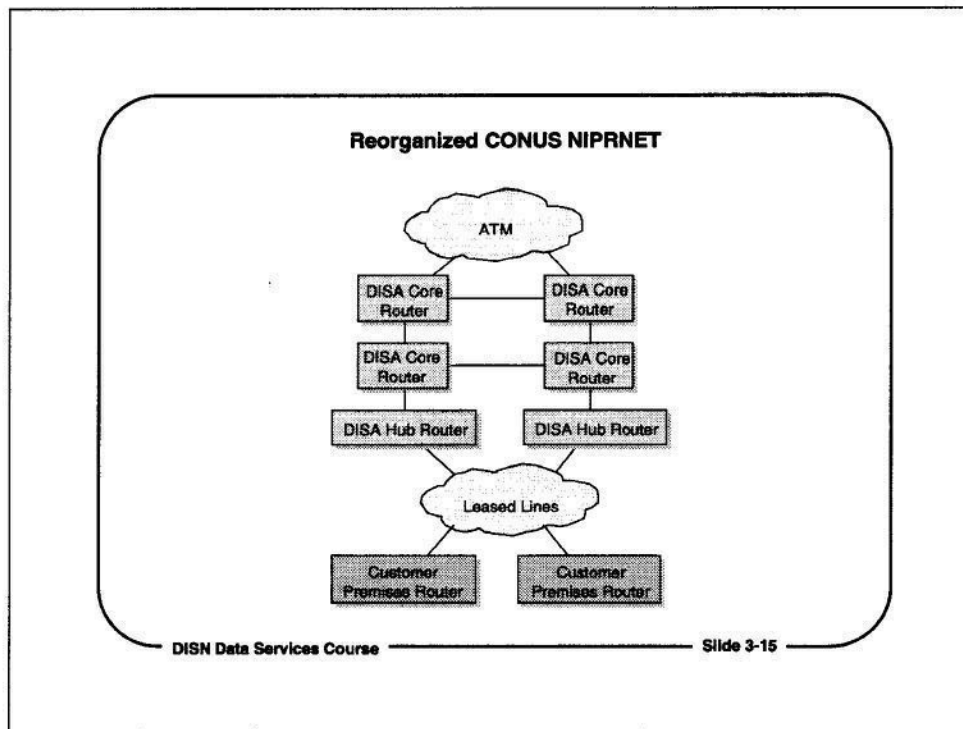


NIPRNET Core Routers

The Core routers in CONUS are connected to each other with double T-1 circuits, or with T-3 circuits. Each Core router is connected to two or more other Core routers. Core routers tie each of the regions together.

Some Core routers in CONUS were also connected together by the high-speed ATM network. More core routers will be deployed in the future based on the requirements for higher bandwidth.

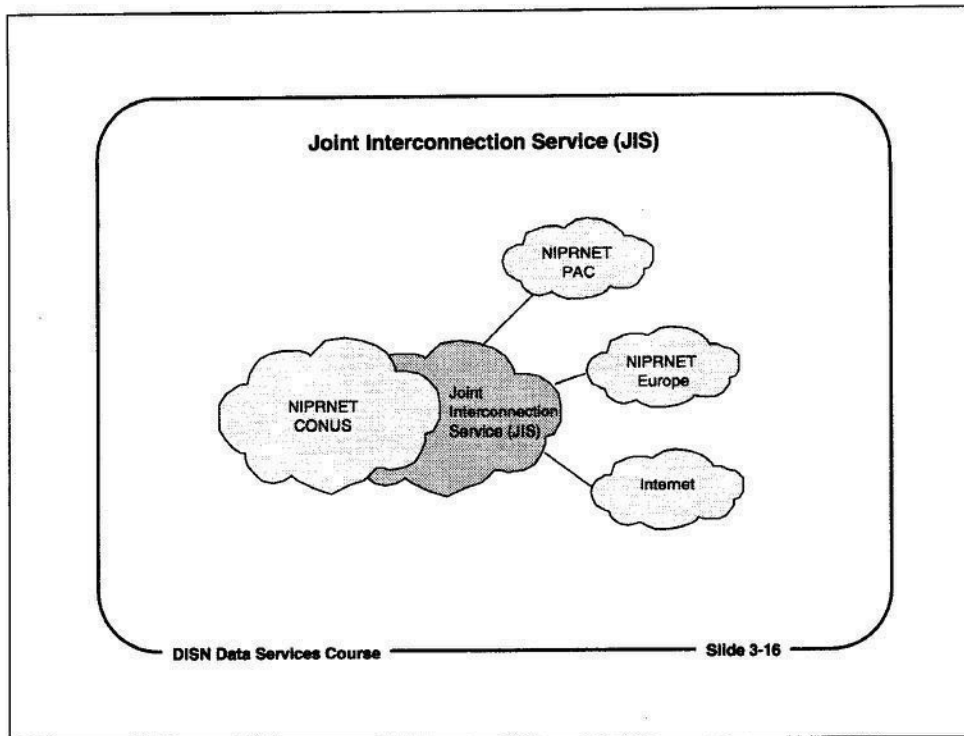
DISA has also extended the ATM backbone to Europe and the Pacific, as well as to the SIPRNET.



Reorganized CONUS NIPRNET

There are two levels of DISA routers. The Hub routers have T-1 or T-3 links to the Core routers, and the Core routers have either double T-1s, a T-3, or the ATM network between them.

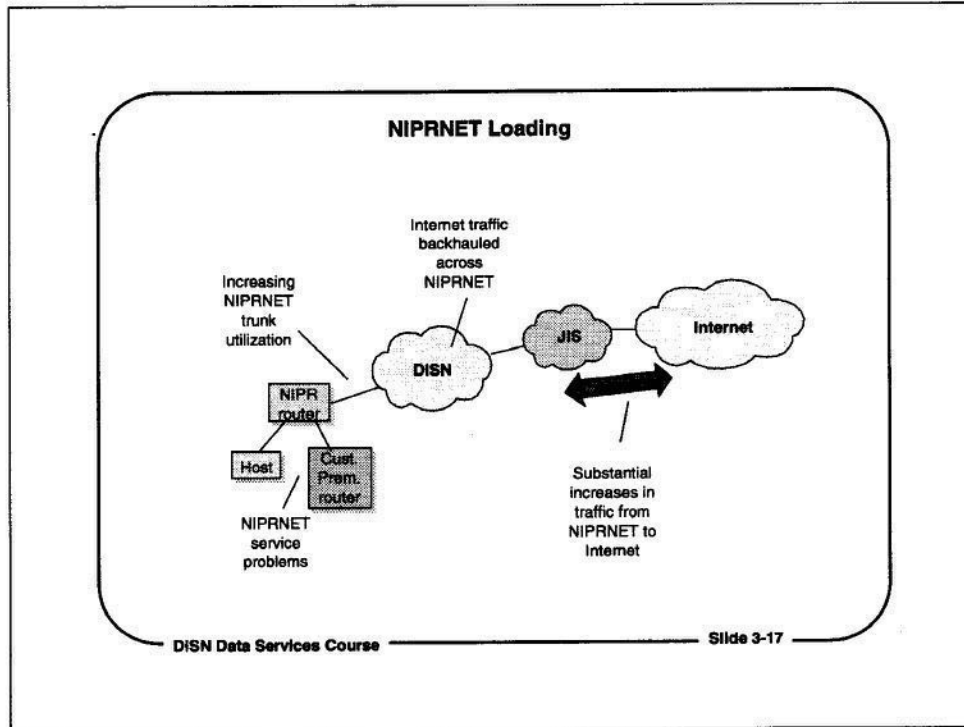
The IDNX multiplexer network will eventually be replaced by the ATM backbone, but IDNX multiplexers are still widely used in the DISN backbone.



Joint Interconnection Service (JIS)

DISA also established a second high-speed network, the Joint Interconnection Service (JIS), to interconnect the CONUS NIPRNET with the NIPRNET networks in Europe and the Pacific. The JIS also connects the NIPRNET with the Internet, as well as with other DoD networks.

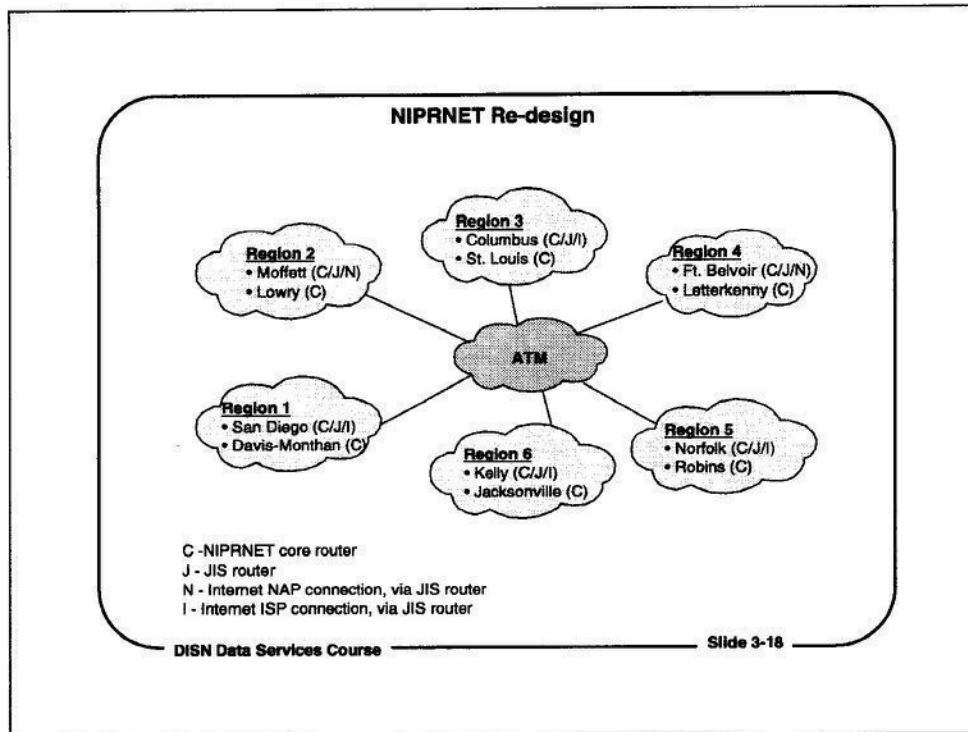
The JIS is a separate network of six DISA routers. These six JIS routers are interconnected over a high-speed ATM network running at 155 Mb. Five of the JIS routers are connected to the NIPRNET Core routers through the DISN ATM backbone.



NIPRNET Loading

The changes that were made in the first reorganization of the NIPRNET, which was completed in 1998, improved service somewhat, but traffic on the NIPRNET and the DISN backbone continued to grow. A substantial and growing part of the bandwidth on the DISN backbone was being consumed to handle traffic going to and from the Internet, and utilization of some of the DISN backbone circuits was approaching saturation.

To solve these problems, and to improve service for NIPRNET customers, DISA began a second re-organization of the DISN backbone and the NIPRNET in 1999.

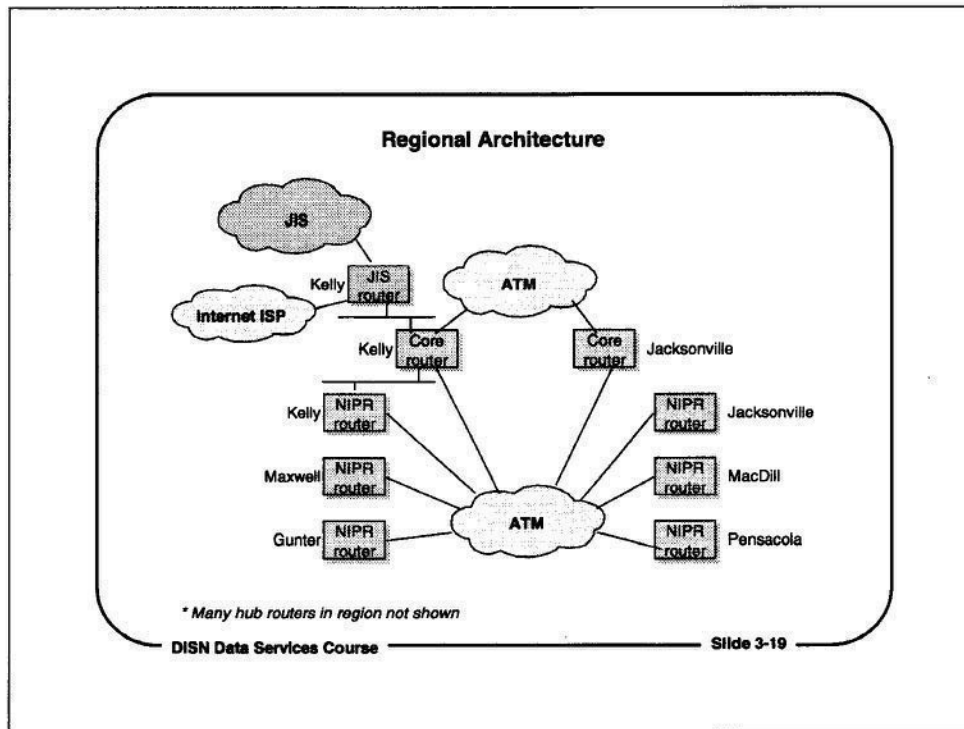


NIPRNET Re-design

To meet rising demand for NIPRNET services, DISA has started a second re-design phase of both the router and the ATM WAN connectivity of the CONUS NIPRNET. The changes that are being made are:

- Reorganize the twelve CONUS NIPRNET router regions into six router regions.
- Give each region a dedicated connection to a JIS router.
- Give each region a direct connection to an Internet exchange point, or to an Internet Service Provider (ISP).
- Create a two-level router hierarchy in each region, to bring the hub routers closer to the core routers.

The second re-design is scheduled to be completed by the end of 2000.

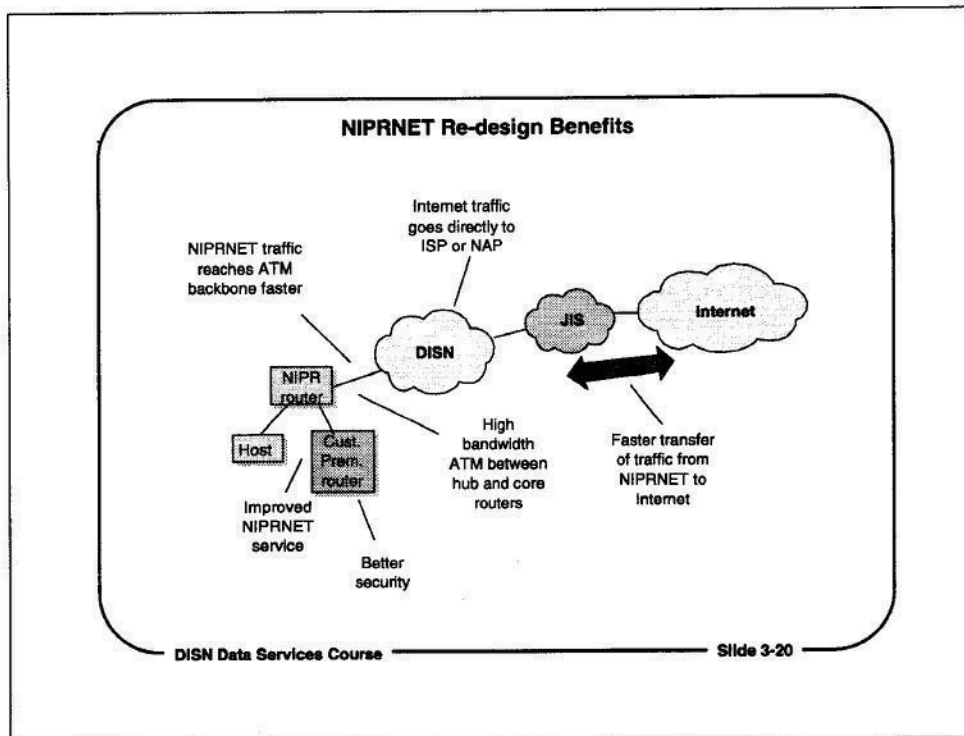


Regional Architecture

To improve NIPRNET service within each region, the following changes will be made to the NIPRNET router connections in each region:

- Each of the hub routers will be linked directly to the ATM backbone, and be part of a region-wide Emulated LAN (ELAN).
- The two core routers in each region will be part of a second ELAN on the ATM backbone, which will link the core routers in each region together.
- Each region will have its own JIS router (for Internet and NIPRNET Pacific and NIPRNET Europe connectivity), which will be reached through one of the two core routers in the region.

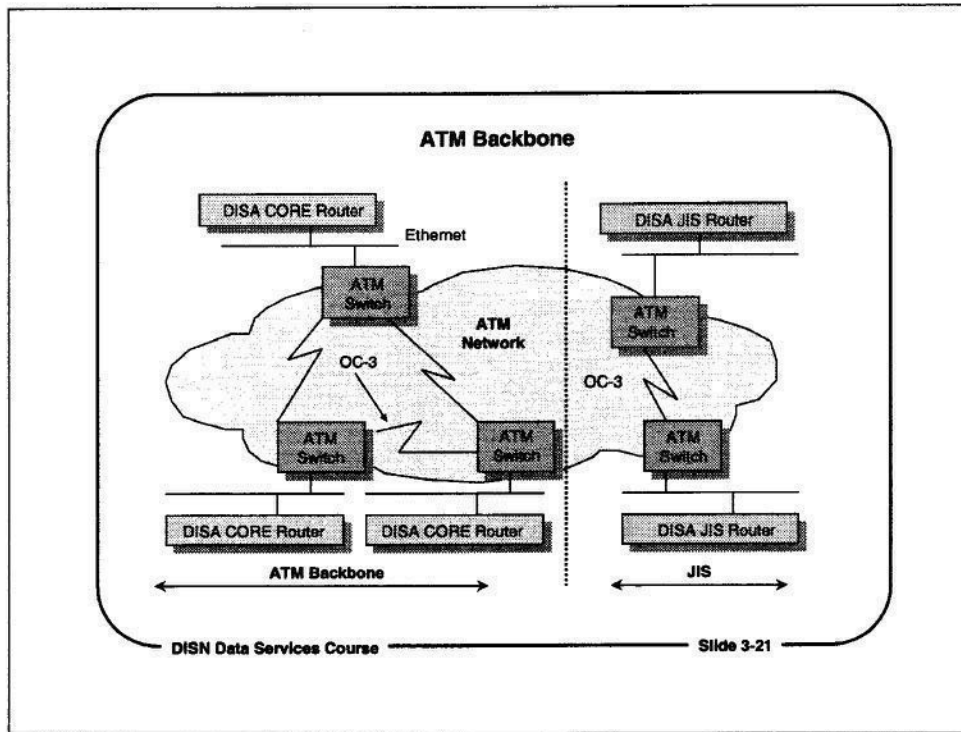
Regions that do not have direct connectivity to an Internet exchange point through a JIS router will be connected to a commercial ISP, to improve Internet access.



NIPRNET Re-design Benefits

DISA hopes to achieve the following benefits from reorganizing the CONUS NIPRNET routers:

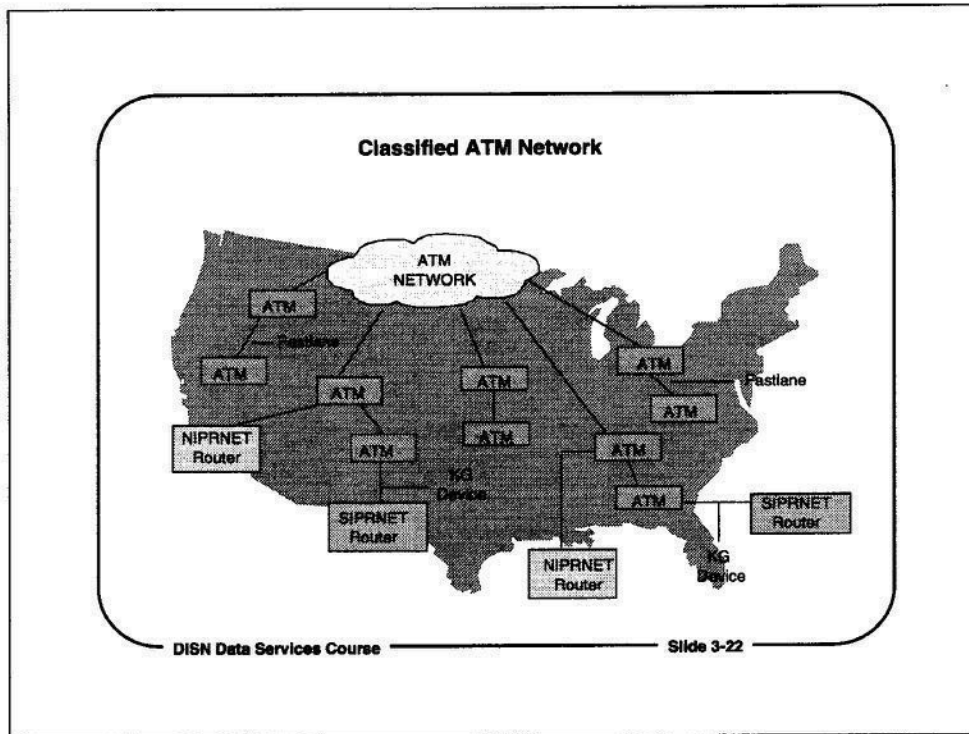
- Bring NIPRNET subscribers closer to the high-bandwidth ATM backbone
- Reduce delays in passing Internet traffic from a hub router to the Internet
- Reduce the amount of Internet traffic backhauled over the NIPRNET to an Internet access point
- Improve NIPRNET security, by reducing the need for backdoor ISP connections
- Improve the performance and reliability of NIPRNET core routers and ATM switches



ATM Backbone

Although they are considered to be separate networks, the DISN ATM network that serves the NIPRNET DISN and the Joint Interconnection Service (JIS) network are the same ATM network.

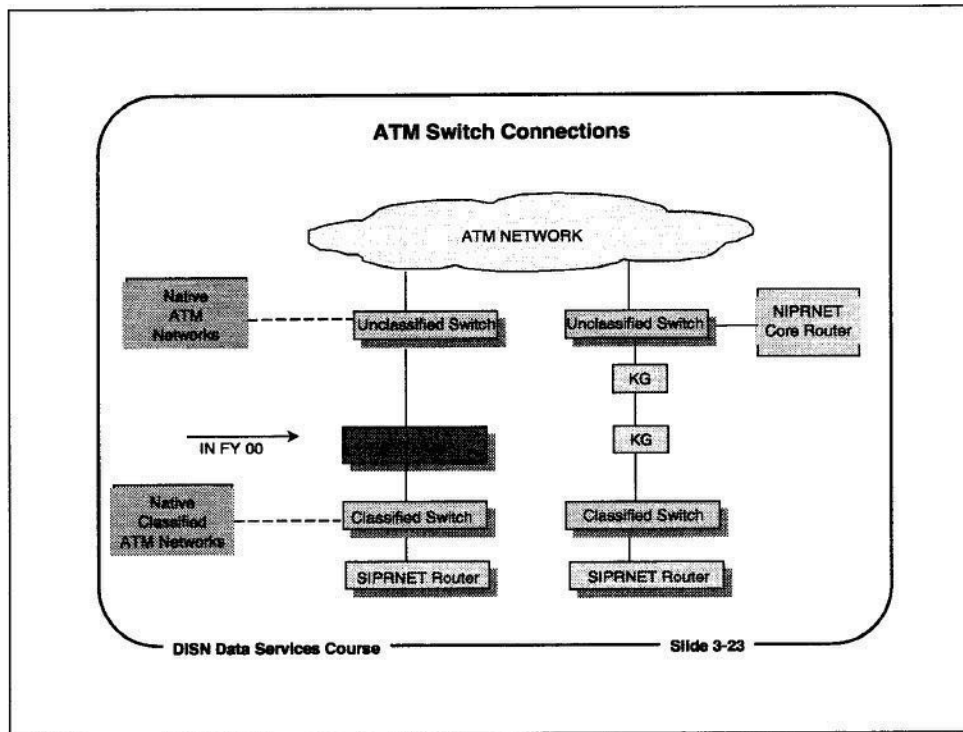
However, the Core routers on the CONUS NIPRNET and the routers on the JIS serve different purposes. Consequently, the ATM backbone network is partitioned into two separate logical networks.



Classified ATM Network

The classified DISN ATM network is a separate network of ATM switches used for high-speed interconnectivity for SIPRNET systems. This secure network uses point-to-point encryption but it will use FASTLANE encryption devices in the future to encrypt the data portions of each cell.

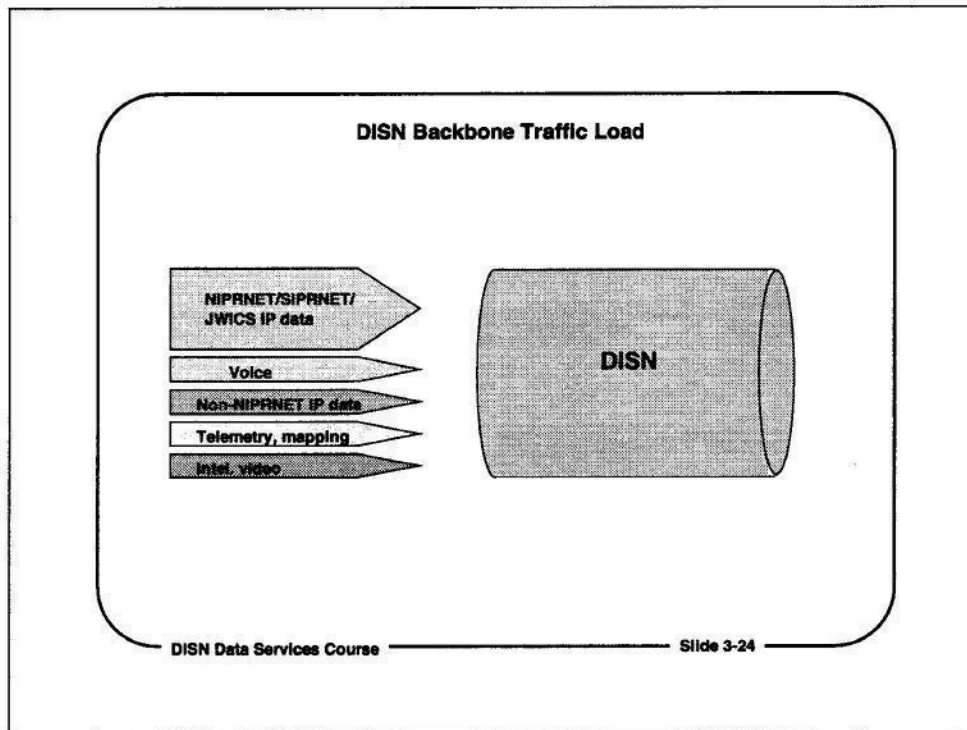
In the next phase of network reorganization and consolidation, the classified ATM network, which has been taken from the Leading Edge Service (LES) network, will become part of the new backbone network for the SIPRNET.



ATM Switch Connections

The unclassified ATM switches connect to a commercial ATM cloud in CONUS, and to a dedicated ATM network in The Pacific and Europe. Most of the classified ATM switches connect to the ATM network through unclassified ATM switches, but some connect directly to the commercial ATM network.

The top-level NIPRNET Core routers connect directly to the unclassified ATM switches, while SIPRNET routers connect to the classified ATM switches. Native ATM networks, such as base or area-wide ATM networks, may be permitted to connect directly to the unclassified or classified ATM switches at some time in the future.

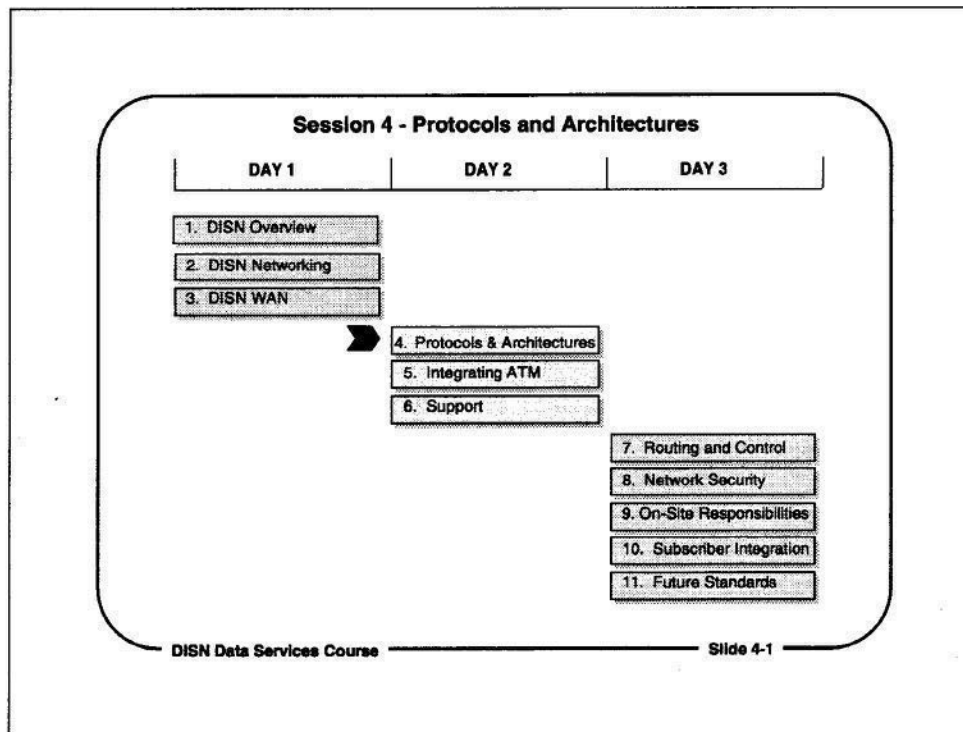


DISN Backbone Traffic Load

While the majority of the traffic on the DISN backbone is IP data traffic (NIPRNET, SIPRNET, and JWICS), the DISN network also serves a number of other purposes. Extra capacity has been engineered into the DISN backbone, so that it has the bandwidth necessary to carry these other applications, which include:

- Legacy system data
- Non-NIPRNET/SIPRNET IP data (e.g. Tricare)
- Video (e.g., DIA)
- Telemetry and mapping data
- Voice

Some kinds of traffic are only carried within certain theaters. For example, the DISN backbone carries voice in Europe, but today, only a small amount of voice traffic is carried on the DISN in CONUS. This situation may change in the future when more DoD traffic is moved to the DISN.

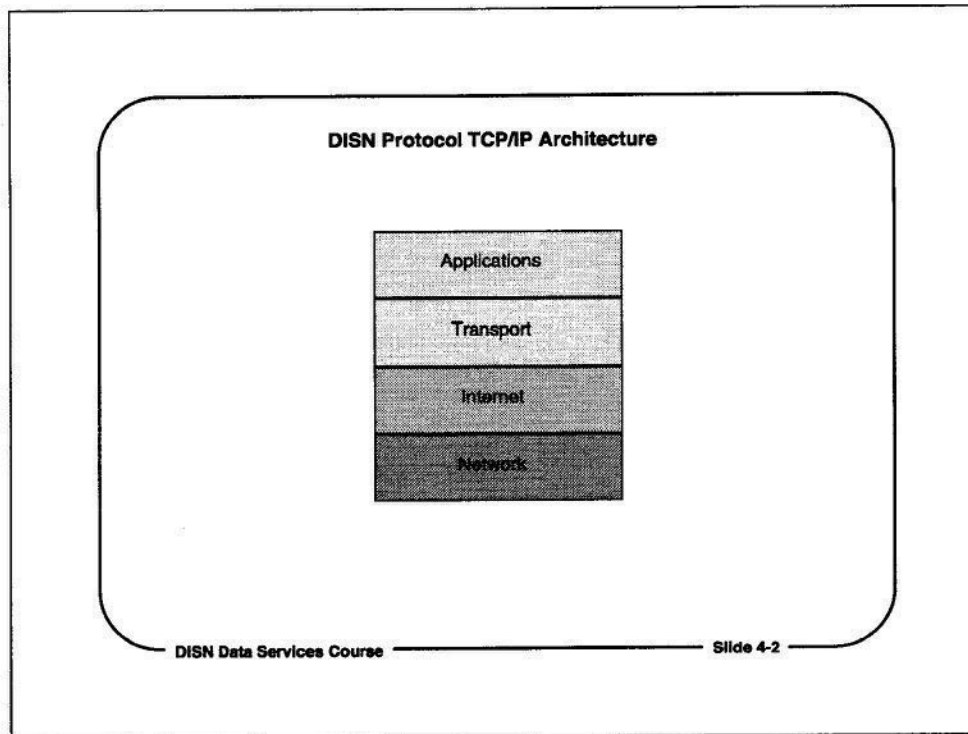


Session 4 - Protocols and Architectures

Upon completion of this module, the students will have a general understanding of network protocols and architectures that will provide them with a consistent framework for understanding the issues involved in connecting to the DISN data services networks. In addition, the students will be able to understand the level of computer interoperability required in DoD systems, in order to implement systems that meet these requirements.

This session will focus on:

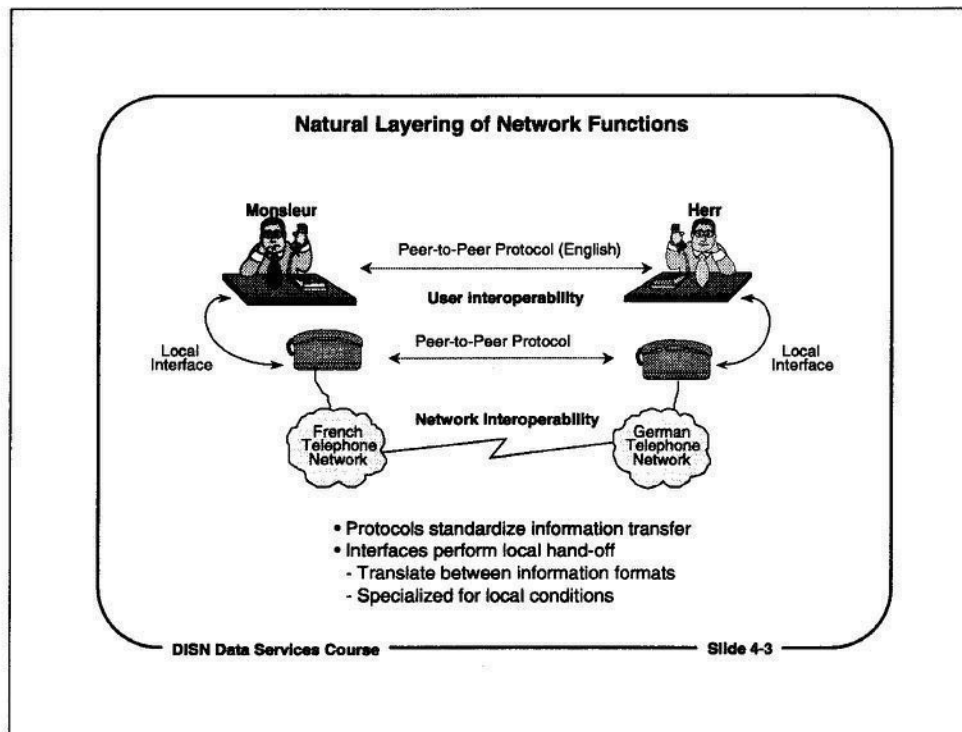
1. Describing the DoD TCP/IP protocol architecture
2. Describing protocol layering
3. Identifying the functions of the protocols used in the DoD protocol architecture
4. Expressing the benefits of applications protocols
5. Describing IP address types
6. Describing methods for network address resolution



DISN Protocol TCP/IP Architecture

The four components of the DISN Data Services network architecture are:

- **Application** - An end-user service or capability
- **Transport** - Reliable, end-to-end connection-oriented data transfer service
- **Internet** - An addressing and data routing scheme between networks and hosts on the internetwork
- **Network** - Physical interfaces and communications paths that carry bits across a network.



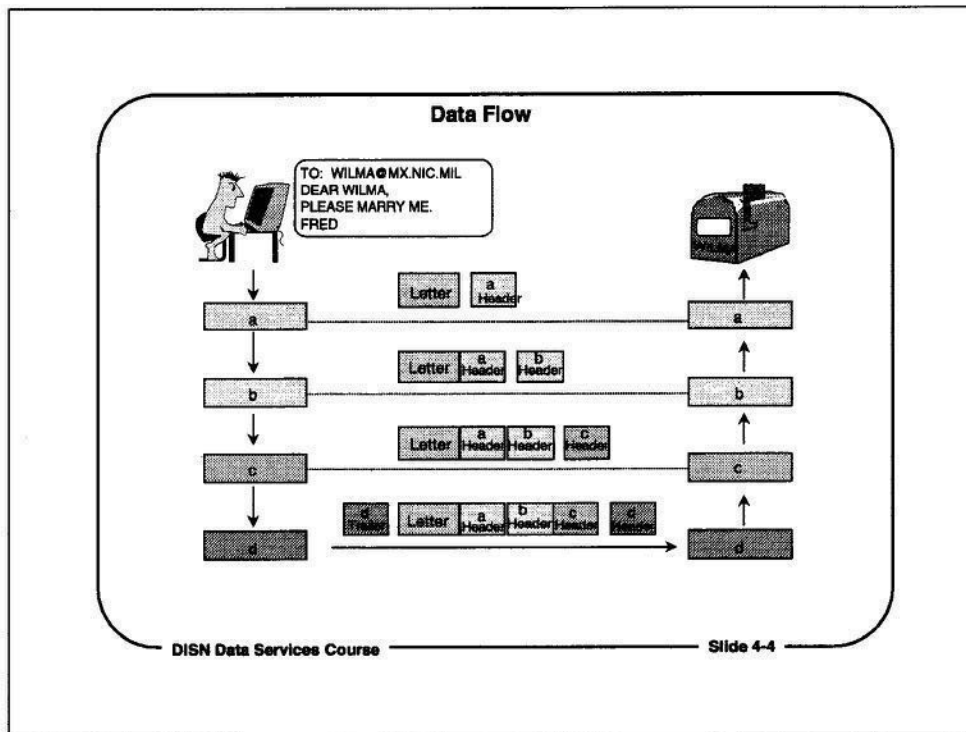
Layered Network Functions

Definitions:

- A peer process is a functionally equivalent process.
- A protocol is a set of rules and format specifications with which peer processes can effectively transfer information.
- An interface is a set of rules and format specifications with which non-peer processes hand information across functional boundaries through local coupling.

Functions:

- | | |
|--------------------------------|---------------------|
| • Synchronization | • Flow control |
| • Error detection | • Multiplexing |
| • Correction by retransmission | • Call set-up |
| • Transparency | • Call clearing |
| • Sequencing | • In-band signaling |
| • Accounting | • Addressing |



Data Flow

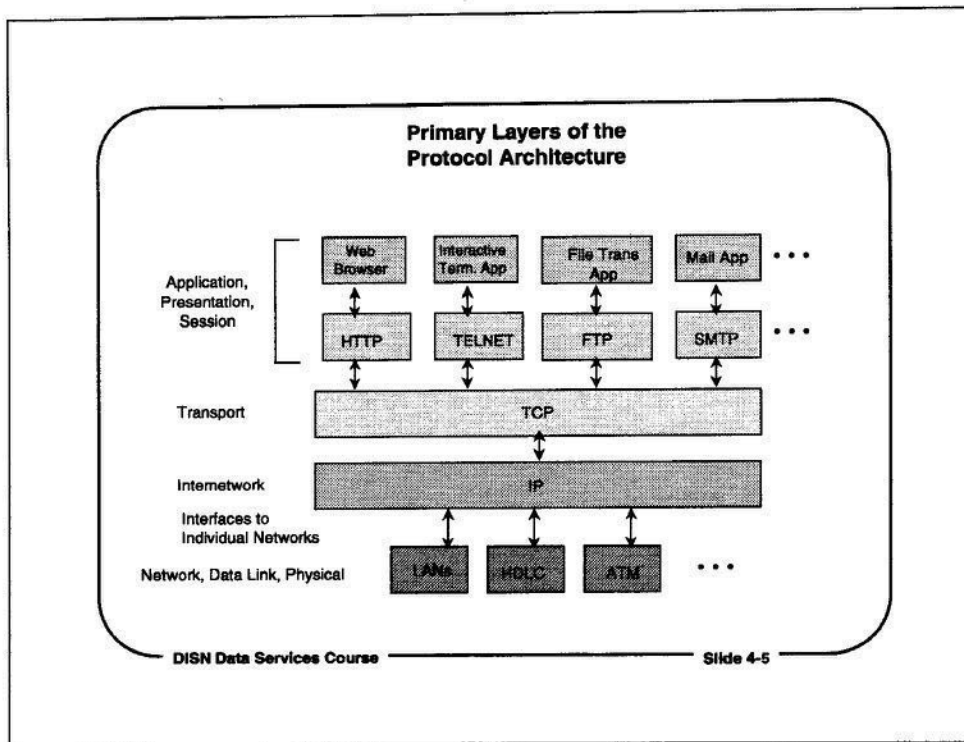
Each message moves through the network architecture to provide for end-to-end communication.

At the source:

- Each layer receives data from the layer above and considers it a sealed package to be sent through the network without regard to its contents.
- Each layer adds some control information such as an address, sequence number, byte count, error checking information, etc., by attaching a header and/or trailer to the data and passing this to the layer below. The layer below considers this to be a sealed package to be sent through the network.

At the destination:

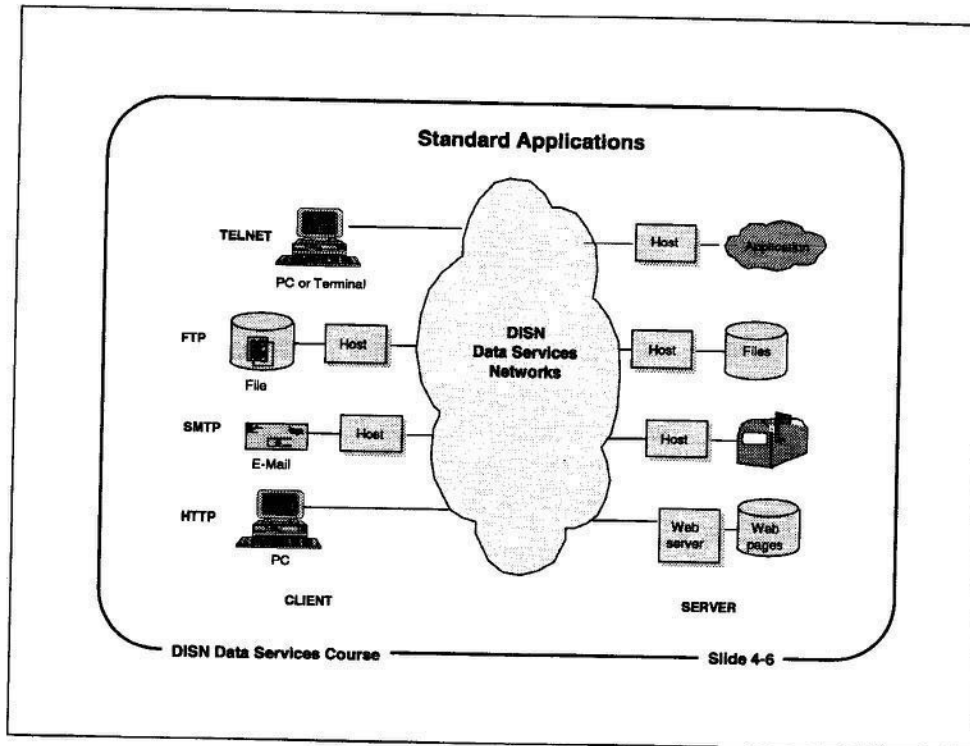
- Each layer receives the sealed package of data from the layer below, strips off the header and/or trailer of control information sent to it by its peer layer at the source, and passes the remaining package to the layer above.
- Thus, two peer layers communicate by means of attached headers and trailers. The format and content of a header/trailer is specified by a layer's protocol.
- The last layer strips off the last header and trailer and reproduces the data as it was sent.



Primary Layers of the Protocol Architecture

The DoD protocol architecture supports many different protocols, but the primary protocols are those in the TCP/IP protocol suite. This diagram depicts the parts of the DoD protocol architecture that are relevant to the users of the DISN Data Services networks.

The DoD protocol architecture follows widely-accepted protocol layering conventions. End-user applications are at the highest layers of the protocol suite, and network transport protocols, such as LAN protocols and the HDLC data link control protocol, are at the lowest layers of the protocol suite. The transport and internetwork protocols assure reliable delivery of data to specific network addresses.

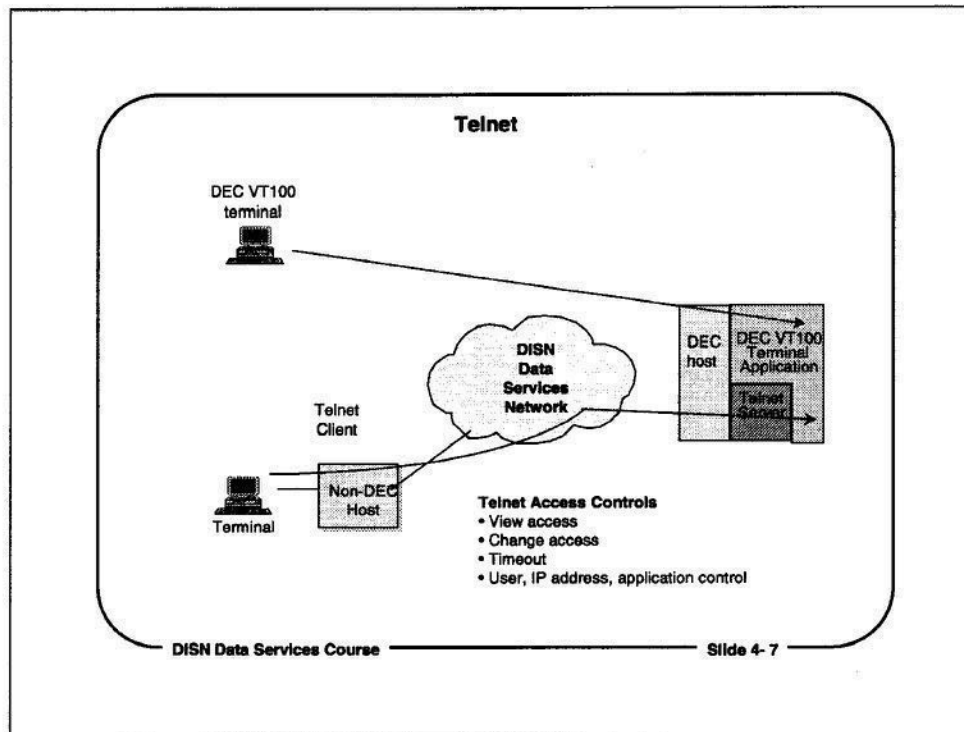


Standard Applications

The standard applications-layer protocols used in DISN Data Services networks, and the functions they support, are:

- Telnet - a virtual terminal service for accessing host applications as an interactive, on-line terminal
- File Transfer Protocol (FTP) - Protocol for transferring files from one host to another
- Simple Mail Transfer Protocol (SMTP) - Protocol for sending and receiving e-mail messages.
- HyperText Transfer Protocol (HTTP) - Protocol for Web site browsing

These applications may be used from the windowed interface or the command line of a PC or terminal, or they may be hidden beneath other applications that use the capabilities of Telnet, FTP, HTTP, and SMTP.

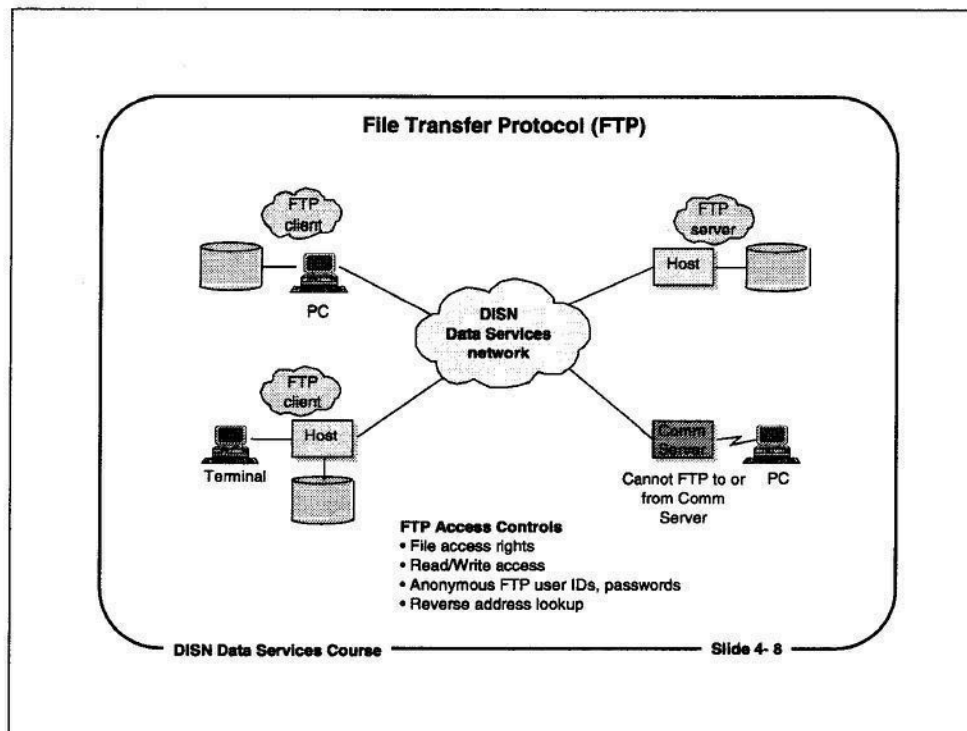


Telnet

Telnet is a virtual terminal protocol. It lets a user access applications on another host computer system on the network, without requiring the user to have the type of terminal that is normally used by that host.

Telnet eliminates the need for terminals or PCs to emulate all of the operational characteristics of the specific terminal types with which hosts normally communicate.

A standard Telnet session may not incorporate terminal-specific functions, such as screen colors, cursor blink, protected fields, etc.. It is divided into Client and Server operations. A PC running a Telnet Client session can communicate with a host running a Telnet Server session.



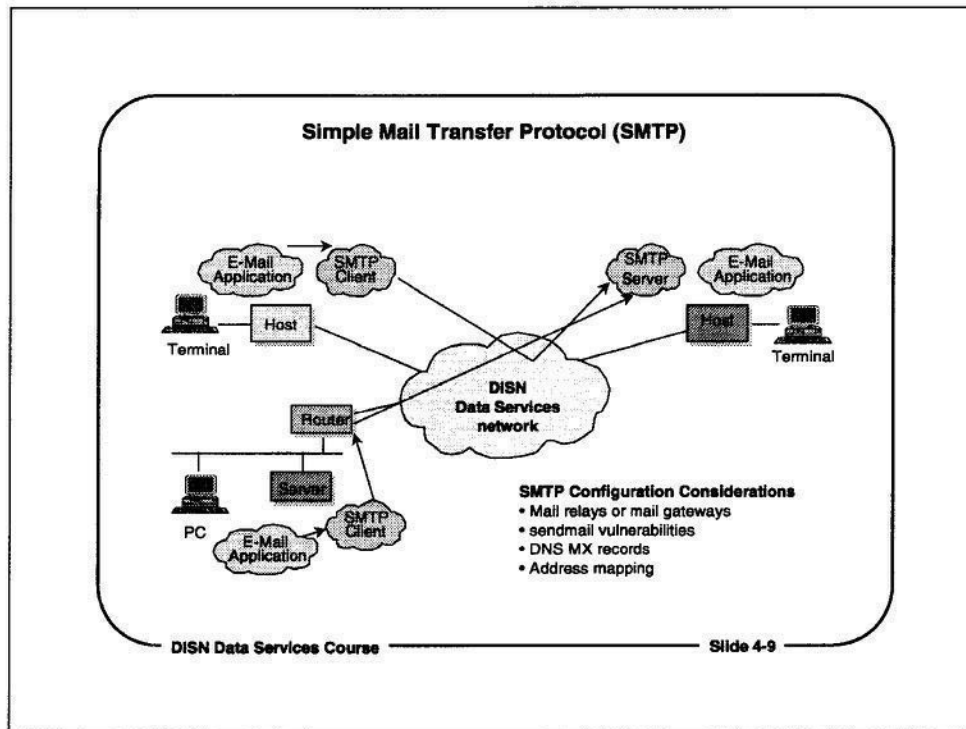
File Transfer Protocol (FTP)

FTP lets a user access files on another host computer system on the network, without requiring the user to be connected directly to that host.

Anonymous FTP sessions are accepted by most hosts, so that FTP users don't need specific user accounts to access files. Anyone who can establish an FTP session can FTP to or from the host.

A user who accesses the network from a Comm Server can FTP from one host to another, but not to the Comm Server.

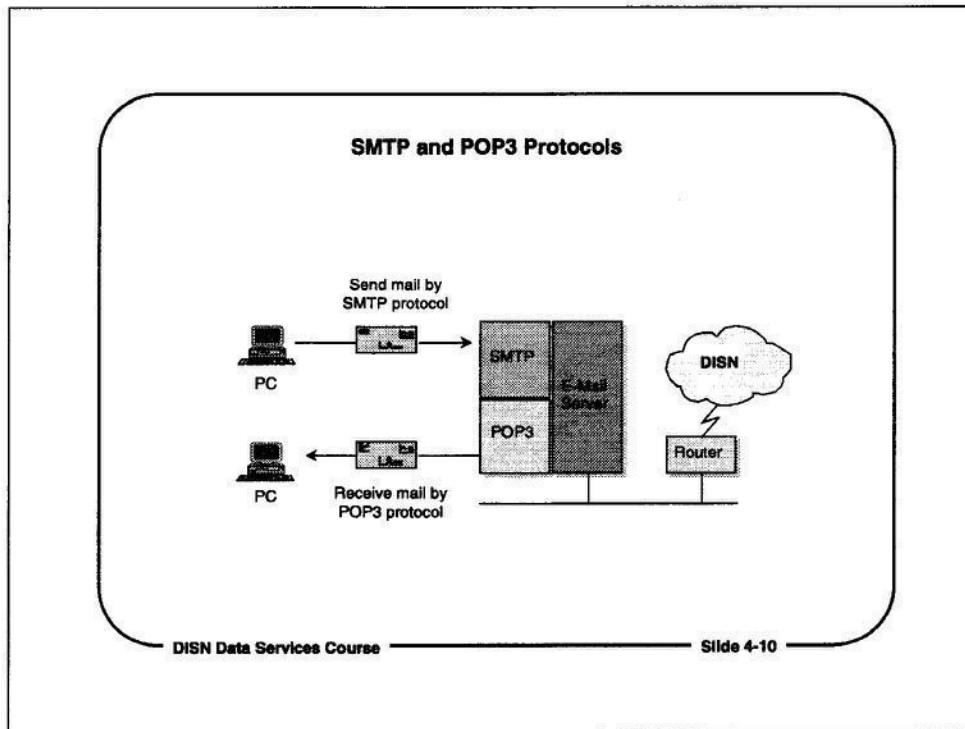
An FTP session is divided into Client and Server operations. A host must first be running an FTP Server process before a Client FTP session can be established to it.



Simple Mail Transfer Protocol (SMTP)

SMTP is a protocol for delivering e-mail messages between hosts that run e-mail. SMTP is a mechanism to deliver mail. The SMTP Client delivers mail to an SMTP-compliant POP (Post Office Protocol) server, which is responsible for delivering mail, when polled by an SMTP client. SMTP is not an e-mail editor or viewer. It only delivers mail.

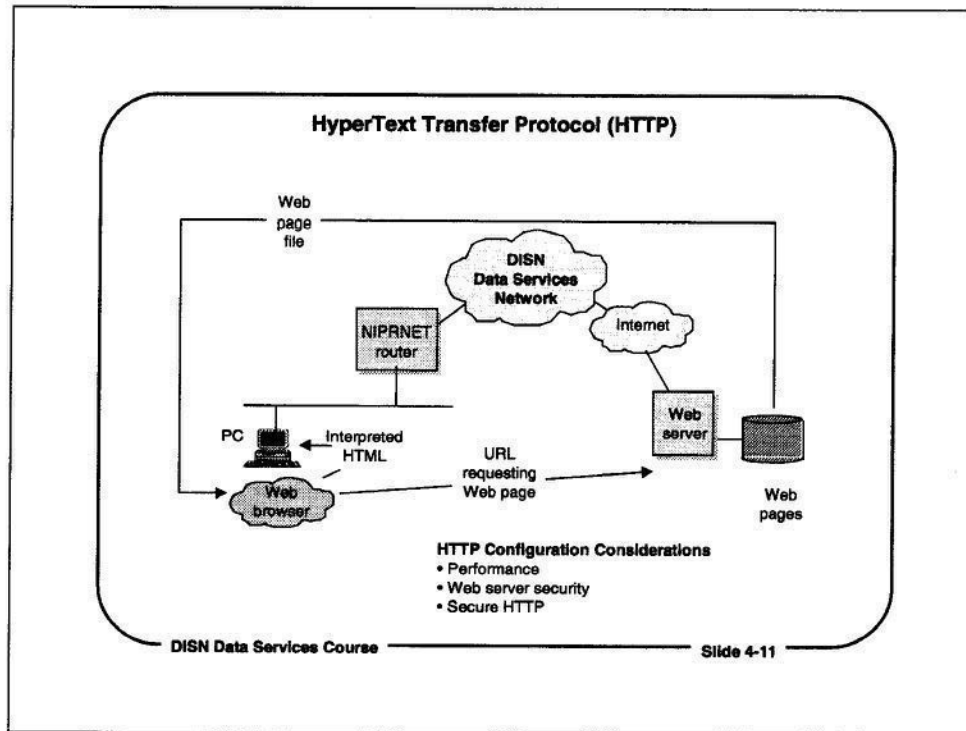
SMTP makes its best attempt to deliver e-mail to a destination that can either deliver it to the recipient's mailbox, or forward it to its eventual destination.



SMTP and POP3 Protocols

The SMTP protocol transfers mail between e-mail hosts. It is also used by e-mail application programs to submit mail to an e-mail host for delivery.

Many client e-mail applications use another protocol, Version 3 of the Post Office Protocol (POP3), to retrieve e-mail from an e-mail host. If the client application uses POP3 to retrieve mail, the e-mail server must be running a POP3 server process.

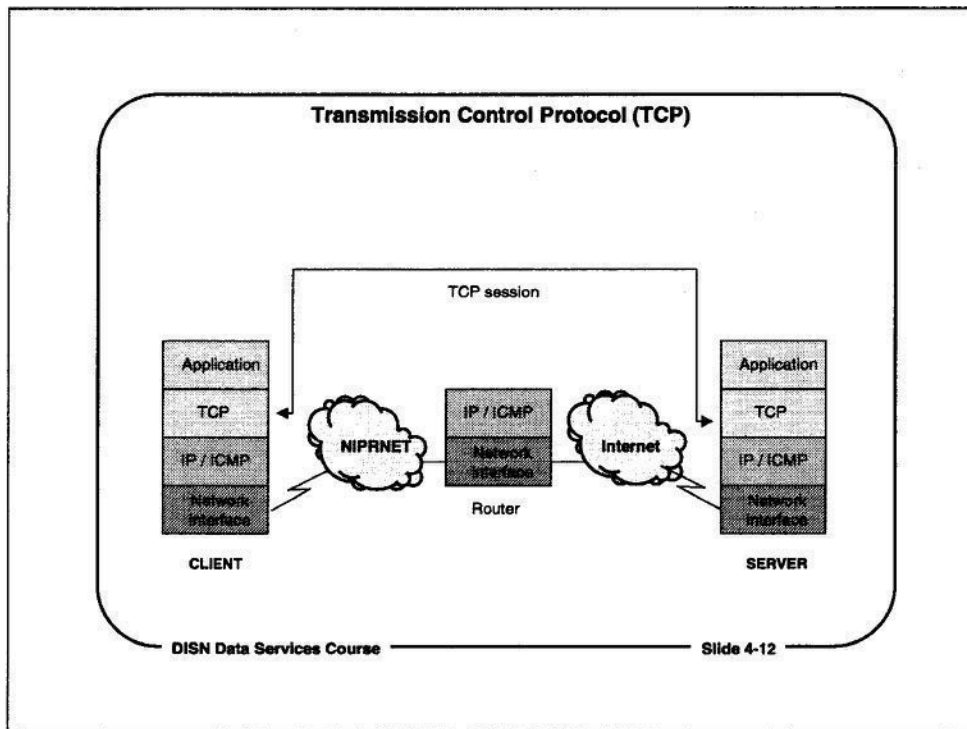


HyperText Transfer Protocol (HTTP)

While it is not one of the traditional TCP/IP applications, the widespread use of the Internet has made the HyperText Transfer protocol (HTTP) a de facto standard applications protocol.

HTTP works like a file transfer protocol, using Uniform Resource Locators (URLs) entered in a Web browser to specify files to be transferred from a Web server. HTTP also handles embedded file transfer requests, in that a single Web page may contain links to graphics, Java applets, or other programs that must also be transferred along with the base Web page.

The client side of the HTTP protocol is a Web browser. In addition to providing a user interface, the Web browser also interprets Web page HTML for display.



Transmission Control Protocol (TCP)

Introduction:

- TCP guarantees delivery of message and protects against duplicate segments
- TCP is a connection-oriented process
- TCP complements IP to provide a reliable connection.

Description:

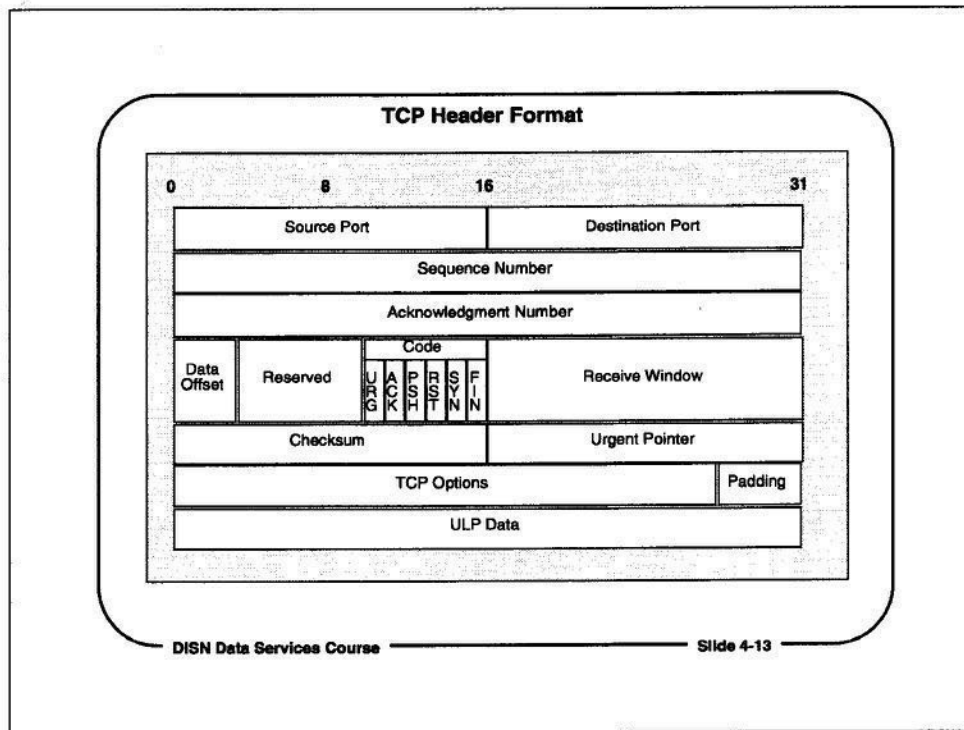
- Provides reliable interprocess communication between pairs of processes in hosts
- Responsible for flow control, sequencing, reliability and host-to-host services
- Interfaces to user application process on one side and to a lower level protocol such as IP, on the other side.

Reliability:

- Capable of recovering from data that is damaged, lost, duplicated, or delivered out of order.

Flow Control:

- The receiver must be able to control the amount of data being sent to it by the sender so it does not get overloaded. The receiver uses a "window" to indicate an allowed number of bytes the sender may transmit.



TCP Header Format

Source Port = Identifies TCP port number that identifies the application program at the client

Destination Port = Identifies TCP port number that identifies the application program at the server

Sequence Number = Identifies position of the segment in the sender's byte stream

Acknowledgment Number = Identifies position of the highest byte the source has received

Data Offset = Specifies data offset of the segment

Reserved = For future use

Code = Used to determine purpose and control of segment

Receive Window = Specifies how much data the recipient can accept

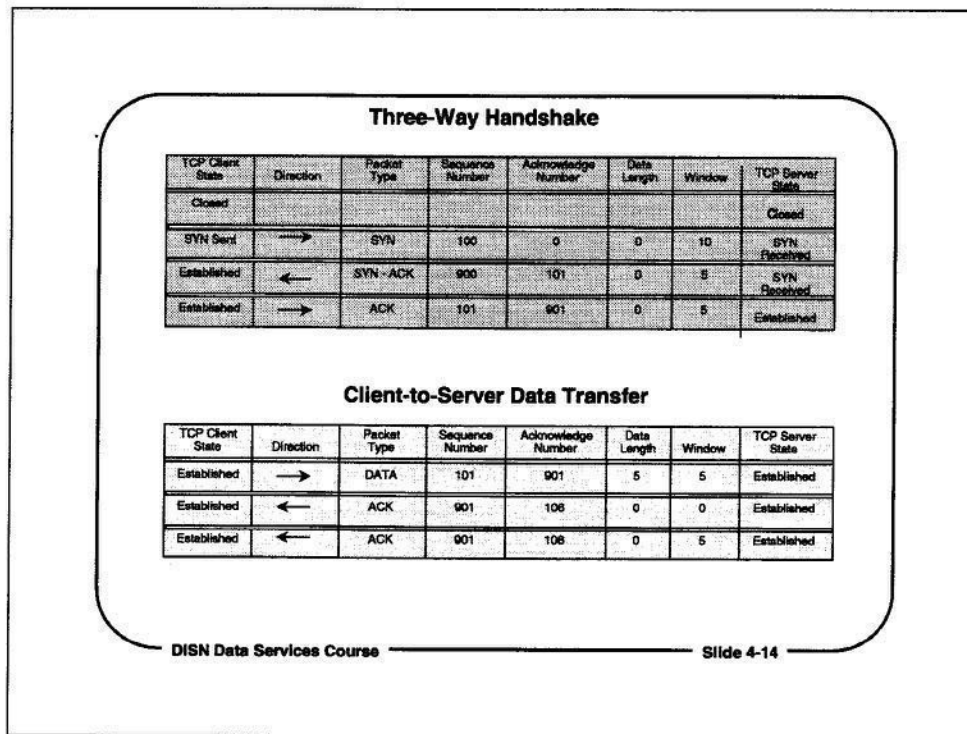
Checksum = Used to verify the integrity of TCP segment header as well as the data

Urgent Pointer = Identifies data as urgent (e.g., keyboard interrupt)

TCP Option = Used to communicate options during pre-session negotiations

Padding = Used to ensure header is an exact multiple of 32 bits

ULP Data = Data supplied by application program

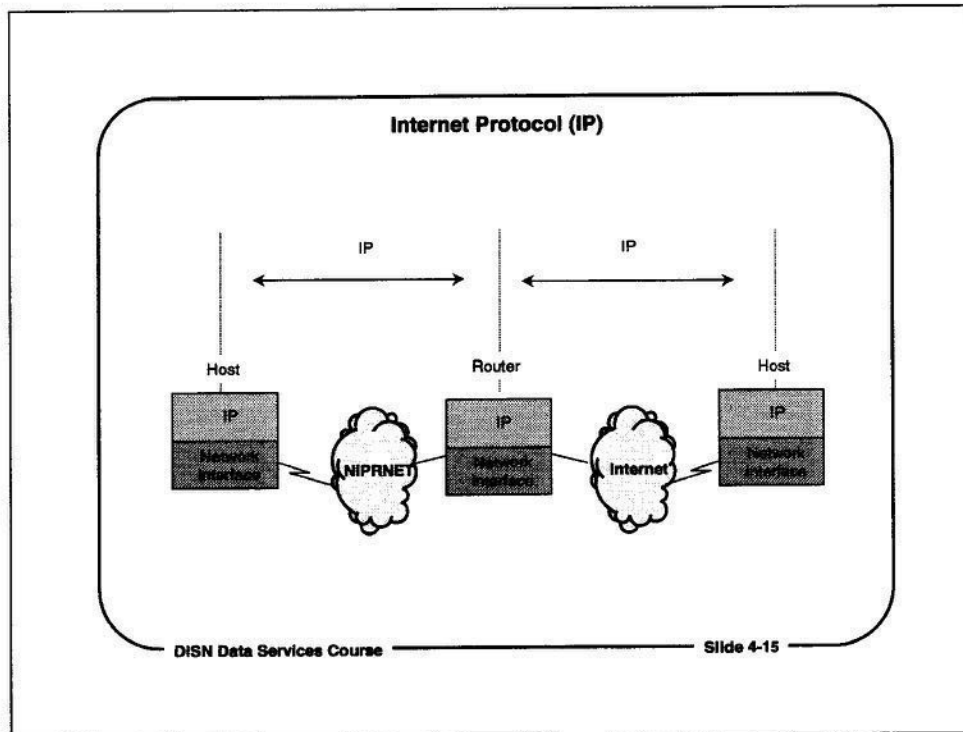


Three-Way Handshake

The three-way handshake procedure establishes a TCP session between a client and a server. Once a TCP session has been established, data can flow in either direction.

With the TCP session established, the TCP module in the client and the server use the session to transfer data. The client and the server use the Sequence Number and Acknowledgement Number in the TCP header to control the session, and to control the flow of data between them.

The mechanics of the session that ride above the TCP connection are the concern of the protocol in use, such as Telnet, FTP, or SMTP. When data transfer starts, neither the client nor the server explicitly acknowledges receipt of blocks of data. The Sequence Number and Acknowledge Number track the number of bytes of data that have been sent and received by each system.



Internet Protocol (IP)

The IP protocol:

- Interconnects networks with minimal impact on each network
- Interconnects networks with different internal protocols and performance
- Supports delivery of datagrams from source to destination.

Type of service:

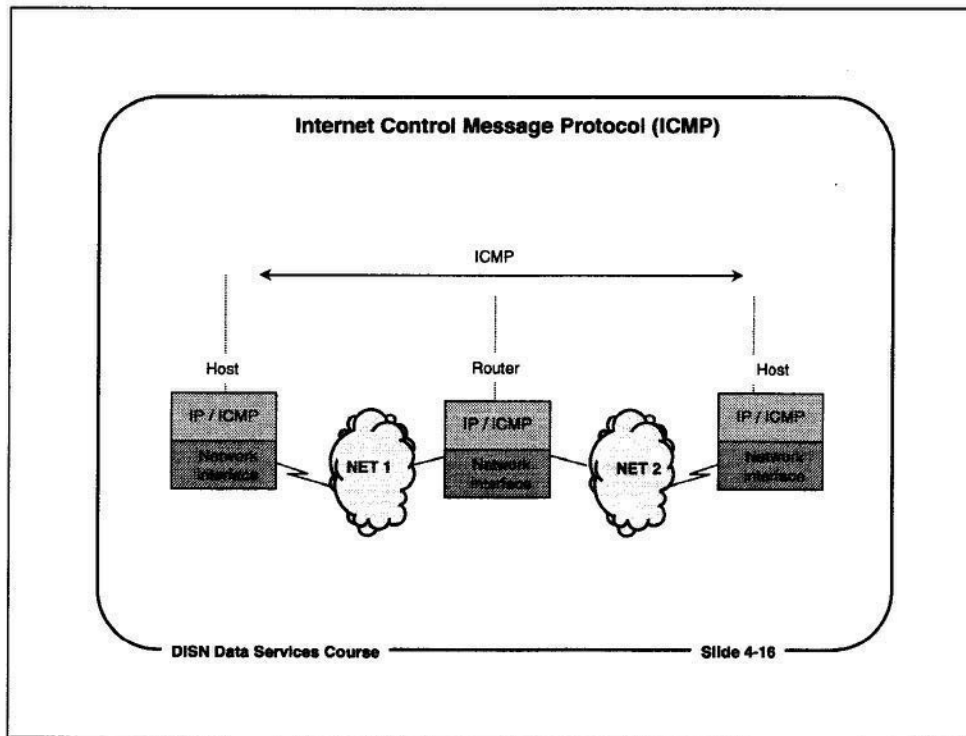
- A generalized set of parameters is used to select characteristics for transmission
- Parameters require trade-offs between low-delay, high-reliability, and high-throughput

Fragmentation and reassembly:

- Required when a datagram originates in a local network that allows for a large packet size and must traverse another network that limits packets to a smaller size.

Supported options:

- Security - Includes compartmentation, handling restrictions, transmission control
- Loose source routing - Gateway or host may use any intermediate gateways
- Strict source routing - Gateway or host must specify gateway to reach destination
- Three classes of Internet addresses - A, B, and C



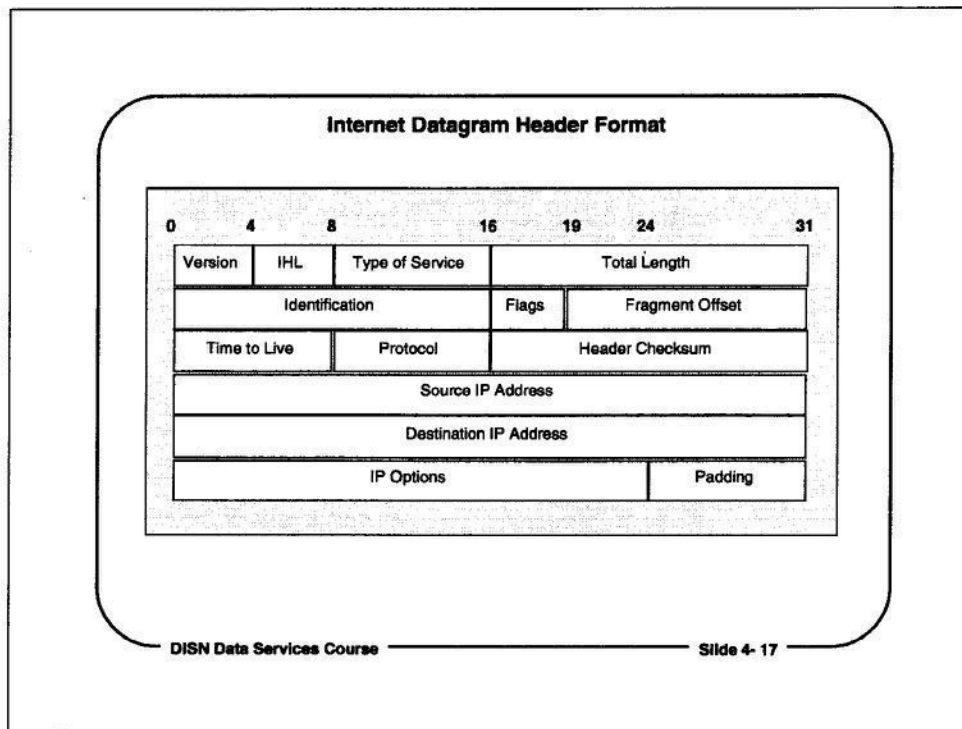
Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol:

- Must be implemented in every IP module
- Used by gateway or host to notify a source host of error conditions
- Uses the basic support of IP, including IP headers
- Designed to supply feedback about problems in network communications only
- Not designed to make IP reliable
- ICMP messages are sent when:
 - Datagram cannot reach its destination
 - Gateway does not have buffering capacity to forward a datagram
 - Gateway can direct host to send traffic over a shorter route.

Message types:

- Redirect - Indicates a shorter route
- Time exceeded - Gateway discarded datagram because TTL (Time-to-live) = 0
- Destination unreachable - Destination host or network is unreachable
- Parameter problem - Either header is incorrect or options field is incorrect.



IP Datagram Header Format

Version = Specifies Internet protocol version

IHL = Internet Header Length in 32 bit words

Type of Service = Specifies how datagram should be handled (precedence, delay, throughput, reliability)

Total Length = Specifies length of datagram (Header plus data)

Identification - Identifies datagram by using UNIQUE integer

Flags = Specifies whether datagram is to be fragmented

Fragment Offset = Specifies the offset of a fragment in its original datagram

Time to Live = Specifies how long datagram is allowed to remain in the internetwork

Protocol = Identifies upper level protocol being serviced

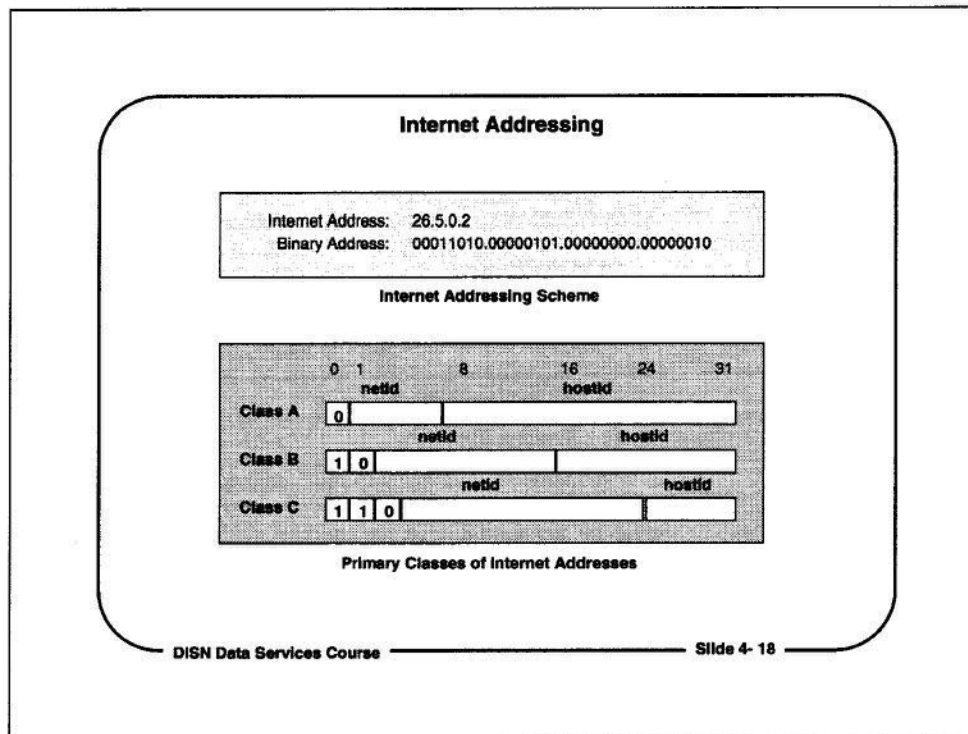
Header Checksum = Used to verify the integrity of the Internet header

Source IP Address = Identifies datagram sender

Destination IP Address = Identifies datagram intended recipient

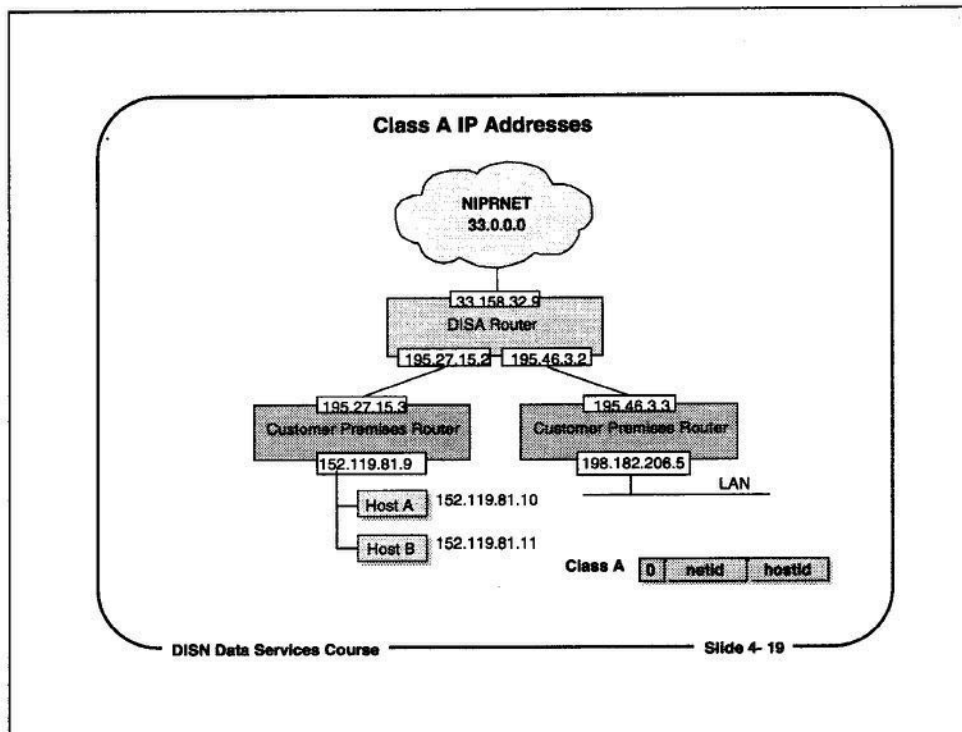
IP Options = Used for network testing or debugging

Padding = Used to ensure header is an exact multiple of 32 bits



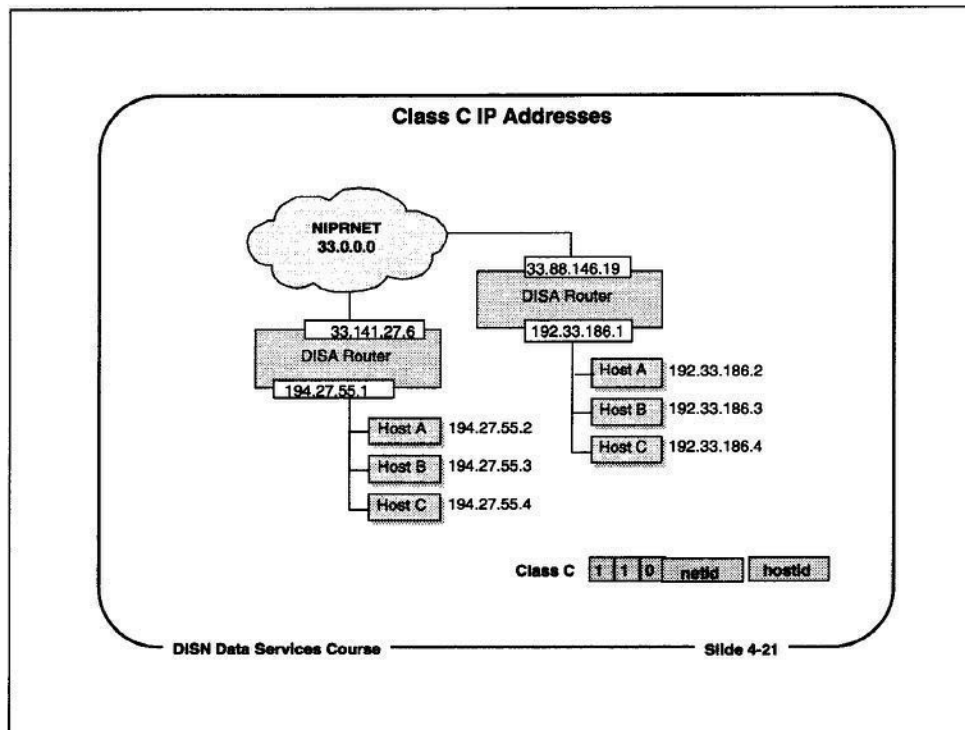
IP Addressing

- The network address is the numeric address of a host, Comm Server, or gateway (as opposed to the text name by which these entities are addressed).
- Internet addresses are assigned by a central authority, the Network Information Center (NIC). The standard Internet address is divided into two parts (netID, hostID), where netID identifies a network, and hostID identifies a host on that network. The NIC Internet Registry assigns the netID portion of an address. The local network coordinator for a specific host assigns the hostID portion.
- Network addresses take the dotted decimal format "nnn.nnn.nnn.nnn," where nnn represents a 1 to 3 digit decimal identifier from 0 through 255. Each numeric component (called a field) is separated from the next with a period. Each field is represented by an 8-bit number. Each decimal part represents one octet of a 32-bit network address.
- Based on this two-part division, three classes of Internet addresses have been defined: Class A, Class B, and Class C. The first three bits within the first field of the 32-bit address indicates the class of the network.



Class A IP Addresses

- Composed of a 1-byte network address and a 3-byte local host address
- The highest-order bit of the (1-byte) network address is set to 0, which means the first byte of a Class A address must be in the range 0 to 127
- Class A could have as many as 126 networks with 2^{24} (16,777,214) hosts on each of these networks.



Class C IP Addresses

- The network number is contained in the three high-order bytes of the Internet address, while the local host address is represented in the single low-order byte
- The three highest order bits of the network address are set to 110, which means the byte must be in the range 192 to 223
- Class C could have as many as 2,097,150 networks with 2⁸ (256) hosts on each of these networks.

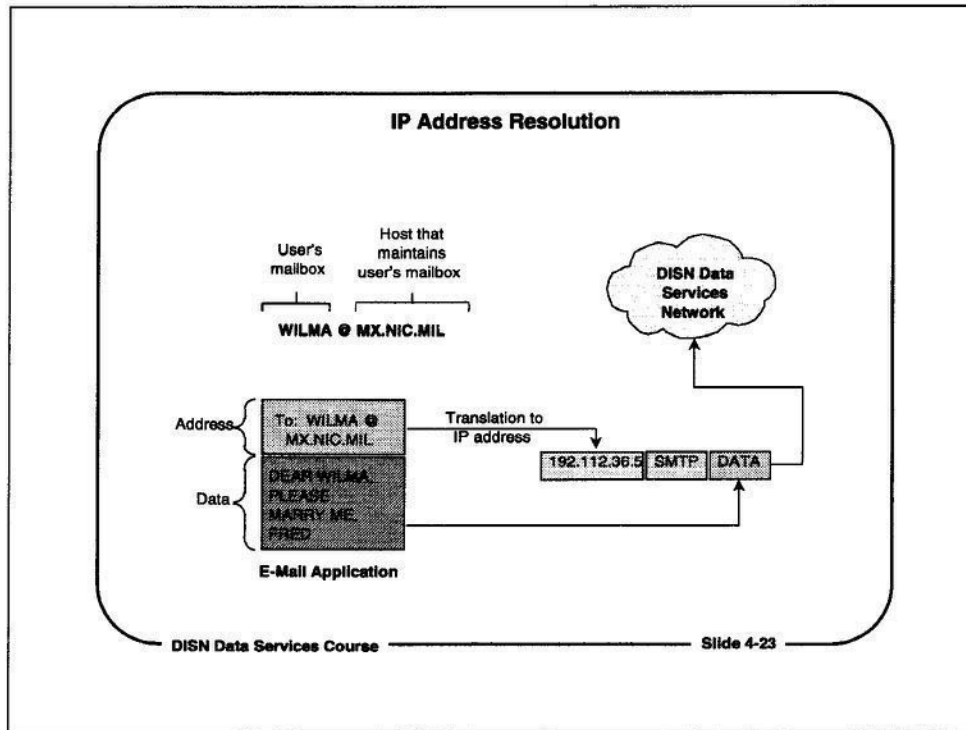
DISA Network IP Addresses	
NIPRNET	
CONUS	33.0.0.0
Europe	140.35.0.0
Pacific	140.45.0.0
SIPRNET	
Worldwide	140.49.0.0
STEP sites	
Unclassified	192.208.32-41.0
Classified	192.208.42-51.0

DISN Data Services Course Slide 4-22

DISA Network Addresses

The networks that comprise the NIPRNET, SIPRNET, and the ITSDN/STEP have been assigned specific ranges of IP addresses by DISA. The Comm Servers on NIPRNET and SIPRNET have also been assigned specific IP address ranges.

DISA has done this so the security classification and general geographic location of each type of network can be determined by examining its IP network address.

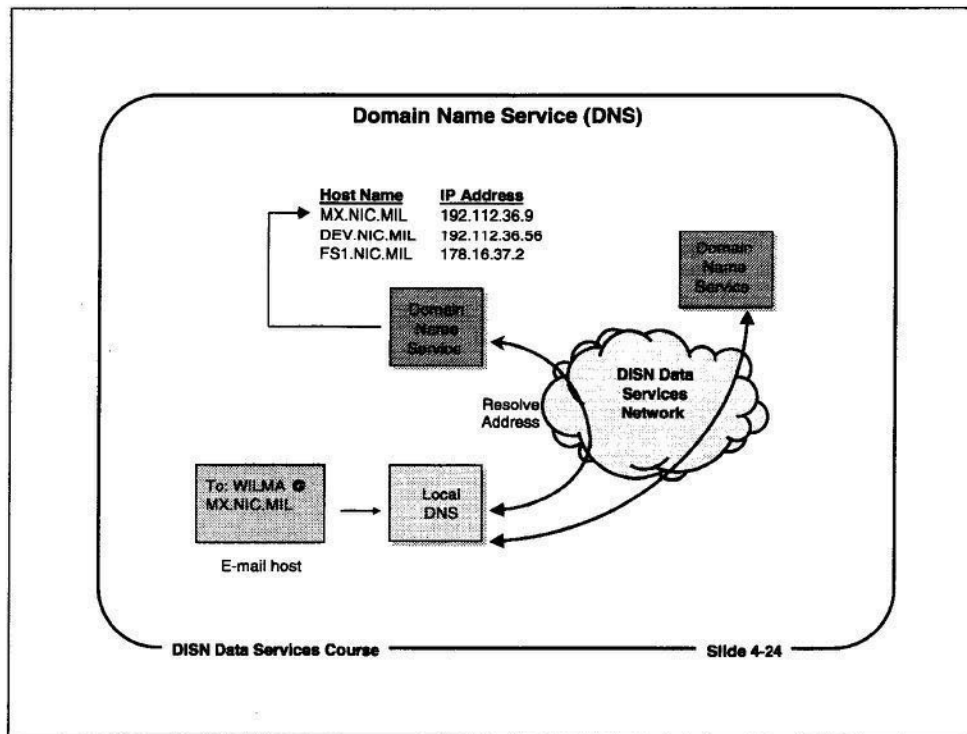


IP Address Resolution

Text addresses used in e-mail messages and in Telnet and FTP commands must be translated to IP addresses for delivery on the network. The process of translating text addresses to numeric IP addresses is called address resolution.

Address resolution must occur before any request or data can be passed onto the network, because the DISN network routes IP datagrams. Data cannot be delivered to a network address if it does not have a valid IP address.

In the example of an e-mail message addressed to wilma@mx.nic.mil, the name to the left of the @ is the name of the recipient's mailbox. The text to the right of the @ specifies the host and domain(s) in which the host is located.

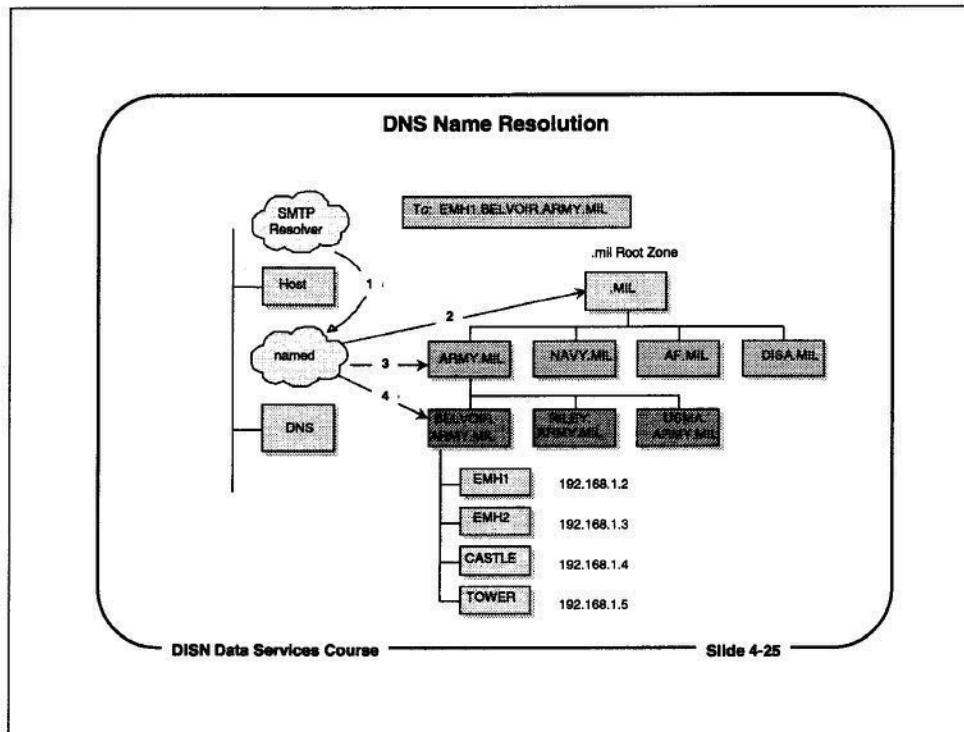


Domain Name Service (DNS)

The Domain Name Service is distributed network service that maps text host names to IP addresses. Instead of a single, master directory, DNS servers are usually set up to serve a specific part of the name space, such as the .army.mil domain. DISA's DoD NIC maintains a master DNS for the .mil domain. That DNS points to other name servers for other sub-domains in the .mil domain.

Local hosts must be set up to use the Domain Name Service. They must know the IP address of the nearest Domain Name Service host, so they can create queries with a valid IP address that will reach the nearest Domain Name Service.

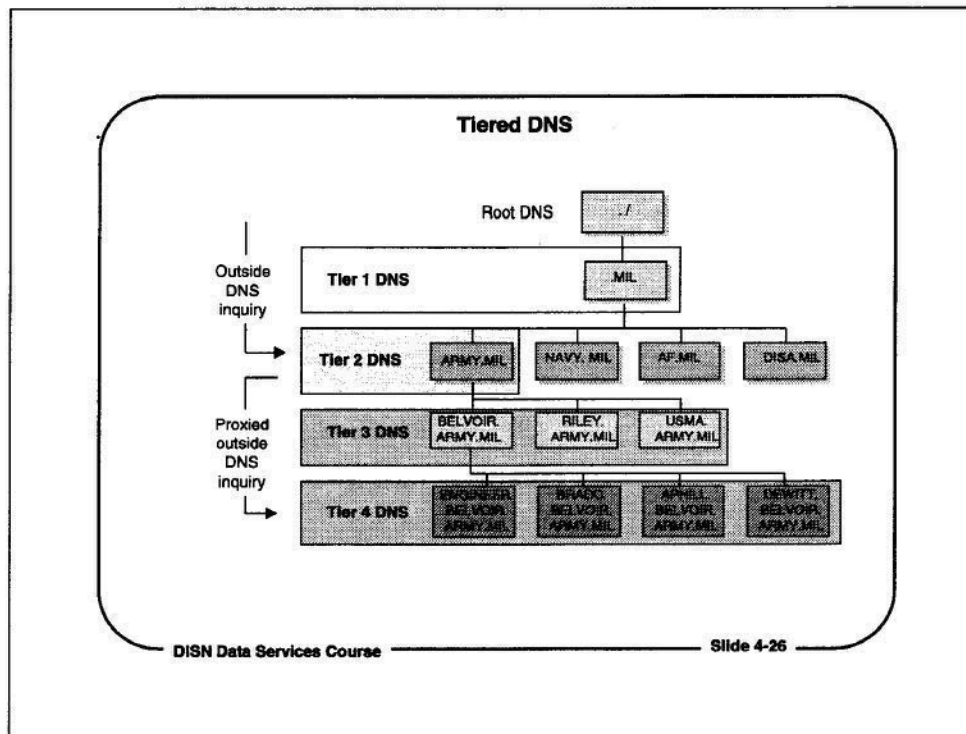
Once the Domain Name Service has resolved a text name to an IP address, and the IP address has been put into the IP header, the data can be sent to the destination system.



DNS Name Resolution

Name resolution requests go first to a local name server, which queries a top-level root-zone server on the NIPRNET (or the Internet). The root-zone server returns the name of a lower-level name server, to which the local name server refers a second request.

The secondary name server may refer the request to other name servers, until the name is finally resolved into an IP address. The IP address is then passed back to the host running the application that made the original request.

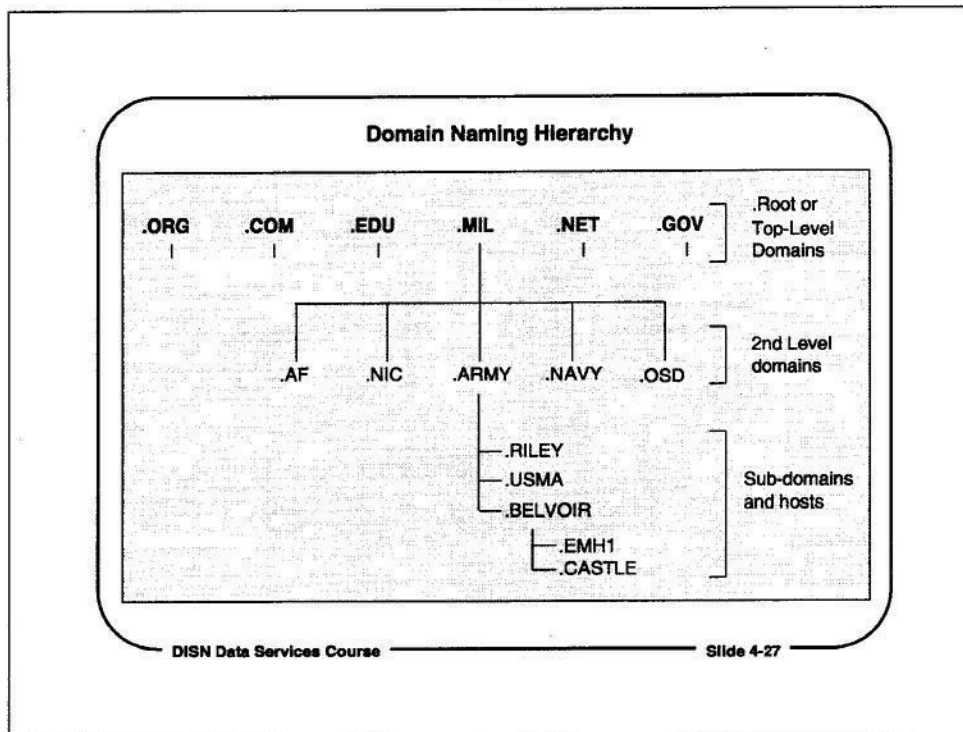


Tiered DNS

The Army is installing a new DNS system, referred to as a Tiered DNS, for all Army DNS services. The goal of the Tiered DNS program is to improve security for Army bases, by disallowing direct access by non-military users to DNS servers in lower-level domains below the .army.mil DNS.

A DNS inquiry from an external user, such as an inquiry that originated on the Internet, would be received by the DNS for the .army.mil domain, which would be designated a Tier 2 DNS. Instead of passing the DNS inquiry to third- and fourth- level domain DNSes within the .army.mil domain, the Tier 2 DNS would proxy the request to the lower-level domains, and then pass the response back to the source.

DISA is planning to implement a new, secure version of the DNS BIND program that is based on the IPsec protocol by the end of 2000.



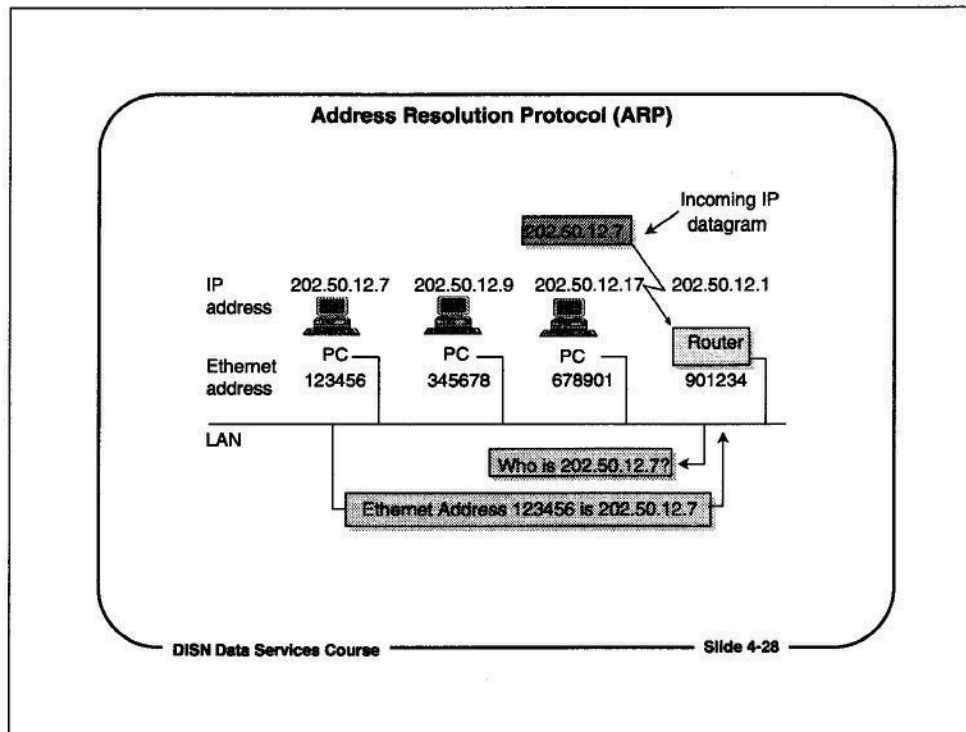
Domain Naming Hierarchy

Instead of having a single Domain Name Service that can resolve every name to an IP address, Domain Name Services have been set up to serve different parts of the domain naming hierarchy.

The left-most part of the text name of a destination is the host name. The rest of the text name is a hierarchical name for the domain(s) in which the host is located.

Inquiries go first to a root domain name server, which usually refers the inquiry to a second level (or lower) domain for resolution.

The hierarchical nature of the Domain Name Service means that maintenance of second level domain names can be handled locally. Hosts can be moved and changed in a second level domain without affecting the operation of a primary top level, or of other second level domains.



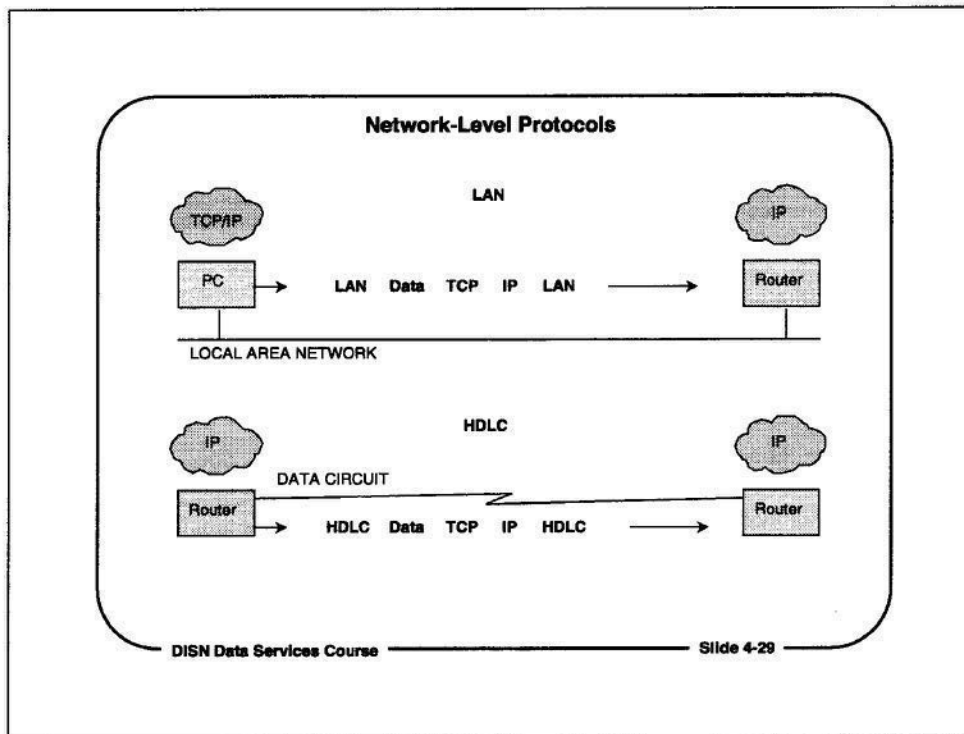
Address Resolution Protocol (ARP)

If the destination device is on a local area network (LAN), the IP addresses must be translated into a LAN address for delivery. LAN devices use LAN adapter addresses (e.g., Ethernet or Token Ring addresses), which are usually hard-coded into LAN adapter cards.

A network router may have to use the ARP protocol to translate an IP address into a LAN address for delivery to the correct device.

Once the data has been delivered to the correct LAN adapter address, the IP process in the destination host receives the IP datagram, and passes it on to the TCP process on the host.

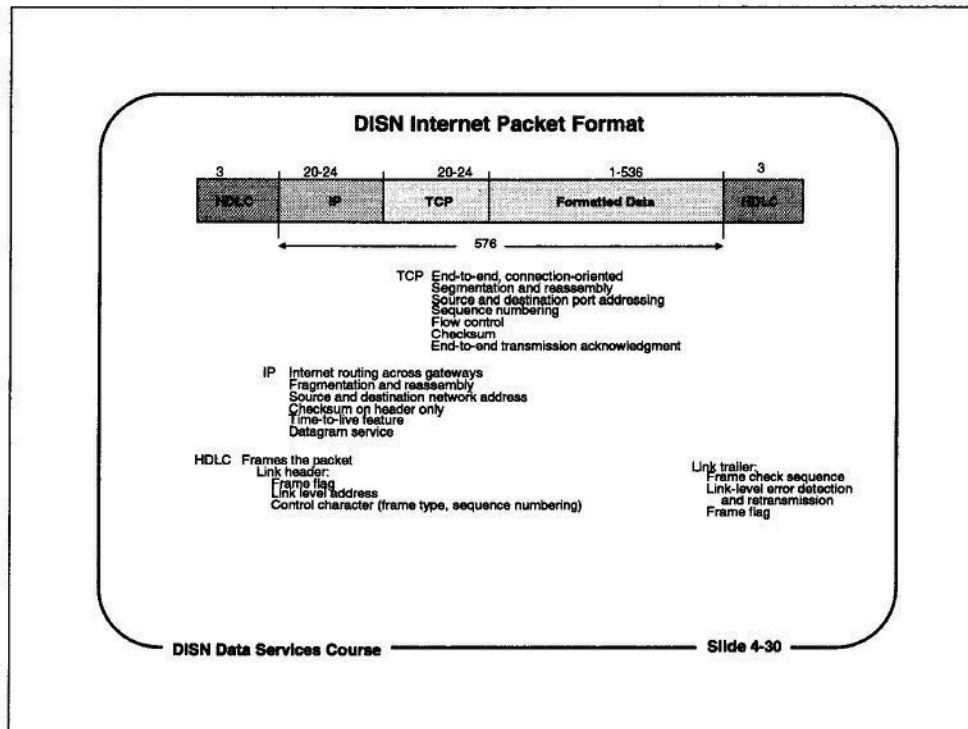
A variation of ARP is the Reverse Address Resolution Protocol (RARP) for translating LAN addresses to IP addresses.



Network-Level Protocols

LAN protocols such as Ethernet, and data link level protocols such as High-Level Data Link Control (HDLC), control the movement of bits or packets across LANs or point-to-point circuits.

The DoD protocol architecture supports many network-level protocols. Network-level protocols may be relevant in a specific network, so most network-level protocols need only interface to the TCP/IP protocol stacks above them.



DISN Internet Packet Format

Formatted data:

- SMTP header and user data
- FTP header and user data
- TELNET header and user data

HDLC:

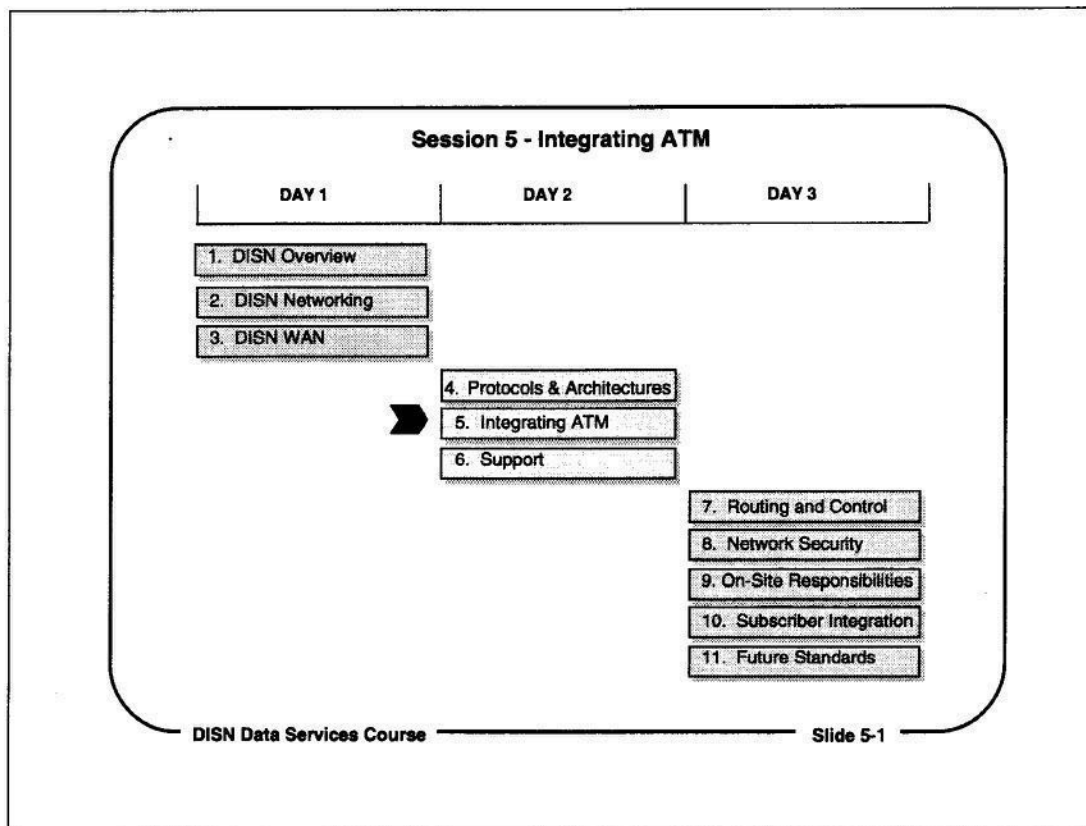
- Data link layer protocol
- Link reliability across one circuit

TCP:

- Transport layer protocol
- End-to-end reliability

IP:

- "Internetwork layer"
- Used to route data between networks
- Fragmentation and reassembly

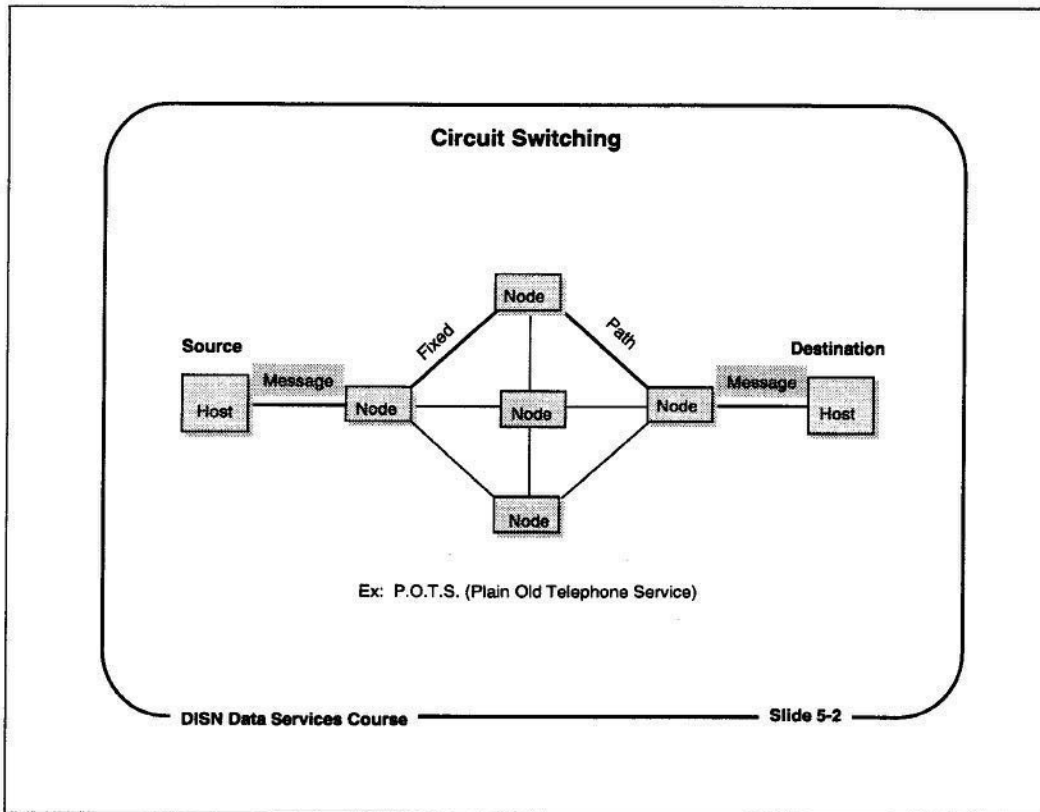


Session 5 - Integrating ATM

Upon completion of this module, the students will have a general understanding of circuit switching, message switching, and packet switching, and be able to compare the advantages and disadvantages of each. They will also understand how packet switching applies to the Internet, the DISN data services networks, and to ATM networks.

This session will focus on:

1. Defining the functions of circuit switching
2. Defining the functions of packet switching
3. Describing the use of packet switching in packet switching networks, and in IP datagram routing
4. Identifying how new packet switching technologies, such as ATM, have been deployed in the DISN backbone network

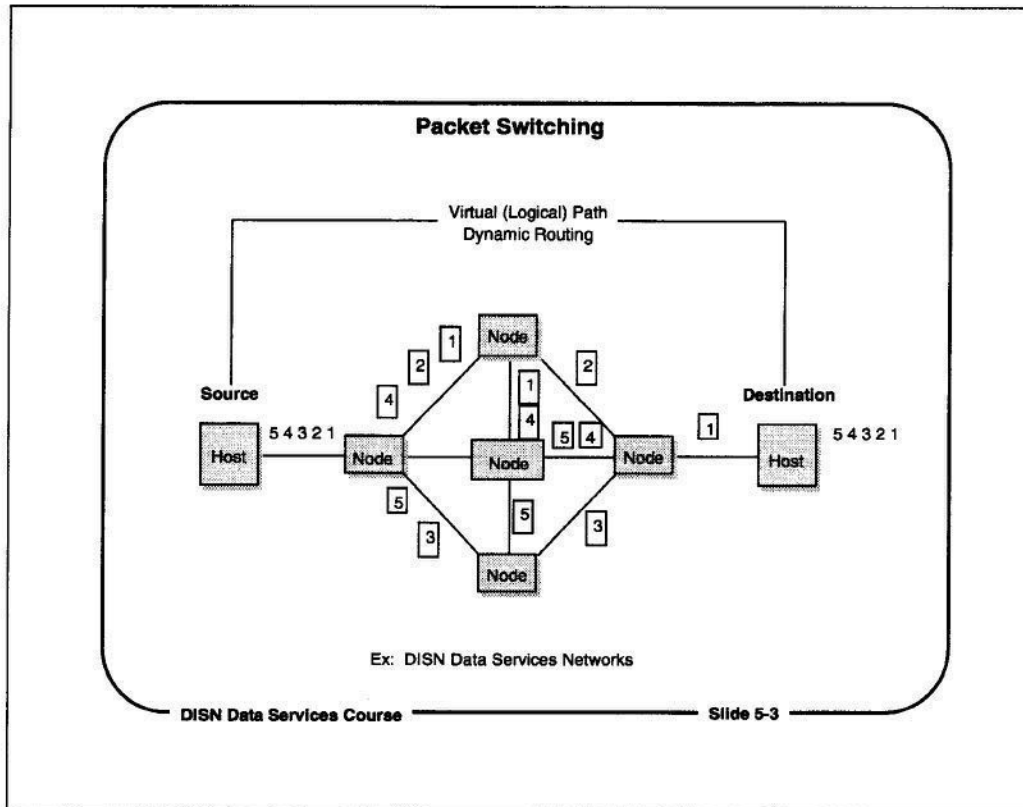


Circuit Switching

- Oldest method of switching; used in public telephone network
- Entails the establishment of a temporary dedicated physical link between two parties
- Best suited to an environment of infrequent call establishment with short call-hold times

Functionality of Circuit Switching Systems

- Call Establishment - Creation of a temporary dedicated physical link; the telephone number provides destination address information to the circuit switch
- Transfer of Information - All information traverses the physical route set up during call establishment
- Call Termination - All circuits freed upon call termination so they can be used for other calls.

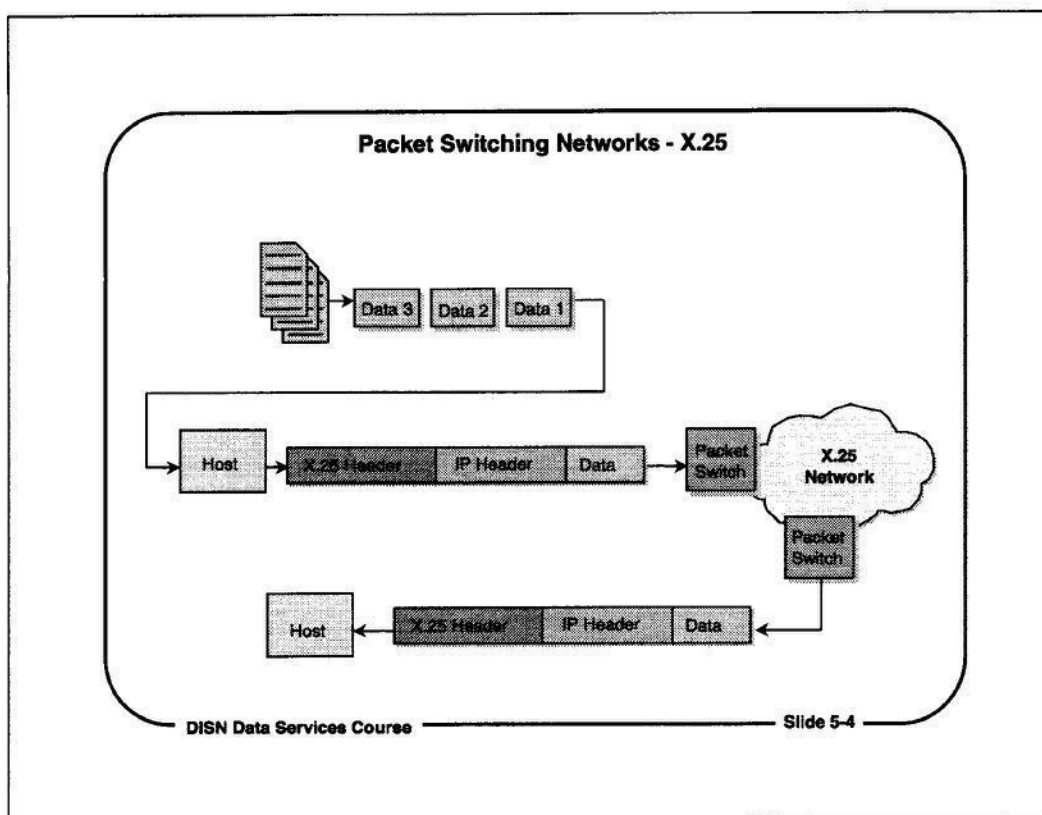


Packet Switching

- Attempts to combine the features of circuit switching and message switching, while minimizing the inherent limitations of both
- Packet switches are specialized digital devices
- Messages are transmitted to a "piece" at a time, called a packet. Packets can vary in size.

Functionality of Packet Switching

- Source breaks message up into standard-sized packets (e.g., 128 bytes), attaches address information, and then sends the packet(s) to the local switch
- Packets are held in the packet switching nodes' buffers just long enough for previous packets to be transmitted and error control/recovery processes to be completed
- Each node forwards the packet to the next node on its way from source node to destination node.

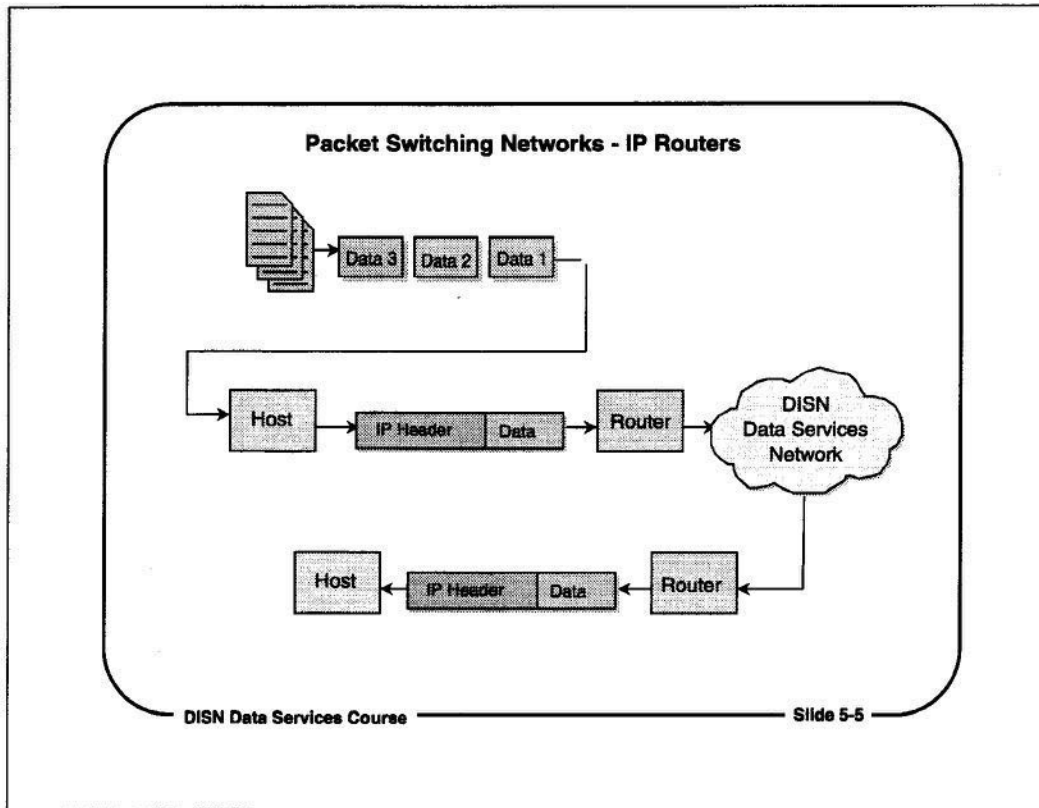


Packet Switching Networks - X.25

Many commercial packet switching services and private packet switching networks use the X.25 CCITT standard protocol. The X.25 packets have X.121 addresses, which indicate the destination node to which the packets are to be delivered.

When X.25 is used as a transport mechanism for IP datagrams, an X.25 header "envelops" the IP datagram, and delivers it to a destination router.

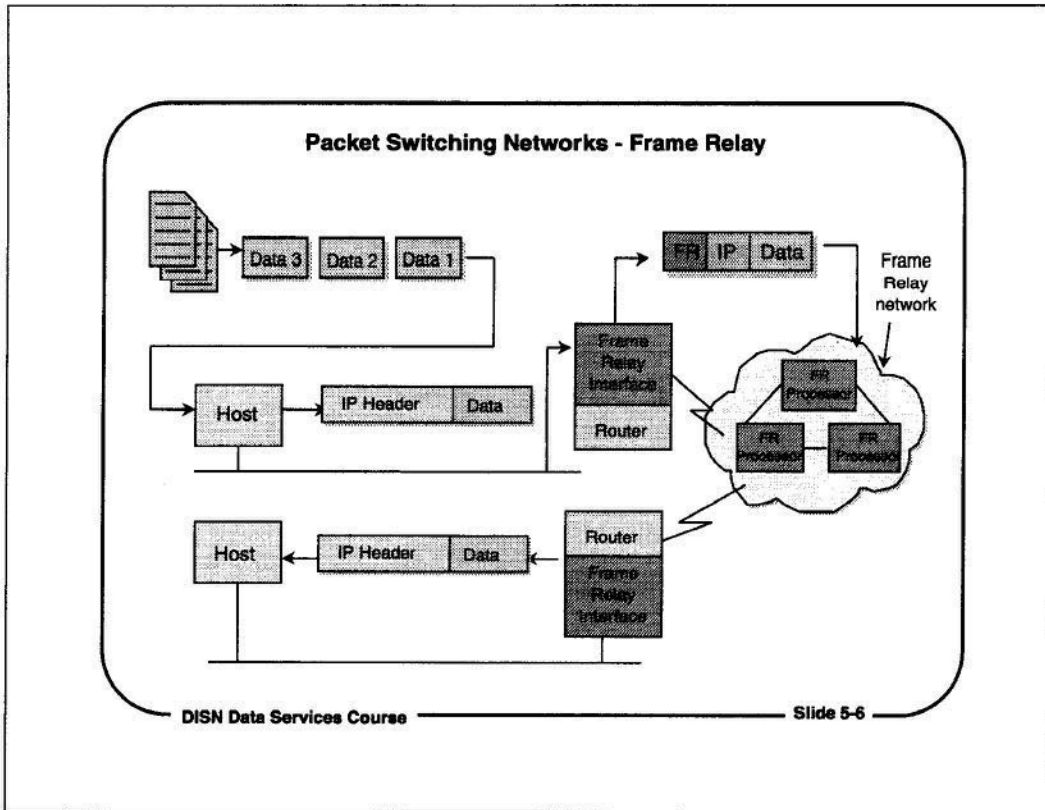
In the Defense Data Network (DDN), the DDN Packet Switching Nodes (PSNs) used a special version of X.25 to transfer data packets across the DDN.



Packet Switching Networks - IP Routers

The IP routers in the DISN Data Services networks transfer IP datagrams to other DISA routers, using the DISN as a general-purpose transport service.

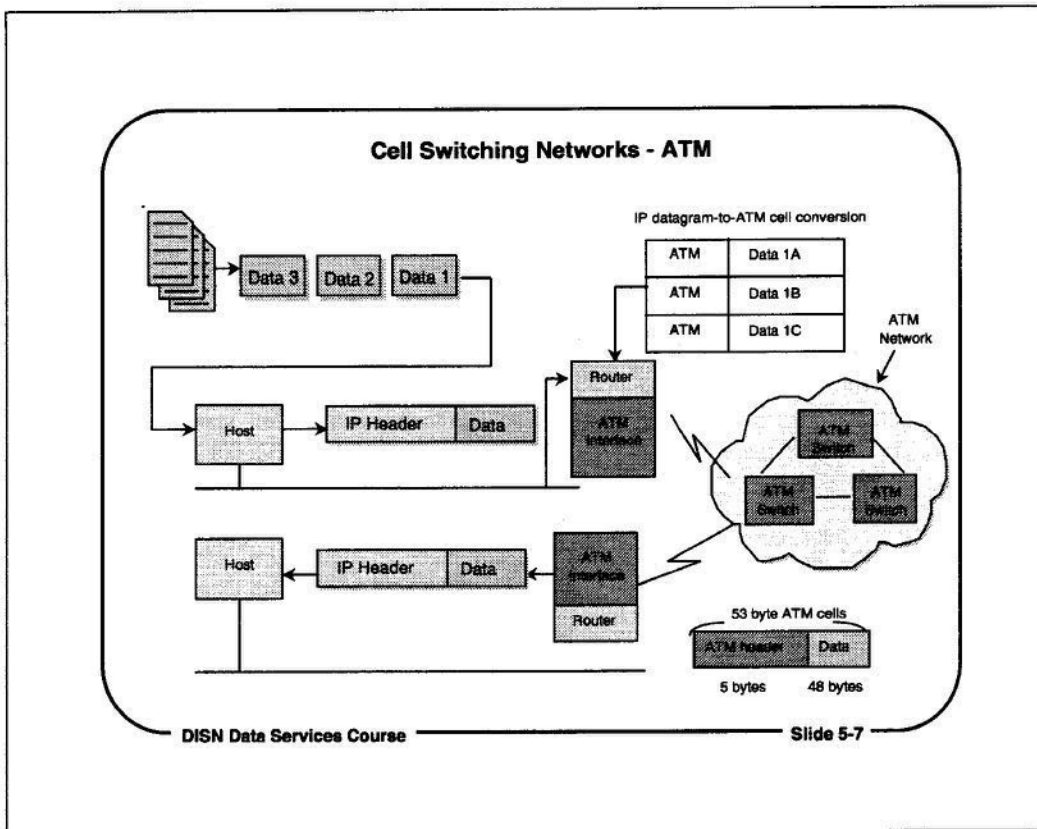
When IP datagrams are transmitted across the DISN backbone, the IP datagrams are "wrapped" in HDLC data link frames. HDLC is the default link-level protocol for the DISA routers.



Packet Switching Networks - Frame Relay

The concept of packet switching has been carried forward from the older X.25 networks to newer packet switching technologies. One of the newer packet switching techniques is Frame Relay.

Frame Relay networks rely on specially-provisioned transmission networks, and on special communications interfaces in routers. One of the primary applications for Frame Relay services today is LAN to LAN interconnection.

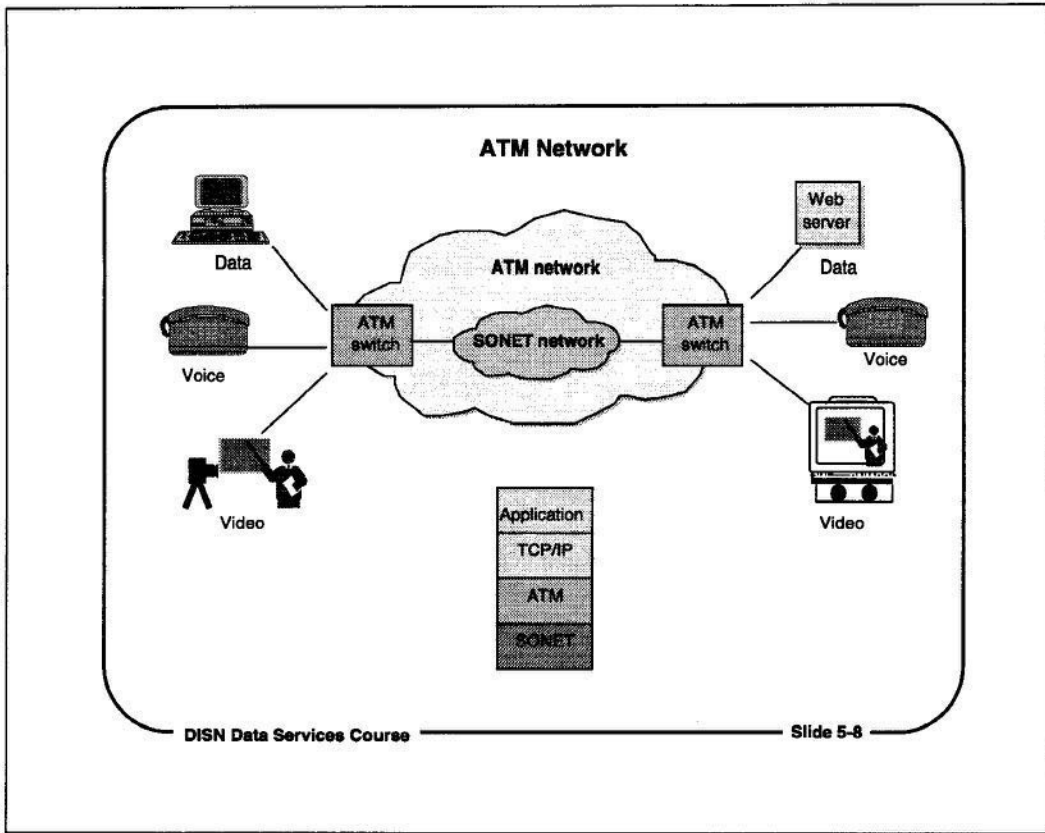


Cell Switching Networks - ATM

Parts of the DISN backbone are being upgraded from high-speed point-to-point circuits to an Asynchronous Transfer Mode (ATM) network.

An ATM network is a specially-provisioned network composed of very fast switches. After call path setup has been established, the ATM switches direct the data to its destination. DISA routers connect to the ATM network, to transfer IP data and, in some locations, voice, across the DISN backbone at high speed.

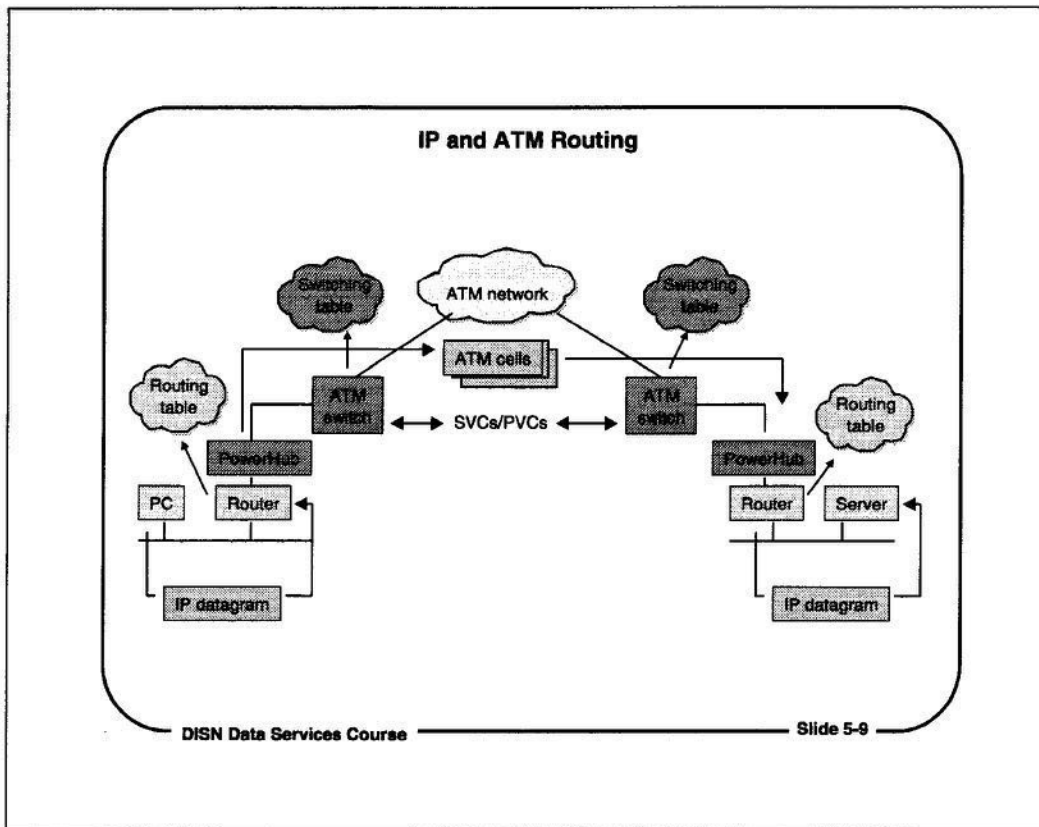
ATM networks handle large amounts of data quickly because they handle only small, fixed-length packets of data. Each cell or frame is 53 bytes long, and is composed of 48 bytes of data, and a five-byte ATM address header. The ATM header may contain addressing or control information.



ATM Network

Although the ATM network's initial use has been in backbone data networks, such as the classified and unclassified wide area networks for NIPRNET and SIPRNET, ATM has also been designed to carry voice, video, and data on the same network. DISA intends to use the ATM backbone for all three services. The ATM network has been put to use primarily for carrying data traffic in CONUS. The ATM network carries voice and data in Europe and in the Pacific.

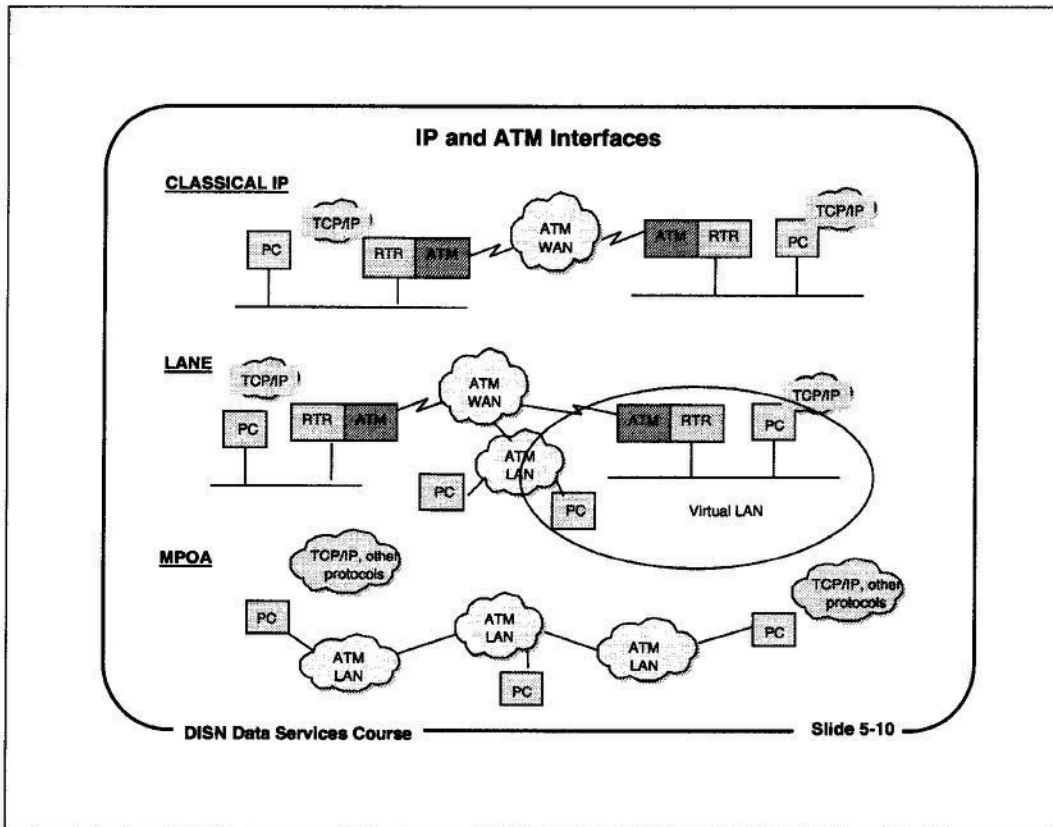
The North American communication system standard for the digital optical fiber transmission systems that interconnect ATM switches is the Synchronous Optical Network Standard, or SONET. In Europe, telecommunications systems use a different standard, the Synchronous Digital Hierarchy (SDH).



IP and ATM Routing

Even though they both use packet technologies, IP datagrams and ATM cells use different addressing and framing formats. IP and ATM also use fundamentally different assumptions about how devices communicate. ATM is "connection-oriented," much like the switched telephone system, while IP is "connectionless," relying instead on another protocol, TCP, to establish a logical connection with the destination system.

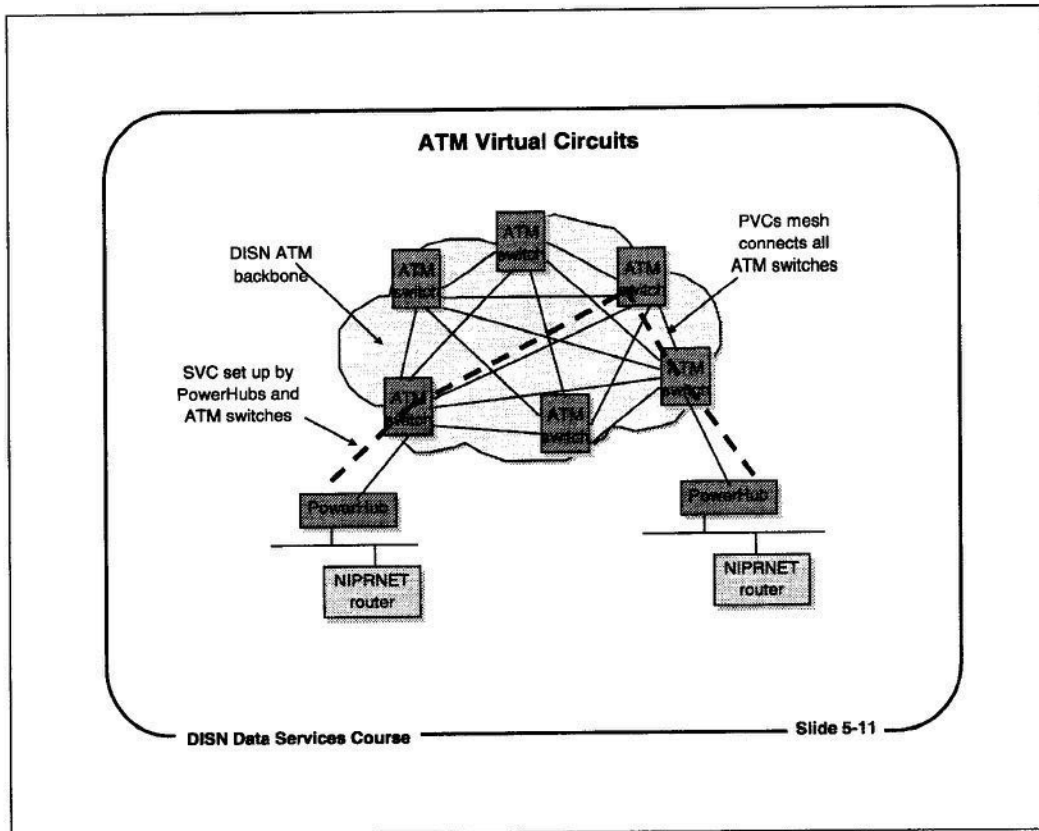
IP datagrams must be re-packaged in ATM cells that bear ATM addresses before they can be transmitted across an ATM network. For NIPRNET and SIPRNET users, this will be done transparently by the ATM interfaces to the classified and unclassified wide area networks. Advantages to ATM include speed and high bandwidth.



IP and ATM Interfaces

There are several ways to run IP over an ATM network. Each makes different assumptions about where the ATM network is with respect to the host computer, server, or PC, and the modifications or additions that can be made to host, server, or PC. The most common methods are:

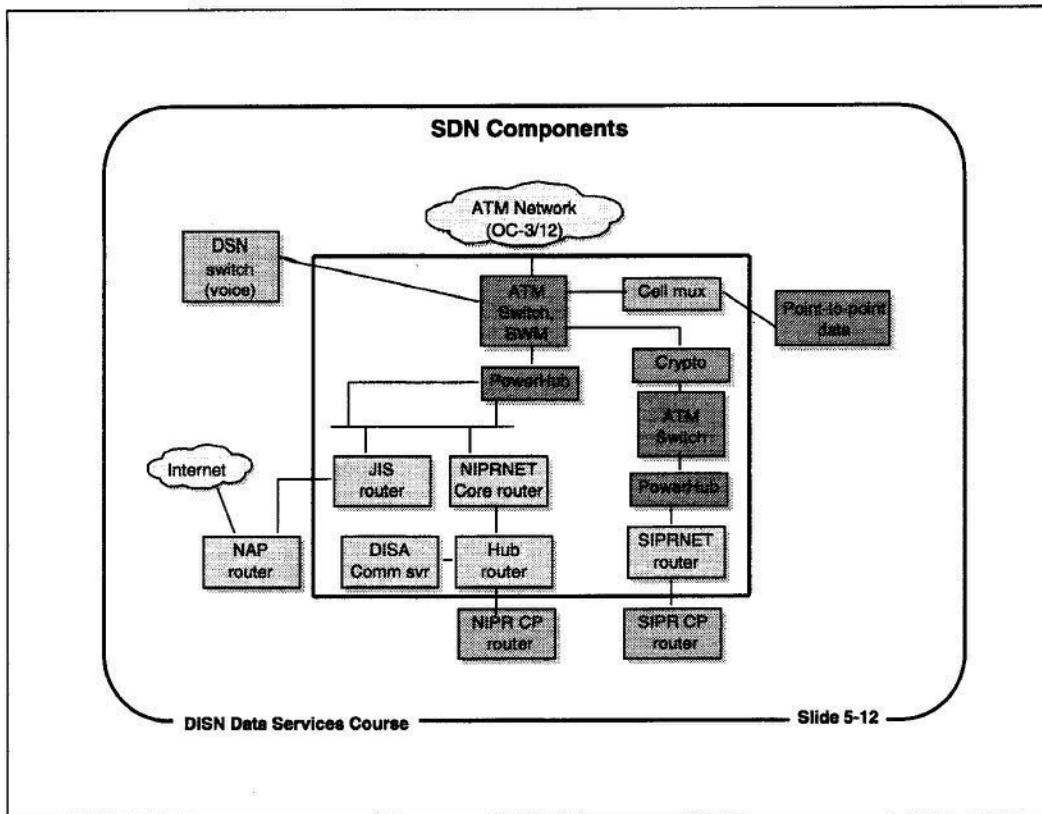
- **Classical IP** - PC, hosts, and servers know nothing about ATM. Before being sent out to the ATM network, IP datagrams go to a router with ATM interface, which repackages IP datagrams in ATM cells.
- **LAN Emulation (LANE)** - PCs, hosts, and servers may have ATM interfaces instead of Ethernet adapters, but they still use the TCP/IP protocols. The LANE interface in an edge device translates between the IP and ATM protocols. A router is still required to interface to the ATM WAN backbone.
- **Multiprotocol Over ATM (MPOA)** - PCs, hosts, and servers use special network interface software, which supports TCP/IP and other protocols. On the ATM a Router Server maps IP addresses to ATM network addresses, eliminating the delays that may be introduced by routers that map IP addresses to ATM addresses.



ATM Virtual Circuits

The CONUS DISN ATM backbone network has 13 ATM switches that are connected together over OC-3 trunks. The trunks are provided by the commercial ATM carriers (Sprint and MCI Worldcom), and are configured with a mesh of permanent virtual circuits (PVCs) connecting the core ATM switches.

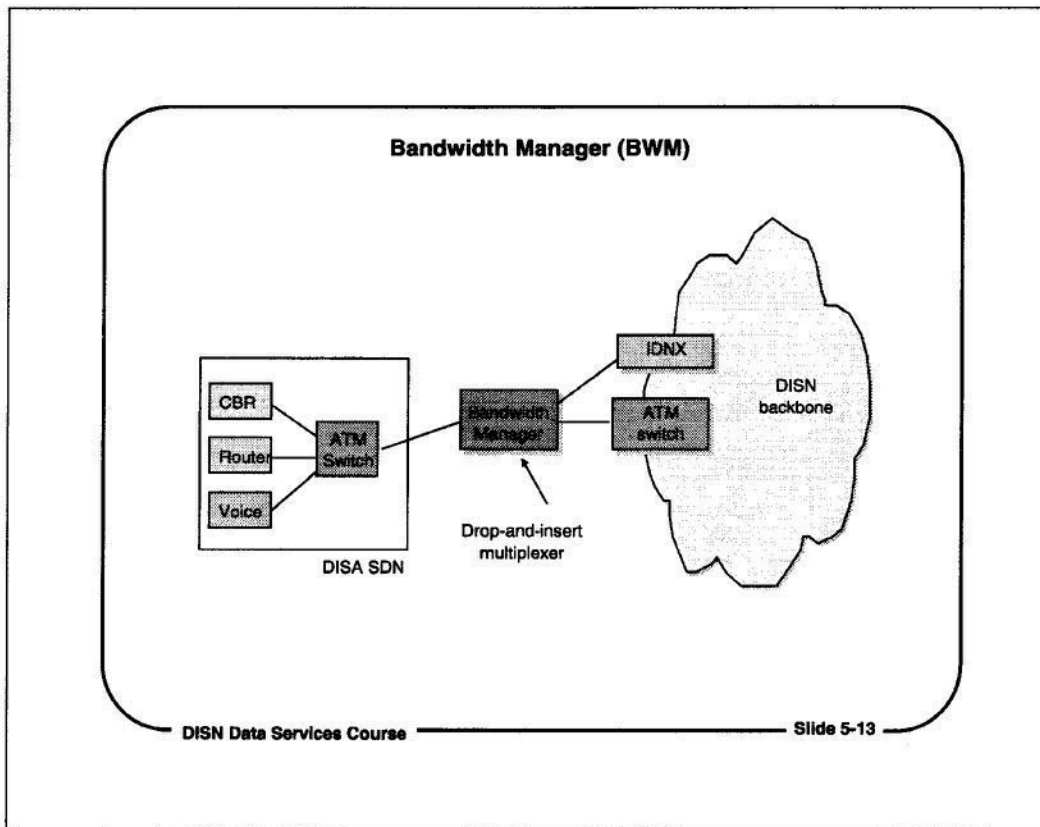
The PowerHubs behind the ATM switches connect the NIPRNET core routers to the ATM backbone. When a NIPRNET core router sends traffic across the ATM backbone to another NIPRNET core router, the PowerHub sets up a switched virtual circuit (SVC) across the PVCs that connect the ATM switches.



Service Delivery Node (SDN) Components

DISA is consolidating customer access to the DISN backbone in the Service Delivery Node (SDN). The SDN corresponds to the current DISA Node Site, which is where the DISA NIPRNET and SIPRNET routers, and, if installed, an ATM switch are located.

The SDN will be the customer interface to the DISN backbone. All customer services that require backbone transport, such as NIPRNET and SIPRNET data, legacy and point-to-point data requirements, voice, and video will be homed to the SDN. The SDN will then connect to the DISN backbone for transport to other SDN locations, or to the Internet.



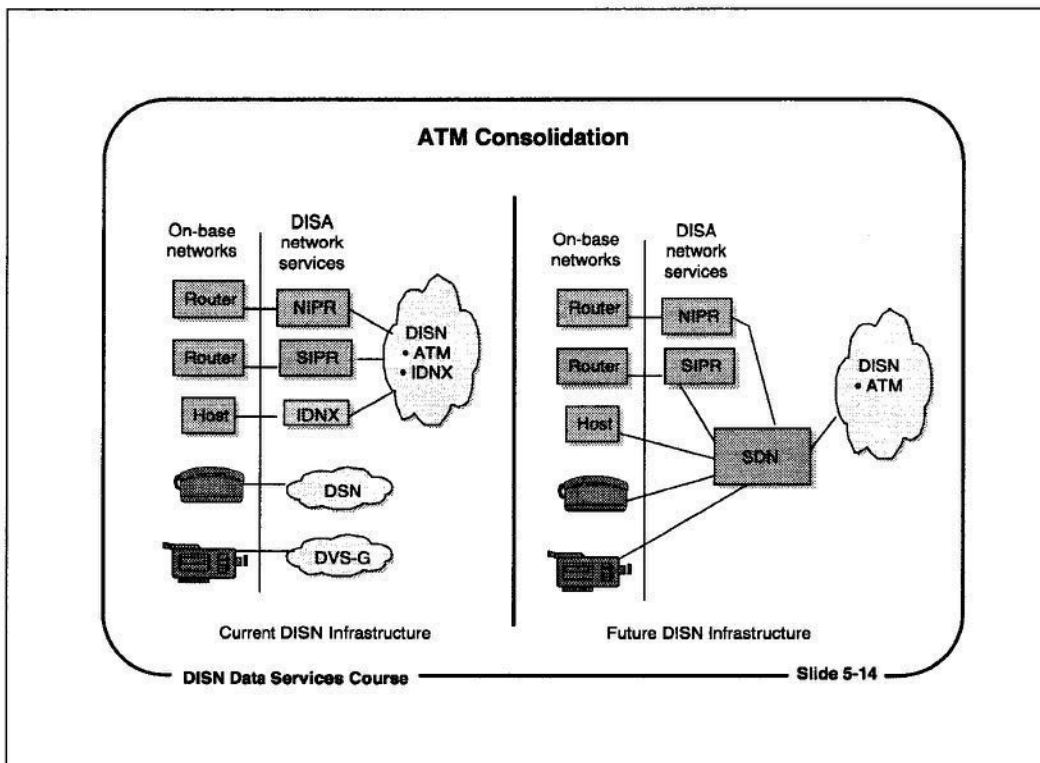
Bandwidth Manager

The Bandwidth Manager (BWM) is a drop-and-insert multiplexer that will be the primary interface between the DISA routers and the DISN backbone. It will also accommodate point-to-point links connecting older systems that use dedicated circuits across the DISN backbone.

In the DISN Data Services networks, the BWMs will replace the dedicated connections from NIPRNET and SIPRNET routers to ATM switches, IDNX multiplexers, and point-to-point circuits in the DISN backbone.

Instead, the BWMs will manage all of the bandwidth on the DISN backbone, and assign whatever DISN backbone transmission path is most suited to the DISN data service, most immediately available, or most cost-effective. The goal is to give DISA the flexibility to use the DISN backbone in the most efficient way, and to provide more reliable, lower-cost data services to DISN Data Services network subscribers.

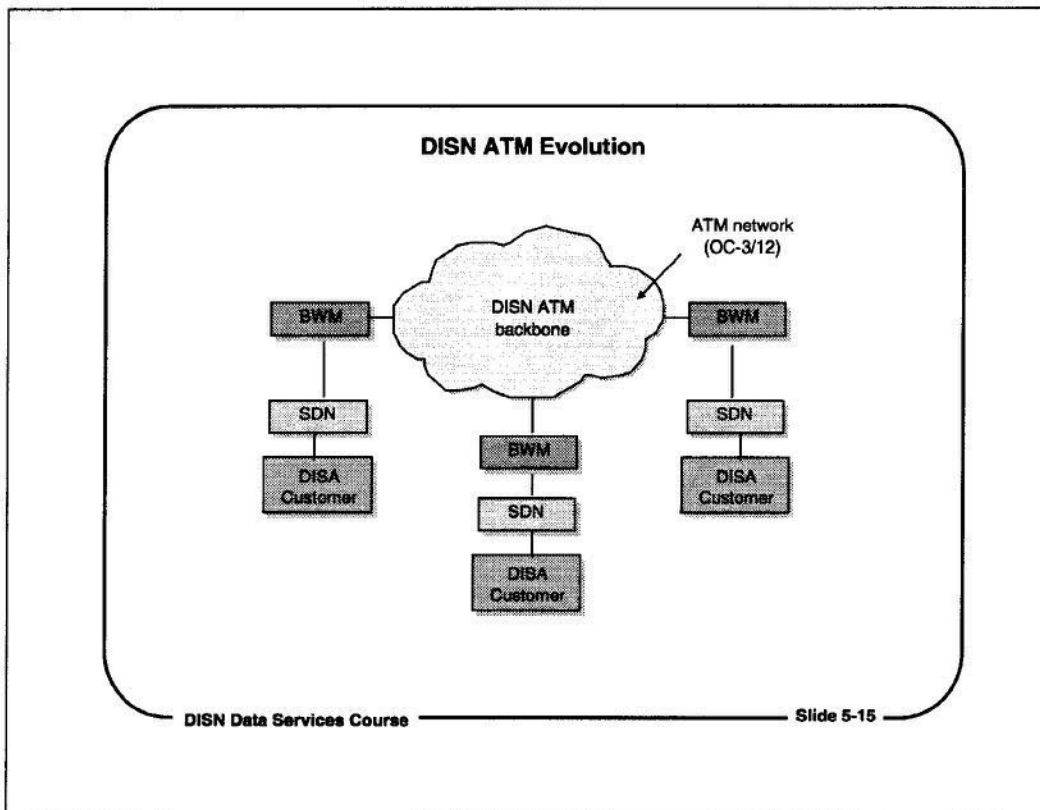
The BWMs are being provided to DISA by MCI Worldcom under the DSS-G contract.



SDN Consolidation

The Service Delivery Nodes will be used to interface many types of communications systems to the DISN backbone. A typical large military base has the equivalent of more than 100 T-1 external communications circuits, carrying NIPRNET and SIPRNET traffic, switched voice (DSN), video (DVS-G), and other, special-purpose communications services. In many cases, each of these services connects to its own, dedicated long-haul service, and few may consolidate traffic on more economical, high-bandwidth services.

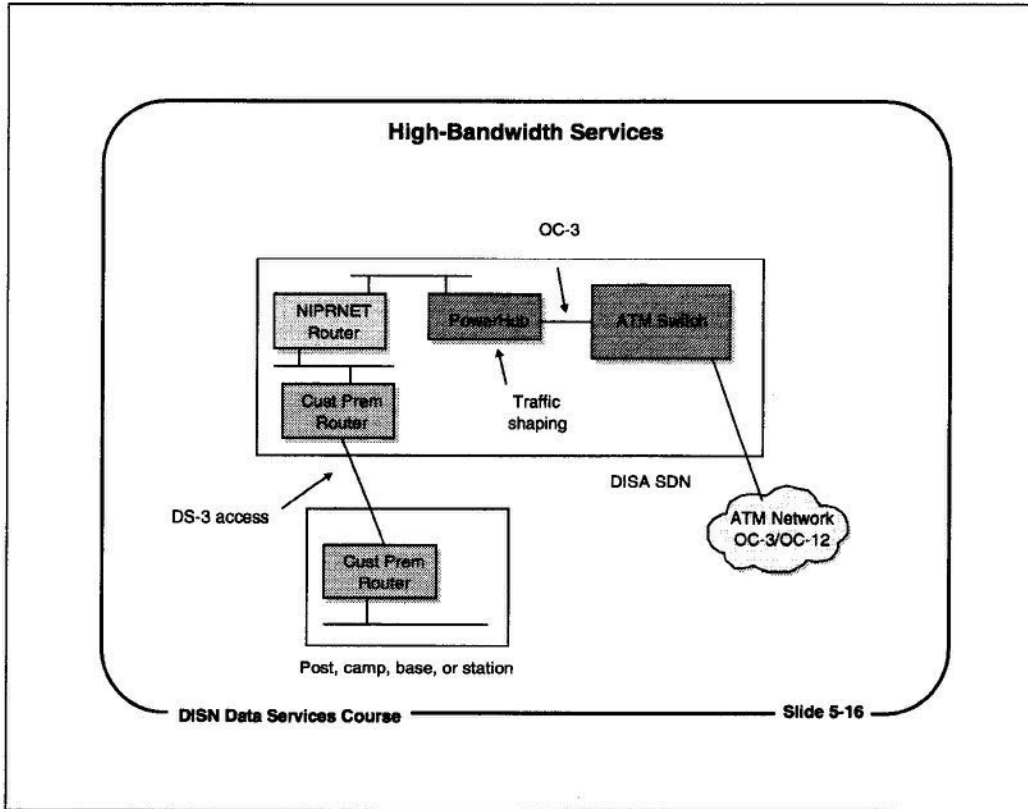
The objective of the SDNs, and the Bandwidth Managers to which they connect, is to provide a single interface for all base communications into the DISN WAN, not just for NIPRNET and SIPRNET traffic. DISA's plan is to replace the lower-bandwidth circuits that serve the separate external communications requirements with a smaller number of more economical, high-bandwidth services. For example, two OC-3 DISN backbone circuits would provide twice the bandwidth of 100 separate T-1s, at about the same cost as the separate T-1s they replaced.



DISN ATM Evolution

DISA's long-range plan for the evolution of the ATM network is to migrate away from the commercial ATM services that provide the backbone ATM network today, and to a private ATM network that is dedicated to the DISN. The Bandwidth Managers (BWM) will connect the Service Delivery Nodes to the ATM cloud, as well as to other types of backbone transmission services. The bandwidth of the ATM backbone in CONUS will range from OC-3 (155 Mb) to OC-12 (622 Mb). The ATM backbone will run at lower data rates in the Pacific and European theaters.

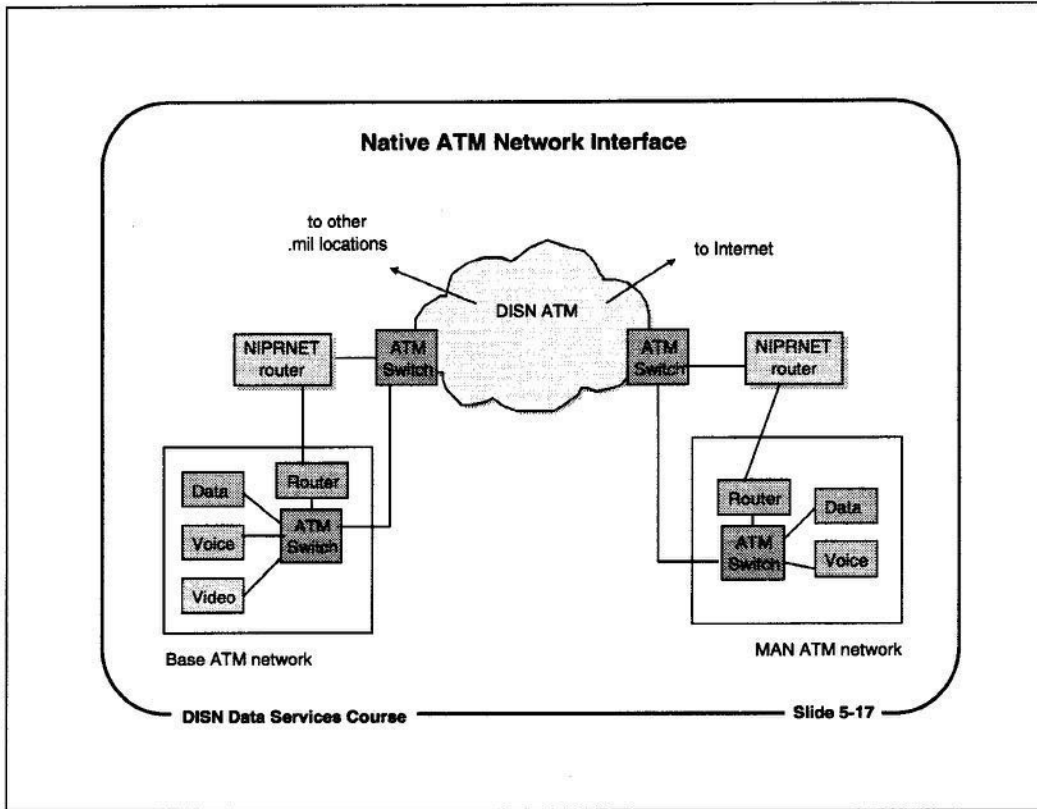
The ATM network will be provided to DISA by AT&T, and the Bandwidth Managers will be provided by MCI WorldComm, as part of the DISN Support Services-Global (DSSG) contract. The dedicated ATM backbone will give DISA higher guaranteed bandwidth and greater availability at a lower cost than it gets today from its current ATM commercial service providers.



High-Bandwidth Services

Customer access to DISN Data Services networks at high bandwidth data rates (3 Mb to 39 Mb) is usually done through a customer premises router that is co-located at the DISA Service Delivery Node (SDN). A high-speed access circuit, which is usually a DS-3, connects the co-located customer premises router back to another customer premises router on the post, camp, base, or station.

At the SDN, the co-located customer premises router is connected to the NIPRNET router over fast Ethernet. The traffic from the co-located customer premises router is "shaped" at the PowerHub to reduce the data flow back to the data rate to which the customer has subscribed.

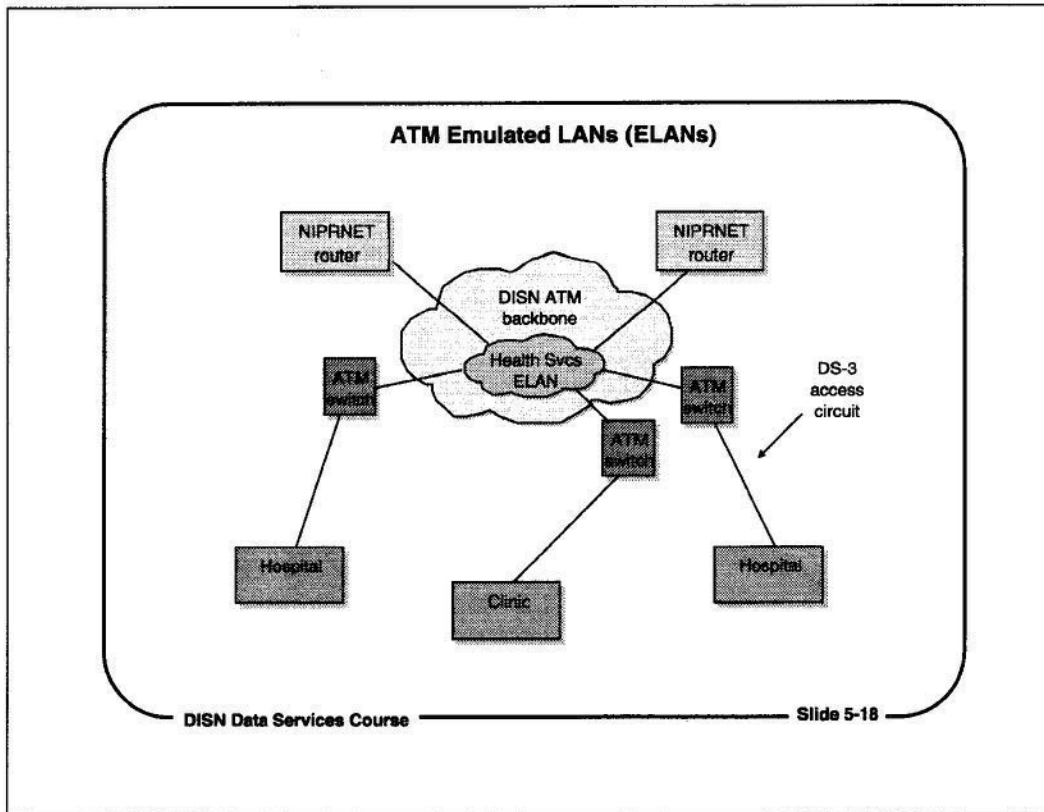


Native ATM Network Interface

Some military organizations and bases have their own, native ATM networks that they would like to connect to the DISN backbone at the ATM level. These ATM networks may also be metropolitan area networks (MANs) that connect several bases together over an ATM network that covers a large metropolitan area that has several military bases. The base ATM LAN or the ATM MAN may carry data, voice, or video, or traffic for other, specialized applications.

While it is technically feasible to connect a native ATM network to the DISN ATM backbone network, that network would not have universal NIPRNET connectivity across the DISN. The ATM traffic would not be handled by NIPRNET routers, so the native ATM network could only connect to other native ATM networks.

DISA's policy for native ATM network connections is that IP traffic must be split out to a router, so that it can be handled by a NIPRNET router, to get NIPRNET and Internet connectivity.

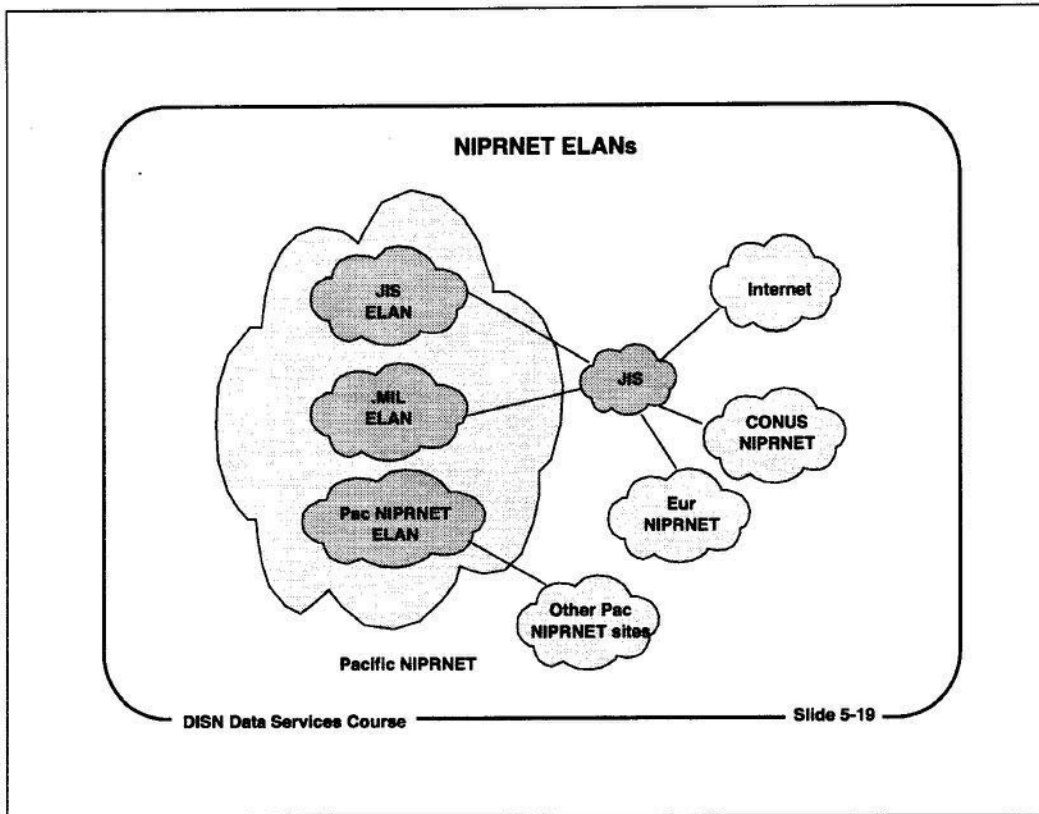


ATM ELANs

DISA has configured Emulated LANs (ELANs) across the DISN ATM backbone in CONUS for the DoD Health Services (TRICARE) organization, as well as for other NIPRNET "communities of interest". The TRICARE ELAN connects DoD hospitals and clinics together so that they can use special Combined Health Care System (CHCS) applications. The ELAN makes it appear that all of the Health Services locations are on a single LAN, which runs across the DISN ATM backbone.

Network access from each of the Health Services hospitals and clinics is through a dedicated DS-3 circuit. The Health Services ELAN is connected back into the NIPRNET through seven NIPRNET routers.

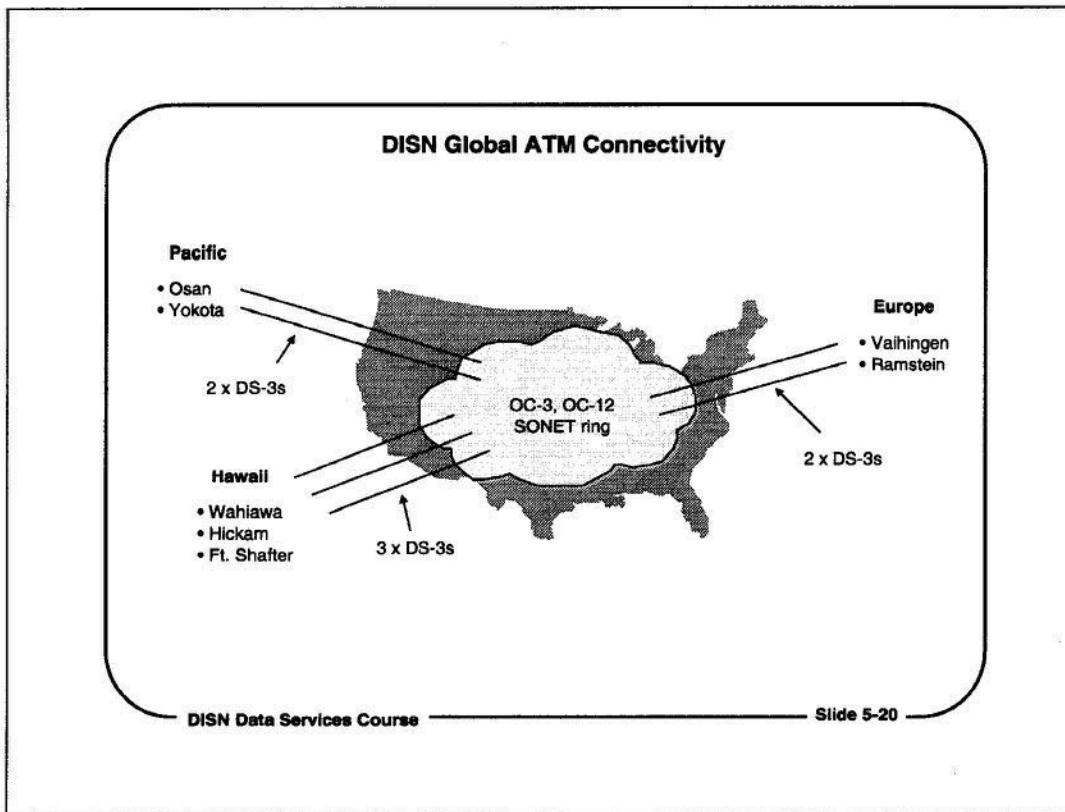
DISA has created similar ELANs on the ATM backbone for the CONUS NIPRNET, and for the European and Pacific theater NIPRNET routers. ELANs reduce latency across the ATM backbone, and they allow DISA to use the ATM backbone efficiently.



NIPRNET ELANs

DISA has established a number of ELANs within the NIPRNET, each of which is attached to other parts of the NIPRNET across the DISN ATM backbone. The purpose of the ELANs is to create communities of interest within the NIPRNET, so that traffic is delivered more quickly to its destination.

For example, the ATM network PowerHubs in the Pacific theater identify NIPRNET traffic destined for other .mil locations in the Pacific, other .mil sites in the U.S and Europe, and for the Internet. The PowerHubs router the traffic across the appropriate ELAN. For example, Internet traffic is sent over ATM PVCs to the JIS, where it is sent to one of the ISPs or NAPs in the U.S.



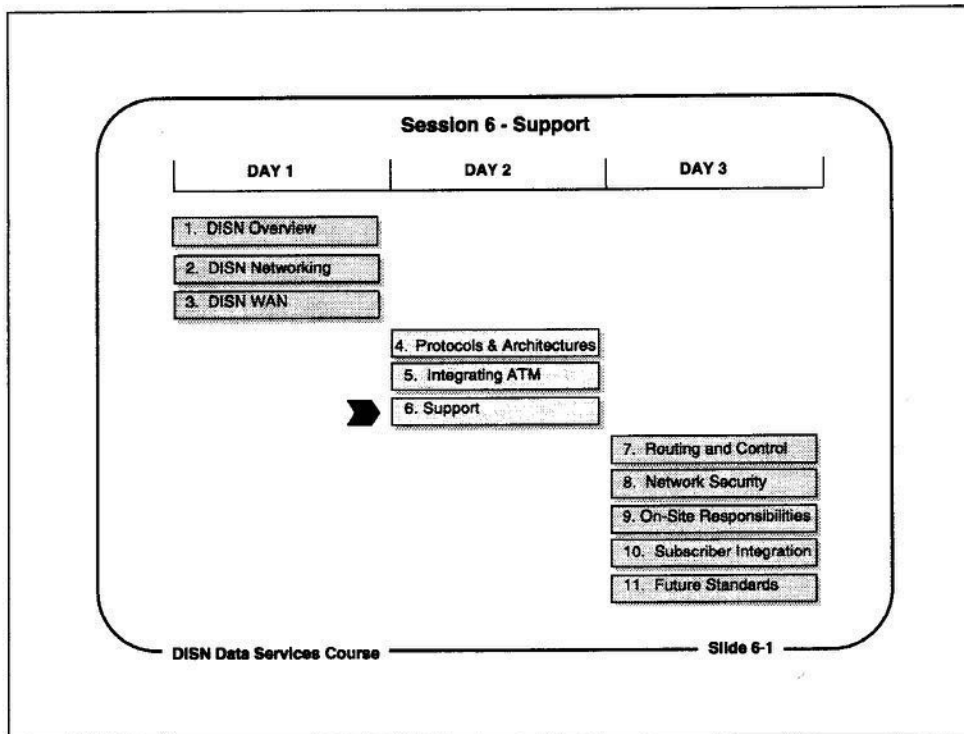
DISN Global ATM Connectivity

The initial rollout of the ATM infrastructure for the DISN backbone has been concentrated in CONUS, rather than overseas, for three reasons:

- Most of the users of the DISN Data Services networks are based in CONUS
- Commercial ATM services are more widely available in CONUS
- Costs for high-bandwidth transmission and access services are lower in CONUS

DISA has extended the ATM backbone to Europe, the Pacific, and Hawaii on DS-3 links. Most locations in the Pacific, including Hawaii, are served by DS-3 links that use part of the bandwidth of the DS-3 trunks for other DISA services, such as DSN.

The ATM backbone will be brought up in the Pacific theater sometime in 2000. In Europe, the ATM backbone is replacing the older Digital European Backbone (DEB).

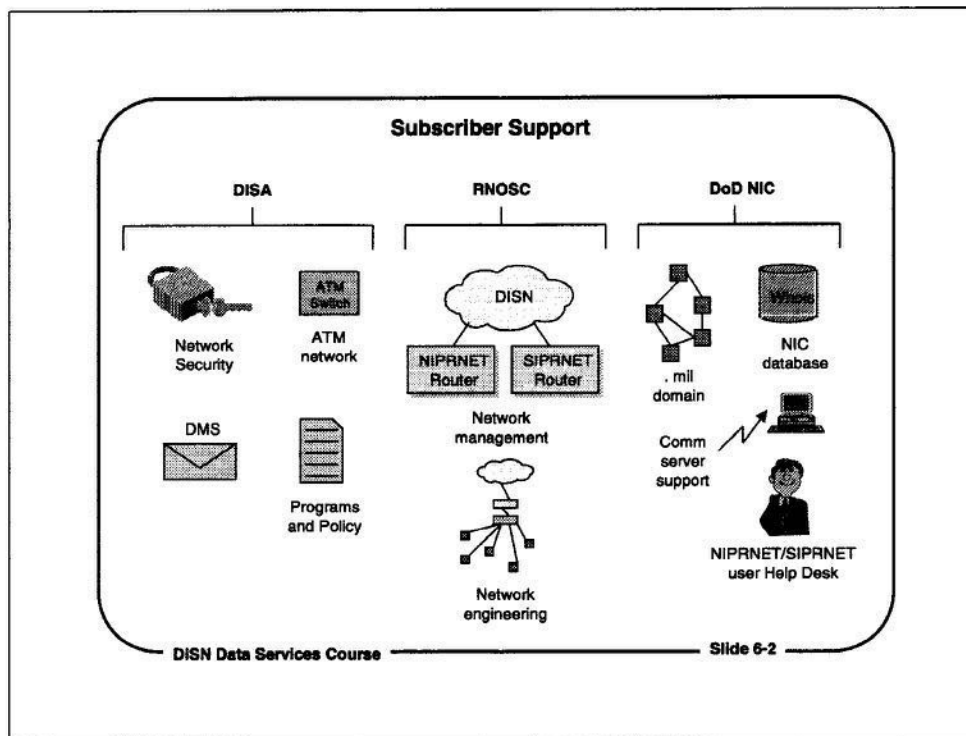


Session 6 - Support

Upon completion of this module, the students will have a general understanding of the support provided by DISA organizations to subscribers of the DISN data services networks.

This session will focus on:

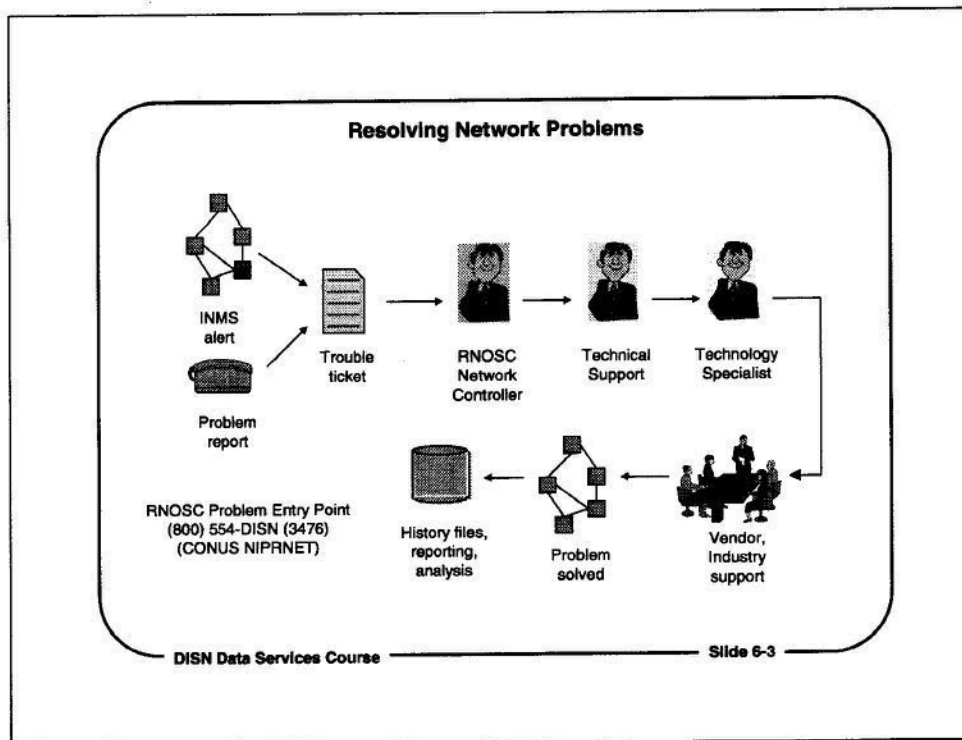
1. Identifying the types of support DISA provides
2. Describing the support functions of the RNOSC
3. Describing the support functions of the DoD NIC
4. Describing alternatives for dial-up DISN network access



Subscriber Support

Several different organizations are sponsored or operated by DISA to provide different types of support to DISN Data Services network customers. They include:

- **DISA headquarters** - Various parts of the DISA headquarters operation provide support for security monitoring and compliance assessment, run the DMS program, and determine DISA policy and programs. DISA headquarters also runs the DISN ATM Network Operations Center.
- **Regional Network Operations and Support Center (RNOSC)** - The RNOSCs monitor and control the NIPRNET and SIPRNET, the DISN backbone, and the DMS system, and they provide network engineering for DISA.
- **DoD Network Information Center (NIC)** - The DoD NIC is responsible for IP addressing and the .mil domain DNS, the DISA database of network resources, the DISA comm servers, and DISN Data Services Network subscriber support.

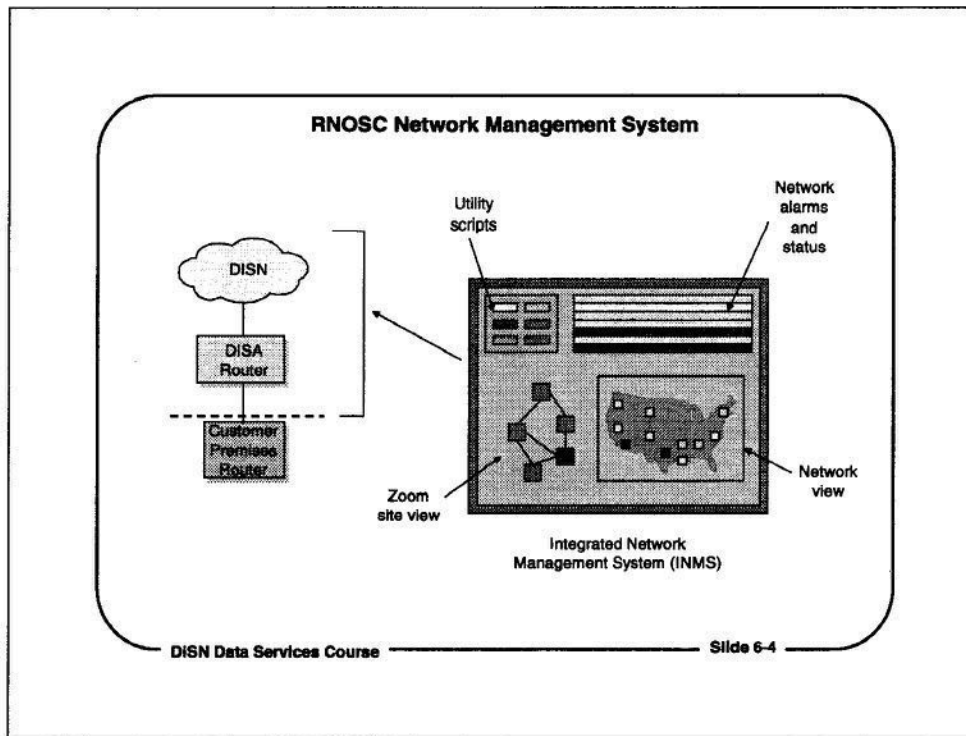


Resolving Network Problems

The RNOSC may be made aware of a network problem by an alert on the INMS display, or by a problem report to the Help Desk. If there is a problem with the network, a trouble ticket is opened, which will help the RNOSC controllers manage the problem.

The RNOSC network controllers can use utilities available on the INMS display to troubleshoot the problem, and to verify the problem. If the network controllers can't solve the problem, the controllers may escalate the problem to RNSOC or network technical support, or to local technology specialists on routing, transmission, or other services. If none of these steps solves the problem, the RNOSC can call on the equipment vendor or carrier for more assistance. The RNOSC may also contact the Node Site Coordinator or local network or telecommunications support for assistance in troubleshooting problems.

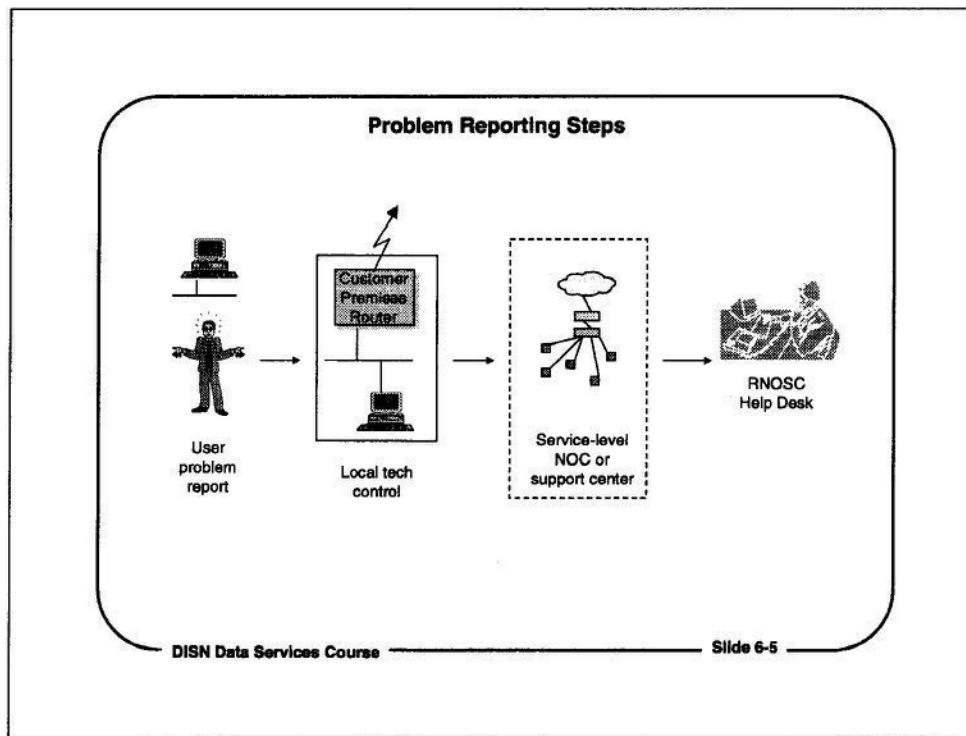
Once a problem has been resolved, a report of the problem goes in the RNOSC problem logs. Reports, problem trends, and network performance reports are drawn from the information in the problem logs.



RNOSC Network Management System

System managers and analysts at the Regional Network Operations and Security Centers (RNOSCs) use the Integrated Network Management System (INMS) to manage DISA networks. The INMS system gives DISA a consolidated view of the status of the DISN Data Services networks, and of the DISN backbone. The INMS system is a "manager of managers", in that it takes data from several other network management systems to present a consolidated view of the network. Separate INMS systems monitor the NIPRNET and SIPRNET.

The INMS display shows a diagram of the network throughout the world, and it shows color-coded status maps of network router status, link status, and link performance. RNOSC controllers can zoom in on any NIPRNET or SIPRNET router node, and determine the status of the router or the link. The system also monitors the access links that connect customer premises routers to NIPRNET and SIPRNET routers.

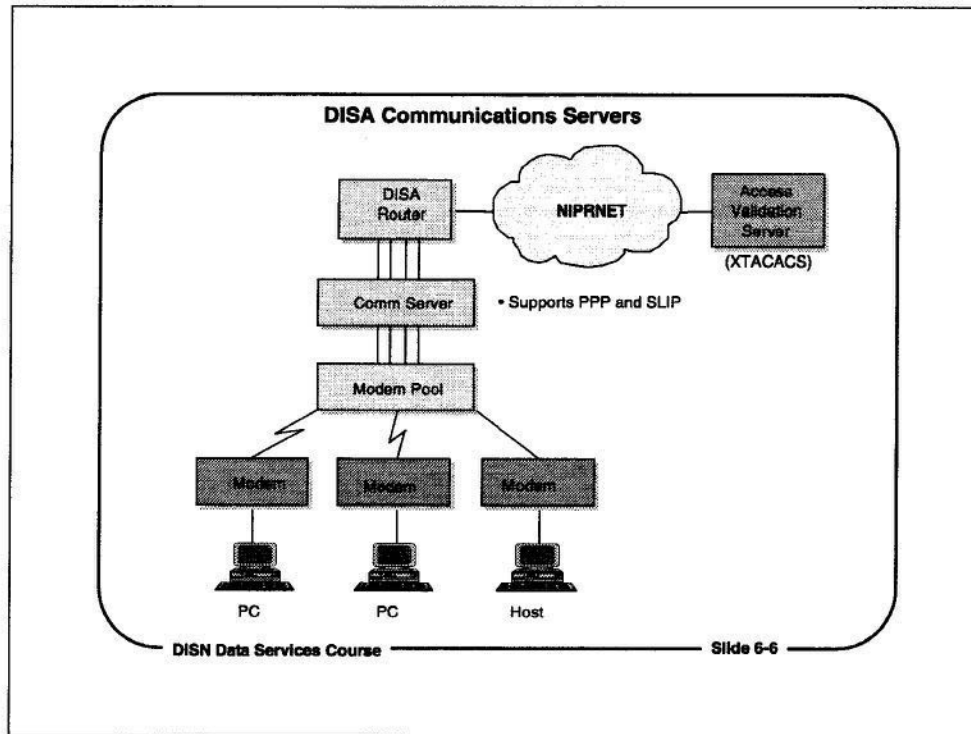


Problem Reporting Steps

Reports of user problems with networks, systems, Internet access, and other communications problems should first be investigated by local network or systems administrators. If the problem does not seem to be in the local network or local systems, the post, camp, base, or station's local tech control people should be contacted to see if they can solve or identify the problem.

Base tech control may have a service-level Network Operations Center or network support operations center to which it can report problems. If the problem cannot be solved locally, then either base tech control or the service-level NOC should contact the RNOSC Help Desk to resolve the problem.

Individual bases, branches of the armed services, DoD agencies, or bases in other parts of the world may have established other procedures for identifying and resolving network problems, and for contacting the RNOSC for assistance.

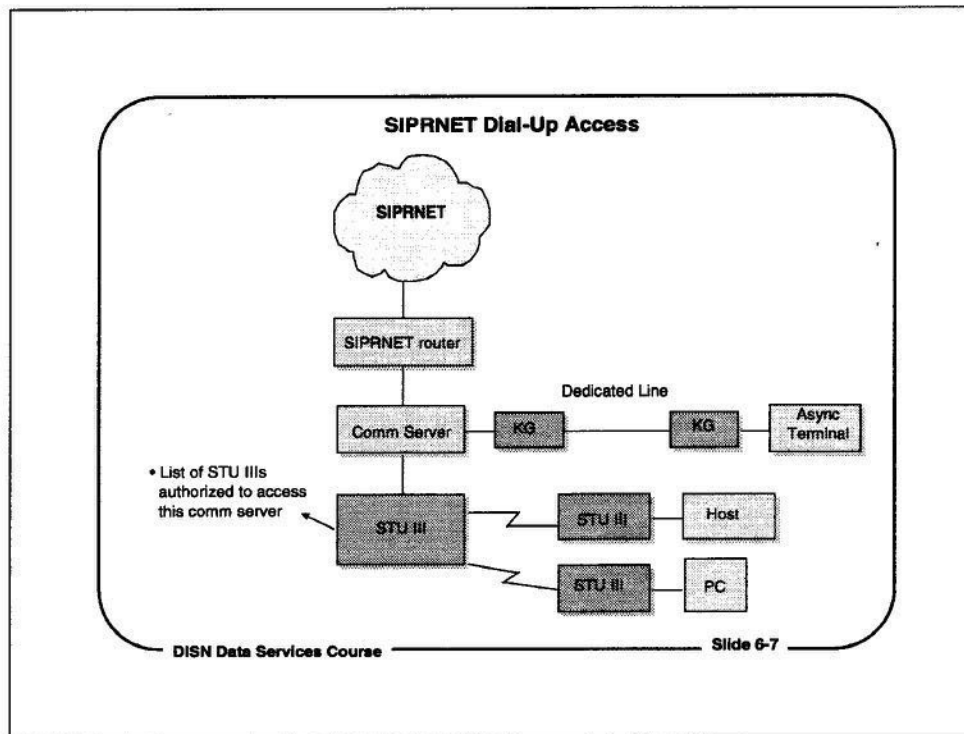


DISA Communications Servers

DISA communications servers, referred to as comm servers, give DISN Data Services network subscribers the option of dialing into the NIPRNET or SIPRNET from anywhere in the world. The DISA comm servers are connected to DISA routers, and they are maintained and managed by DISA. The routers pass traffic to the DISN Data Services network to which they are connected.

Communications servers support asynchronous, dial-up connections for users who have a terminal or standard communications software.

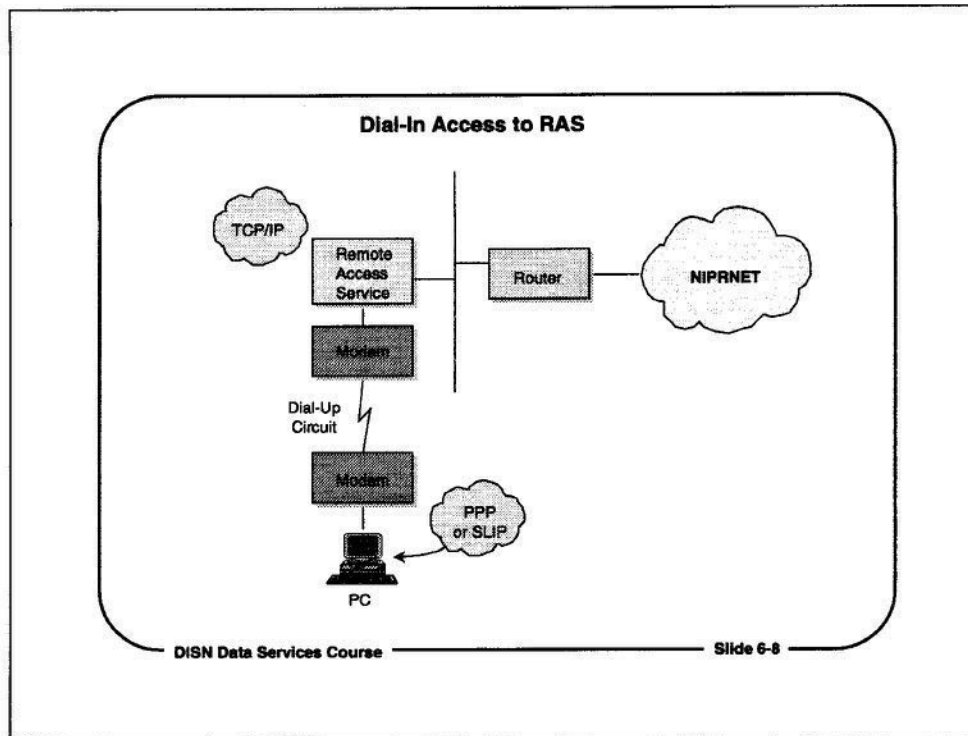
The DISA communications servers support Telnet, the Serial Line Interface Protocol (SLIP), and Point-to-Point Protocols (PPP), among others. SLIP and PPP allow dial-up users who run TCP/IP to act as a host that is directly connected to the router.



SIPRNET Dial-Up Access

The classified, Secret router network, SIPRNET, has communications servers for dial-up access. However, the dial-up connection must be made across a KG-encrypted dedicated circuit, or on a dial-up line with a STU III or KIV-7 device.

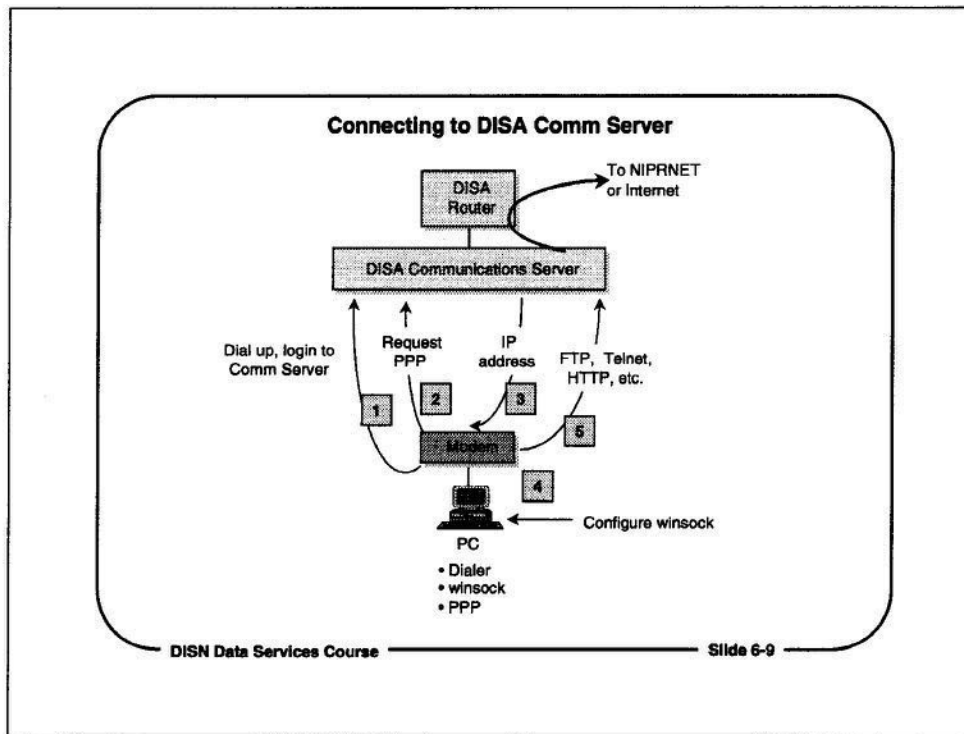
All SIPRNET comm servers are run by DISA, which controls all access to the SIPRNET.



Dial-In Access to RAS

Some customer networks have a Remote Access Server (RAS) that provides dial-in ports to the customer network. This type of dial-in service is not a DISA-managed dial-in service, because it is provided by local installations or by branches of the service for their own use.

Users who dial into a RAS, such as a Windows NT RAS server, can log into the local network domain and access resources on the network, just as if they were directly attached to the LAN.



Connecting to Comm Server

The DISA Comm Servers will permit a host (i.e., a PC running the TCP/IP protocols) to connect to the network, and then act like a network host. The Comm Server must give the PC an IP address to use for the duration of the Comm Server session, and the PC's software must be configured to use it.

After logging into the Comm Server, the user has to request a PPP session. The Comm Server will transmit an IP address to the PC, but the PC's Winsock interface (Winsock.dll) must be configured to accept that address. After that has been done, the Comm Server will pass TCP session setup transactions, and FTP, Telnet, SMTP, and HTTP requests to the network.

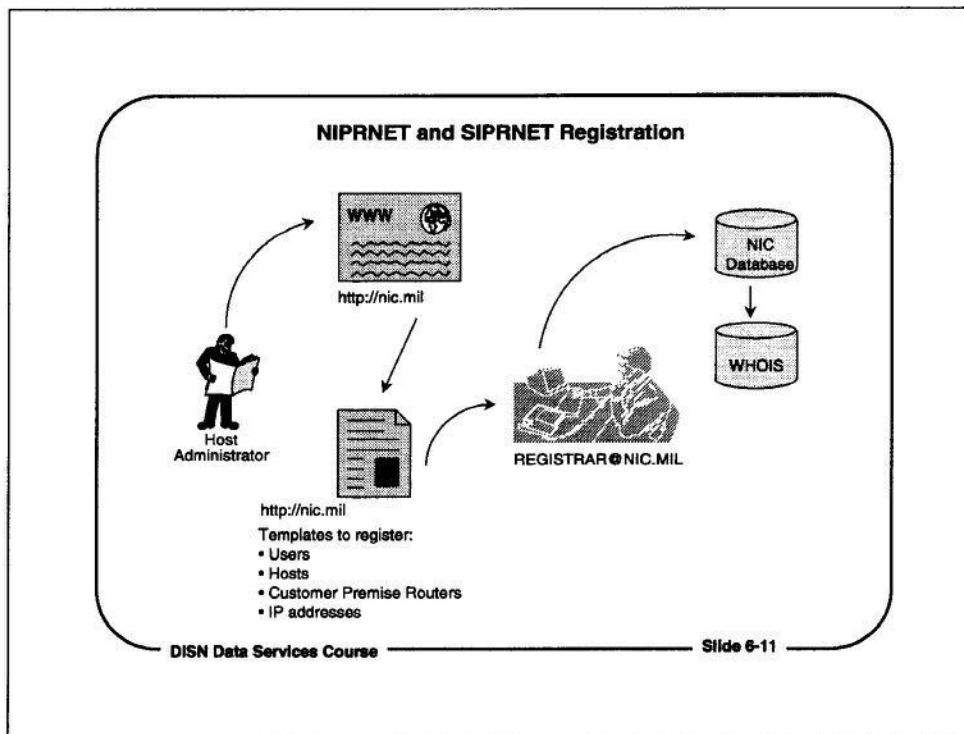
E-Mail Assistance
NIC Mailbox Accounts

NIC@NIC.MIL	General user assistance questions
HOSTMASTER@NIC.MIL	Templates for registering domains, IP networks, Internet hosts, and other network entities
REGISTRAR@NIC.MIL	Templates for registering new users, deleting and updating current user records, general questions relating to registration
ACTION@NIC.MIL	Questions concerning general NIC computer operations, problem resolution requests
SERVICE@NIC.MIL	Provides automated mail service for users who need to retrieve on-line documents via E-Mail
SCC@NIC.MIL	Requests for general security-related information and security incident reporting
SIPRNET ASSISTANCE:	<MAILBOX>@SSC.SMIL.MIL

DISN Data Services Course Slide 6-10

E-mail Assistance

If you cannot get help over the phone from the DoD Network Information Center (NIC), you can direct questions, registration requests, and other inquiries to the NIC through e-mail.



NIPRNET and SIPRNET Registration

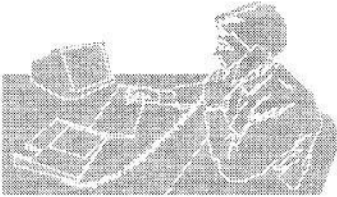
The DoD NIC is responsible for maintaining a database of NIPRNET and SIPRNET facilities and users. The NIC database includes the following DISA and customer premise entities for both the NIPRNET and the SIPRNET:

- User names, handles, addresses, and phone numbers
- User e-mail addresses
- Hosts and host administrators
- DISA Comm Servers
- DISA Comm Server card holders
- Autonomous system numbers (ASNs)
- Domain names
- IP network numbers

DISA requires that everything in the NIPRNET and SIPRNET must be registered in the NIC database, so that it can be found through WHOIS. Registration templates are available at <http://nic.mil>. Completed templates must be returned to the address specified in the template.

NIC Help Desk

E-Mail <ul style="list-style-type: none">• NIC@NIC.MIL• REGISTRAR@NIC.MIL• HOSTMASTER@NIC.MIL• SCC@NIC.MIL• ACTION@NIC.MIL	Telephone <p>Monday - Friday 7 a.m. - 7 p.m. Eastern Time 1-800-365-3642 (703)821-6266</p>
---	---



<ul style="list-style-type: none">• Registration• Protocol Questions• Dial-In access• Network Access• Database Updates• General Reference
--

DISN Data Services Course Slide 6-12

NIC Help Desk

The NIC (Network Information Center) Help Desk is available to any NIPRNET user who needs help on using the system, registering hosts or users, or finding documentation.

The Help Desk is open from 0700 to 1900 ET from Monday to Friday. The phone numbers for the NIPRNET Help Desk are:

- (800) 365-3642
- (703) 821-6266
- There is no DSN access.

SIPRNET Support Center


E-Mail

- SSC@SSC.SMIL.MIL
- REGISTRAR@SSC.SMIL.MIL
- HOSTMASTER@SSC.SMIL.MIL
- SCC@SSC.SMIL.MIL

Telephone

Monday - Friday
7 a.m. - 7 p.m. Eastern Time
*1-800-582-2567
(703)821-6260

*STU-III capable



• Registration
• Protocol Questions
• Dial-in access
• Network Access
• Database Updates
• General Reference

DISN Data Services Course Slide 6-13

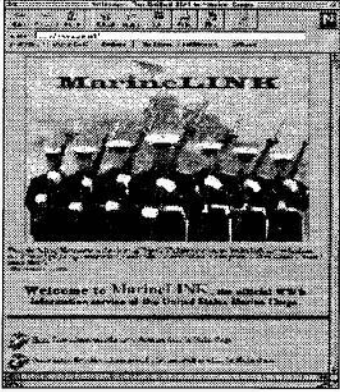
SIPRNET Support Center

The SIPRNET Support Center (SSC) is available to any SIPRNET user who needs help using the system, registering hosts or users, or finding documentation.

The Help Desk is open from 0700 to 1900 ET from Monday to Friday. The phone numbers for the SIPRNET Help Desk are:

- (800) 582-2567
- (703) 821-6260.

DoD Web Pages



DoD NIC	http://nic.mil
.mil Domain POCs	http://nic.mil/poc
Air Force	http://www.af.mil
Army	http://www.army.mil
Navy	http://www.navy.mil
Marine Corps	http://www.usmc.mil
DoD DefenseLink	http://www.defenselink.mil
DISA	http://www.disa.mil
*SIPRNET SSC	http://ssc.smil.mil

*accessible only on SIPRNET

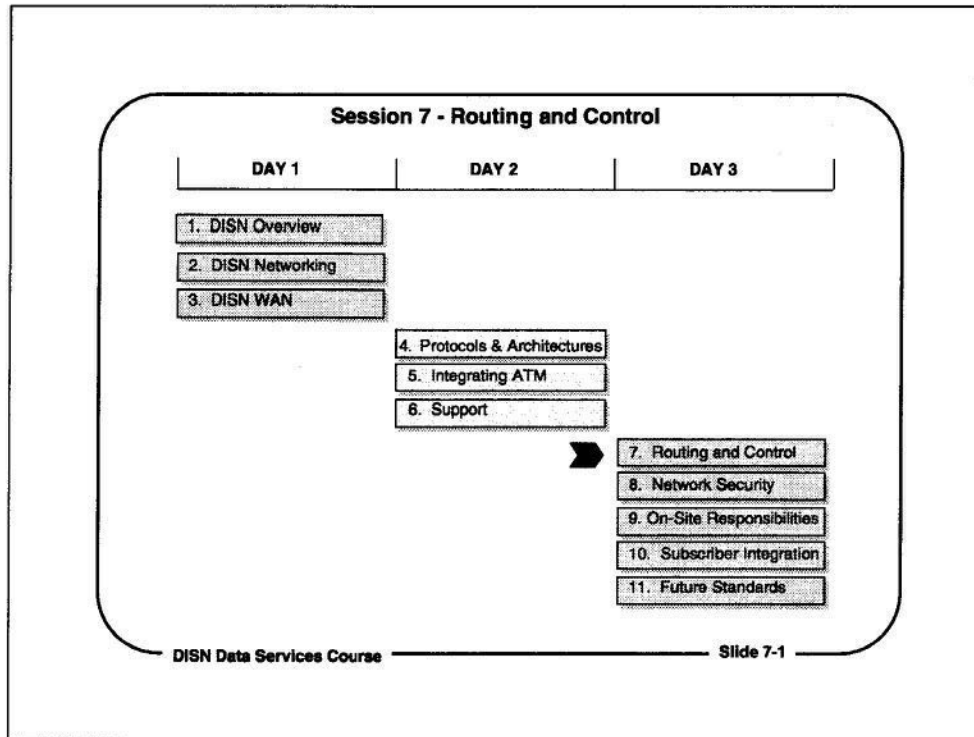
DISN Data Services Course Slide 6-14

DoD Web Pages

The World Wide Web (WWW) has become the primary vehicle for Internet information access and presentation, and its use is spreading rapidly on the NIPRNET.

Each of the branches of the armed services has its own main Web site, which contains links to other DoD sites, as well as other Internet Web sites.

The SIPRNET uses the same applications and protocols as the NIPRNET, so Web access is being deployed there also. However, SIPRNET hosts and Web sites are only accessible from other SIPRNET hosts and networks.

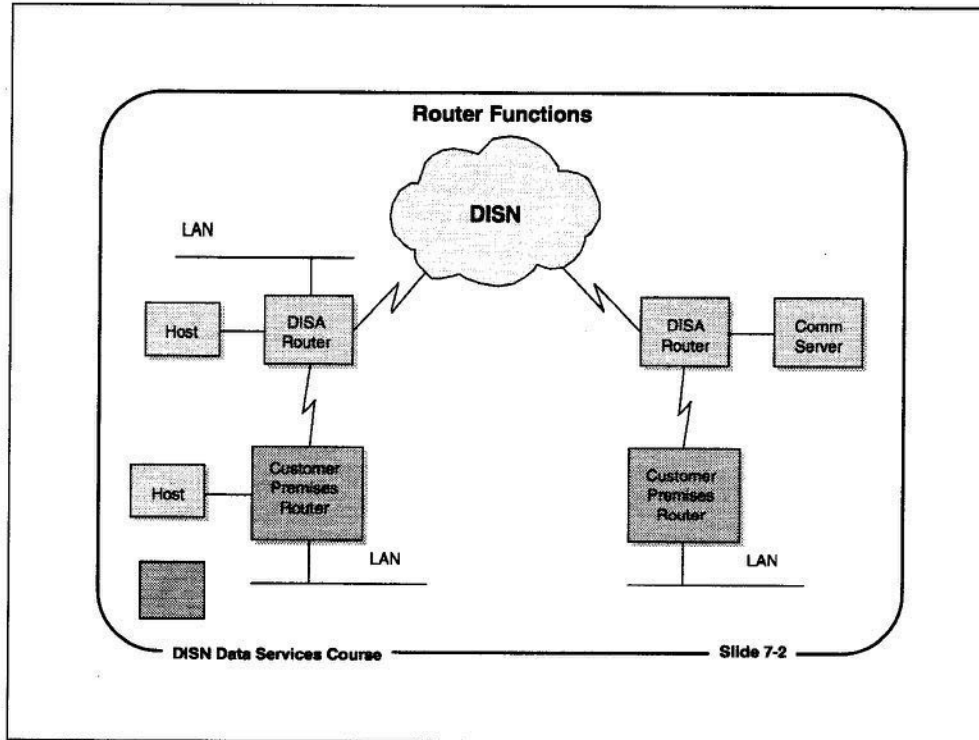


Session 7 - Routing and Control

Upon completion of this module, the students will have a general understanding of the operation of the DISA routers and customer premise routers, router configuration and routing tables, router table updates, default routers, and routing between networks.

This session will focus on:

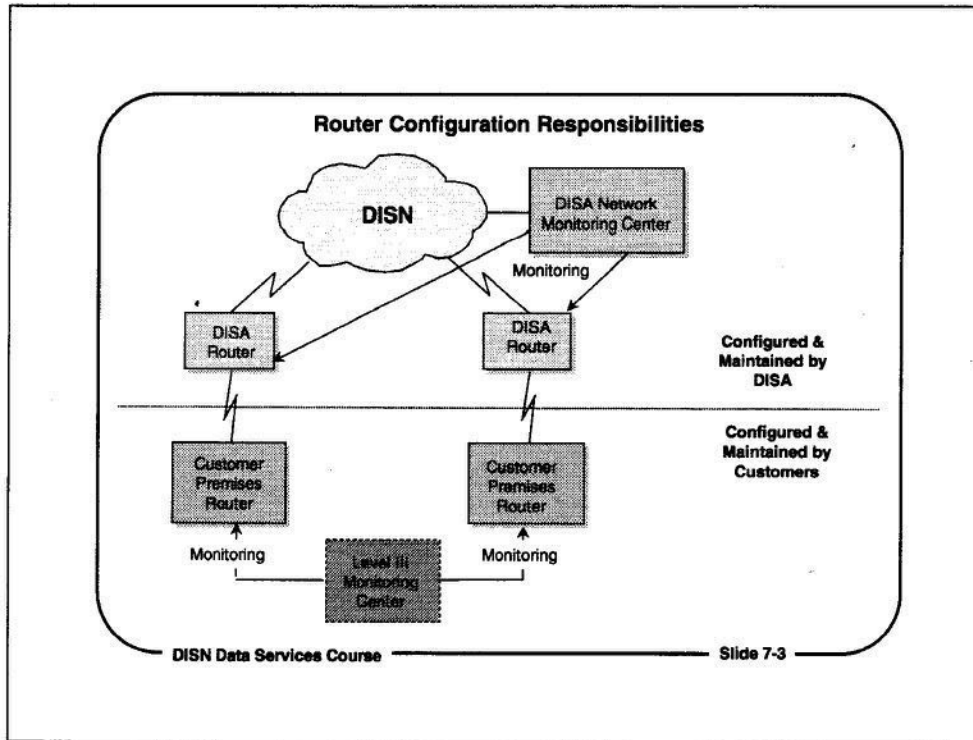
1. Defining the functions of DISA and customer premise routers
2. Describing the operation of IP routing
3. Describing the processes by which routers are configured
4. Describing the methods by which routing tables are maintained
5. Showing methods by which data is routed between different networks



Router Functions

The purpose of routers is to determine where to send IP datagrams, so that they reach the correct destination network. Routers forward IP datagrams from one router to another until they reach a router connected to the destination network.

In DISN Data Services networks, routers are designated DISA routers or Customer Premise routers. Some DISA routers connect to the DISN backbone, and some are designated "hub" routers. Customer Premise routers connect behind DISA routers. They handle local traffic and route traffic that will cross the backbone to the DISA routers.

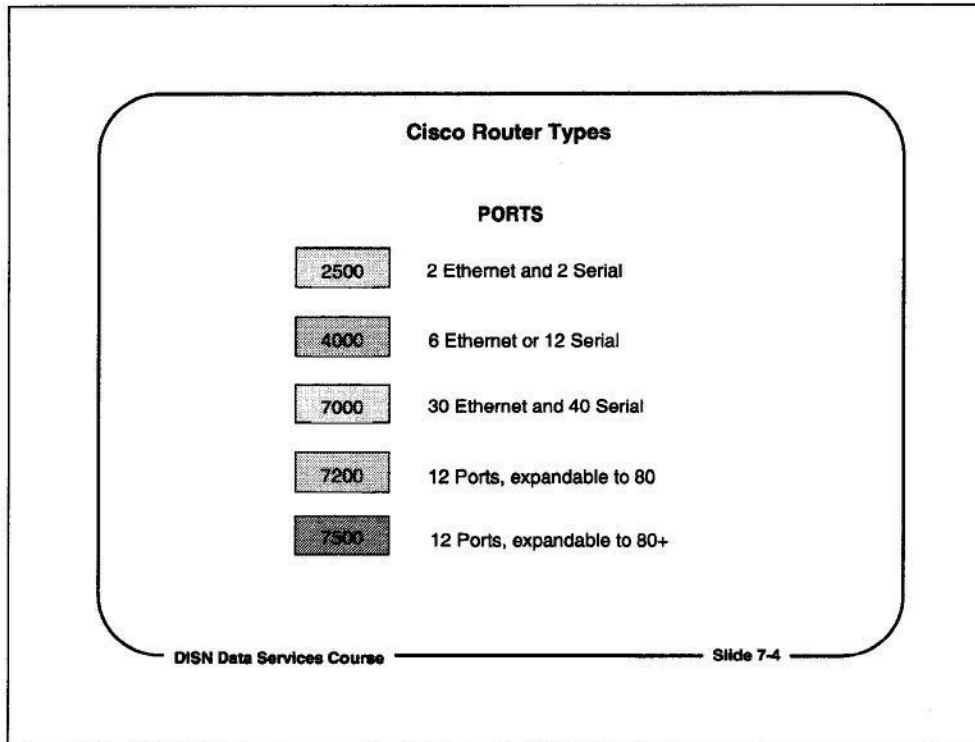


Router Configuration Responsibilities

DISA owns the DISA routers, so DISA is responsible for configuring and maintaining the NIPRNET and SIPRNET router networks. DISA routers are also monitored and controlled by the DISA Remote Network Operations and Security Centers (RNOSCs).

Customer premises routers are configured and maintained by DISA customers, and by local agencies that own the routers. These routers are monitored by customer, service-wide, or agency monitoring centers, if such monitoring centers exist.

For a fee of \$50 a month, DISA will configure and manage customer premise routers (Cisco and Nortel / Bay Networks routers only).



Cisco Router Types

Routers used on the DISA backbone are Cisco routers which are produced by Cisco Communications, Inc. DISA decided to standardize on Cisco products because they are widely used by NIPRNET and SIPRNET customers.. In addition, standardizing on one vendor's equipment simplifies configuration issues, eliminates many compatibility issues among router types and router protocols, and allows DISA to maintain a consistent version of router software.

Cisco routers will interoperate with customer premises routers from other vendors, although other vendors' routers may not use some features that are proprietary or specific to Cisco routers.

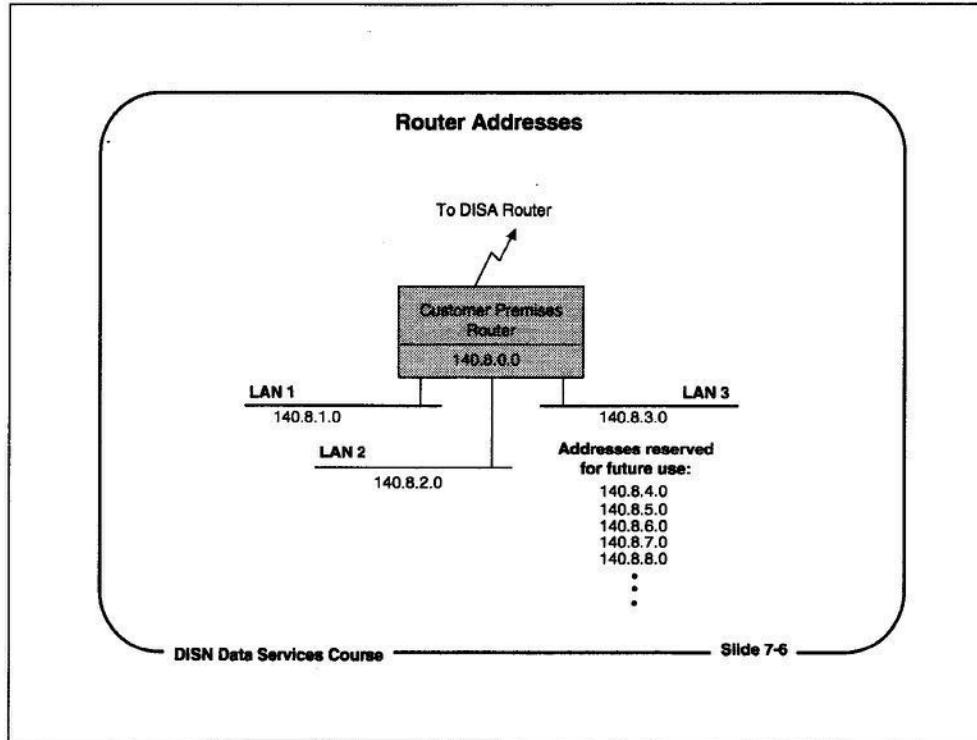
Router and ATM Switch Throughput		
ATM Switch		
Typical Trunks	Typical Switching Capacity	Available Throughput
OC-3 (155 Mbps) OC-12 (923 Mbps)	400,000 cells/second	~ 900 Mbps
IP Router		
Typical Trunks	Typical Routing Capacity	Available Throughput
T-1 (1.5 Mbps) T-3 (45 Mbps)	50,000+ packets/second	~ 25 Mbps
DISN Data Services Course		Slide 7-5

Router and ATM Throughput Comparison

The IP routers used in the DISN Data Services networks today deliver far greater performance at lower cost than the original routers in the networks. The IP routers in the DISN Data Services networks use faster microprocessors than were available even a few years, they use better software, and they have very large scale integrated circuits, which also operate faster.

DISA is installing an ATM network in the DISN backbone to increase the throughput of the DISN backbone. ATM switches do less processing on each cell, and they interface cleanly to high-speed digital circuits. Consequently, the throughput of an ATM switch is much higher than that of an IP router.

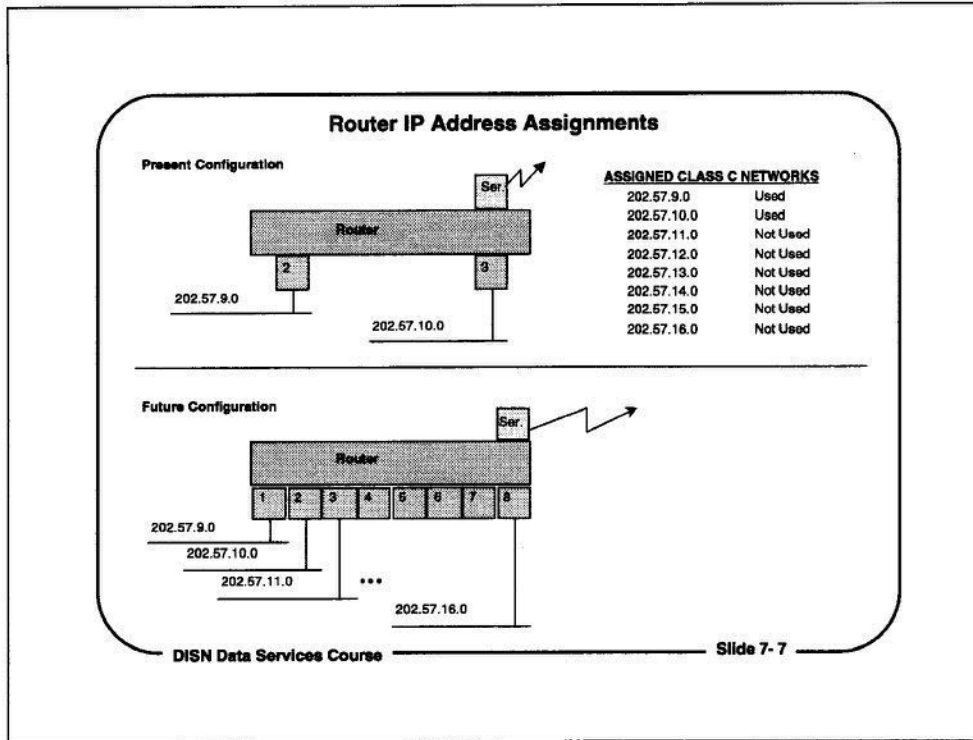
The figures in the tables indicate average performance and throughput. Actual performance varies by vendor, interface type, memory configuration, and processor speed.



Router Addresses

Each network interface on a router has a separate address. Each IP address corresponds to a physical port for a network connection, and it maps to a network that is reachable through that port.

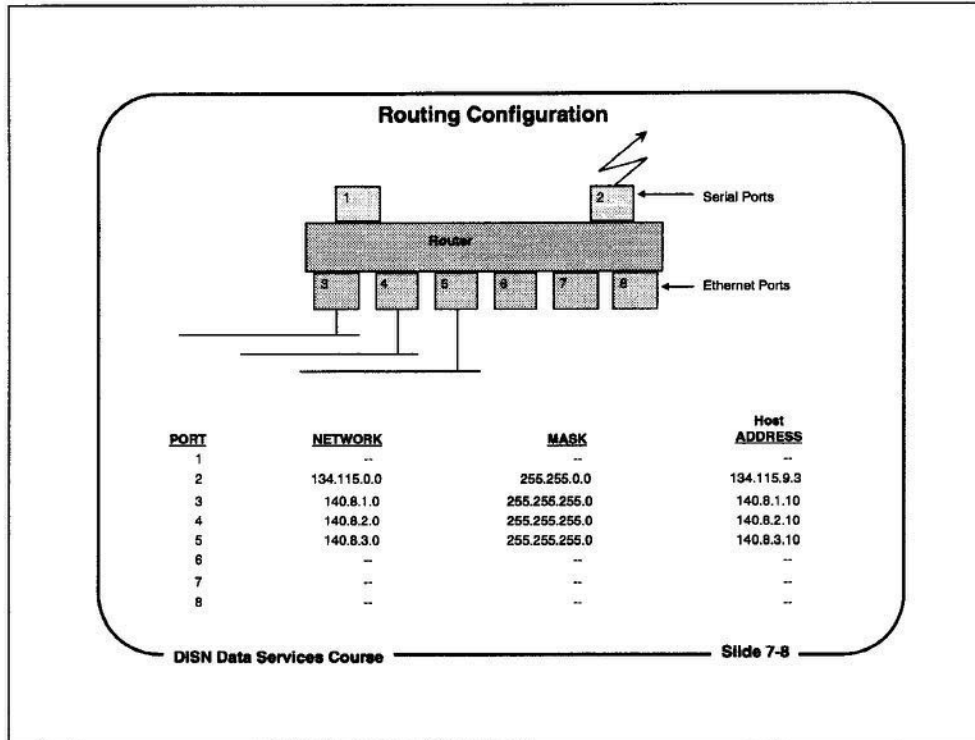
Each network port on a router has an IP network number associated with that port. The port also has a host address on that network.



Router IP Address Assignments

A router may be assigned more than one IP network address, even though only a few of the network addresses may be in use. As more ports and networks are added to the router, the unused IP network addresses can be used from the assigned IP address range, without applying for more IP addresses.

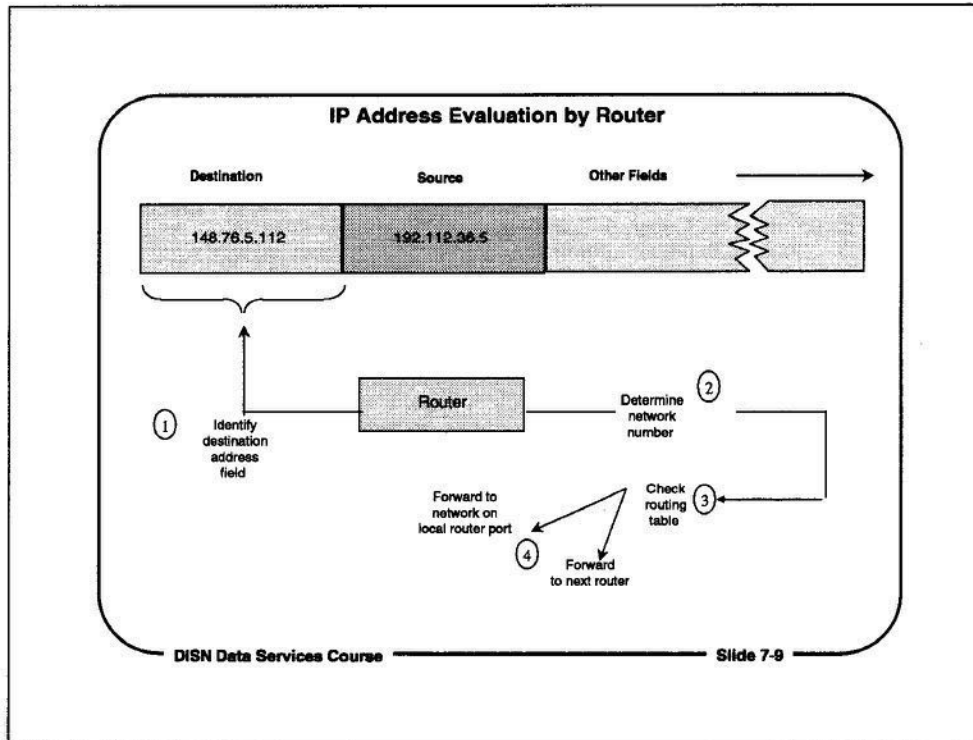
All IP network addresses for Department of Defense installations are assigned through the DoD Network Information Center (NIC).



Routing Configuration

Routers make routing decisions on their internal routing tables. Routing tables indicate the networks that are attached to specific router ports, or networks that are reachable through other, neighboring routers. Routers do not distinguish between local ports and WAN ports.

IP networks can be divided into smaller units, called subnetworks. Subnetworks provide extra flexibility for the network administrator. When an IP network address is subnetworked, the router maintains a bit pattern, referred to as a mask, that indicates the bits of each IP address that are being used for the network address. The mask is expressed as a four-part decimal number that when translated to a binary number, indicates the bits of each IP address byte used for the IP network address.

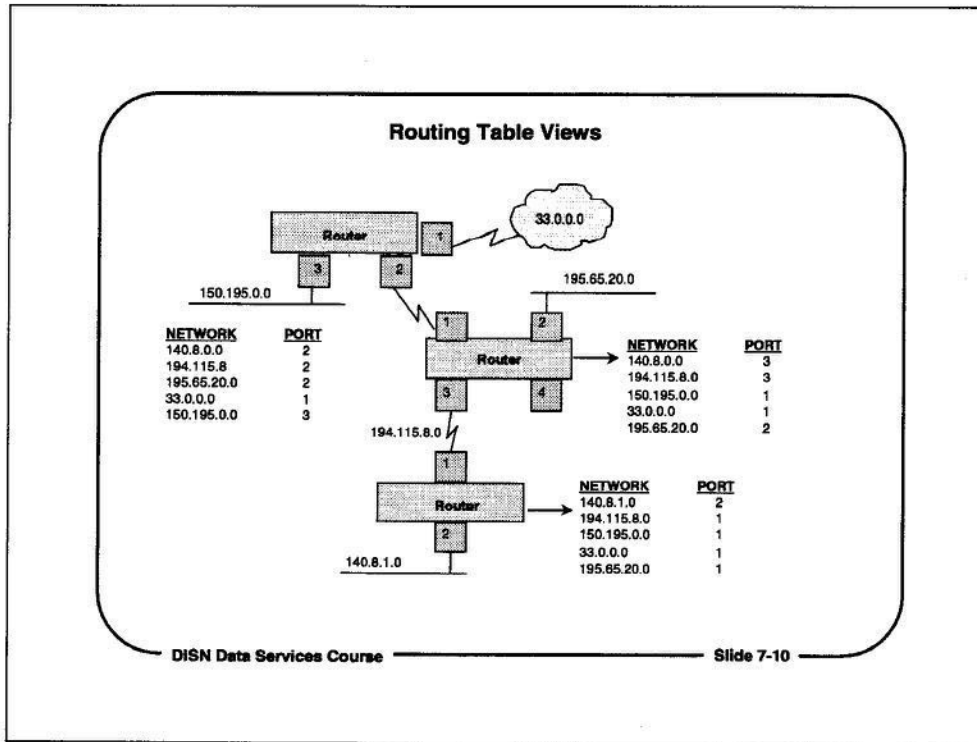


IP Address Evaluation by Router

Routers evaluate the destination IP address field of IP datagrams to make routing decisions. After the router locates the bits of the destination IP address field, it applies an IP mask to identify the network ID bits, and then makes a routing decision.

The steps of the routing process are:

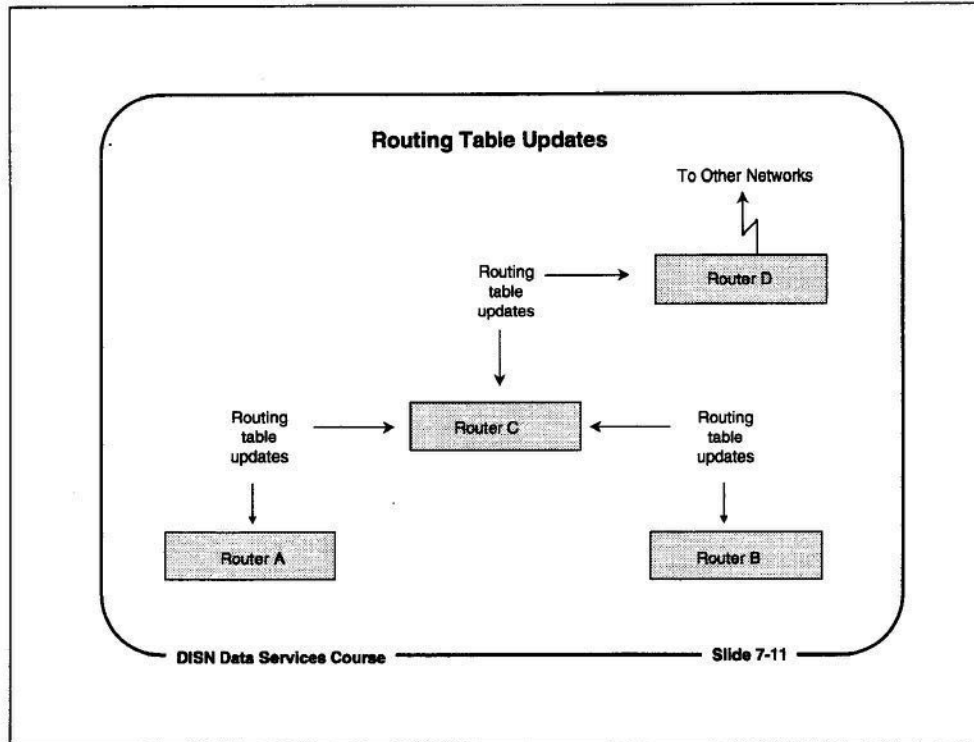
- Identify bits of the destination IP address field
- Identify bits of IP address used for network address
- Refer to routing table to map network ID to a port
- Forward IP datagram through a local port to another router, or to a locally-connected network.



Routing Table Views

Each router has its own view of the networks to which it is connected, and which it can reach. Its view is different from that of neighboring routers, which build their routing tables based on the networks to which they are connected.

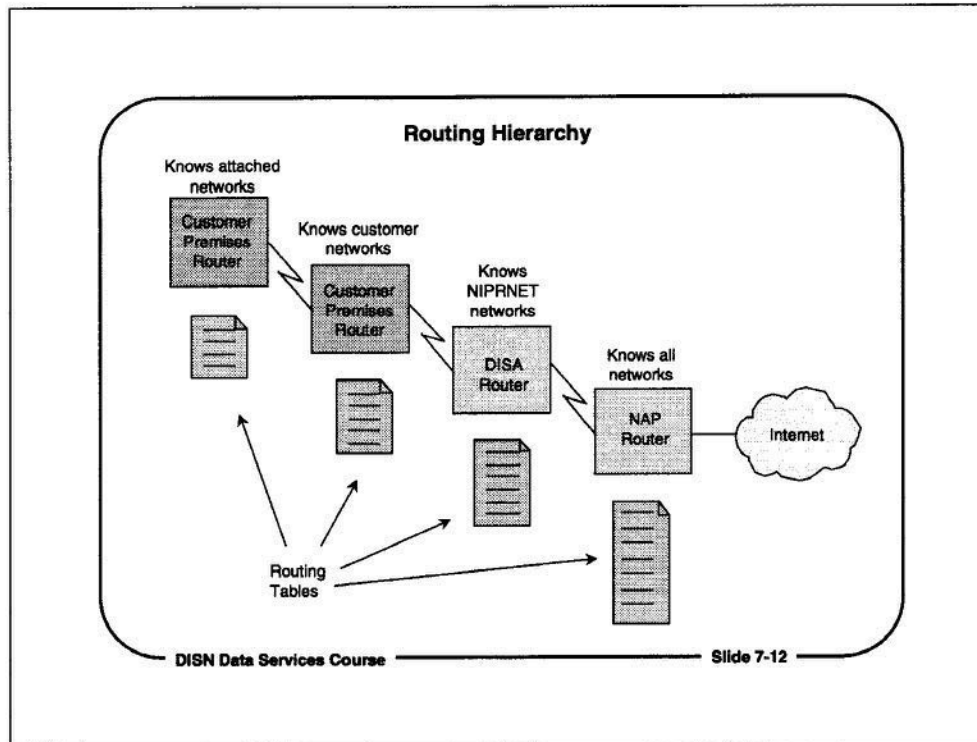
Each router's routing tables reflect the networks reachable through that router's local ports. In addition, each router's routing tables contain entries that indicate how many router links, or hops, an IP datagram must cross to reach a destination network. The routing table may also contain a value for the relative cost of crossing a specific router-to-router link, in order to force traffic between routers across specific network links.



Routing Table Updates

Each router updates its routing tables periodically in order to get a fresh picture of changes in the configuration of the network, or the addition or deletion of networks. Routers may send messages to all neighboring routers at intervals from 30 seconds to every five minutes, indicating that they are active. At that time, routers may also indicate changes, if any, to their local routing tables.

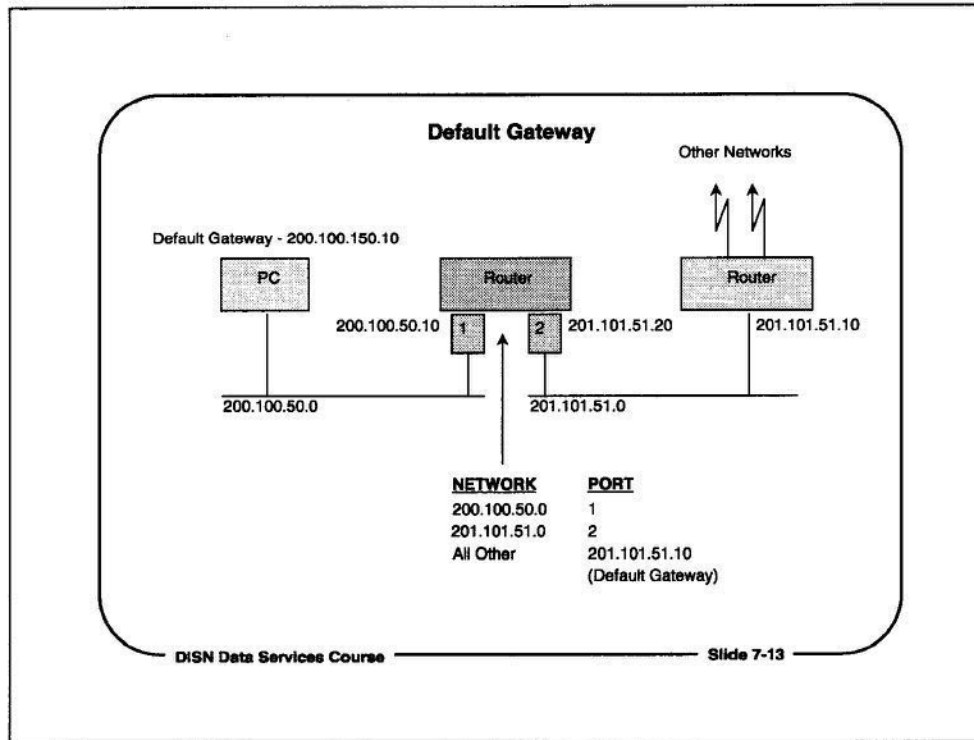
Routers save changes reported to them by neighboring routers in their routing tables. Current routing tables are maintained by routers, periodically updating their routing tables based on reports from neighboring routers.



Routing Hierarchy

All routers have an equivalent routing capability, but some routers are aware of a greater range of reachable networks than other routers. Memory size and CPU capabilities determine the number of routes and networks a router can maintain, so most routers have only a partial picture of network connectivity.

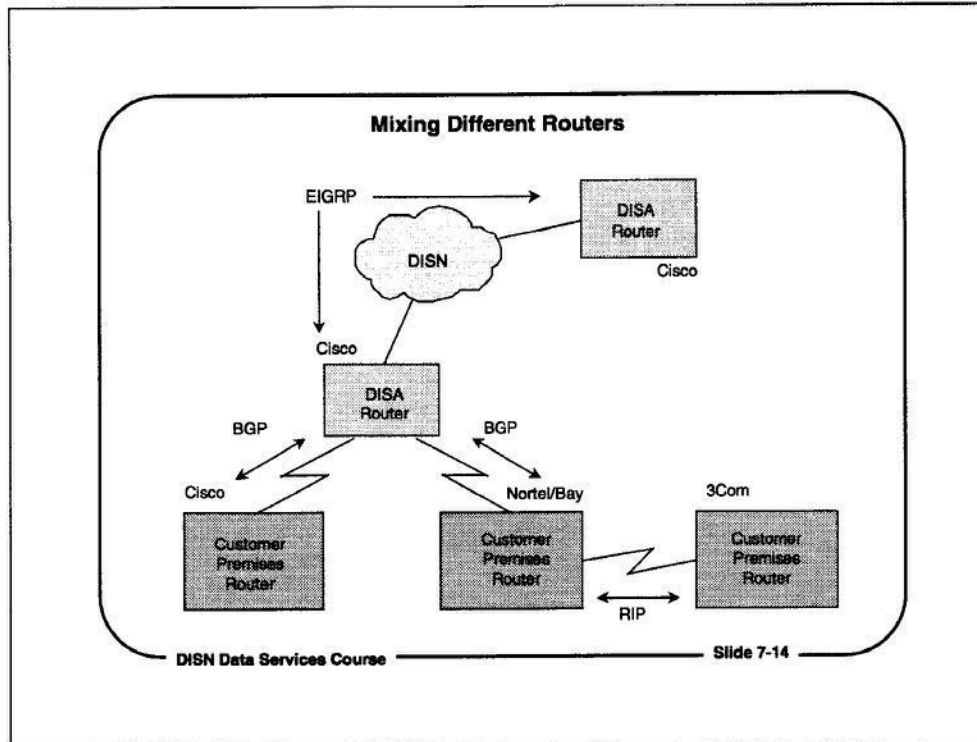
Most routers are aware of most networks in the network to which they are connected, but post, camp, base, or station routers may only know about the networks to which they are directly connected. Some routers, such as the JIS routers connected to the NAPs or to FIX-W, are aware of most networks, so they serve as top-level routers.



Default Gateway

In order to simplify routing tables and routing decisions, many routers do not have a complete picture of all of the networks that are reachable through other routers. Most routers know about a default gateway, which can help locate otherwise unknown networks.

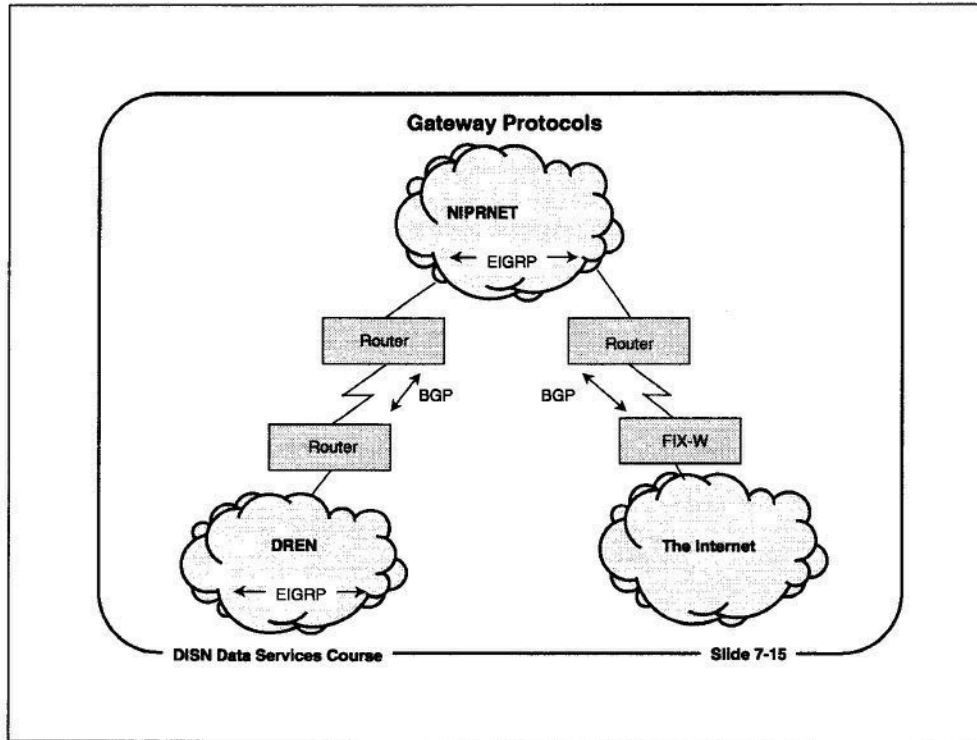
A default gateway is a router port to which IP datagrams may be sent if a router cannot locate a route to a destination network. The default gateway points to another router to which IP datagrams can be sent if the router does not have an entry for a specific destination network. Presumably, the other router has a larger and more comprehensive list of networks in its routing table. However, the other router may also have a default gateway to which it sends IP datagrams for unknown networks.



Mixing Different Routers

In most cases, the DISA routers are Cisco routers, but customer premises routers may be any type of router that can route IP. A customer premises router may also be a host that is configured to do IP routing. Most UNIX hosts, for example, can act as IP routers.

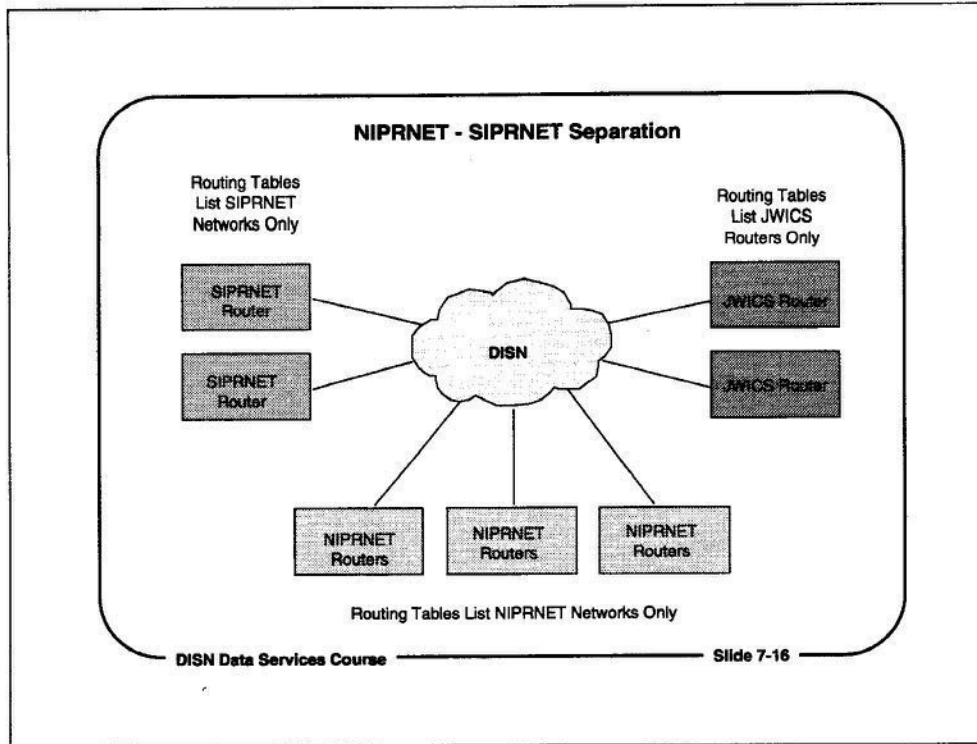
Cisco routers use the Cisco-proprietary EIGRP protocol to pass routing table information between routers. Other vendors' routers may use their own routing protocols. If other vendors' routers are connected to DISA Cisco routers, they may use the Routing Information Protocol (RIP), an industry standard, non-proprietary routing protocol, to exchange routing table information.



Gateway Protocols

EIGRP, Enhanced Interior Gateway Routing Protocol, developed by Cisco, is a protocol for routing within an Autonomous System (AS).

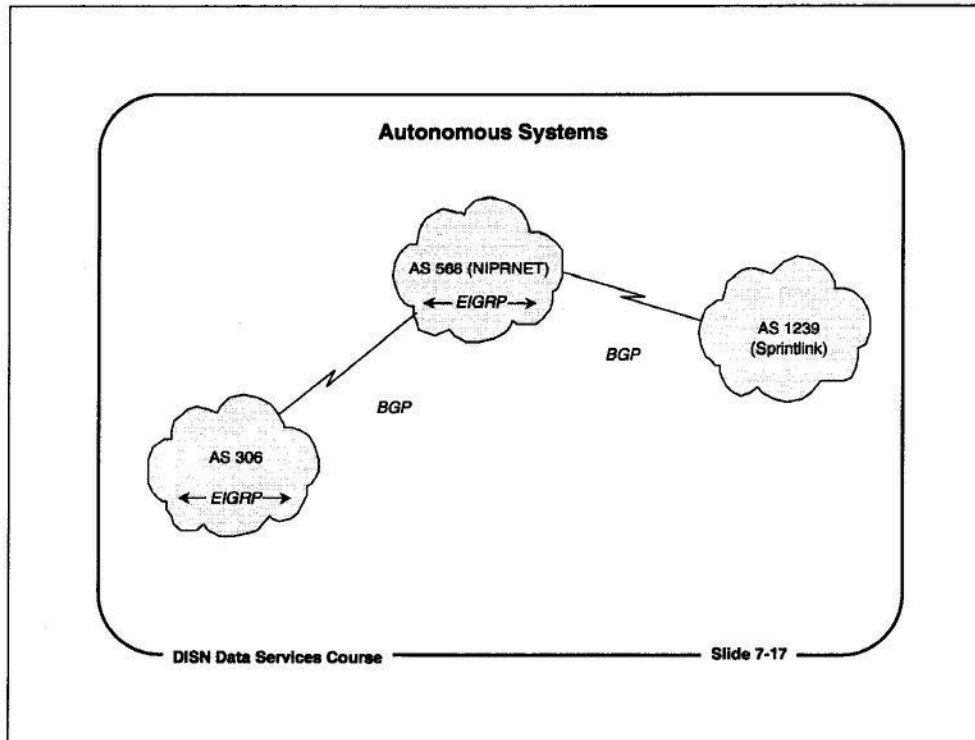
The DISA routers that connect the DISN Data Services networks to other networks, such as the Internet and the DREN, use an external routing protocol to exchange routing information with external networks. The older Exterior Gateway Protocol (EGP) is being replaced by the newer Border Gateway Protocol, Version 4 (BGP4).



NIPRNET - SIPRNET Separation

The DISA routers for NIPRNET and SIPRNET are connected to the same DISN backbone network. However, the two DISN Data Services networks are logically separated from each other, because the NIPRNET routers only talk to other NIPRNET routers, and the SIPRNET routers only talk to other SIPRNET routers.

The SIPRNET and the JWICS network are also physically separated, and they use different forms of encryption. JWICS routers maintain the same logical separation from the routers of the other DISN Data Services networks.

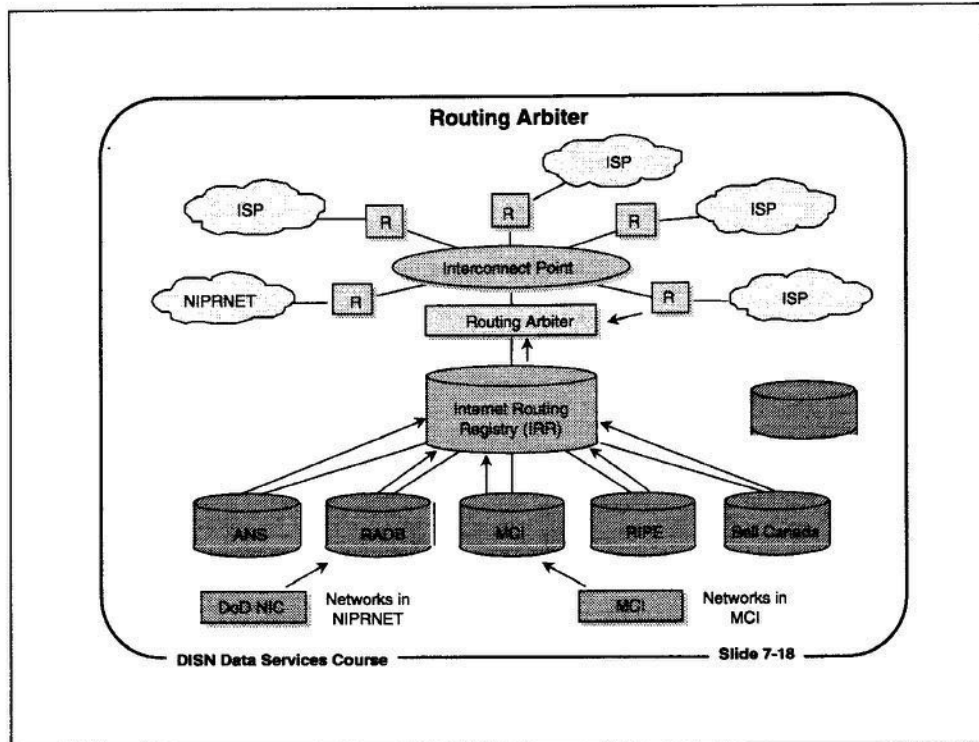


Autonomous Systems

Today, there are so many networks in the Internet that one agency or organization can't control all of the routers in the Internet. So, networks that are under the administrative control of one organization or agency are grouped into Autonomous Systems (AS), each of which is assigned a unique Autonomous System Number (ASN):

The ASN identifies the networks that are part of the AS, as well as the organization that controls the networks in the AS. For example, networks in the NIPRNET in CONUS are part of AS 568.

Autonomous Systems communicate with neighboring ASs, passing information about the networks within each AS. Neighboring ASs may also pass "routing policy" information that specifies the networks for which they will accept network traffic.

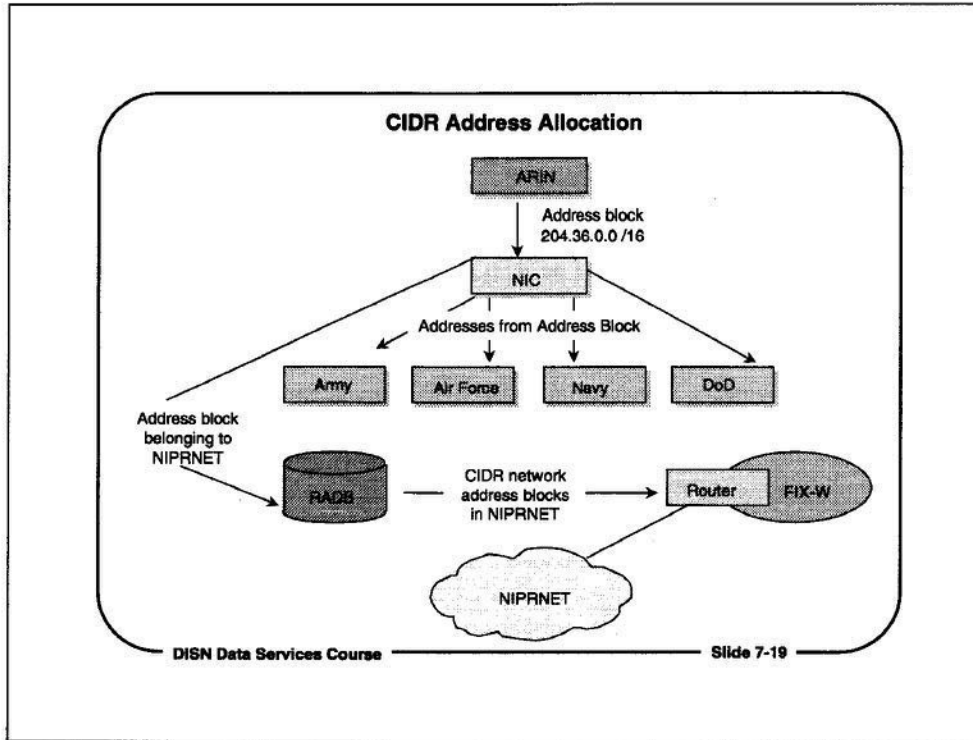


Routing Arbiter

The Autonomous Systems of many Internet Service Providers, including the NIPRNET, exchange traffic at several major network interchange points around the world. In the United States, these are called Network Access Points (NAPs), Metropolitan Area Exchanges (MAEs), or a Federal Internet Exchange (FIX). The FIX-West exchange point transfers traffic between the networks of the armed forces and those of other federal government agencies.

The routers at the exchange points may refer to a central database, called the Routing Arbiter, that maps networks in the Internet and the ASs to which they belong. When a new IP network address is assigned to a NIPRNET customer, the DoD NIC registers the network in the Routing Arbiter Database (RADB). This makes the network visible to the rest of the Internet, so that traffic can be routed to it.

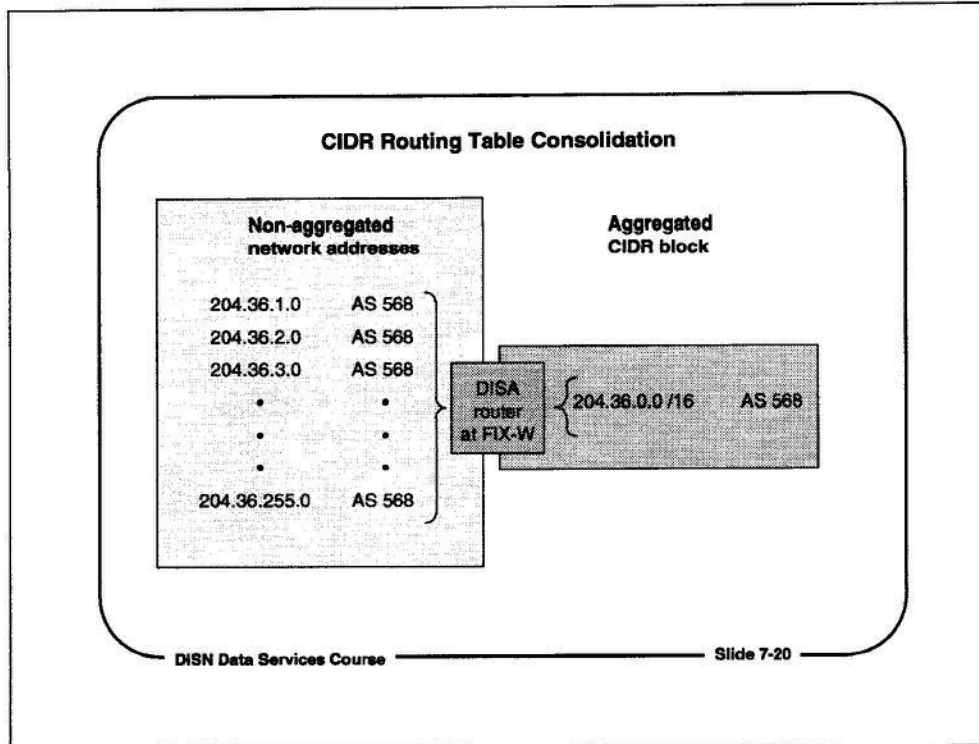
RADB registrations are done by the DoD NIC at the request of the administrators of NIPRNET networks. Contact netreg@nic.mil for information on registering a network in the RADB.



CIDR Address Allocation

Both DISA and many ISPs have taken steps to reduce the proliferation of network addresses in the routing tables of the routers at the major exchange points. One technique is Classless Inter-Domain Routing (CIDR), which consolidates many contiguous IP network addresses into a block of addresses. An AS tells neighboring ASes about the block of addresses it controls, instead of each individual address.

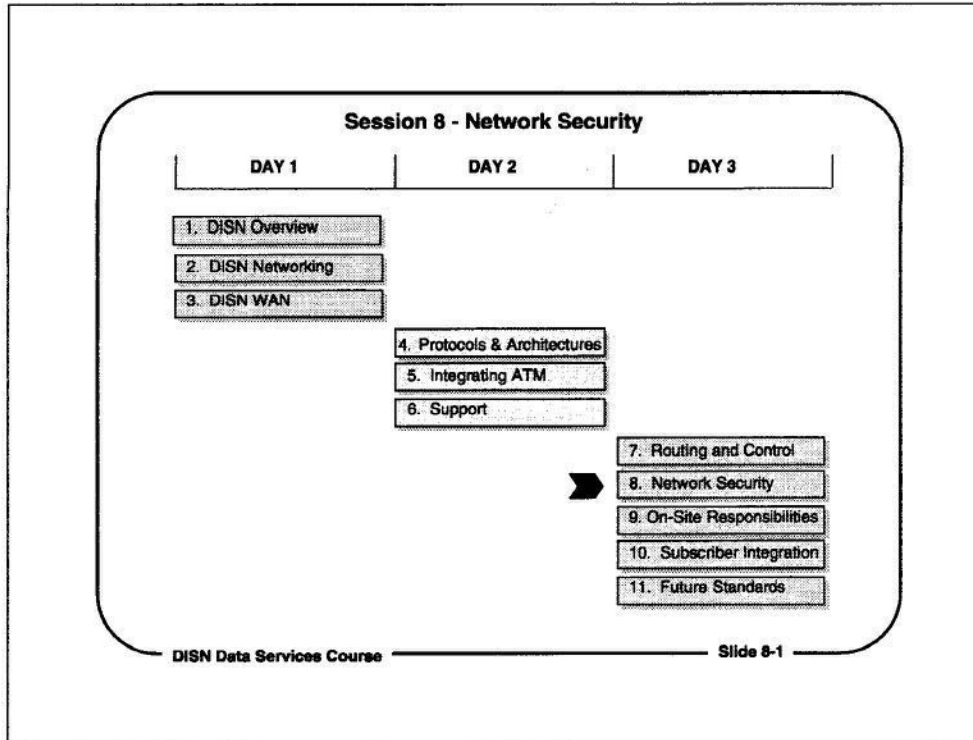
For example, the DoD NIC assigns IP addresses to branches of the armed services from a block of IP addresses that ARIN has assigned to the NIC. The NIPRNET routers at FIX-W and the NAP "announce" the CIDR blocks to which those addresses belong, rather than the individual network addresses.



CIDR Routing Table Consolidation

CIDR addressing consolidates many contiguous IP network addresses into a block of addresses. "CIDRized" addresses belong to a specific block of addresses, which belongs to a specific ISP. For Internet routing purposes, DISA is considered another ISP, to which specific network addresses or blocks of network addresses belong.

The CIDR address notation convention uses a route prefix and an extension. For example, all of the 255 IP network addresses in the range from 204.36.1.0 to 204.36.255.0 can be specified by one CIDR block, which is 204.36.0.0/16. The "/16" indicates all addresses falling after the first 16 bits of the first network address in the CIDR block.

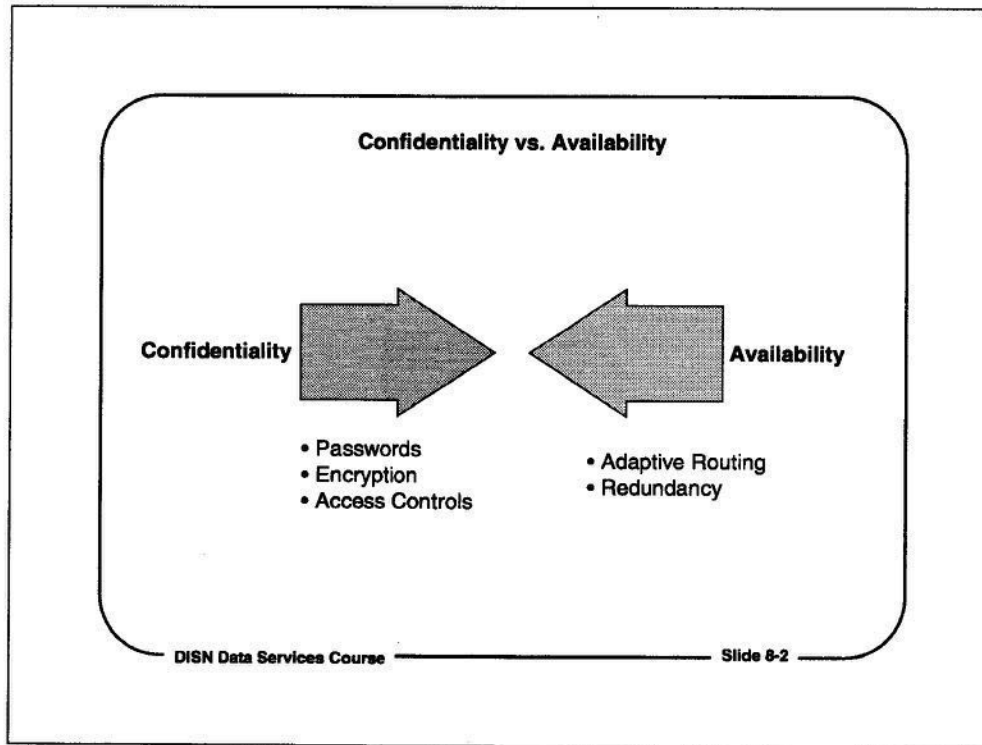


Session 8 - Network Security

Upon completion of this module, the students will have an understanding of the security threats the network and its users face, as well as DISA programs to protect the network and its data. The students will also be able to describe the XTACACS access control system, and DISA and user security responsibilities. They will also be able to describe host and end-to-end encryption, different types of encryption devices, and the function of firewalls.

This session will focus on:

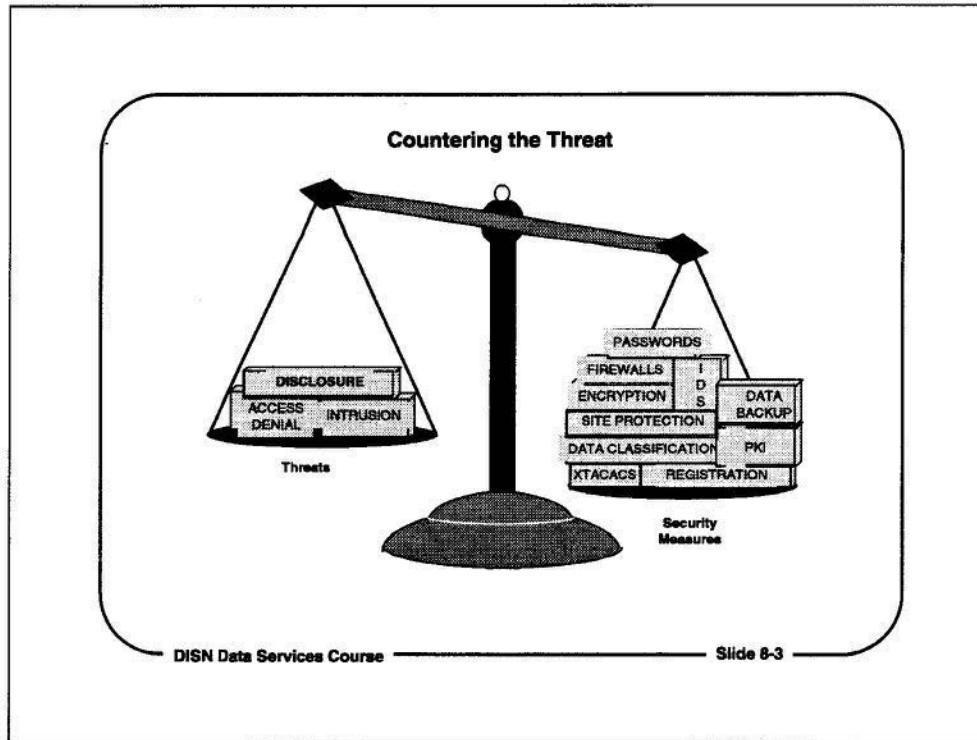
1. Defining the threats to network security
2. Describing DISA programs to protect the network
3. Describing the DISA Comm Server access control system
4. Identifying DISA and user security responsibilities
5. Describing encryption methods and devices
6. Describing the operation of firewalls and intrusion detection systems



Confidentiality vs. Availability

Network security is a compromise between two conflicting goals: protecting the confidentiality of information, while still making it available to users.

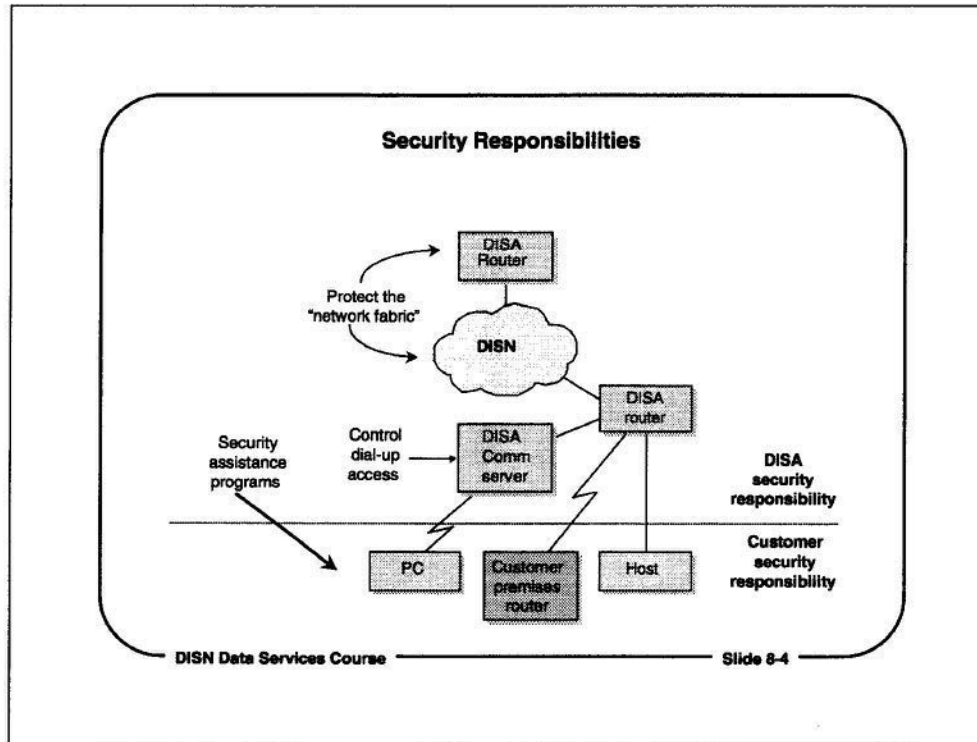
Confidentiality of the information on the DISN Data Services networks is maintained by a variety of methods, including passwords, encryption, and file access controls. The adaptive routing capabilities of the network and its redundancy assure that the network will be available when users need it.



Countering the Threat

Some of the most significant threats to the DISN Data Services networks are intrusion by unauthorized users, disclosure of confidential or classified data, and hackers or intruders whose actions could deny service to legitimate or authorized users.

DISA, the branches of the services, local installations, and end-users can take a variety of security measures to counter these threats, including firewalls, intrusion detection systems, passwords, encryption, access controls, data classification, physical separation of networks, and physical site security. Some of these measures are DISA's responsibility, and some are subscriber responsibilities, and some are shared by both.



Security Responsibilities

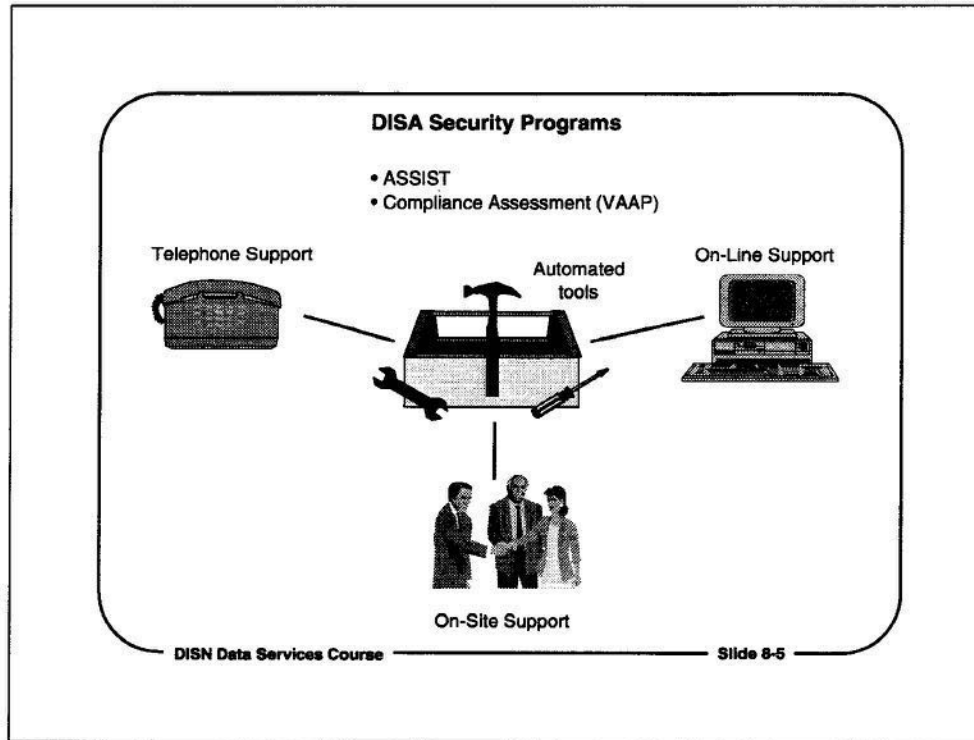
DISA and its customers share responsibility for security. DISA is responsible for the following:

- Protection of the "network fabric" - This includes the DISA routers, the DISN backbone, and connections from customer premise routers and hosts into the network.
- Control of dial-up access - DISA manages and monitors dial-up access through DISA Comm Servers, which are DISA-sponsored dial-up access ports into the NIPRNET and SIPRNET.

DISA's customers are responsible for the following security measures:

- Host Access - Protecting host accounts, local dial-up ports, local files, and local networks is the responsibility of DISA customers.
- Protecting application data.

DISA also provides security assistance programs to DISN Data Services network subscribers.



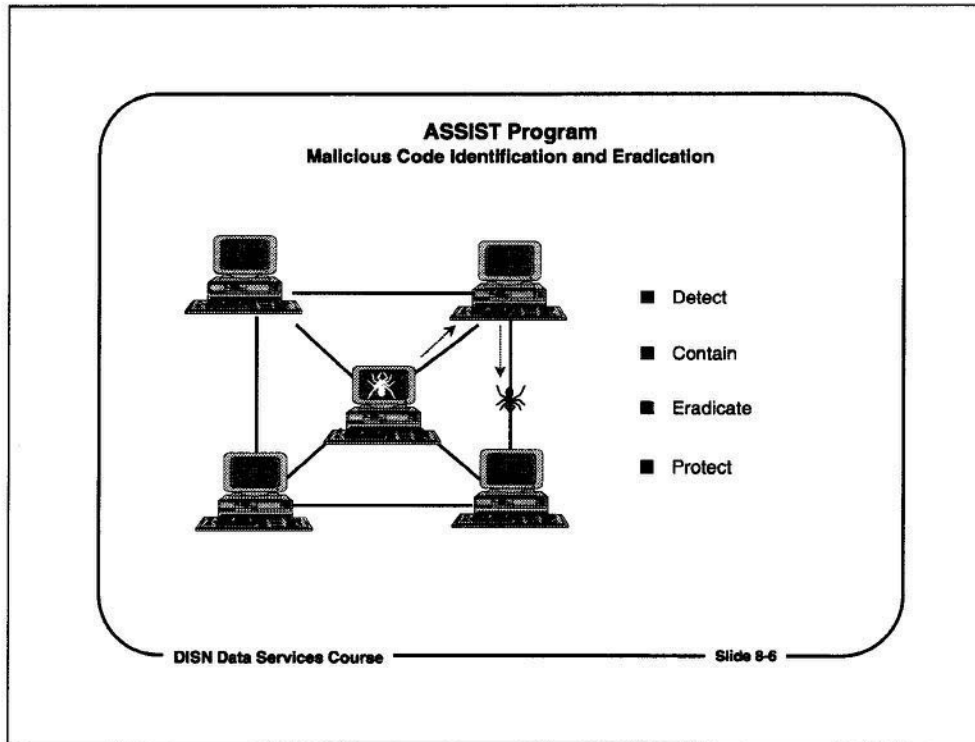
DISA Security Programs

DISA runs several programs that can improve or verify the security of DoD networks.

The two primary programs are:

- ASSIST - Automated System Security Incident Support Team
- VAAP - Vulnerability Analysis and Assistance Program

DISA provides these programs free and confidentially to any DoD agency that suspects that it has a security problem. The nature of the problem determines the type of support provided, but it ranges from telephone support to on-site surveys. Automated security analysis software is also available to analyze security problems.



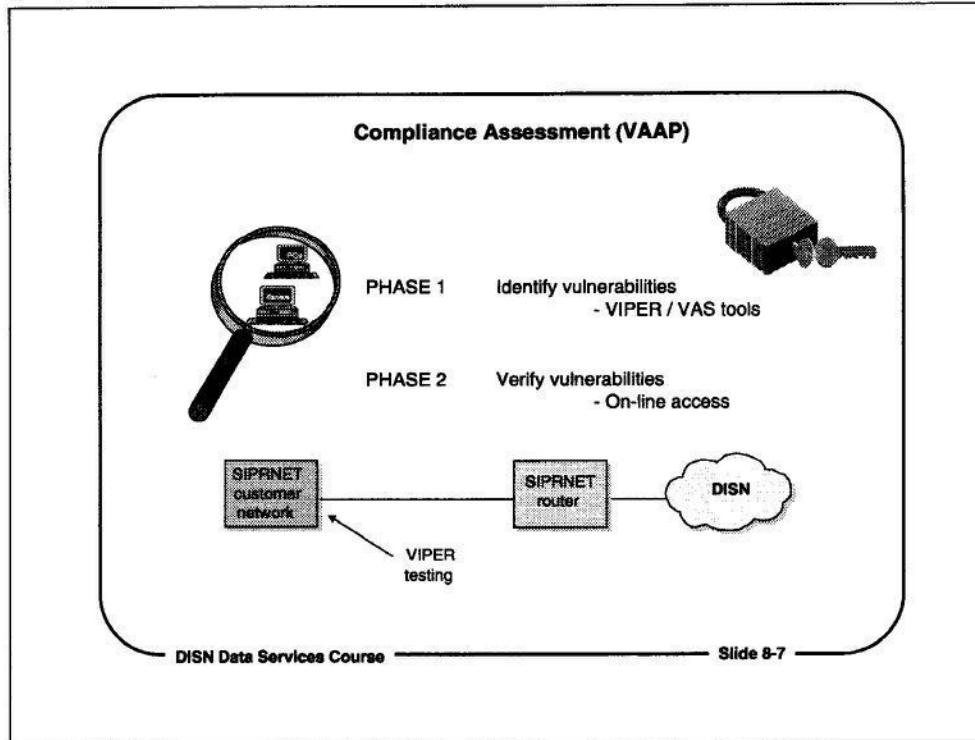
ASSIST Program

ASSIST is the program under which DISA responds to and contains information security incidents, and then restores the security of a DoD information system. If a violation is discovered, DISA supports counterintelligence and law enforcement investigations into the incident.

ASSIST personnel handle routine inquiries on file security, computer viruses, file access permissions, and computer security measures. If the situation merits, DISA will conduct an on-site investigation of a security incident.

For example, if a system becomes infected with a computer virus, worm, or Trojan Horse, DISA may do an on-site analysis to detect, contain, and eradicate the virus, and then install software to protect the system from further intrusion.

All ASSIST functions are provided free of charge to any DoD service or agency. In order to encourage DoD agencies to seek help when they need it, no report is made to higher commands about ASSIST actions.




Compliance Assessment (VAAP)

The second major DISA security program is the Compliance Assessment program, which was formerly called the Vulnerability Analysis and Assistance Program (VAAP). The Compliance Assessment program evaluates the vulnerability of information systems, and helps agencies establish more effective security measures.

Compliance Assessment assesses the effectiveness of the security of an operational system. It can also evaluate the security of products and system designs. In an operational system, it emulates the techniques and software tools that would be used by knowledgeable intruders. Its purpose is to determine where the system is vulnerable to intrusion, and to test commonly available intrusion tools against the system. The data files on the system can also be searched for files that may not be protected adequately.

Compliance Assessment is used by DISA to analyze SIPRNET systems, as part of the SIPRNET connection approval process. Compliance Assessment tests are conducted periodically on SIPRNET systems, to determine ongoing compliance with SIPRNET security programs.

Compliance Assessment or ASSIST Requests




Center for Information Systems Security
ATTN: ASSIST (ISBL)
Skyline Four
5113 Leesburg Pike, Suite 400
Falls Church, VA 22041-3230

Commercial: (800) 357-4231 (STU III capable)
DSN: 327-4700

Commercial Fax: (703) 607-4735
DSN Fax: 327-4735
Secure Fax: (703) 607-4700

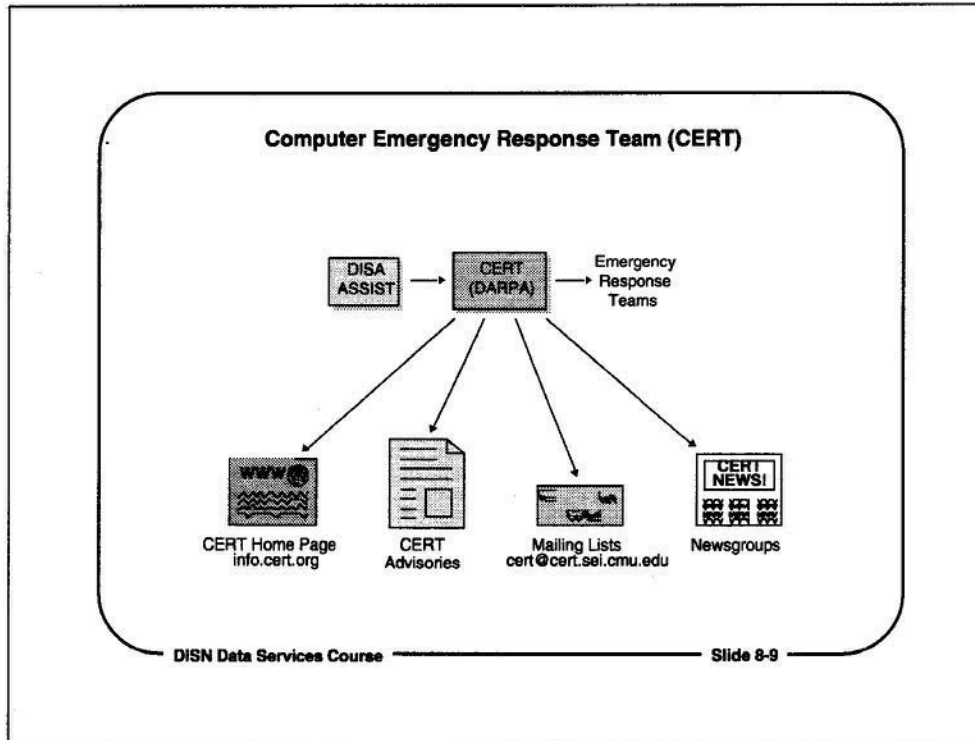
AUTODIN: DISA Washington, DC//ISBL//
DISCAS: SSO DISA Washington, DC
E-mail: assist@assist.mil
FTP: [assist.mil](ftp://assist.mil) (199.211.123.11)
BBS: Commercial: (703) 607-4710
DSN: 327-4710



DISN Data Services CourseSlide 8-8

Compliance Assessment or ASSIST Requests

Compliance Assessment or ASSIST requests must be forwarded to the DISA Center for Information Systems Security. SIPRNET Compliance Assessment requests must be sent to the DISA SIPRNET Security Branch.

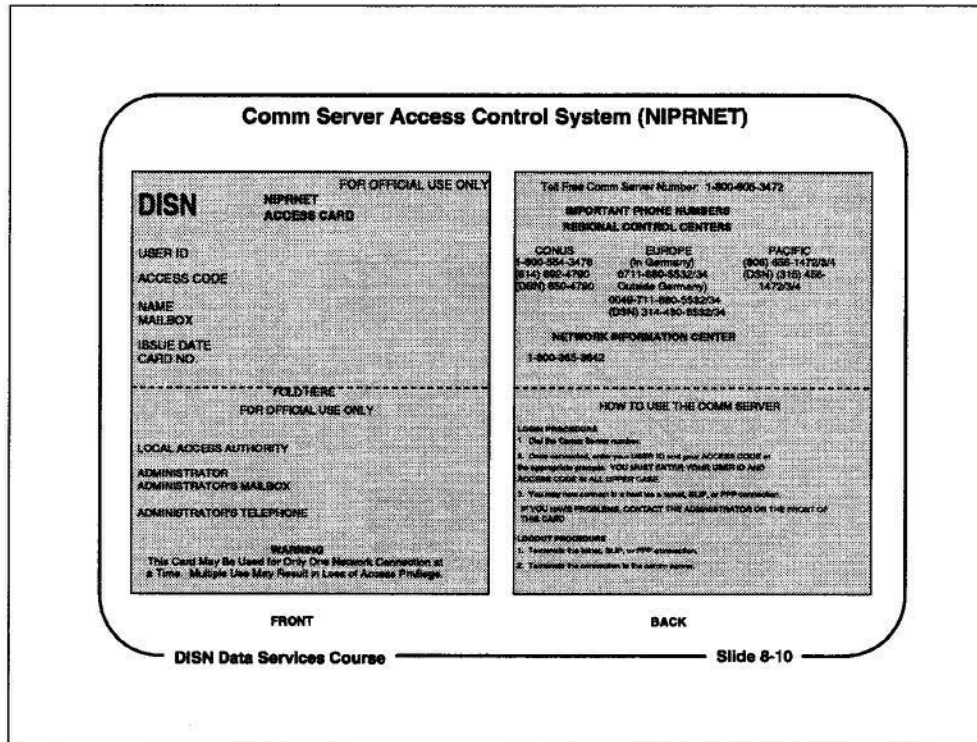


Computer Emergency Response Team (CERT)

DISA coordinates its activities with those of the Computer Emergency Response Team (CERT), which is run by Carnegie-Mellon University in Pittsburgh. CERT responds to security problems on the Internet, and serves as a worldwide clearinghouse for Internet security issues, alerts, and bulletins.

CERT coordinates its activities with the security activities of service-specific security operations, such as the AFCERT, ARCERT, and NAVCERT.

For information on the CERT mailing list, contact the CERT mail list manager at cert@cert.sei.cmu.edu.

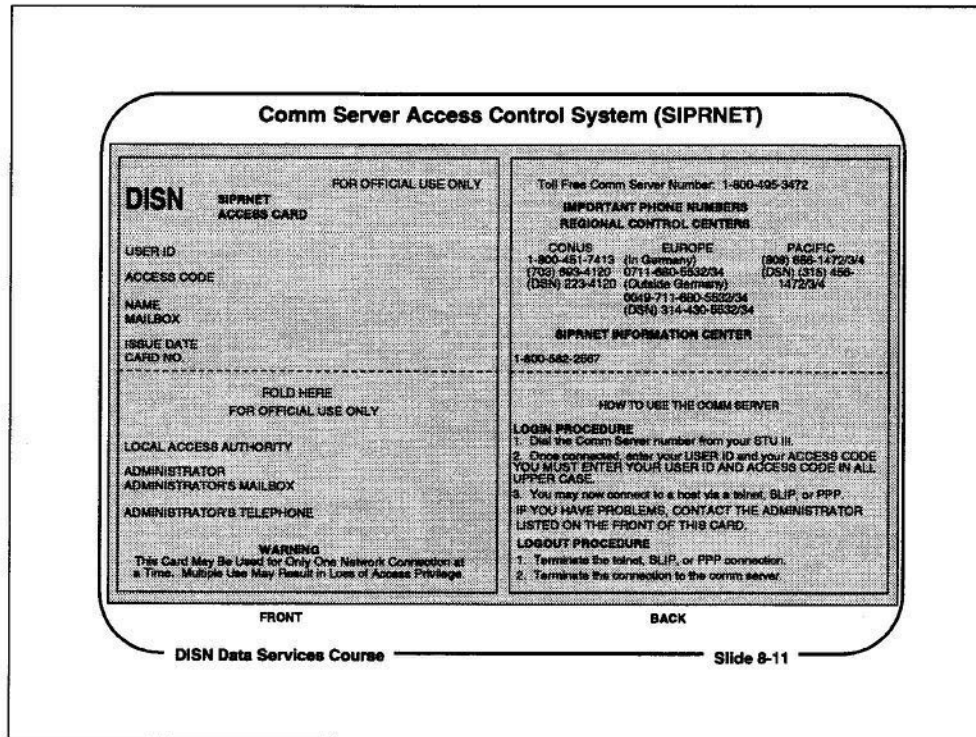


Comm Server Access Control System (NIPRNET)

The XTACACS (External Terminal Access Control Access Control System) system protects the NIPRNET and the SIPRNET from unauthorized access to the DISA Comm Servers. Any user who wants to dial into the NIPRNET or SIPRNET through a DISA Comm Server must have a valid DISA Comm Server access card.

The use of a NIPRNET Comm Server Access Card is validated and monitored by the DoD NIC each time the user dials into the network. Every user who uses a NIPRNET Comm Server must have a current NIPRNET Comm Server Access Card.

The Army, Navy, and Air Force run their own comm server programs, but users of these systems are validated through XTACACS or RADIUS authentication services. These services are identical or similar to DISA's XTACACS system.

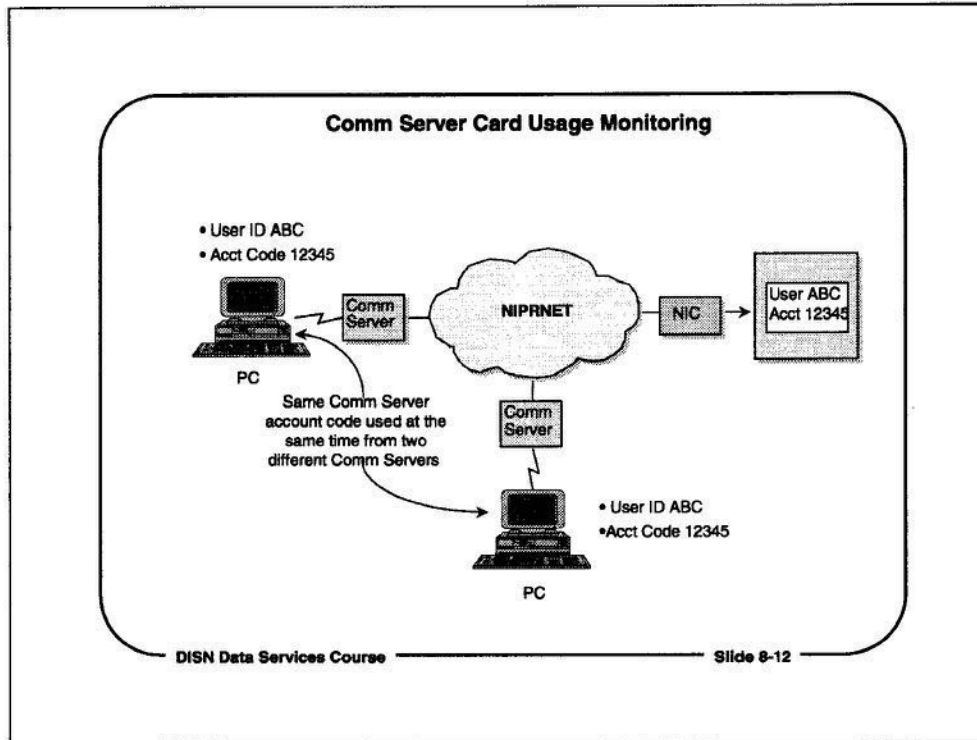


Comm Server Access Control System (SIPRNET)

SIPRNET users can have dial-up access to the network through a SIPRNET Comm Server. A STU III B-12 device protects the SIPRNET from unauthorized access. Users who want to dial into the SIPRNET must have a SIPRNET Comm Server Access Card and the STU III KSD-64 key.

Use of a SIPRNET Comm Server Card is validated and monitored by the SSC (SIPRNET Support Center) each time it is used. Anyone who uses a SIPRNET Comm Server must have a current SIPRNET Comm Server Card and a KSD-64 STU III key.

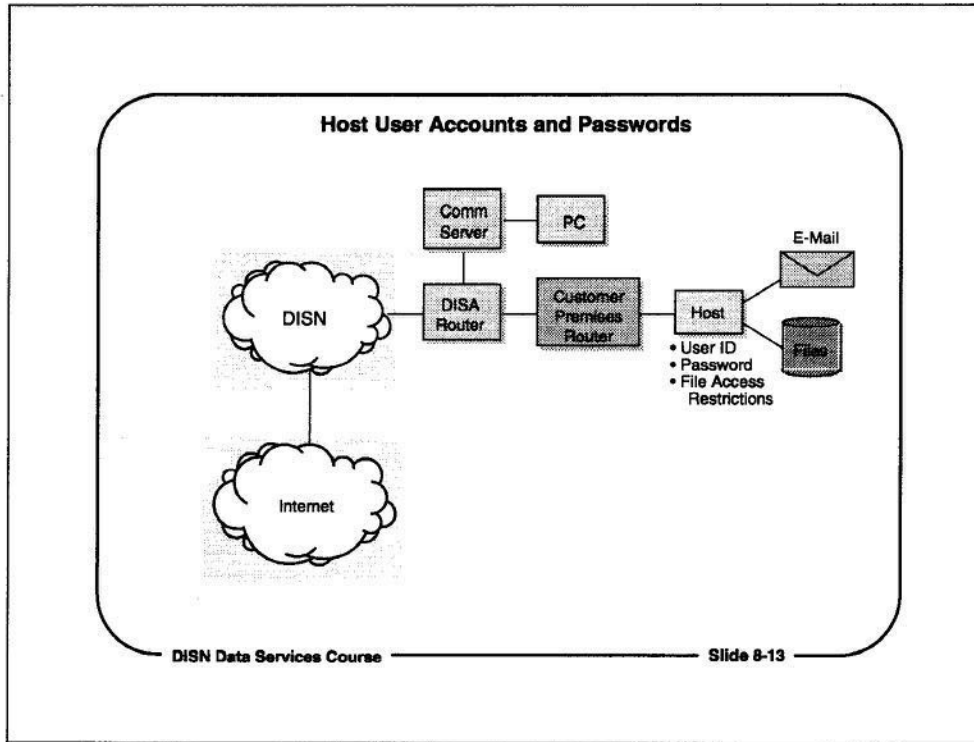
The user ID is not activated until DISA receives the return receipt for SIPRNET Comm Server Card.



Comm Server Card Usage Monitoring

Comm Server cards are issued only to users who need to access a DISN Data Services network remotely. Comm Server cards for dial-up access to the NIPRNET or the SIPRNET are issued by the DoD NIC/SSC in response to requests submitted by the services or DoD agencies.

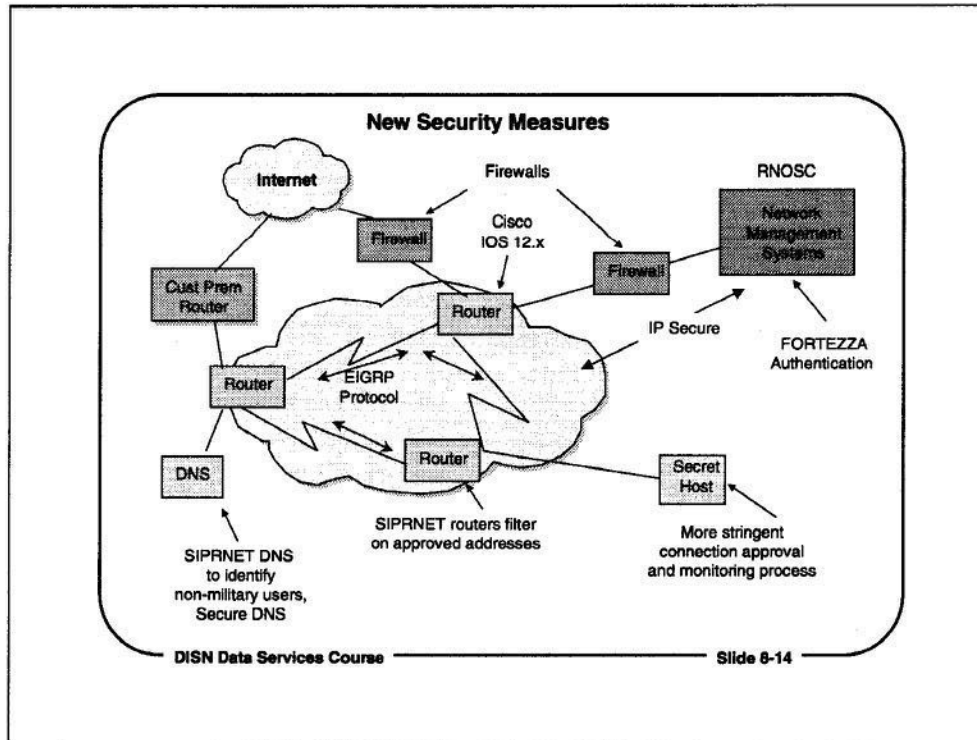
Once a user receives a DISA Comm Server card, he or she is on the access list. This list is maintained at the NIC/SSC. A user ID will be logged off and may be removed from the list if logged on for more than 8 hours. If two or more users are logged on with the same user ID simultaneously the command will be notified.



Host User Accounts and Passwords

Other forms of security are host user accounts, passwords, and file access rights. These are not DISA-sponsored security measures. They are local measures that augment link-level and host-to-host encryption.

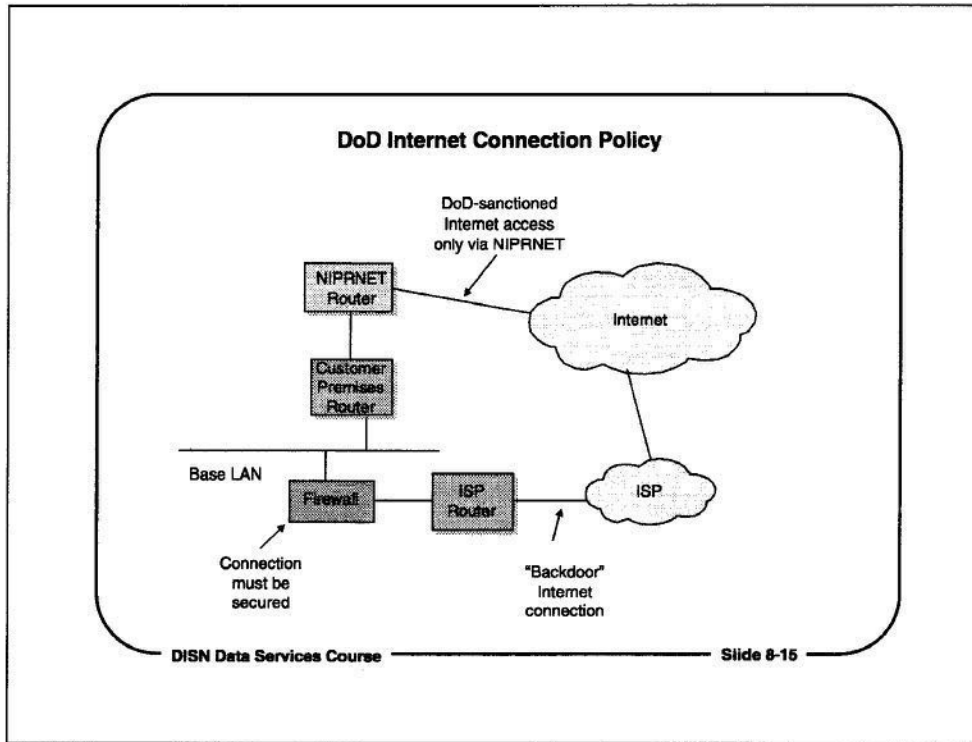
Host user accounts, passwords, and file access rights are the responsibility of local host administrators. File access rights can prevent unauthorized users from modifying or deleting host or server files. Access rights are commonly established through the host's operating system, or a local area network operating system's file administration, backup, and security processes.



New Security Measures

DISA has added a number of security measures to protect both the NIPRNET and the SIPRNET, including:

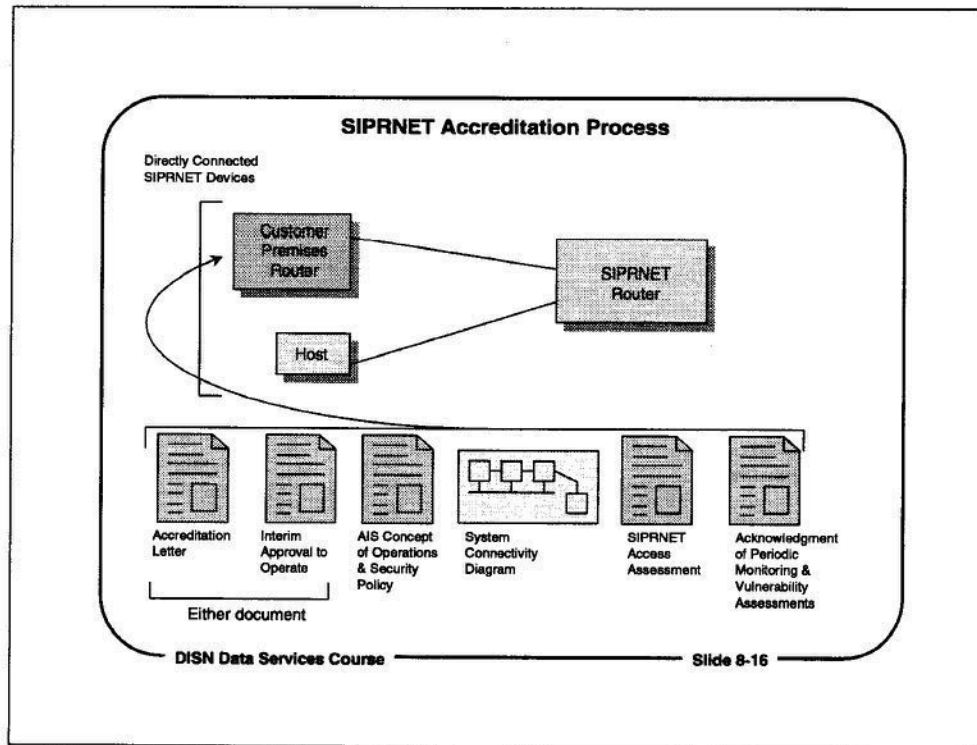
- Installing firewalls on NIPRNET Internet connections, and on RNOSC connections
- Upgrading the operating system of DISA routers to use keyed MD5 authentication
- Fortezza encryption and IP Secure for RNOSC traffic for better data security
- Secure DNS project and special DNS services for SIPRNET
- Restrictions and mandatory screening on backdoor ISP connections
- SIPRNET connection approval process



DoD Internet Connection Policy

The only type of Internet access that is sanctioned by the Office of the Secretary of Defense (OSD) is through the NIPRNET. However, a number of bases have their own Internet connections through local ISPs, in addition to Internet access through the NIPRNET.

The OSD has mandated that these "backdoor" Internet connections be terminated (OSD Policy Memorandum, NIPRnet Internet Connectivity, 22 Aug 99), and that all Internet access from DoD bases must go through the NIPRNET. In some cases, waivers may be granted if DoD operations will be disrupted by removing a backdoor ISP connection before DISA can provide NIPRNET service. All waived ISP connections must be secured with a firewall or some other security device.



SIPRNET Accreditation Process

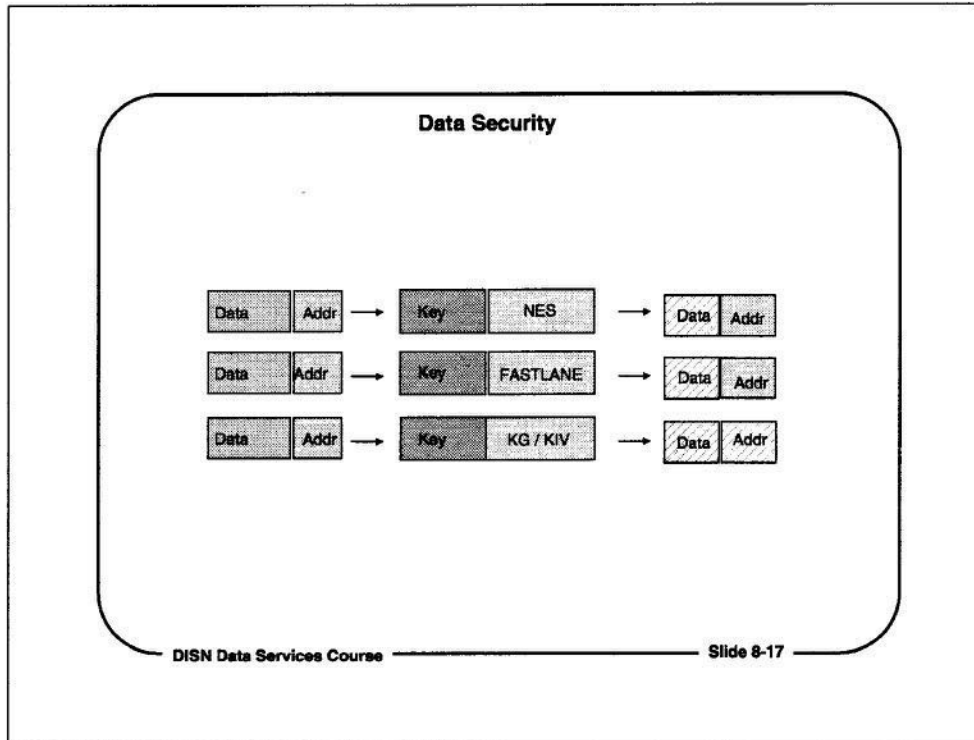
The SIPRNET defines a closed community of Secret users, so all connections to SIPRNET routers must be accredited by DISA. The following documents must be submitted to DISA to gain or to keep SIPRNET accreditation:

- Accreditation letter
- Interim approval to operate
- Automated Information System (AIS) concept of operations and security policy
- System connectivity diagram
- Foreign Access Assessment (if applicable)
- Acknowledgment of periodic monitoring and vulnerability assessments.

The documents must be submitted to the DISA SIPRNET Security Branch. SIPRNET subscribers who have not received SIPRNET security accreditation will be disconnected from SIPRNET.

The front channel messages that govern this policy are 121713Z DEC 95, 181100Z APR 96, and 042136Z APR 97.

For more information on SIPRNET subscriber accreditation requirements, contact John Staples of the DISA SIPRNET Security Branch (staplesj@ncr.disa.mil) at (703) 735-3236, or Leon Walker at (703) 735-8388.

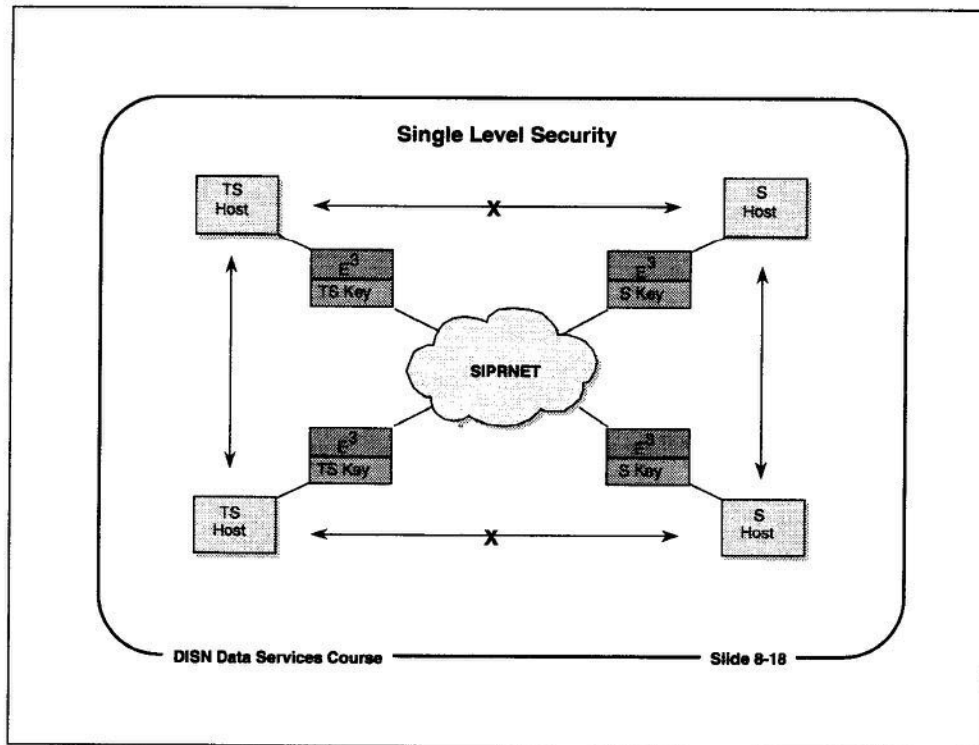


Data Security

DISN Data Services networks use several types of encryption devices, according to the level of security needed.

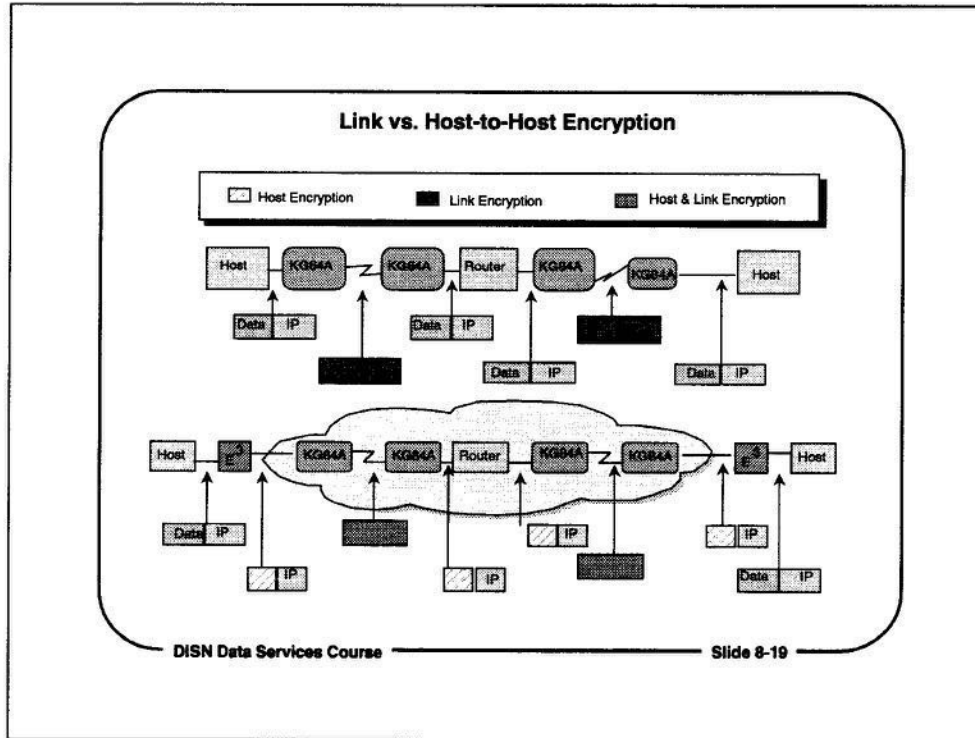
End-to-End encryption (E-3) devices, such as NES and FASTLANE, encrypt only the data portion of the cell or IP diagram. An end-to-end IP encryption device leaves the destination IP address intact so IP routers can direct the datagram to its destination. Using the same basic concept, a FASTLANE encryption device encrypts only the data portion of an ATM cell, leaving the destination address intact so ATM switches can direct the cell to its destination.

KG devices encrypt an entire data stream, so they do link-level encryption.



Single Level Security

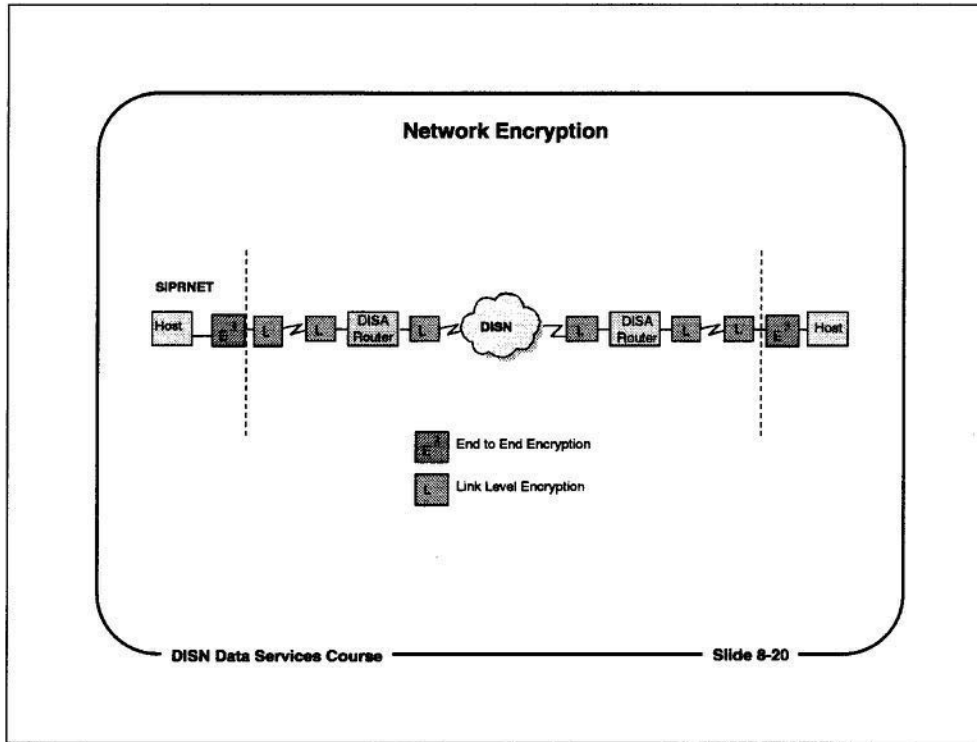
An NES device can encrypt data for hosts that handle data of one security classification. NES devices encrypt data at only one security level, and their keys can only match the keys of other NES devices with the same security level.



Link vs. Host-to-Host Encryption

- Link Encryption (DISA responsibility)
 - Encrypts data and IP header
 - Inhibits traffic analysis
 - Must be decrypted at nodes so that IP address can be read.

- Host-to-Host encryption (Customer responsibility) with link encryption
 - Source E³ encrypts red input
 - Message is link encrypted
 - Message is routed to destination encryption device
 - Destination E³ receives message, decrypts it, and passes it to host or gateway.



Network Encryption

Data on all SIPRNET circuits worldwide is protected with data link encryption. There are times when both link-level and end-to-end encryption devices may be used.

End-to-end encryption offers further information protection on the customer's premises, as data packets transverse a local distribution system to or from a secure facility.

If data information is the primary customer concern, end-to-end encryption would suffice. However, if traffic volume and addressing are a concern, then link level encryption would suffice.

Types of KG Encryption Devices

TYPE	LINE SPEED	NOTES
KG 84A	256 Kb	Used in DISN
KIV 7 / KIV 7HS*	256 Kb to 1.544 Mb	KG 84 equivalent
KG 94**	13 Mb	Not installed in DISN
KG 95	50 Mb	Used in DISN
KG 194**	13 Mb	Has KSD-64A Capability
KG 194A**	19Mb	Does not need FPA
KG 194 (CCITT)	2.048 Mb support	E-1 interface for OCONUS
KG 75 (Fastlane)	OC12	ATM

* KIV 7 to be replaced by KIV 13
 ** KG 94 / 194 / 194A to be replaced by KG 19

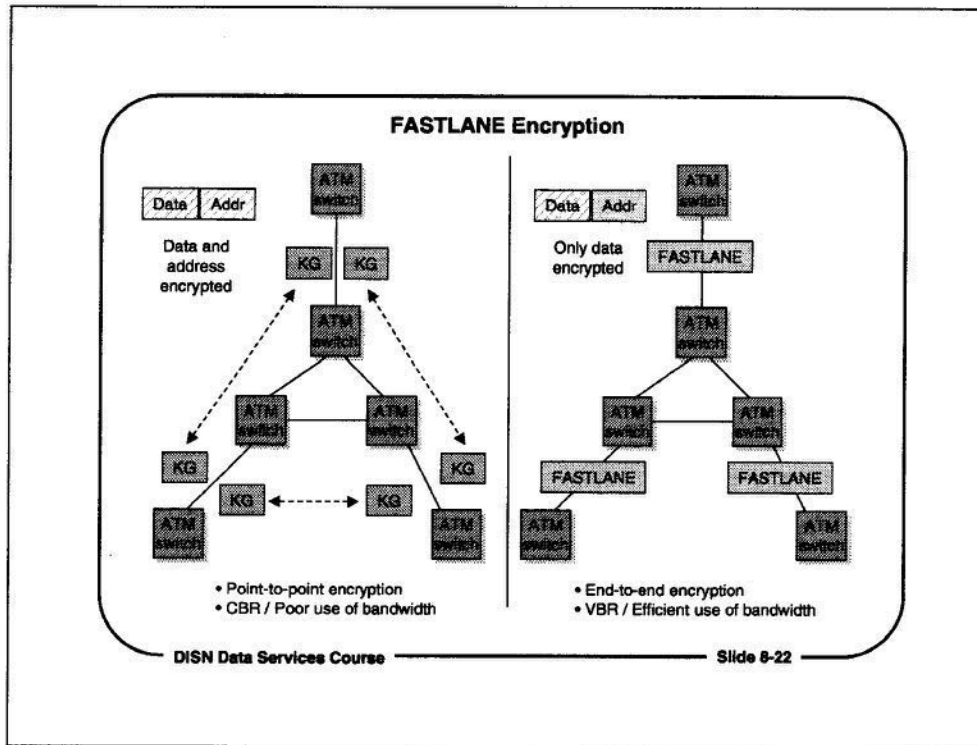
DISN Data Services Course Slide 8-21

Types of KG Encryption Devices

The KG 84A is the most widely used encryption device in DISN Data Services networks. It can encrypt access circuits at 64 Kb. The trunks that connect the IDNX multiplexers run at T-1 or E-1 speeds (1.5 Mb and 2 Mb respectively), so they require KG 194 encryption devices. The KG 194 also has a KSD-64A encryption key capability. The KG 194 (CCITT) is used outside CONUS, where the E-1 interface is the high-speed digital standard.

The Fixed Plan Adapter (FPA) is a chassis that houses two KG 194s. The KG 194A does not need an FPA, but it requires a separate power supply module.

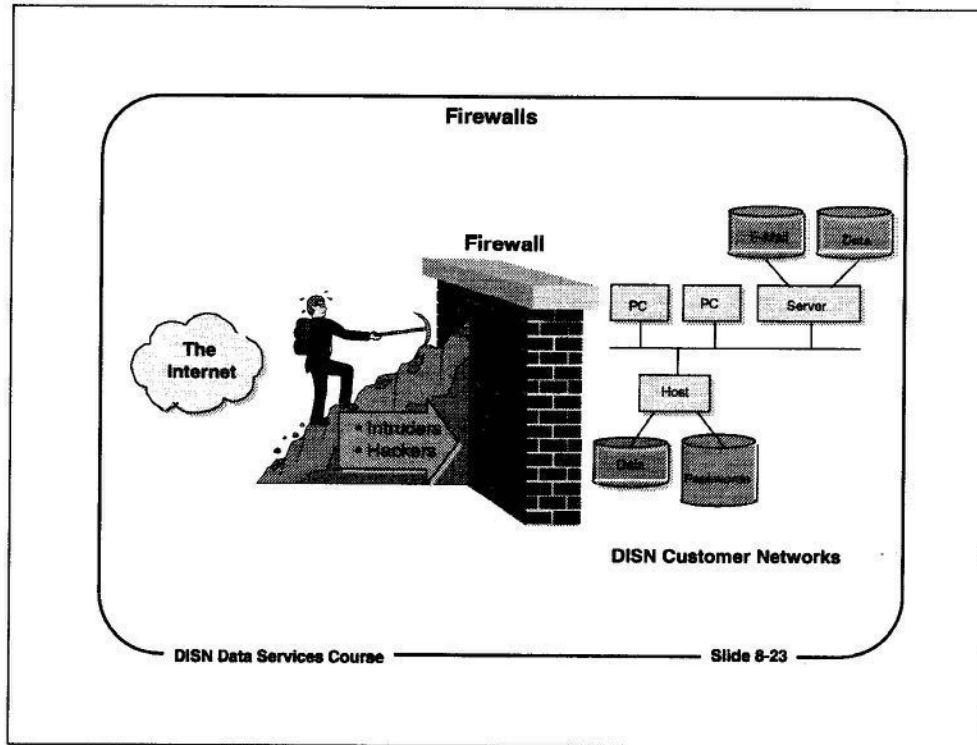
ATM circuits are encrypted with either FASTLANE devices or KG crypto devices and SLI boxes.



FASTLANE Encryption

The FASTLANE device is the encryption device that will replace several other encryption and crypto devices, such as the older Blacker box and the NES box. When it is used to encrypt ATM traffic, FASTLANE encrypts the data portion of the ATM cell, but not the header that contains the address. This allows the ATM switch to handle traffic from a FASTLANE device as if it were standard, variable bit-rate ATM cell traffic.

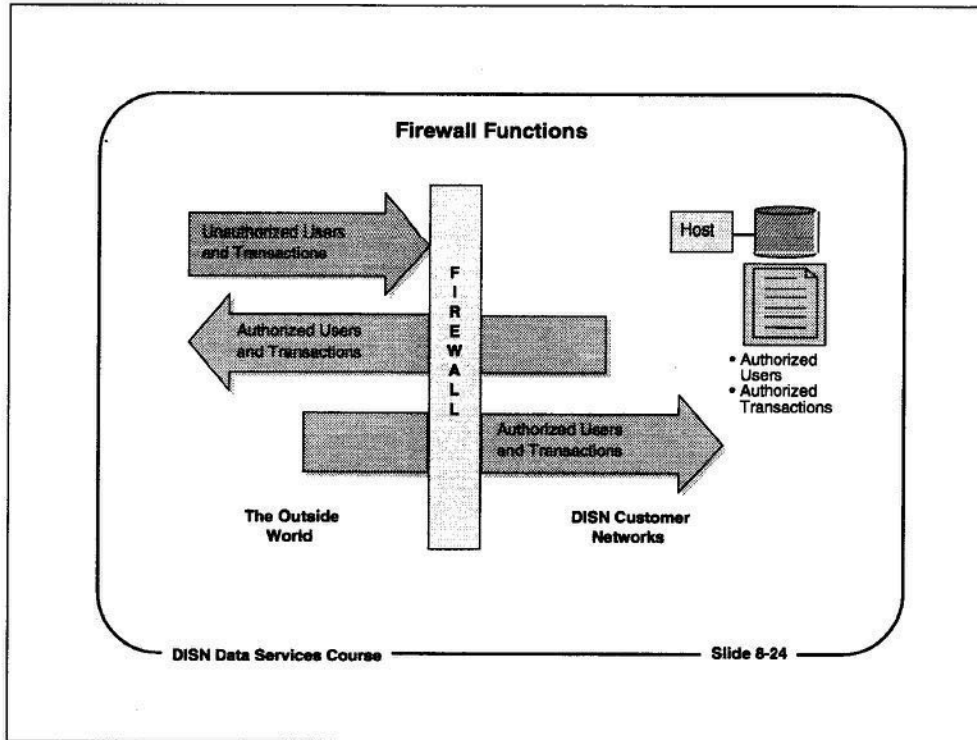
By contrast, KG or KIV devices completely encode IP datagrams or ATM cells, and they send a constant stream of bits across the network. This results in poor utilization of bandwidth, and decreases the flexibility of the network.



Firewalls

A firewall is a device that prevents intruders, hackers, and interlopers from entering a network. This prevents unauthorized users who are outside the network, or who are screened from a protected system by the firewall, from accessing confidential or classified data, compromising sensitive files, and tampering with system configurations.

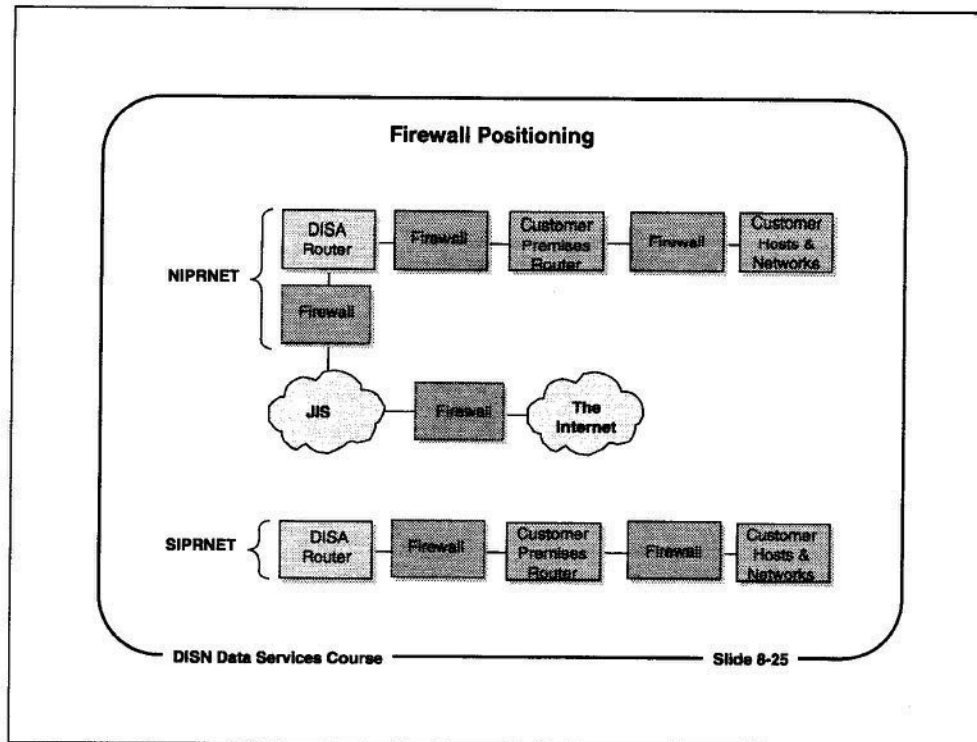
The Internet is the source of most attacks on DoD networks. Many DoD systems, such as NIPRNET, are connected to the Internet and are therefore vulnerable to attack. Depending on their level of sophistication, firewalls can protect networks from many types of malicious attacks.



Firewall Functions

A firewall protects by limiting traffic and protocols going to and from networks and systems behind it. The firewall is a two-way port, as it allows certain kinds of traffic through it.

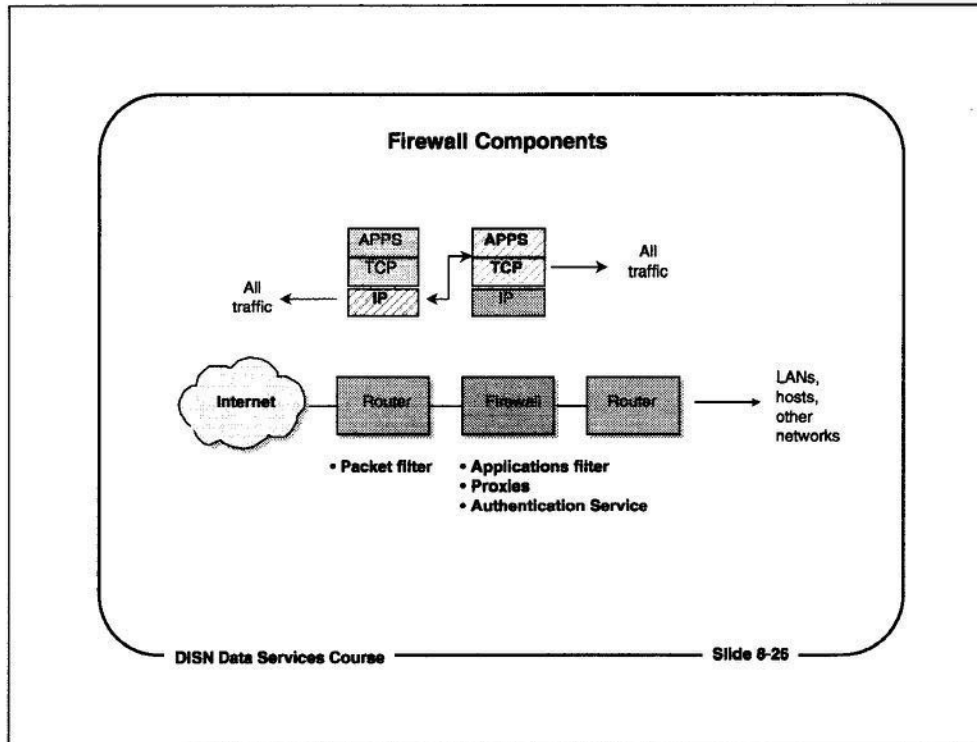
For example, the firewall stops traffic from unauthorized users and hosts that are outside the firewall. Systems and users behind the firewall can get past the firewall to reach hosts on external networks. Responses and replies to inquiries and transactions from hosts and users behind the firewall can pass back through the firewall.



Firewall Positioning

Firewalls may be located anywhere in a network, to protect systems and networks behind them. They are frequently positioned outside customer premises routers to protect subscriber networks and hosts, or the customer premises routers themselves.

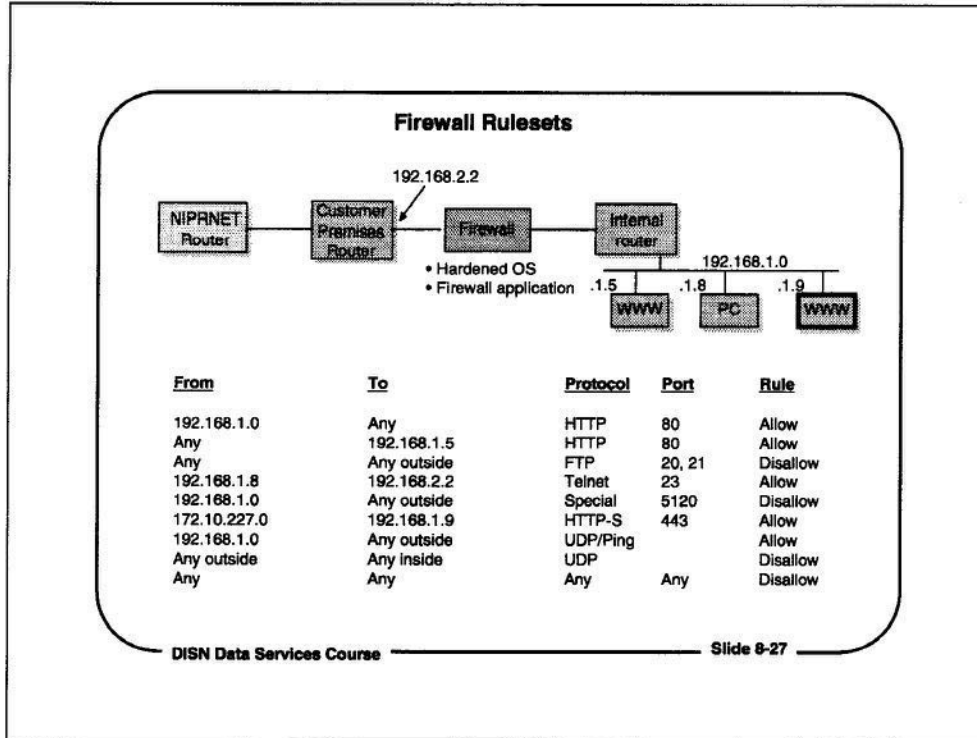
Firewalls may also be positioned between DISA routers and customer premises routers, or between DISA routers and the Internet.



Firewall Components

A firewall is composed of one or more routers or computer systems that run customized programs or specialized firewall software. A router can act as a firewall, but it may only be able to filter traffic at the IP datagram level, to distinguish traffic from authorized and unauthorized IP addresses.

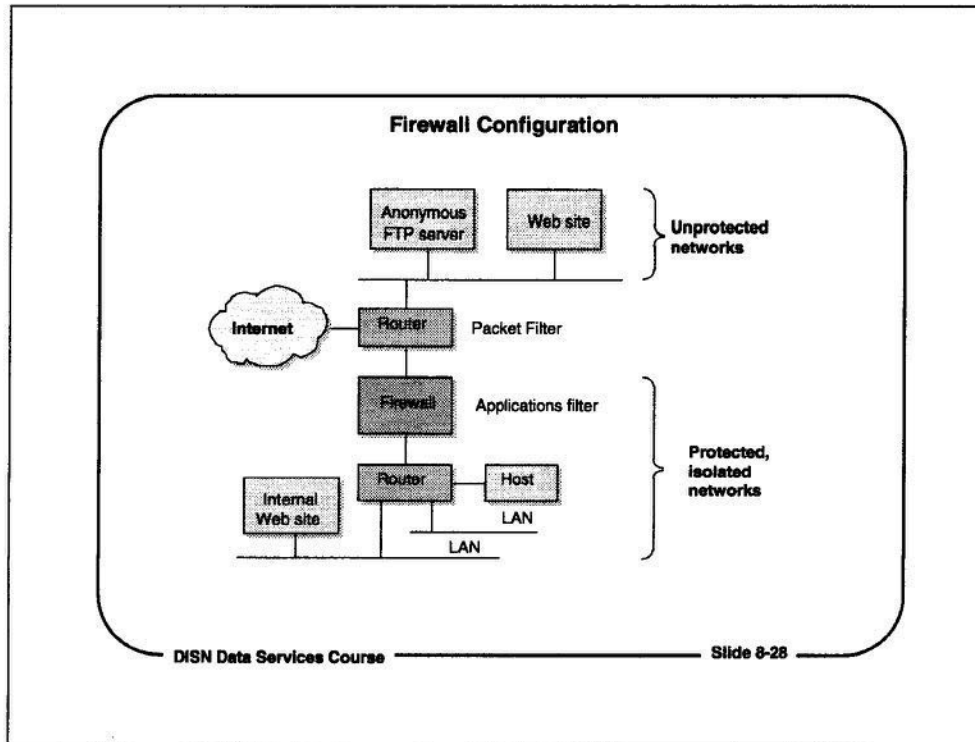
A separate host, which runs firewall software, is usually the key element of the security perimeter. The firewall filters applications-level protocols, and maintains access control lists and access logs.



Firewall Rulesets

Firewalls screen traffic based on the screening rules, or rulesets, that have been established by the firewall administrator. Firewall rules may be created to screen on individual IP addresses, specific TCP ports, or other combinations of parameters. The purpose of customized rulesets is to control traffic through the firewall so that traffic monitoring and screening meets the organization's security requirements, and so that it matches an organization's security policies.

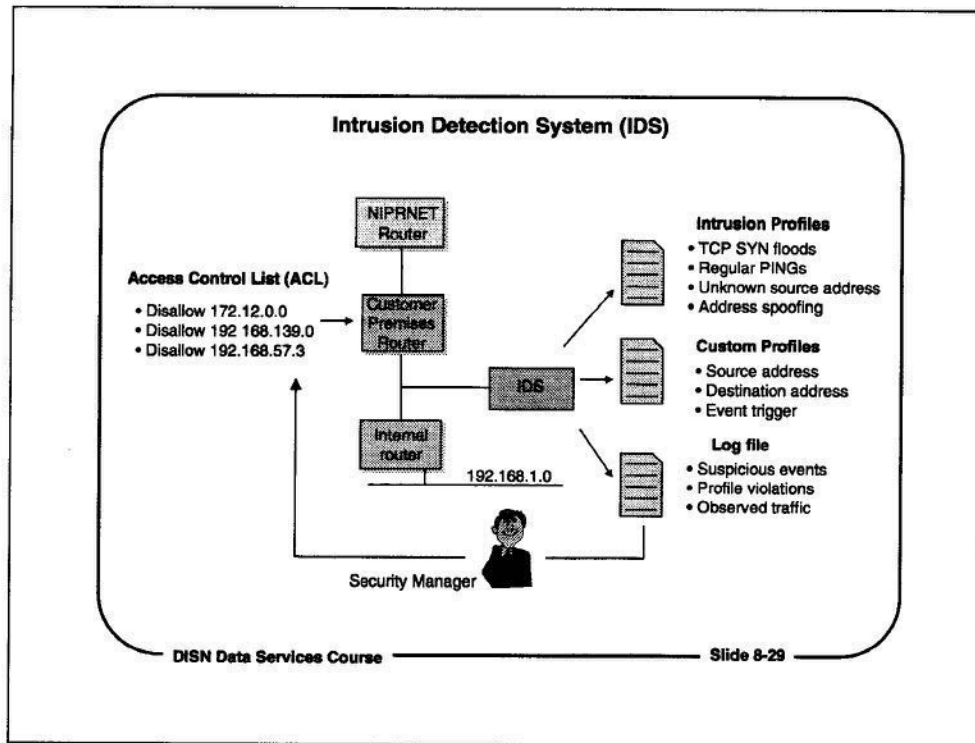
Firewalls may also have other capabilities, such as running a DNS, an SMTP mail relay, and doing network address translation (NAT), in addition to logging traffic and generating alarms.



Firewall Configuration

If a network has resources intended to be accessed by anyone on an outside network, those hosts can be placed on a separate network outside the firewall.

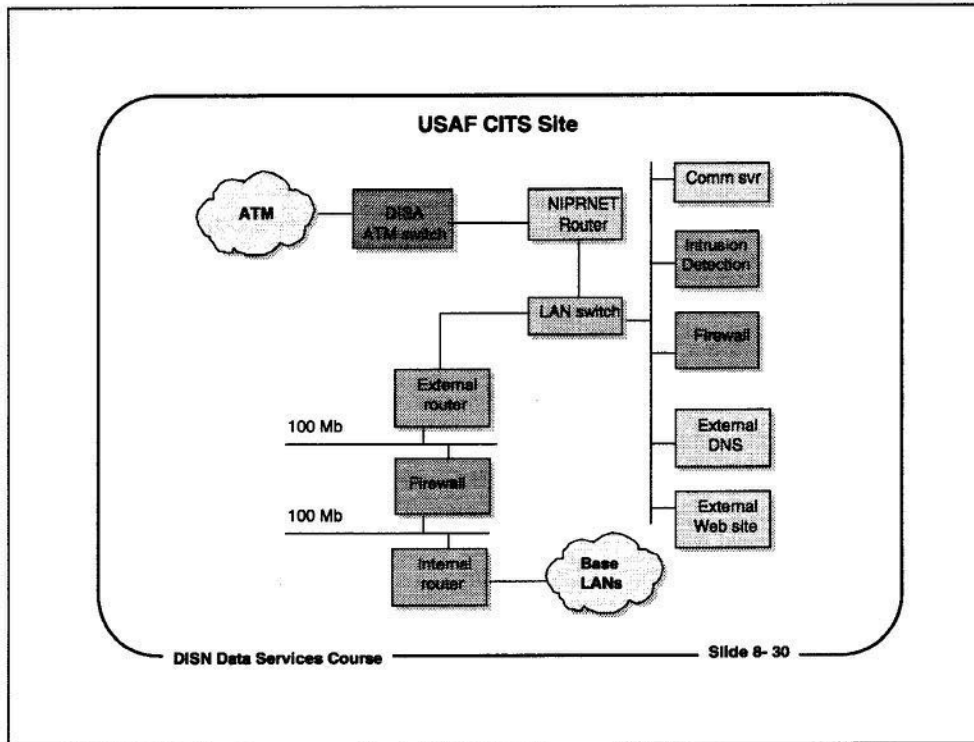
For example, if an Anonymous FTP host or a Web site can be reached by anyone on an outside network, those servers can be on an external, unprotected network. The firewall does not filter traffic going to unprotected resources on the outside network. However, all traffic going to or from a protected, "inside" network can be filtered, examined, and logged by the firewall system.



Intrusion Detection Systems (IDS)

An intrusion detection system (IDS) watches traffic going to and coming from a network, in order to identify suspicious or potentially harmful activity. A typical IDS observes network traffic passively, watching for known patterns or types of suspicious activity, or for traffic to or from certain IP addresses. The IDS logs suspicious activity, according to detection parameters set by the IDS administrator.

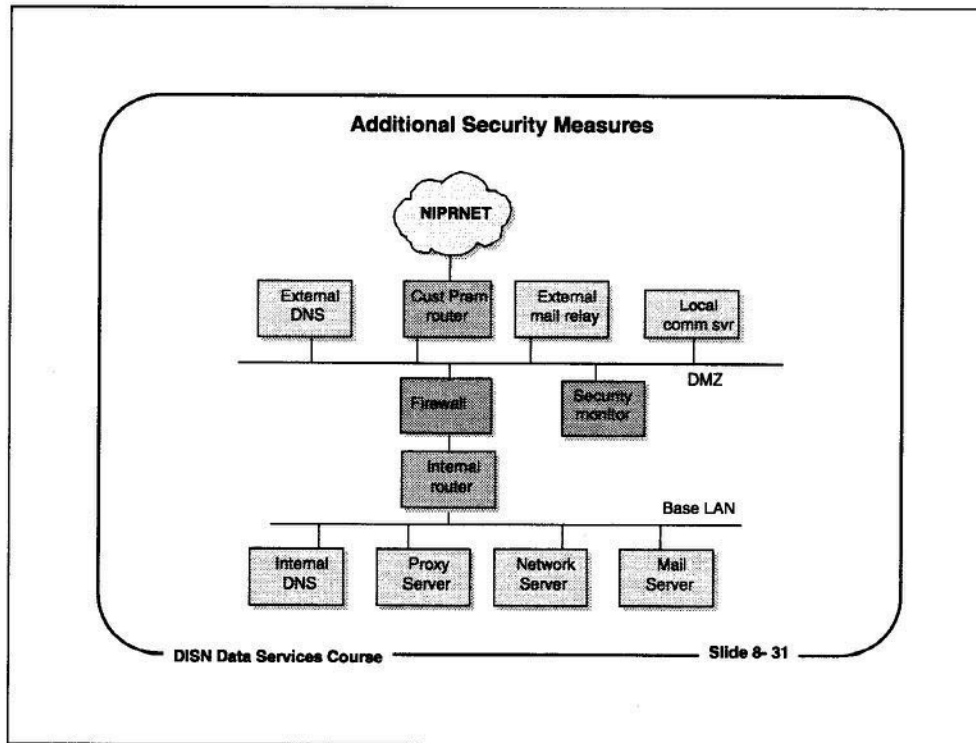
The IDS administrator or network security managers analyze the IDS logs to determine if their networks are being attacked, or if an intruder is attempting to probe their networks. The security manager can use the results of this analysis to set access control lists and filters in screening routers, and to develop firewall rules to protect networks.



Air Force CITS Site

The Air Force has started a program to install a firewall system called the Combat Information Transport System (CITS) at each Air Force base. The CITS site is a set of two routers – one internal, and one external, with a Sidewinder firewall between the two routers.

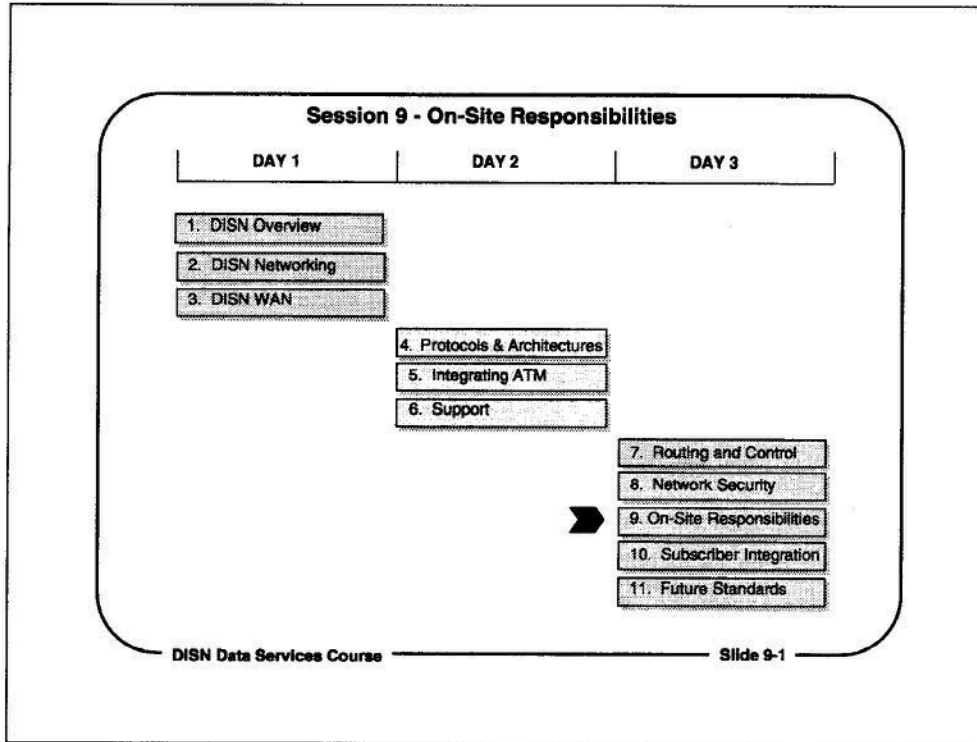
The CITS site will provide local firewall protection to each Air Force site. It will also permit each base to monitor traffic to and through its firewall. In a standard CITS site, the externally-accessible Web site is located outside the firewall. CITS also moves dial-up access outside the firewall, so that dial-up users must be authenticated through the firewall.



Additional Security Measures

Many DoD agencies and organizations are adopting a number of other local security measures, in addition to adding firewalls and IDS systems, to protect NIPRNET connections. Some of the other security measures that may be taken include:

- Dial-up authentication – Some firewall vendors offer a special remote client authentication program, which may include encryption, that lets the firewall authenticate a user, regardless of whether the dial-up service has done so. Many organizations are also moving local dial-up services outside of the firewall, instead of behind it.
- Proxy servers – A proxy server can manage and screen all external traffic, and log Internet usage
- Firewall and server logging - Firewalls, security monitoring tools, and servers can be configured to keep logs of network activity.
- Split DNS – An external DNS only lists the network hosts that should be known to the outside, while an internal DNS maintains internally-known hosts
- Mail relay – A separate mail relay host transfers mail from external to internal mail servers.

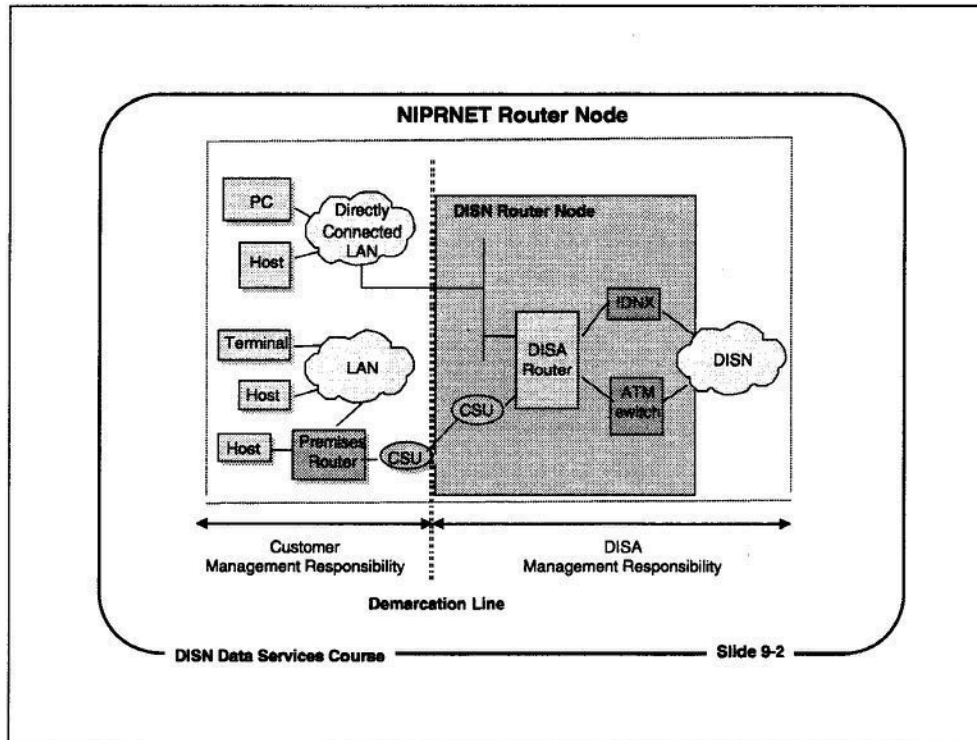


Session 9 - On-Site Responsibilities

Upon completion of this module, the students will have a general understanding of the components of the DISA node site, and the responsibilities of the node site coordinator.

This session will focus on:

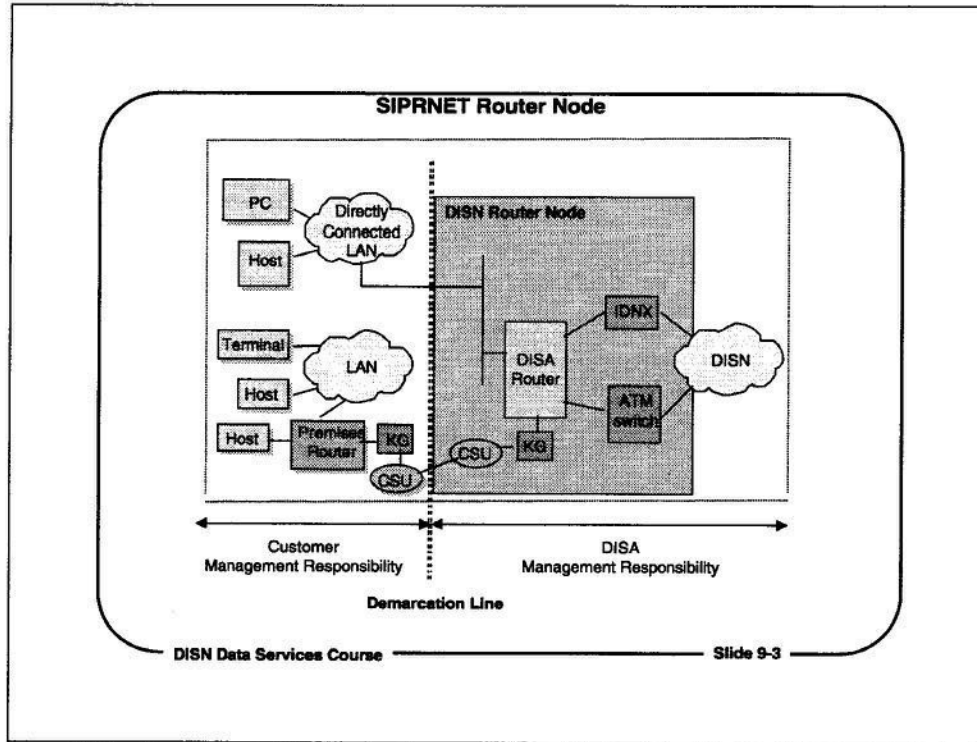
1. Describing the components of the DISA node site
2. Describing the responsibilities of the Node Site Coordinator (NSC)



NIPRNET Router Node

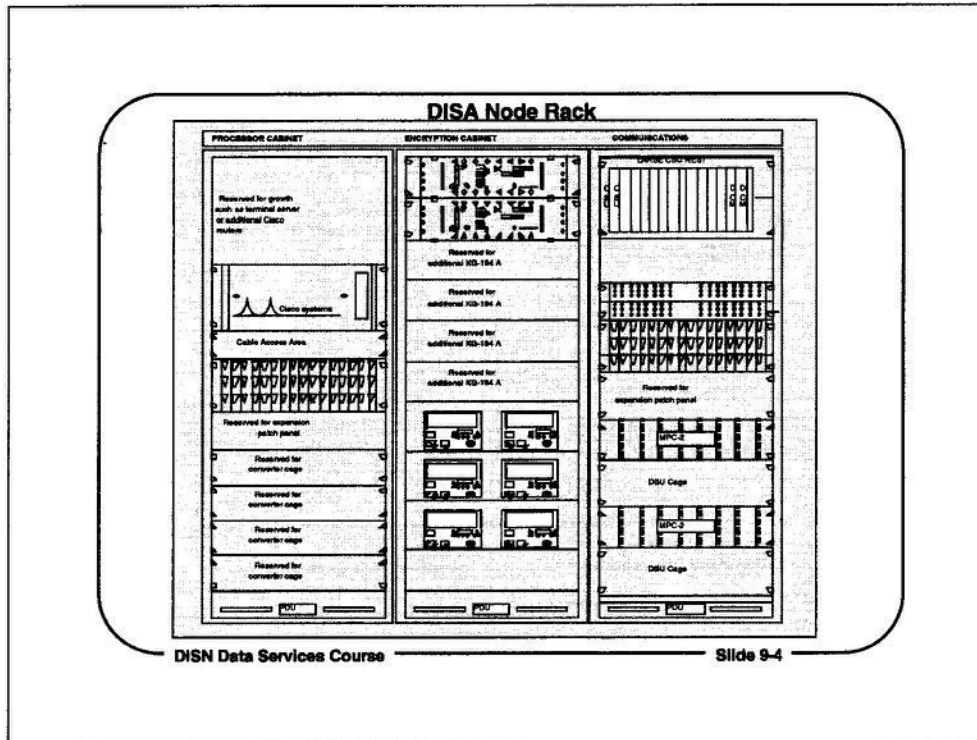
Responsibility for managing the components of a DISN node site is shared by the DISA Global Network Operations and Security Center (GNOSC) and the DISA Regional Network Operations and Security Center (RNOSC). All DISA equipment is monitored by the RNOSC. Connections from customer premise routers to DISA routers is monitored by the RNOSC. The GNOSC performs global monitoring of all DISA assets.

The RNOSC provides management of the circuits and equipment up to the point of connection to the customer equipment. This includes the DSU/CSUs and the circuits used to connect customer premises routers to DISA router ports.



SIPRNET Router Node

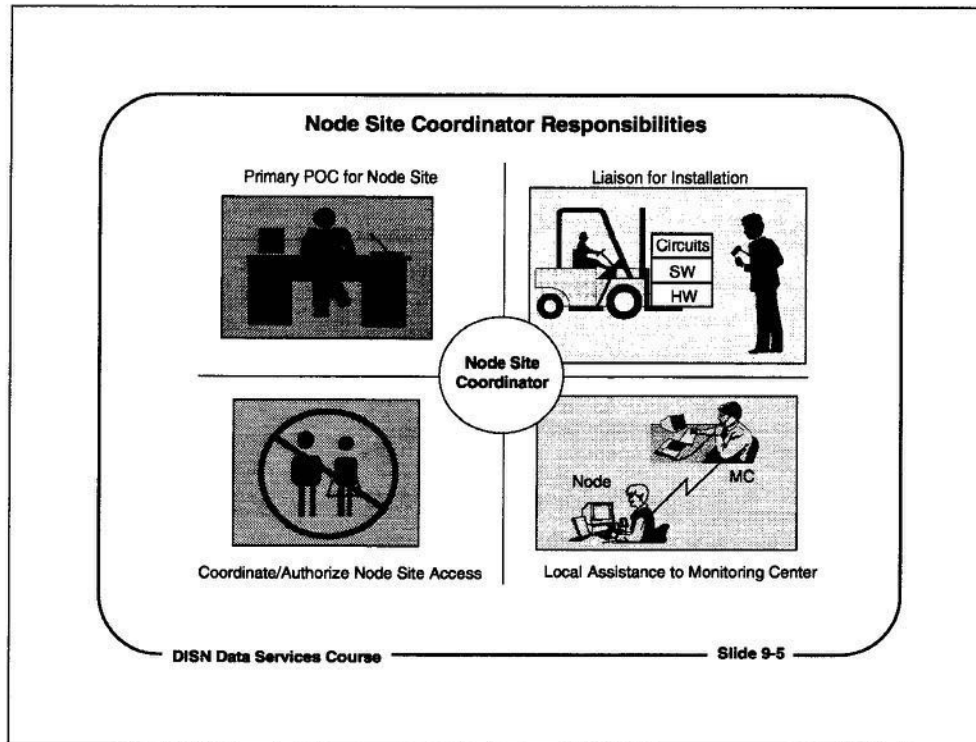
NIPRNET and SIPRNET router nodes have a high degree of similarity. The primary difference is in those things that are required to provide encryption. All connections to SIPRNET routers are via trusted paths. In those cases where the customer premise router is not co-located with the DISA router, KG encryption is used on the circuits. In both NIPRNET and SIPRNET, DISA provides management up to the point where the customer's equipment connects to the network.



DISA Node Rack

The equipment in a DISN equipment rack is divided into three sections. The exact configuration of equipment in the DISA node site depends on the location, purpose, and connectivity of the node site. The equipment is generally organized into the following groups:

- Processor modules (routers and terminal servers)
- Encryption devices (KG devices)
- Communications devices (modems, CSU/DSUs, IDNXes, ATM switches and PowerHubs)



Node Site Coordinator Responsibilities


The Node Site Coordinator (NSC) is DISA's appointed representative at a DISA node site. The NSC works with DISA, the Regional Network Operations and Security Center (RNOSC), and the node's subscribers to manage the node site.

The Node Site Coordinator's primary responsibility is to act as the primary point of contact for DISA at the node site. The NSC acts on behalf of DISA at the node site, because there usually is no DISA person stationed at the site.


NSC Responsibilities: Node Site POC

- Keep local primary and backup POC list updated for RNOSC
- Inform RNOSC of current POC phone numbers
- Maintain POC list for attached hosts, routers, and LANs
- Maintain DISA documentation and node configuration
- Act as POC for Telecommunications Service Request (TSR) & Telecommunications Service Order (TSO)


Primary POC for Node Site




Liaison for Installation




Node Site Coordinator





Coordinate/Authorize Node Site Access

Node MC



Local Assistance to Monitoring Center

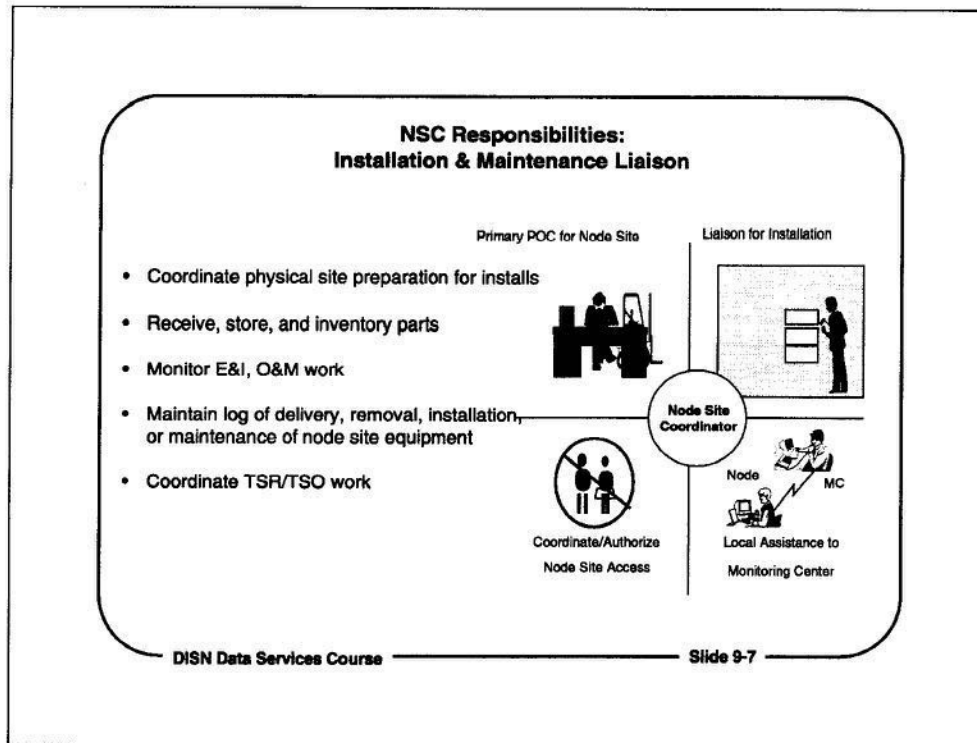
DISN Data Services Course Slide 9-6

Node Site Coordinator Responsibilities - Node Site POC

The NSC is the person the RNOSC personnel will call to determine the status of node site conditions, and to maintain the node site.

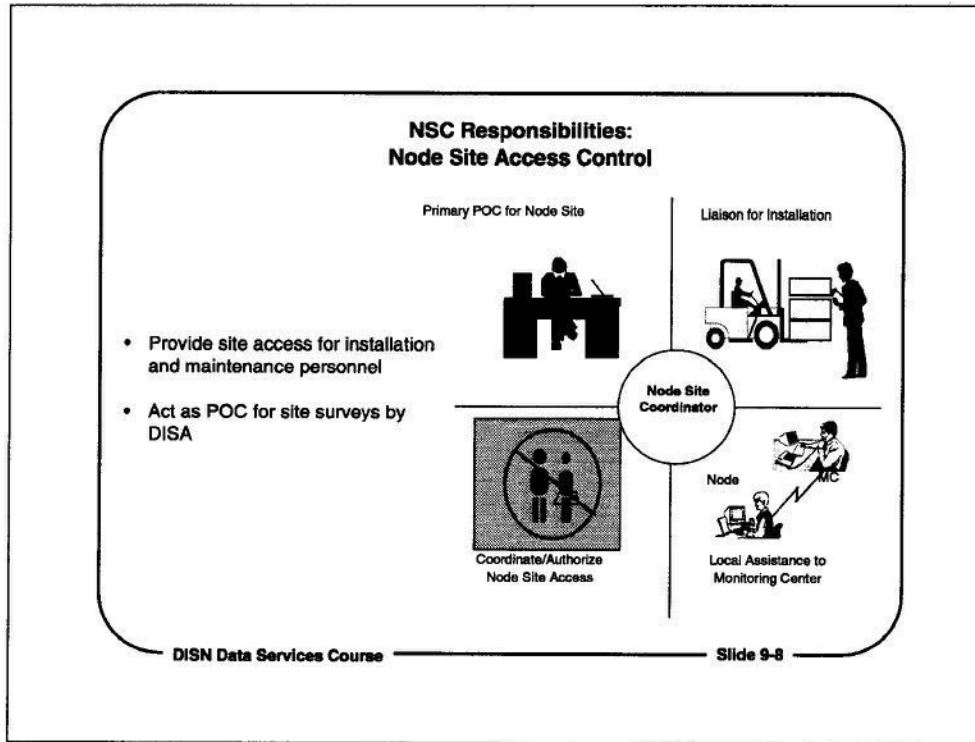
The NSC should keep documentation on the devices and hosts connected to the node ports, as well as any node documentation provided by DISA.

The NSC must keep the RNOSC informed of current names and phone numbers for the NSC, as well as other personnel who have access to the node site.



Node Site Coordinator Responsibilities - Installation and Maintenance Liaison

When hardware and software is installed in the node site, the NSC is the liaison between the RNOSC, DISA, and the contractors who perform maintenance and installation. The NSC should maintain a log of people who install equipment in and maintain the node site, to record what maintenance and installation work was done.



Node Site Coordinator Responsibilities - Node Site Access Control

The NSC is responsible for maintaining security on the node site. The NSC provides access to the node site for contractors, and assists DISA personnel who survey the node site.

**NSC Responsibilities:
Assist RNOSC**

- Act as 24-hour POC for RNOSC
- Provide on-site information
- Provide RNOSC with alternate POC
- Act as RNOSC's local rep
- Request support from RNOSC

• NIPRNET - 800-554-3476	DSN - 850-4790
• Europe - 49.711.680.5532	DSN - 314-430-5532
• Pacific - 1-808-656-2777 x105	DSN - 315-456-2777 x 105

• SIPRNET - 800-451-7413	DSN - 223-4120
• Europe - 49.687.776.8443	DSN - 314-430-5532
• Pacific - 1-808-656-2777 x 105	DSN - 315-456-2777 x 105


DISN Data Services Course
Slide 9-9

Note Site Coordinator Responsibilities - Assist RNOSC

The NSC is the RNOSC's on-site representative. If problems occur, the RNOSC must know whom to call, and how to reach that person, either to monitor the node site, or to grant maintenance personnel access to the node site.

In turn, the RNOSC is available to assist the NSC to answer questions and to solve problems about node site procedures and issues.

Node Site Coordinators' Conference



23 - 25 May, 2000
Regional Network Operations and Security Center
Columbus, OH

AGENDA

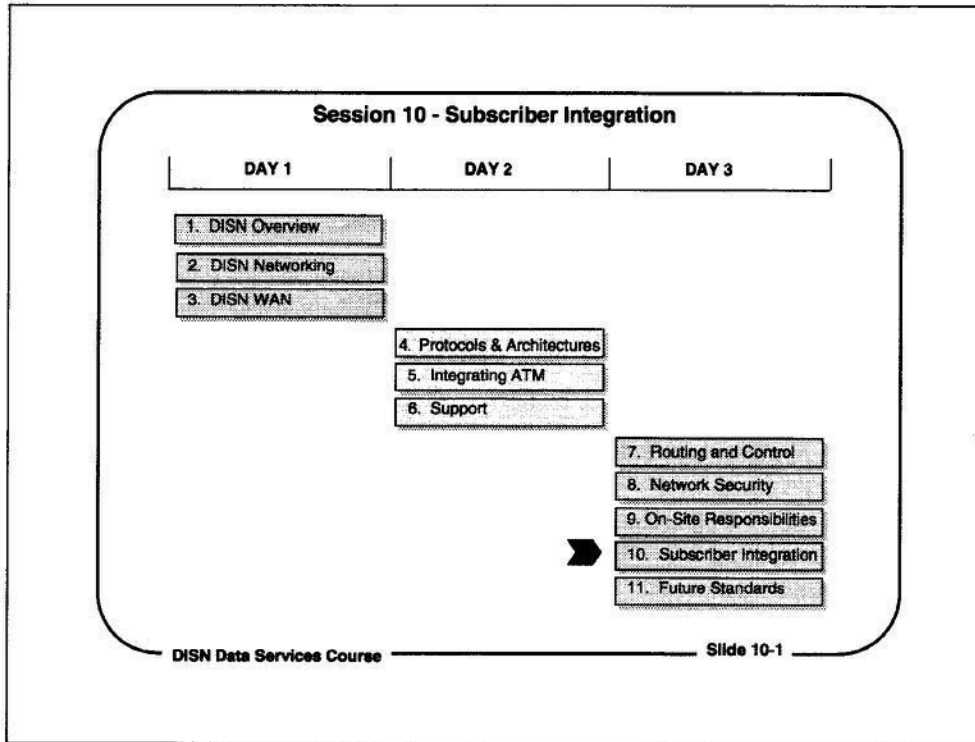
- Network briefing
- ATM status
- Technology update
- Help desk briefing
- Network Operations

DISN Data Services Course Slide 9-10

Node Site Coordinators' Conference

Each year, the CONUS RNOSC in Columbus, OH sponsors a Node Site Coordinators' Conference. The purpose of the conference is to update the Node Site Coordinators on RNOSC support procedures, network status, and node site upgrade programs, as well as to train NSCs on their on-site responsibilities.

This year, the annual Node Site Coordinators' Conference will be held in Columbus, OH on 23-25 May, 2000. For information on the conference, contact Alice Bontrager at the RNOSC (abontrager@crcc.disa.mil).

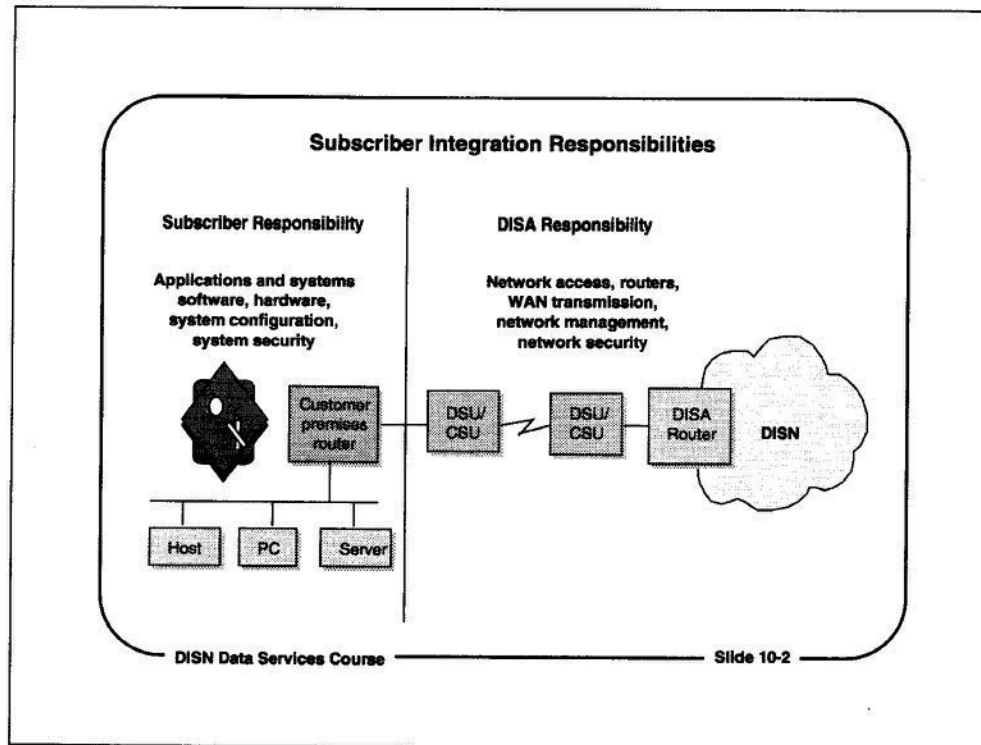


Session 10 - Subscriber Integration

Upon completion of this module, the students will have an understanding of the DISA subscriber integration process, and of the DISN data services network tariffs. The students will also have a general understanding of the purpose and functions of the DISA network management systems, and they will be able to distinguish between DISA and customer responsibilities for system integration and network management

This session will focus on:

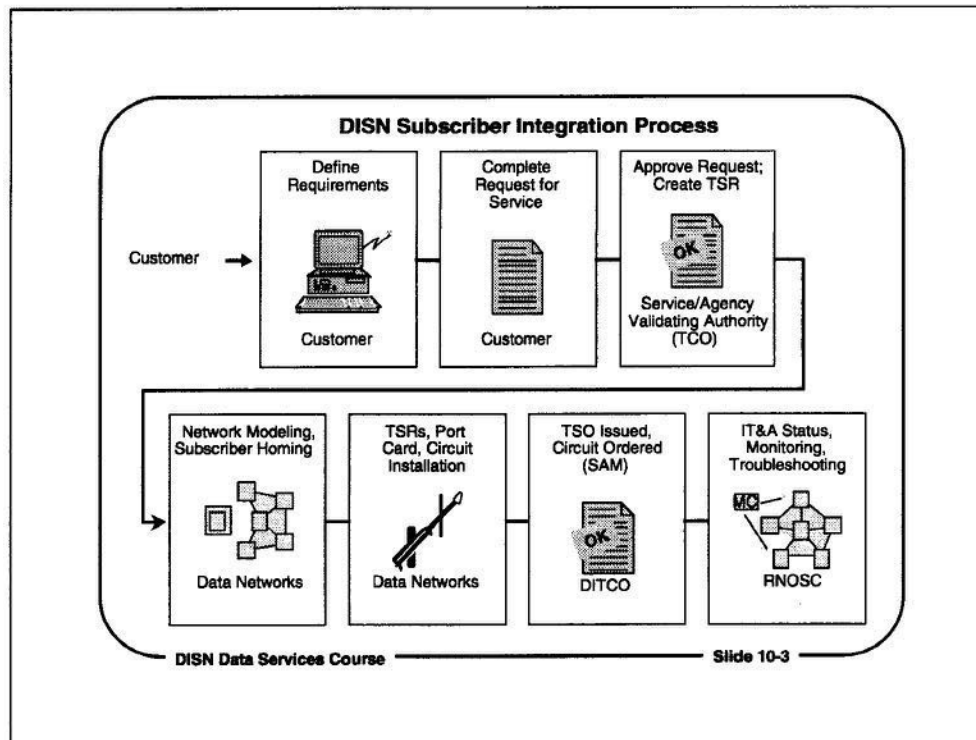
1. Describing the DISN subscriber integration process
2. Describing the DISN data services network tariffs
3. Defining the purpose and functions of the DISA network management systems
4. Distinguishing between DISA and customer responsibilities for systems integration and network management



Subscriber Integration

The process of adding a host, a router, a LAN, or another type of network to a DISN Data Services network is called Subscriber Integration. DISA must know about everything that is directly connected to a DISA router, so new connections to DISA router ports must go through a subscriber integration process.

For new devices or networks that will be connected to DISA router ports, DISA bears most of the responsibility for the hardware, software, and access line costs needed to bring a new subscriber system into the network. DISA is responsible for - and pays for - the installation and operation of the access lines that connect devices to DISA router ports, and for the modems or CSU/DSU units on both ends of an access line. DISA is also responsible for everything in and directly connected to the DISN backbone.

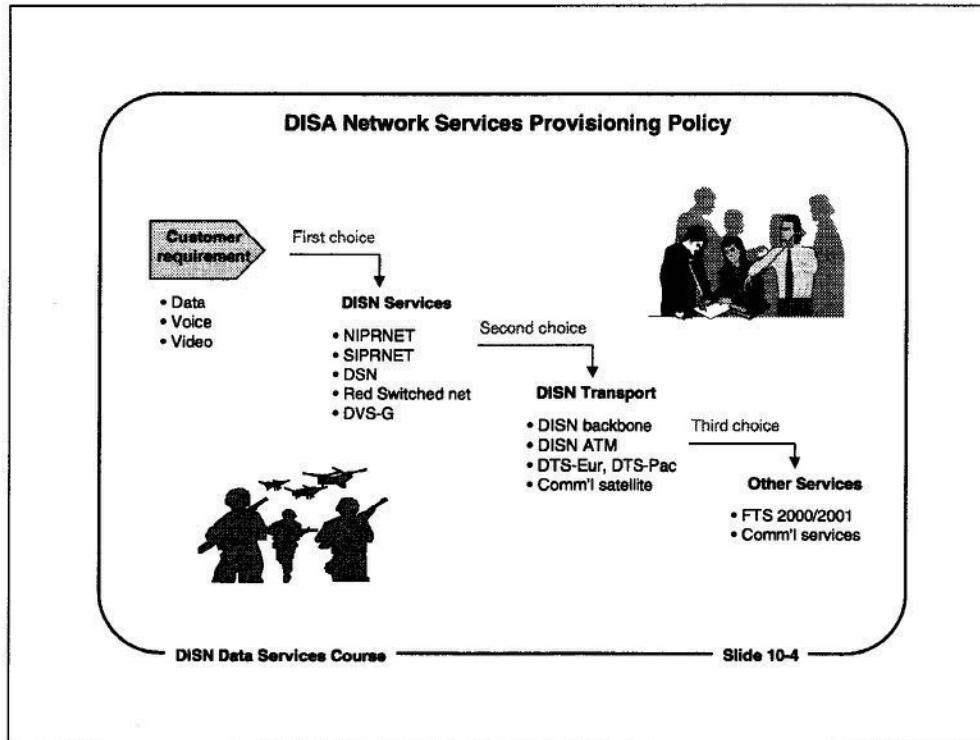


DISN Subscriber Integration Process

The steps in the subscriber integration process for connecting to a DISN Data Services network are divided into four phases. DISA, the subscriber, and several contractors are involved in the subscriber integration process. The phases of the subscriber integration process, and the activities in each phase are:

- **Planning** - Determining requirements for connecting devices to the network, modeling its effect on the operation of the network, and completing the Request for Service (RFS) documentation.
- **Implementation** - Installing and configuring the hardware, software, and communications equipment for the network connection, and issuing the Technical Service Order (TSO) and the Service Activation Message (SAM).
- **Testing** - Testing and activating the connection.
- **Operational** - Making the connection operational.

Billing for the connection to the network begins when the circuit is declared operational. Subscribers will be billed for a network connection that has been declared operational, whether or not they use it.

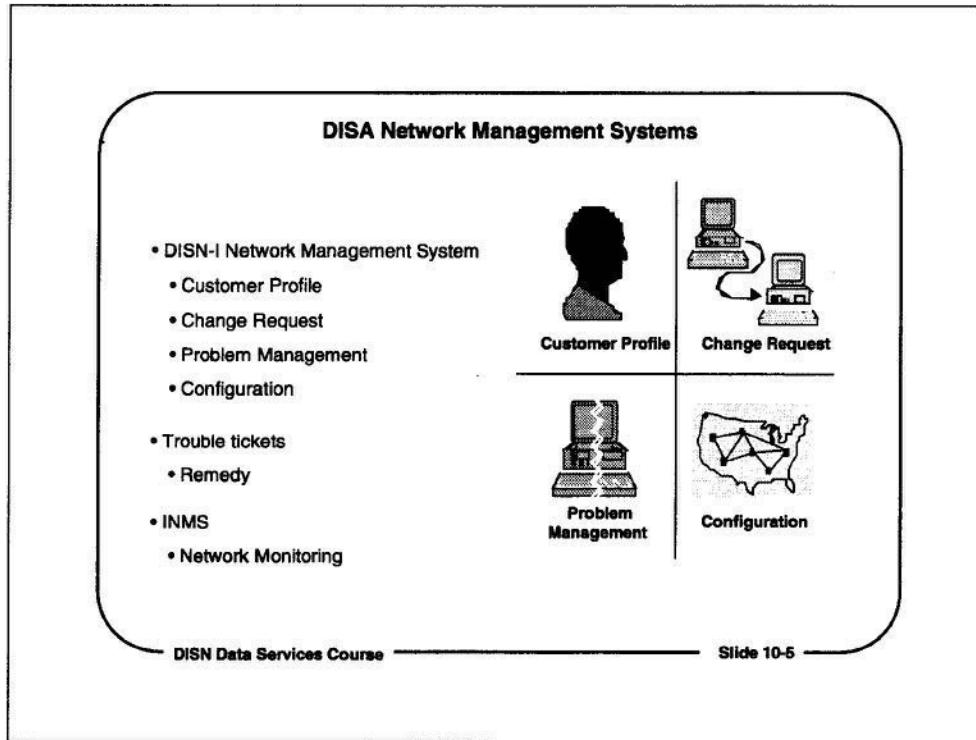


DISA Network Services Provisioning Policy

The DISA policy for provisioning services to meet customers' requirements for data, voice, and video services is to analyze the customer application requirements, then provide a service that best meets the customer's needs.

DISA provisions network services for data, voice, and video according to the following policies:

- If it will meet the requirements of the application, DISA will provision one of its existing network services, such as NIPRNET for unclassified data applications, and DSN for unclassified switched voice.
- If an existing DISA network service will not meet the requirement, DISA will provide network transport across a DISA-controlled WAN, or across a commercial network.
- If neither of these will meet the requirement, DISA will provision the service on a commercial network, the FTS network, or another network.

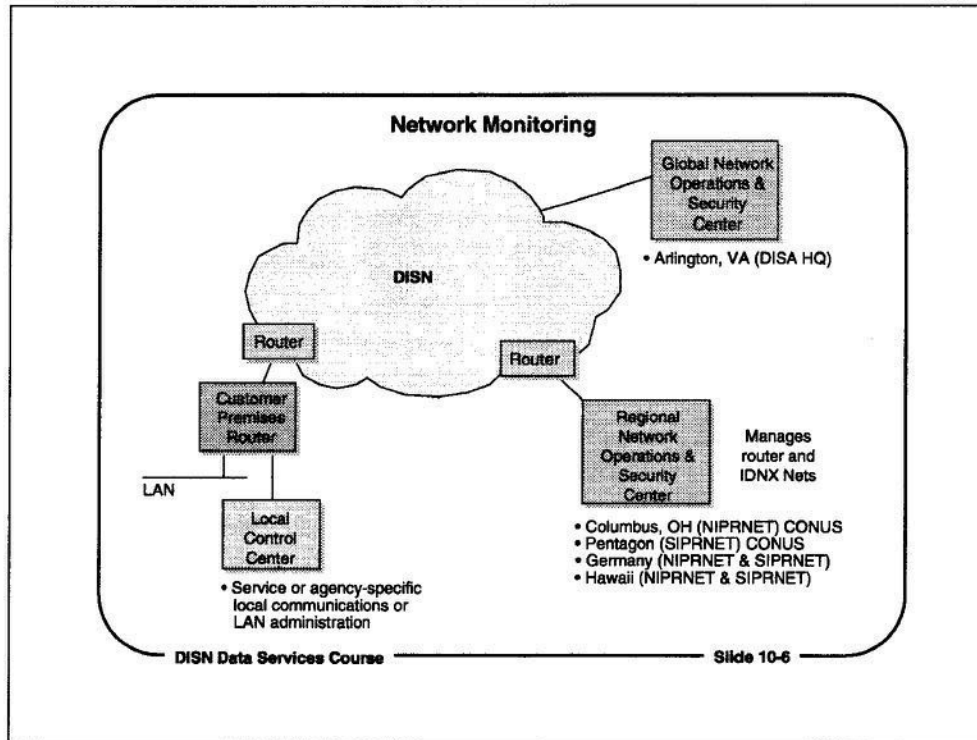


DISA Network Management Systems

DISA uses its Network Management System to monitor the subscriber integration process, as well as to manage the configuration and operation of the network. The DISA Network Management System is a database management system that is accessible by both DISA and its customers.

The four components of the DISA Network Management System are:

- Customer Profile
- Change Request Management
- Problem Management
- Configuration

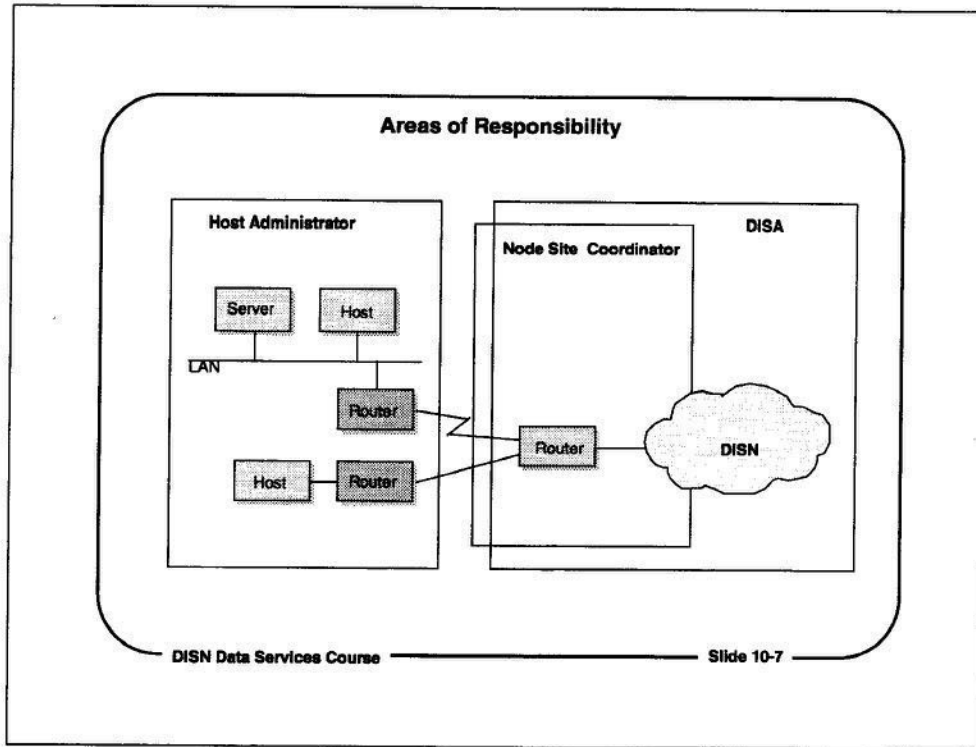


Network Monitoring

There are three levels of network control centers for the DISN Data Services networks. The Global Network Operations and Security Center (GNOSC) and the Regional Network Operations and Security Centers (RNOSCs) manage DISA networks and DISA-owned assets. Local Control Centers (LCC) manage service- or agency-specific assets and networks at each post, base, camp, or station, or in service-wide centers.

DISA has one GNOSC at DISA headquarters in Arlington, VA, and four RNOSCs. The GNOSC has overall administrative responsibility for the DISN backbone and the DISN Data Services networks, but it has no operational control over the networks. The RNOSCs are responsible for monitoring and operating the DISN backbone and the DISN Data Services networks.

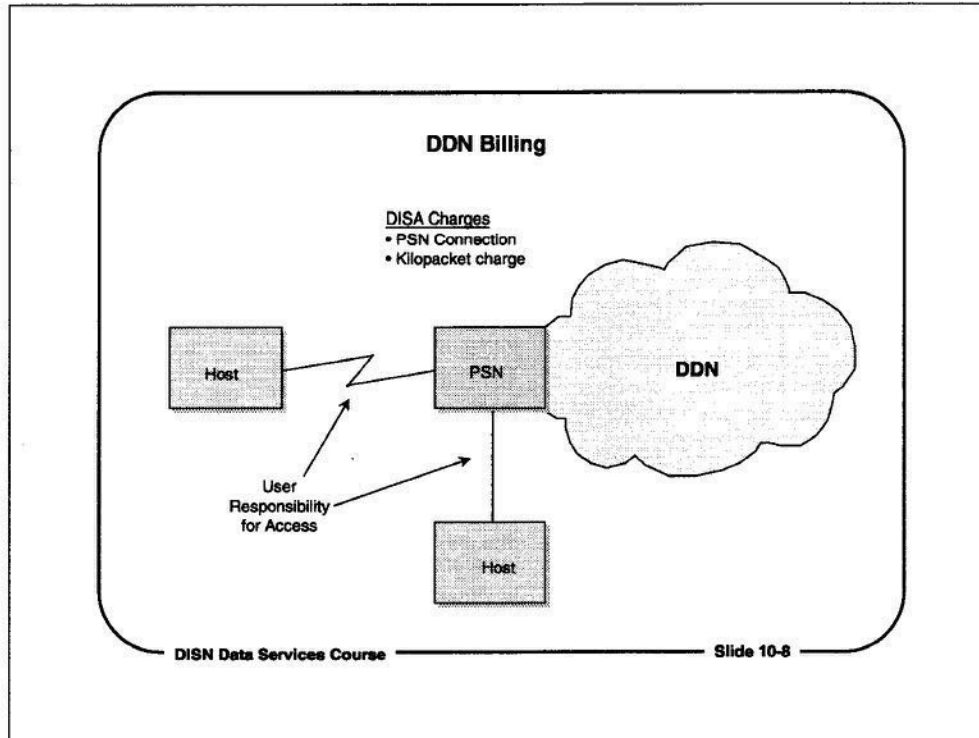
Local control centers are run locally, or by the branches of the armed services to provide network monitoring and first-line assistance to local host and network administrators.



Areas of Responsibility

Responsibility for operation, configuration, and maintenance of the network and its components is shared by DISA and its subscribers. DISA is responsible for everything in the DISN backbone, the DISA routers, and the access circuits behind DISA router ports. DISA is also responsible for the node sites that house DISA equipment.

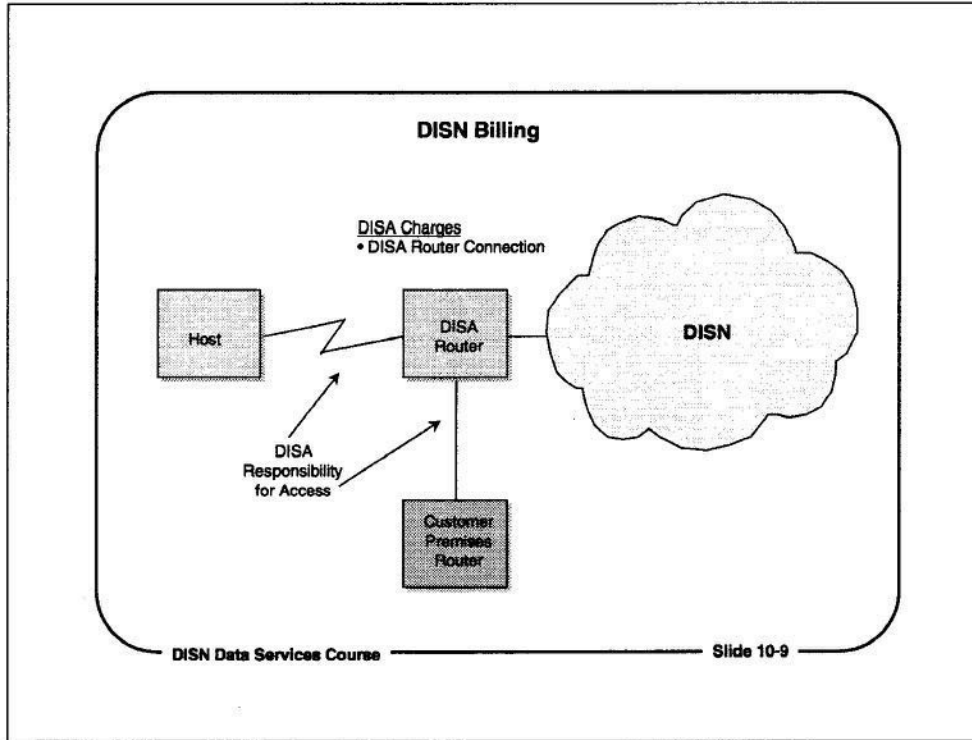
The operation, configuration, and maintenance of everything behind the DISA routers is the responsibility of DISN Data Services network subscribers. For NIPRNET, DISA's responsibility extends to the port of the DISA router or to the customer site CSU/DSU if a CSU/DSU is required. For SIPRNET, DISA's responsibility extends to the customer site KG where KG encryption devices are required to provide a trusted path between the customer's equipment and the SIPRNET router.



DDN Billing

Under the old DDN billing structure, subscribers paid a recurring monthly charge for each Packet Switching Network (PSN) port their hosts or concentrators used, as well as a charge for the number of packets (kilopackets) they sent to the PSN.

In addition, users were responsible for paying for and maintaining access circuits to connect to PSN ports.



DISN Billing

Under the new DISN Data Services networks billing structure, subscribers pay a recurring monthly charge only for each DISA router port their hosts or concentrators use. There is no additional charge for the number of packets sent to the DISA router.

In addition, DISA is responsible for paying for and maintaining access circuits to connect user hosts or customer premise routers to DISA router ports. The cost of the access circuit (if it is required) is bundled into the monthly DISA router port connection charge.

FY 00 DISN Data Services Network Charges

**IP Router (NIPRNET & SIPRNET) Service
All Theaters
Monthly Recurring Charges**

Access bandwidth	CONUS, HI, AK	Europe	Pacific
64 Kb	\$405	\$600	\$700
128 Kb	709	1,049	1,225
256 Kb	1,215	1,799	2,100
384 Kb	1,620	2,389	2,801
512 Kb	2,025	2,998	3,501
768 - 896 Kb	2,228	3,298	3,851
1 Mb	2,329	3,488	4,026
1.024 - 1.544 Mb	2,430	3,598	4,201
2-2.048 Mb	2,532	3,748	4,376
3 Mb	2,633	3,898	4,551
4 Mb	2,937	4,347	5,076
5 Mb	3,241	4,797	5,601
Ethernet, 6Mb	3,646	5,397	6,301

DISN Data Services Course Slide 10-10

FY 00 DISN Data Services Network Charges

Subscribers to DISN Data Services networks pay a flat connection charge, regardless of the amount of network traffic they generate or receive. The charges for DISA router connections are for each DISA router port to which a subscriber is connected. The DISA router port charge is not affected by the number of users, networks or hosts connected behind the DISA router port.

There is also a one-time, non-recurring charge for each DISA router port connection. The charge is \$2,500 for less than 512 Kb or Ethernet, and \$5,000 for 512 Kb and higher. Dual-homed subscriber connections cost full price for the first connection, and 50% of the monthly recurring charge (MRC) for the second connection.

Dial-up service charges are \$27 per month, plus a one-time \$50 registration fee.

The Customer Premises Router management fee for Cisco and Nortel/Bay routers is \$50 per month. The management fee for other vendors' routers will be established on request from the subscriber.

Under some circumstances, subscribers may elect to connect directly to a JIS router. A JIS router T-1 connection charge is twice the theater T-1 (1.544 MBP) MRC.

FY 00 DISN Data Services Network Charges

**IP Router (NIPRNET & SIPRNET) Service
All Theaters
Monthly Recurring Charges**

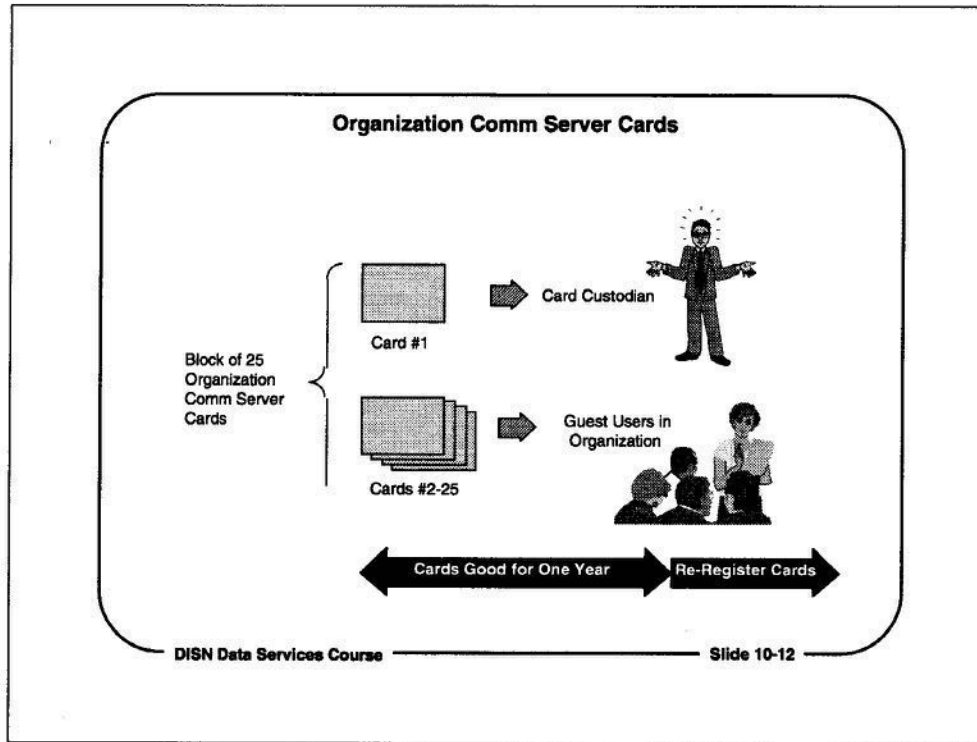
Access bandwidth	CONUS, HI, AK	Europe	Pacific
7 Mb	\$4,051	\$5,996	\$7,001
8 Mb	4,253	6,296	7,352
9 Mb	4,658	6,896	8,052
12 Mb	5,874	8,695	10,152
15 Mb	6,846	10,134	11,832
18 Mb	8,102	11,992	14,003
21 Mb	9,114	13,491	15,753
24 Mb	10,410	15,410	17,994
27 Mb	11,869	17,569	20,514
30 Mb	13,165	19,488	22,755
33 Mb	14,461	21,406	24,995
36 Mb	16,568	24,525	28,636
39 Mb	18,877	27,942	32,627

DISN Data Services Course Slide 10-11

FY 00 DISN Data Services Network Charges

Access charges and tariffs for high-bandwidth NIPRNET and SIPRNET services have been established, starting in FY00. Access at high bandwidth data rates (3 Mb and higher) can be established through either a serial connection, or through a fast Ethernet connection from a customer premises router co-located with a NIPRNET or SIPRNET router.

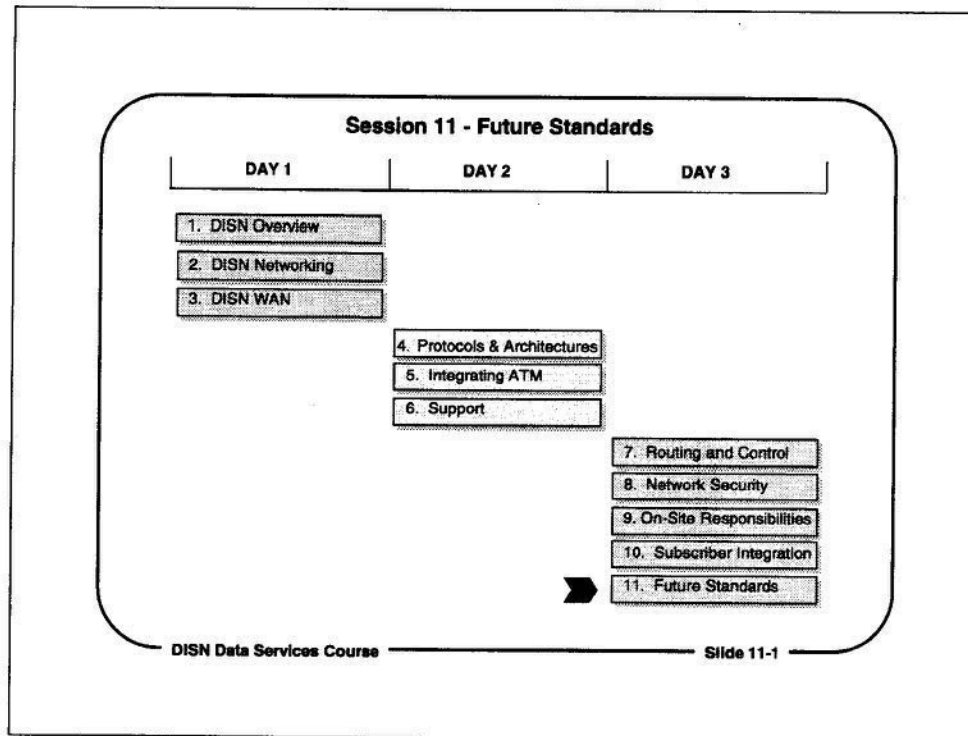
NIPRNET and SIPRNET access at data rates higher than 39 Mb may be available in some locations. Rates and access arrangements for data rates greater than 39 Mb must be negotiated with DISA, and are subject to access, router node, and DISN network capacity constraints.



Organization Comm Server Cards

Guest users of a DISA Comm Server must also have DISA Comm Server cards. An organization may buy a block of as many as 25 Organization Comm Server cards. These cards and their user accounts may be assigned temporarily to users who need them for access during TDY travel, or for occasional access.

Each of the 25 cards is good for one year, after which time it must be re-registered and renewed for another year. One of the 25 cards must be assigned to a Card Custodian, who is the subscriber organization's contact for DISA for the registration and use of the other 24 cards. Each of the Organization Comm Server cards carries the standard \$27 per month usage fee .

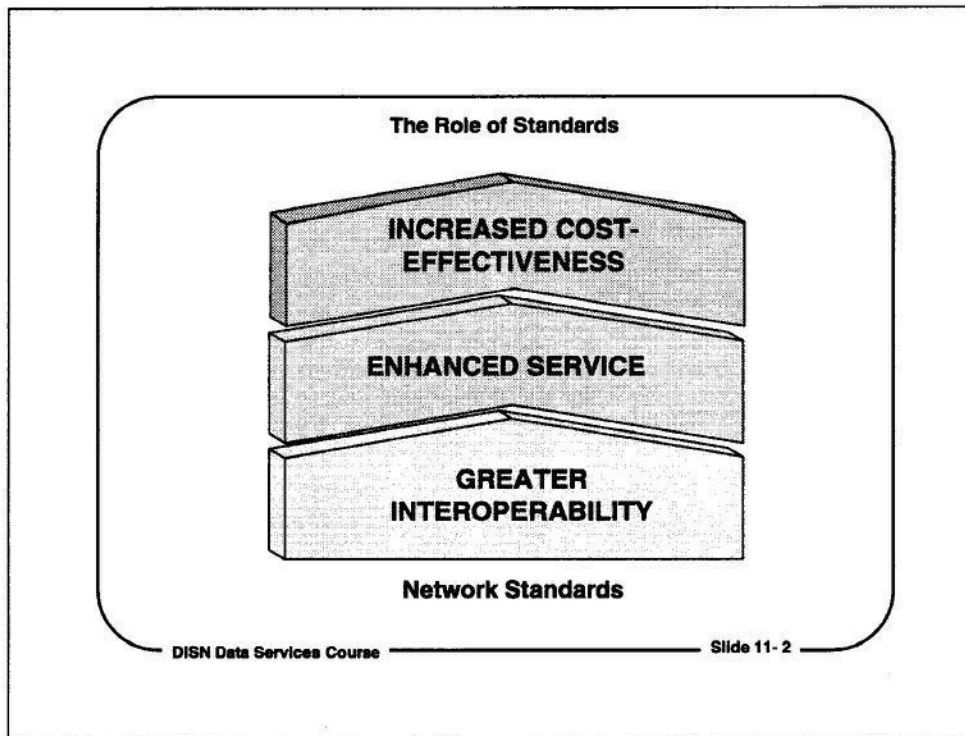


Session 11 - Future Standards

Upon completion of this module, the students will have a general understanding of the role of standards in communication systems, and the potential for the use of other protocols and standards in DISN data services networks.

This session will focus on:

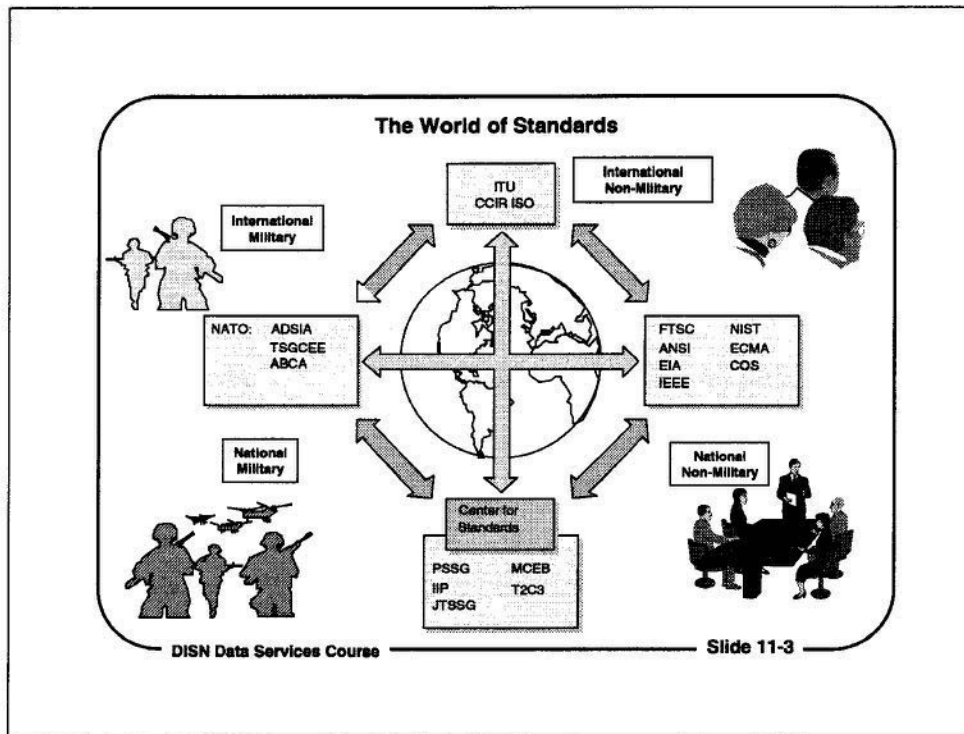
1. Describing the role of standards in communication systems
2. Describing the potential for the use of other protocol and standards in DISN data services networks



The Role of Standards

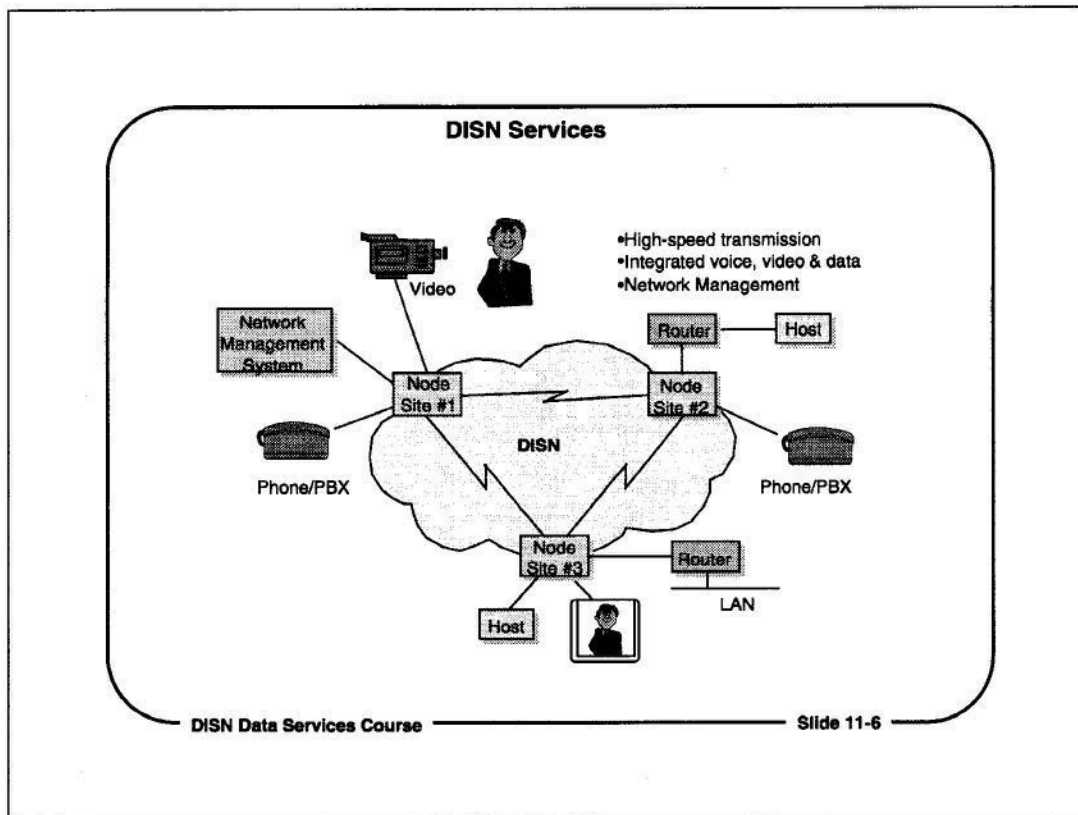
The DoD, other parts of the U.S. Government, and businesses are interested in using a common set of networking standards, instead of the many incompatible standards they use today.

Using a common set of protocols would promote interoperability among different systems, enhance the services available to users, and allow armed services and government agencies to create better communications systems at lower cost.



The World of Standards

- In 1977, the International Standardization Organization (ISO) created the Open System Interconnection (OSI) subcommittee to develop a standard architecture.
- The abstract functional layering of this architecture, the current OSI Reference Model, was approved in 1982 by ISO.
- It is a framework for the current and future development of complete service definitions for these layers and the implementation of the services in standard protocols.
- The International Telecommunications Union (ITU), formerly the International Telegraph and Telephone Consultative Committee (CCITT), has adopted the OSI Reference Model and works closely with the ISO on service definitions and protocol development for each layer.
- Other standards organizations (such as IEEE (Institute of Electrical and Electronic Engineers), EIA (Electronics Industry Association), and ECMA (European Computer Manufacturers Association), are also developing, adopting, and supporting standard protocols and interfacing procedures that provide the services defined by the OSI Reference Model.



DISN Services

DISA's objectives in operating the DISN Data Services networks are to:

- Provide reliable high-quality data communications services for DoD subscribers
- Create a high-speed backbone transmission network that will support a number of applications
- Integrate communications for a variety of applications, including data, voice, and video, over a single backbone network
- Manage the backbone network and the data services carried on the network for an economical, efficient operation.

Eventually, most DoD network services, including much of the voice traffic now carried on special-purpose or dedicated networks, may be moved to the DISN backbone.

GLOSSARY

Access Circuit	A leased line circuit connecting a customer premise router or a host to a DISA router.
Adapter	A board installed in a computer system, usually a PC, to provide network communication capabilities to and from that computer system. Also called a network interface card.
Application Layer Protocol	Concerned with providing services on the network, such as file, print, database, and other network services. Provides an interface whereby applications can communicate with the network.
Architecture	A set of protocols and specifications for network communications.
ARP	(Address Resolution Protocol) A network protocol to map data link-level (LAN) addresses of devices to their IP addresses.
AUTODIN	A U.S. Department of Defense store-and-forward messaging system for transmitting formal message traffic.
ATM	(Asynchronous Transfer Mode) A packet switching technique which uses packets, or cells, of fixed length to transmit multiple types of information (voice, video, data) at speeds from 155 to 622 Mbps.
Autonomous System	(AS) A group of routers under a single administrative entity, that exchange routing information by using the same protocol.
Backbone	A high-capacity network to which several lower-capacity networks are linked. A backbone network carries traffic among the lower-capacity feeder networks.
Bandwidth	The difference between the highest and lowest frequencies of a band. The measure of the capacity of a communication channel, expressed in bits per second.
Bandwidth Manager	(BWM) An ATM switch or an ATM cell multiplexer that connects the DISA SDNs to the DISN ATM backbone network.
Baseband	A method of using time-division multiplexed transmissions on a single channel for short-distance, local area network transmission.

GLOSSARY

Baud	A unit for measuring data transmission speed. One baud is one signal transition per second, but it usually is used to indicate the data transmission rate in bits per second.
BGP	(Border Gateway Protocol) A protocol for communications between border routers in different Autonomous Systems, to pass information about reachable networks in other ASes.
Bit	(Binary digit) The units - 0 or 1 - used in the binary numbering system.
Bridge	A device that connects two or more networks at the data link level. Bridges differ from repeaters because bridges store and forward complete packets while repeaters forward electrical signals. They differ from routers because they use physical addresses, such as Ethernet addresses, instead of network addresses.
Broadband	Transmission facilities capable of handling frequencies greater than those required for voice grade communications, or a carrier that has multiple channels separated by different frequency ranges.
Broadcast	A packet delivery system in which a copy of a packet is sent to all hosts attached to a network. In the IP protocol, packets addressed to host 255 are broadcast packets that are received by all hosts on the network.
Bus	A network topology in which each network node is connected directly to the transmission medium; each node "sees" all messages intended for any other node.
CIDR	(Classless Inter-Domain Routing) A method of aggregating IP network addresses to simplify routing tables.
Coaxial cable	A transmission medium that uses a single copper conductor surrounded by insulation which in turn is surrounded by an outer jacket which also is a conductor.
Communications Server	A computer that provides dial-up access to the NIPRNET or the SIPRNET.
Concentrator	A router that enables several hosts or terminals to use the same communications path to access a network.

GLOSSARY

Control Center	A facility run by DISA that monitors the operation of the DISN Data Services networks; also called the Regional Operation Support Center (ROSC).
Core router	A NIPRNET or SIPRNET router that is connected directly to the DISN backbone.
CSMA/CD	(Carrier-Sense Multiple Access with Collision Detection) local area network access method used by Ethernet and IEEE 802.3. Devices transmit after finding the data channel clear. When two devices transmit simultaneously, a collision occurs and the colliding devices try to re-transmit after a random period of time.
CSU/DSU	(Channel Service Unit/ Data Service Unit) A digital interface unit that connects end user equipment to a digital telephone line; the CSU/DSU corresponds to a modem on an analog line. The DSU converts data into the appropriate digital format for transmission. The CSU terminates the line, conditions the signal, and participates in remote testing of the connection.
Datagram	A logical grouping of information sent as a network-layer unit over a transmission medium, such as an IP datagram. The terms <i>packet</i> , <i>frame</i> , <i>segment</i> , and <i>message</i> are also used to describe logical information groupings at various layers of the OSI reference model. IP datagrams are the primary information transmission units that are handled by the routers in the NIPRNET, SIPRNET, and the Internet.
DCE	(Data Communications Equipment) The devices and connections of a communications network that connect the communications circuit with an end device (Data Terminal Equipment). A modem or a CSU/DSU can be a DCE.
Defense Commercial Telecommunications Network (DCTN)	A high-bandwidth digital network operated by DISA that supports video and voice traffic; features pay-by-use pricing and volume usage discounts.
Defense Information Services Network	(DISN) The worldwide, long-distance backbone network that is operated by DISA to support the DoD common user data networks, such as NIPRNET and SIPRNET.
Defense Information Systems Agency	(DISA) The DoD agency that is responsible for providing and operating communications services to support DoD operations worldwide.

GLOSSARY

Defense Messaging System (DMS)	A DoD-wide messaging system that will consolidate commercial, networked e-mail systems with the AUTODIN messaging system. DMS integrates secure messaging and unclassified electronic mail systems in a single system, along with file encryption and message authentication.
Defense Simulation Internetwork	(DSI) A special-purpose DISN Data Services Network designed for DoD users who need reserved bandwidth, performance guarantees, high-speed access, and multicast capabilities, to support special applications, such as wargame simulations.
Defense Switched Networks (DSN)	Unclassified and classified voice transmission networks.
DISN Data Services Networks	The general-purpose IP data networks operated by DISA for unclassified data (NIPRNET) and classified data (SIPRNET), as well as special-purpose networks, such as the DSI and JWICS.
DNS	(Domain Name System) A distributed directory service used on the Internet to translate text host names to IP addresses.
DSU/CSU	See CSU/DSU.
DTE	End-user equipment or computer systems that use communications for applications, such as computers and terminals. A DTE connects to a DCE, which connects in turn to the communications circuit.
Dynamic Bandwidth Allocation	The ability to drop and add channel bandwidth to respond to different applications requirements.
E-1	A European and Japanese telephone system standard for a digital channel that runs at 2.048 Mbps, and that can carry 32 digitized voice or data channels; corresponds to a T-1 circuit.
E-3	A European and Japanese telephone system standard for a digital channel that runs at 48 Mbps, and that can carry 32 digitized voice or data channels; corresponds to a T-3 circuit.
EGP	(Exterior Gateway Protocol) A protocol by which routers in different networks exchange information about what systems they can reach. Generally, an exterior gateway protocol is any internetworking protocol for passing routing information between Autonomous Systems.

GLOSSARY

Emulated LANs	(ELANs) A technique of connecting separate LANs across a backbone ATM network, such as the NIPRNET, so that the devices on the LANs appear to be on one large LAN, rather than on separate LANs connected by routers.
Encapsulation	Wrapping a data set in a protocol header for transmission. For example, Ethernet data is wrapped in an Ethernet header before transmission. Also, a method of bridging dissimilar networks, where an entire frame from one network is enclosed in the header used by the link-layer protocol of the other network.
Encryption	Applying a specific algorithm to data to encode the data, to prevent other devices from reading the information. Decryption reverses the algorithm to restore the data to its original form.
Ethernet	An IEEE standard (802.3) data link protocol that specifies how data is placed on and retrieved from a local area network. It is the underlying transport vehicle used by upper-level protocols, such as TCP/IP. CSMA/CD is Ethernet's media access method.
Fast Ethernet	A 100-Mbps technology based on the 10BASE-T Ethernet CSMA/CD network access method, to raise Ethernet speeds from 10 Mbs to 100 Mbs.
Fastlane	A multi-level encryption device designed to make more efficient use of network bandwidth, by encrypting only the data portion of IP datagrams or ATM cells sent through the DISN data services networks.
Fiber Distributed Data Interface	(FDDI) A high-speed digital backbone or local area network technology, used to create a 100 Mbps token-passing network using fiber optic cable.
Fiber optics	Thin strands of glass or plastic fiber that are used to transmit digital data at high speed by transmitting pulses of light. A thin strand (fiber) of glass (the core) surrounded by a layer of glass that has a lower refractive index (cladding), which in turn is surrounded by a protective sheath.
Firewall	A computer system that protects networks by screening IP traffic based on applications, source or destination IP addresses, or other criteria.
FORTEZZA	A security and encryption system designed and certified by the National Security Agency (NSA), which will be used in the Defense Messaging System (DMS).

GLOSSARY

FTP	(File Transfer Protocol) The Internet application protocol used to transfer files between computer systems over networks running the TCP/IP protocols.
Firewall	A computer system or group of routers and computers that protect a network from intrusion or invasion.
Frame Relay	A packet switching technology that uses a relatively reliable transmission network to send large blocks, or frames, of data; in wide use as an upgrade to point-to-point private line circuits.
Gateway	A system that converts or transfers data between two systems, or between systems that use different protocols; often used to refer to a router.
Gbps	(Gigabits per second) Transmission at a rate of one billion bits per second.
Hop	A unit that equates to the passage of a packet through one router.
Host	A computer system on a network; similar to the terms <i>device</i> or <i>node</i> , except host usually implies a computer system, whereas device or node generally apply to any networked system, including terminal servers and routers.
HTML	(Hypertext Markup Language) The computer language used by a Web browser to interpret and display a Web page.
HTTP	(Hypertext Transmission Protocol) The application-level protocol used in TCP/IP networks to transfer Web page files from Web servers to Web browsers.
IDNX	A trade name for a digital multiplexer made by Network Equipment Technologies (NET); used to multiplex data from different routers across point-to-point data circuits in the DISN.
Interface	A shared boundary with common characteristics and meanings, or the point where devices connect, such as the RS-232 interface between a DCE and a DTE.
Integrated Services Digital Network	(ISDN) A digital local access method that provides two 64 Kb channels, which may be used for voice or data services.

GLOSSARY

Internet	A group of networks interconnected by a set of routers which allow them to function as a single, large virtual network, such as the NIPRNET.
Internet, the	A system of linked computer networks, worldwide in scope, that facilitates data communication services such as remote login, file transfer, electronic mail, and distributed newsgroups. The Internet's origins lie in a U.S. Department of Defense computer system called ARPANET, an experimental network designed to facilitate scientific collaboration in military research.
ICMP	(Internet Message Control Protocol) A network-level protocol that devices running the IP protocol use to send IP error messages, such as "Host unreachable."
Internet Protocol	(IP) A packet switching protocol, which is part of the TCP/IP protocols, that provides datagram service and that performs addressing and route selection. An IP header is appended to data packets, which are transmitted as frames by lower level protocols. IP routes packets through internetworks.
Internet Service Provider	(ISP) A company or organization that provides access to the Internet, either to end-users, businesses, or to other, smaller ISPs. DISA acts as an ISP for NIPRNET users.
Internetwork	A group of networks interconnected by routers or other devices that functions as a single network; sometimes called an internet, but which is not synonymous with the Internet.
Intranet	A network contained within an enterprise, which may consist of many inter-linked LANs. It may or may not include connections through one or more gateways to the outside Internet, but its purpose is to use Internet technologies for a closed community of users. The main purpose of an intranet is usually to share company information and computing resources among employees, or to facilitate working in groups.
JIS	(Joint Interconnection Service) A special network of DISA routers that interconnects NIPRNET segments in CONUS, Europe, and the Pacific to each other, as well as to the Internet.
JWICS	(Joint Worldwide Intelligence Communications System) One of the DISN Data services networks, operating at a Top Secret/SCI level, that is used by the DoD intelligence community.

GLOSSARY

Kilobit	(Kb) A transmission rate of a thousand bits per second. Used as a measure of a transmission circuit's bandwidth or capacity.
Leased line	A full-period dedicated phone circuit used for data that offers a fixed amount of bandwidth between two locations.
Local Area Network	(LAN) A group of computers and network communications devices interconnected within a geographically limited area, such as a building or campus.
Long-haul Network	A network spanning long geographic distances, usually connected by telephone lines or satellite radio links.
Mail Bridge	A computer system that transfers e-mail messages between two different networks that may have different addressing or format conventions, or operate at different security levels.
Megabit	A million bits, used as an expression of a transmission bandwidth or information carrying capacity. Megabits per second (Mbps) is a frequent measure of bandwidth on a transmission medium such as T-1 digital line or an Ethernet LAN.
Multiplexer	A telecommunications device that consolidates signals from many sources, such as telephones, computers, or other devices, for transmission over a high-capacity communications channel, in which they are separated by time or frequency. At the receiving end, another multiplexer separates the signals into separate transmissions.
Node Site Coordinator	The local DISA contact responsible for the equipment at a DISA node site.
NIPRNET	The common user DISN Data Services network that is for unclassified but sensitive traffic.
Node site	The physical location at a customer site where DISA owned equipment is kept and maintained. This location may be a Data Center or a Base Communications Facility.
OSI Reference Model	The seven-layer network architecture model of data communication protocols developed by ISO and CCITT. Each layer specifies particular network functions such as addressing, flow control, error control, encapsulation and reliable message transfer.
Packet	An individually addressed message or data block that has been divided for transmission across a packet switching network.

GLOSSARY

Packet switching	A type of data transfer that occupies a communication link only during the time of actual data transmission. Messages are split into packets and reassembled at the receiving end of the communications link.
PCMCIA	(Portable Computer Memory Card Industry Association) An industry standard for credit-card-size peripherals for portable computers.
POP3	A protocol for retrieving e-mail messages from a server or host that receives and stores messages for delivery.
PPP	(Point-to-Point Protocol) A protocol for connecting a dial-up computer to a network, so that the computer acts as if it were directly connected to the network.
Protocol	A formal description of messages to be exchanged and rules to be followed for two or more systems to exchange information.
Repeater	A hardware device that copies electrical signals from one network segment to another.
RIP	(Routing Information Protocol) An industry-standard protocol used by routers in TCP/IP networks to exchange routing information.
Router	A hardware device that is connected to two or more networks that use the same network addressing and delivery rules to direct packets to other routers until they can be delivered across a network.
Routing table	A table maintained internally by a router that maps networks to router ports; used by the router to make routing decisions.
SDH	(Synchronous Digital Hierarchy) The European version of SONET. The basic SDH rate (STM-1) is 155.52 Mbps, which is equivalent to SONET's STS-3/OC-3 rate.
Server	A computer that acts as a shared network resource to manage access to data files, store and retrieve e-mail, control printers, and provide dial-up access for remote users.
Service Delivery Node	(SDN) The DISA node site that provides DISA subscribers access to the DISN backbone network; NIPRNET and SIPRNET routers, as well as ATM switches and other equipment, may be located at an SDN.

GLOSSARY

SIPRNET	The secret, classified DISN Data Services network.
SMTP	(Simple Mail Transfer Protocol) The standard Internet protocol for transferring electronic mail from one e-mail host or server to another.
SONET	(Synchronous Optical Network) An industry standard interface for digital transmission on fiber optic systems at rates from 51.84 Mbps to 2.4 Gbps (gigabits per second).
STEP site	(Standard Tactical Entry Point) An access point into the DISN Data Services networks for tactically deployed networks; consists of a satellite earth station and dedicated routers that connect tactical networks to the NIPRNET and SIPRNET.
Subchannel	A part of the information carrying capacity of a communications circuit that has been subdivided to carry more than one transmission at a time; backbone circuits, like the T-1 circuits between IDNX multiplexers, are typically divided into subchannels to carry data between different routers.
T-1	A high speed digital communications channel, capable of supporting transmission speeds of 1.544 Mbps.
T-3	A high speed digital communications channel, capable of supporting transmission speeds up to 45 Mbps.
TCP/IP	(Transmission Control Protocol/Internet Protocol) A set of protocols developed by the U.S. Defense Department's Advanced Research Projects Agency (ARPA) during the early 1970s, but now widely used in DoD networks and the Internet.
TDM	(Time Division Multiplexing) Technique to combine data from multiple channels on a single communications path, by assigning each channel a specific time slot.
Telnet	A TCP/IP application-level protocol for virtual terminal access.
Terminal	A keyboard/display or keyboard/printer device used to input programs and data to the computer and to receive output from the computer.
Trunk	A high-capacity communications circuit, often part of a long-haul network or wide area network.

GLOSSARY

- Twisted pair** A type of simple, low-cost wiring for phone lines and LANs that uses two or more insulated wires twisted together.
- X.25** An international standard, developed by the ITU, that defines a protocol for communication between packet-switched Public Data Networks and user devices in the packet-switched mode. The old DDN network used X.25 packet switches instead of IP routers.
- X.400** An ITU standard for the format and addressing conventions that can be used by e-mail and messaging systems, so that different e-mail and messaging systems will have common ways to exchange messages and identify recipients; DMS will use a version of the X.400 protocols to encode and transfer e-mail and other messages.
- X.500** An ITU standard for the content and structure of a directory of network users and resources; DMS will use an X.500 directory structure to identify and locate DMS users.

ACRONYMS

AFIN	Air Force Information Network
ANS	Advanced Network Systems
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ARPANET	Advanced Research Project Agency Network
ASCII	American Standard Code for Information Interchange
AS	Autonomous System
ASN	Autonomous System Number
ASSIST	Automated System Security Incident Support Team
ATM	Asynchronous Transfer Mode
AUTODIN	Automatic Digital Network
AUTOVON	Automated Voice Network
BBN	Bolt, Beranek, and Newman
BGP	Border Gateway Protocol
BC2A	Bosnia Command and Control Augmentation
BMTA	Backbone Message Transfer Agent
BSC	Binary Synchronous Communications
BWM	Bandwidth Manager
C3	Communications, Command, and Control
CAW	Certified Authority Workstation
CBR	Constant Bit Rate
CCITT	Consultative Committee for Int'l Telegraphy and Telephony
CERT	Computer Emergency Response Team
CIDR	Classless Inter-Domain Routing
COMSEC	Communications Security
CONUS	Continental United States
COS	Corporation for Open Systems
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSU	Channel Service Unit
DARPA	Defense Advanced Research Projects Agency
DBMS	Data Base Management System
DCA	Defense Communications Agency
DCE	Data Communications Equipment
DCS	Defense Communications Systems
DCTN	Defense Commercial Telecommunications Network
DDN	Defense Data Network
DEC	Digital Equipment Corporation
DES	Data Encryption Standard
DIA	Defense Intelligence Agency
DIIS	DISA Installation and Information Services
DISA	Defense Information Systems Agency
DISN	Defense Information Services Network
DISNET	Defense Integrated Secure Network
DoD	Department of Defense
DMS	Defense Messaging System

ACRONYMS

DMZ	Demilitarized Zone (secure network outside a firewall)
DNS	Domain Name Service
DSA	Directory System Agent
DSCS	Defense Satellite Communications System
DSI	Defense Simulation Internet
DSN	Defense Switched Network
DSNET1	former DISNET
DSNET2	former WINCS
DSNET3	former SCINET
DSU	Data Service Unit
DTE	Data Terminal Equipment
DTIC	Defense Technical Information Center
DUA	Directory User Agent
E3	End-to-End Encryption
EBCDIC	Extended Binary Coded Decimal Interchange Code
ECMA	European Computer Manufacturers Association
EDP	Electronic Data Processing
EGP	Exterior Gateway Protocol
EIA	Electronics Industry Association
EIGRP	Enhanced Interior Gateway Routing Protocol
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
FDM	Frequency Division Multiplexing
FEP	Front End Processor
FORTEZZA	NSA encryption and security standard
FTAM	File Transfer, Access, and Management Protocol
FTP	File Transfer Protocol
FY	Fiscal Year
GCC	Global Control Center
GCCS	Global Command and Control System
GFE	Government Furnished Equipment
HDLC	High-Level Data Link Control
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IDNX	Integrated Data Network Exchange
IDUA	Integrated Directory User Agent
IEEE	Institute of Electrical and Electronics Engineers
IGRP	Interior Gateway Routing Protocol
IMTA	Intermediate Message Transfer Agent
INMS	Integrated Network Management System
IP	Internet Protocol
IPX	Internet Packet Exchange Protocol
IRC	International Record Carrier
ISDN	Integrated Services Digital Network
ISO	International Standards Organization

ACRONYMS

ISP	Internet Service Provider
IT&A	Installation, Test, and Acceptance
ITU	International Telegraph Union
IXC	Inter-Exchange Carrier
JCS	Joint Chiefs of Staff
JIS	Joint Interconnection Service
JWICS	Joint Worldwide Intelligence Communications System
JPO	Joint Program Office
KG	An item of cryptographic equipment
LAN	Local Area Network
LANE	LAN Emulation
LATA	Local Access and Transport Area
LES	Leading Edge Services
LCC	Local Control Center
LMTA	Local Message Transfer Agent
LU	Logical Unit
MAC	Media Access Control
MAN	Metropolitan Area Network
MC	Monitoring Center
MFI	Multi-Function Interpreter
MHS	Message Handling System
MILNET	Military Network (DDN)
MILSATCOM	Military Satellite Communications
MINET	Movement Information Network
MLA	Mail List Agent
ML	Mail List
MLS	Multi-level Security
MODEM	Modulator-Demodulator
MPOA	Multi-protocol over ATM
MRC	Monthly Recurring Charge
MS	Message Store
MTA	Message Transfer Agent
MWS	Management Workstation
NAP	Network Access Point
NAU	Network Addressable Unit
NCC	Network Control Center
NCD	Network Change Directive
NCO	Network Change Order
NES	Network Encryption System
NIC	Network Information Center
NIPRNET	Unclassified but Sensitive IP Router Network
NIST	National Institute for Standards and Technology
NMC	Network Monitoring Center
NOS	Network Operating System
NSA	National Security Agency
NSC	Node Site Coordinator

ACRONYMS

NVT	Network Virtual Terminal
OCONUS	Outside the Continental United States
OJCS	Office of the Joint Chiefs of Staff
O&M	Operation and Maintenance
OSI	Open Systems Interconnection
OSD	Office of the Secretary of Defense
PAC	Pacific
PAD	Packet Assembler-Disassembler
PBX	Private Branch Exchange
PC	Personal Computer
PCMCIA	PC Memory Card Industry Association
POC	Point of Contact
POP3	Post Office Protocol, version 3
POTS	Plain Old Telephone Service
PUA	Profiling User Agent
RADB	Routing Arbiter Database
RIP	Routing Information Protocol
RIPE	Registry for European Domain Names
RJE	Remote Job Entry
ROSC	Regional Operations Support Center
SAM	Status Acquisition Message
SCI	Sensitive Compartmented Information
SCINET	Sensitive Compartmented Information Network (now DSNET3)
SDH	Synchronous Digital Hierarchy
SDLC	Synchronous Data Link Control
SDN	Service Delivery Node
SIPRNET	Secret IP Router Network
SMS	Service Management System
SMTA	Subordinate Message Transfer Agent
SMTA/MS	Subordinate Message Transfer Agent/Message Store
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture (IBM)
SONET	Synchronous Optical Network Standard
SPX	Sequenced Packet Exchange Protocol
STEP	Standard Tactical Entry Point
SWA	Southwest Asia
TAC	Terminal Access Controller
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	Time Division Multiple Access
TELNET	Remote Terminal Emulation
TSO	Telecommunications Service Order
TSR	Telecommunications Service Request
TTL	Time To Live
UA	User Agent

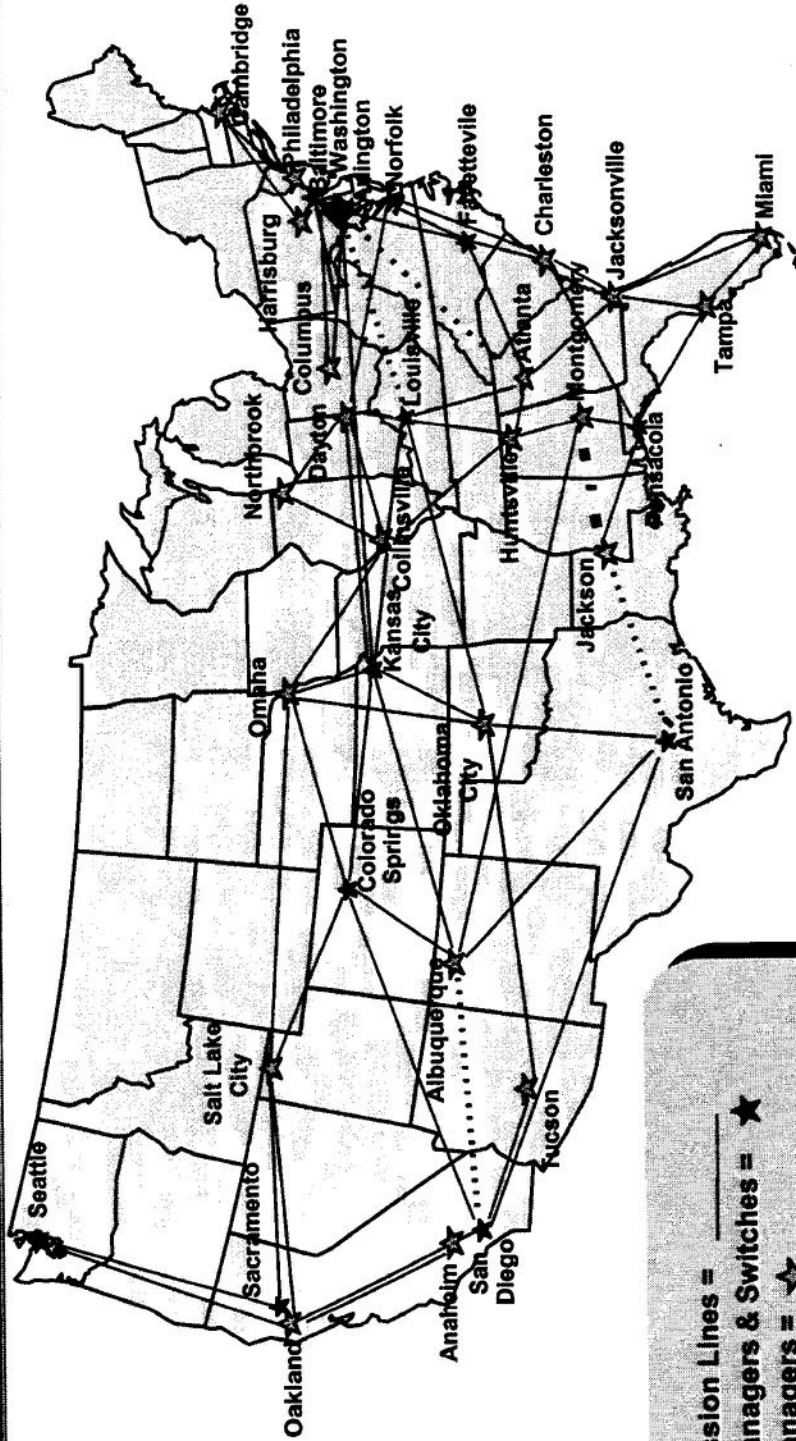
ACRONYMS

UDP	User Diagram Protocol
ULP	Upper Layer Protocol
UTP	Unshielded Twisted Pair wiring
VAN	Value Added Network
VBR	Variable Bit Rate
VC	Virtual Circuit
WAN	Wide Area Network
WINCS	WIN Communications System (became DSNET2)
WWMCCS	World Wide Military Command and Control System
XTACACS	Extended Terminal Access Controller Access Control System
X.25	CCITT packet switching protocol
X.400	CCITT e-mail message protocol
X.500	CCITT directory protocol



DISN CONUS

SONET Backbone



LEGEND:

OC3 Transmission Lines = _____ ★

Bandwidth Managers & Switches = ★

Bandwidth Managers = ★

60 10C-3 Links

9 20C-3 Links

3 30C-3 Links

35 BANDWIDTH MANAGERS

12 w/ Switches

Global Support Services

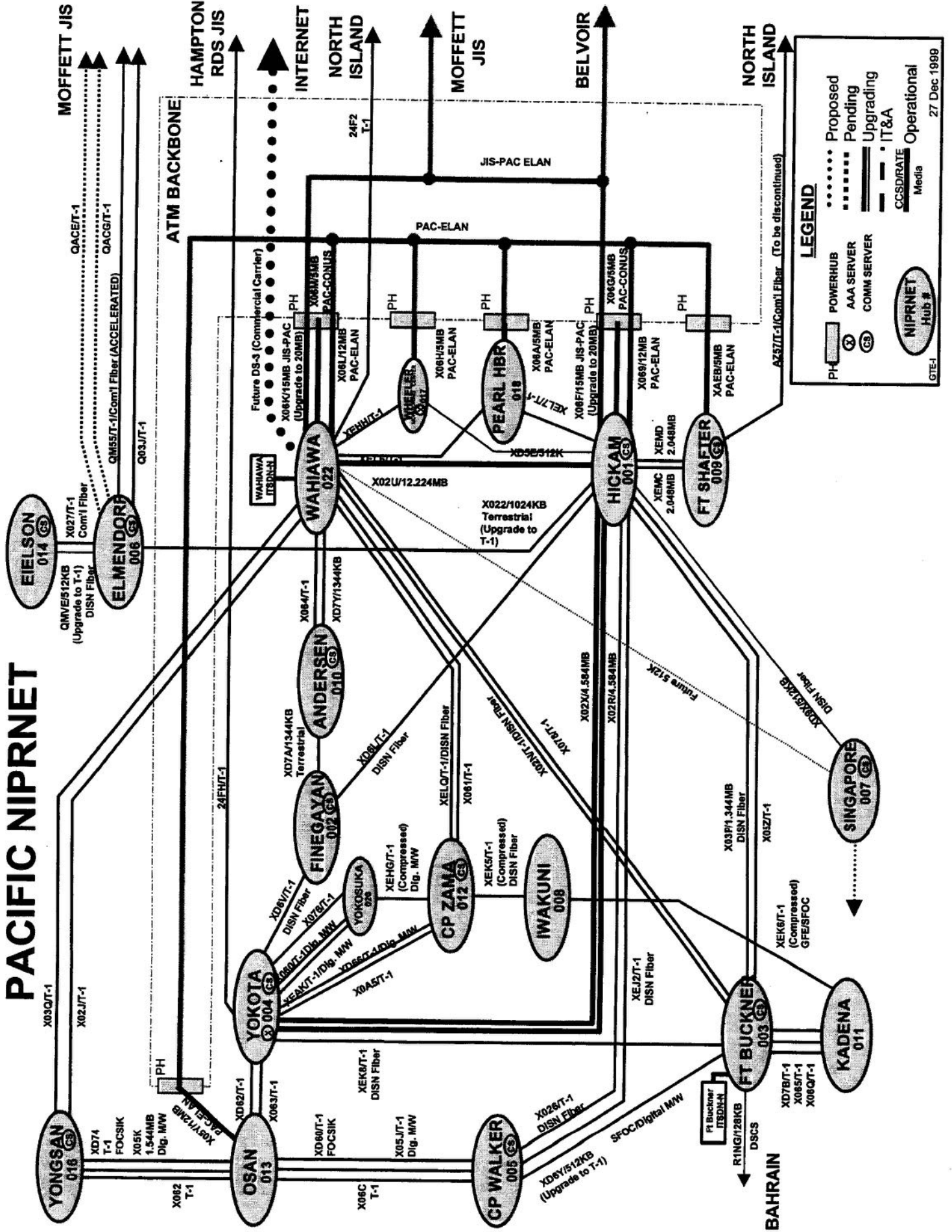
AT&T

MCI

Boeing

- Promotes positive control, information protect
- Takes traffic from open, commercial systems to private, protected DoD system
- Self-healing, restoring (50 ms or less) network

PACIFIC NIPRNET



LEGEND

- Proposed: Dotted line
- Pending: Dashed line
- Upgrading: Solid line with double arrows
- IT&A: Solid line with single arrow
- Operational: Solid line

Media:

- CCSD/RATE: Solid line with 'R' in a box
- Media: Solid line

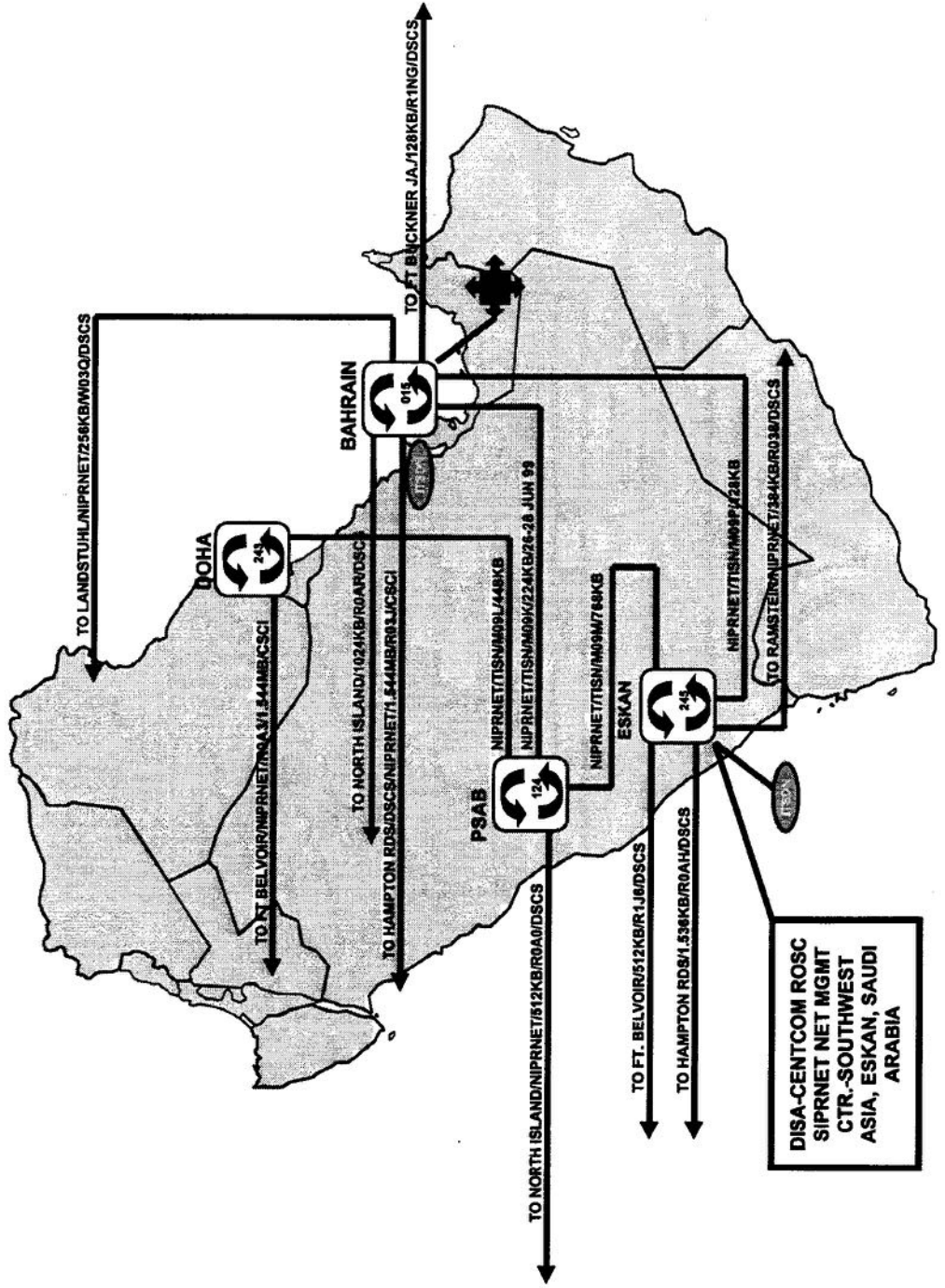
Server Types:

- POWERHUB: PH in a box
- AAA SERVER: A in a circle
- COMM SERVER: CS in a circle
- NIPRNET Hub #: NIPRNET Hub # in a circle

27 Dec 1999



NIPRNet BACKBONE--SWA

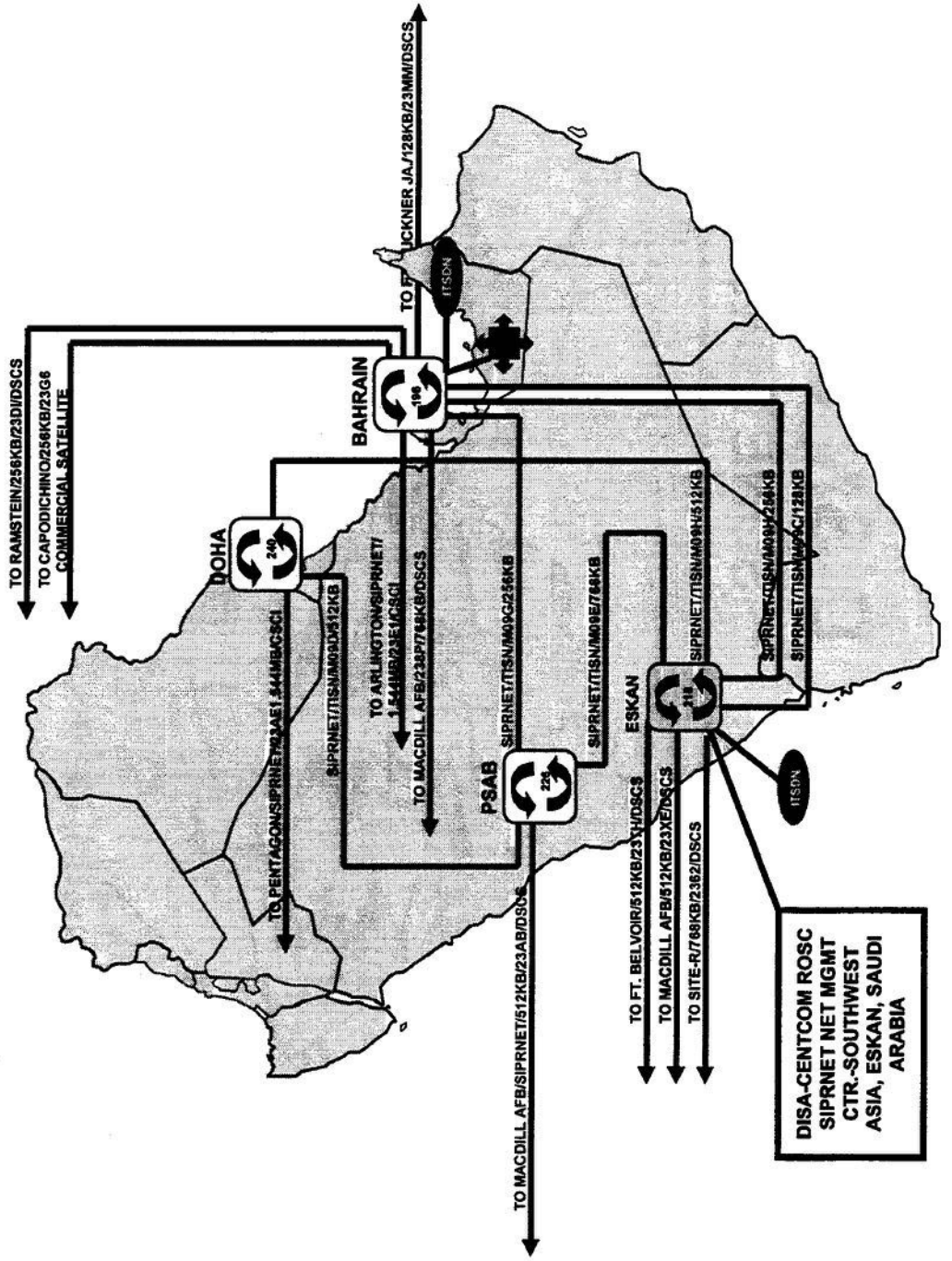


LEGEND 04/27/99

	OPERATIONAL SIPRNET HUB ROUTER (MODE)		PLANNED SIPRNET HUB ROUTER (MODE)		INTER-ROUTER TRUNK (QRYL 1.544MB)		INTER-ROUTER TRUNK GEN ONLY (PLUM)		IT SON/ROUTER		DIAL-UP CONSOLE SERVER		UPS & GEN		UPS ONLY
--	---------------------------------------	--	-----------------------------------	--	-----------------------------------	--	------------------------------------	--	---------------	--	------------------------	--	-----------	--	----------



SIPRNet BACKBONE--SWA



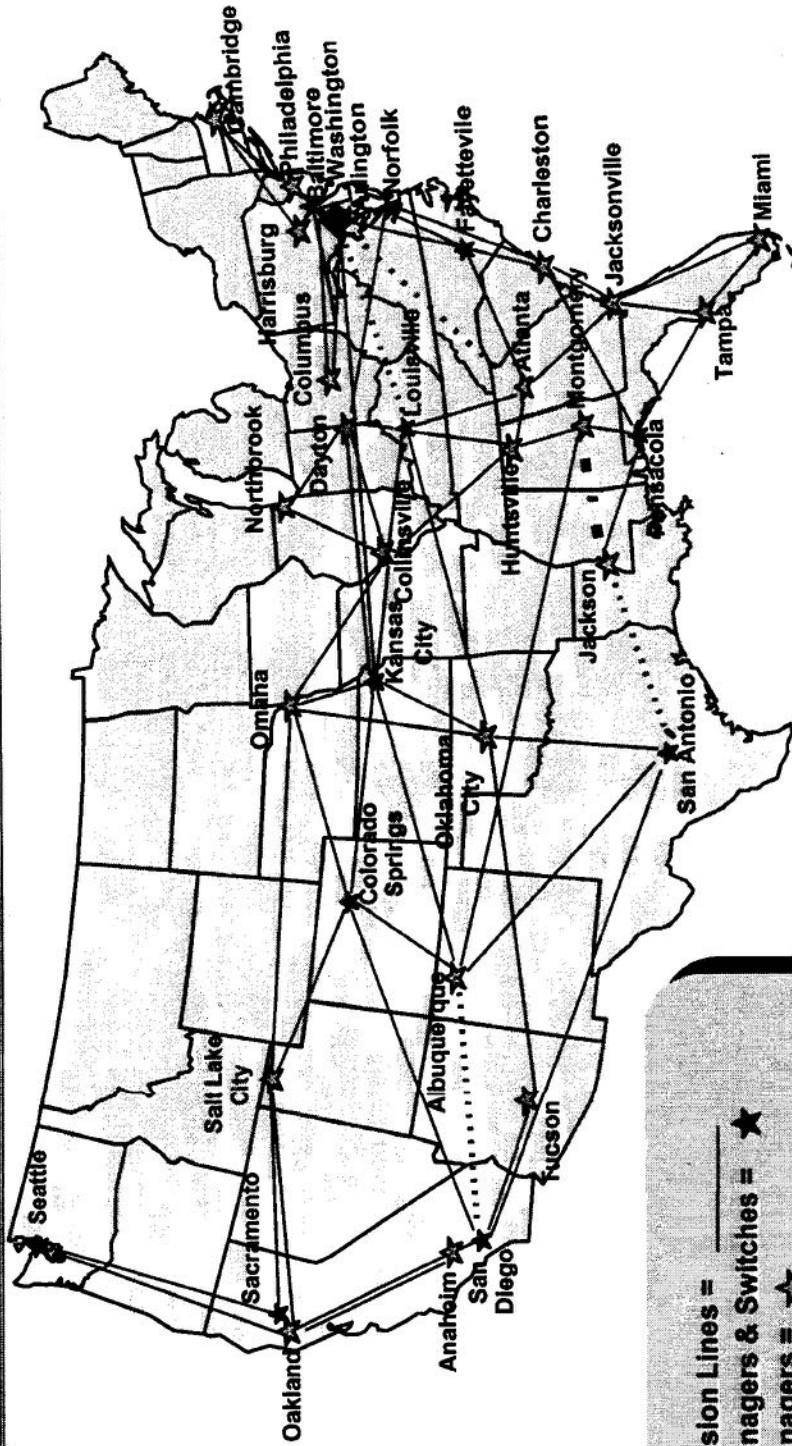
LEGEND 04/27/99

	OPERATIONAL SIPRNET HUB ROUTER (NODE)		UPS & GEN
	PLANNED SIPRNET HUB ROUTER (NODE)		INTER-ROUTER TRUNK
	INTER-ROUTER TRUNK (CON'L. 1.544MB)		INTER-ROUTER TRUNK GEN ONLY (P-LIN'D)
	ITSON ROUTER		DIAL-UP COMM. SERVER
			UPS ONLY



DISN CONUS

SONET Backbone



LEGEND:

- OC3 Transmission Lines = _____
- Bandwidth Managers & Switches = ★
- Bandwidth Managers = ★
- 60 10C-3 Links _____ } AT&T
- 9 20C-3 Links } AT&T
- 3 30C-3 Links } AT&T
- 35 BANDWIDTH MANAGERS } MCI
- 12 w/ Switches } MCI
- Global Support Services = _____ } Boeing

- Promotes positive control, information protect
- Takes traffic from open, commercial systems to private, protected DoD system
- Self-healing, restoring (50 ms or less) network



ATM Europe

CONUS

OC-3 [13DU01/DT4M6ARQ]

Ft. Belvoir

Ft. Belvoir

Pentagon

DS-3 [W0W1]

E-3 [W0W0]

Croughton

DS-3 {CCSD 284Y}

[BC2A/DATMS-C to tunnel through DATMS-U on new OC3]

DS-3 [W0WW]

OC-3 [14DU01/DT4M6ARR]

EUROPE

Heidelberg

Ramstein

OC-3/SDH Ring

Vaihingen

E-3 [W0WP]

Aviano

E-3 [W0WU]

Lago Patria

E3 [W10X]

45Mb use of

155Mb

Navy

Radio Links

Camoldoli

Capodichino

Signonella

OC-3

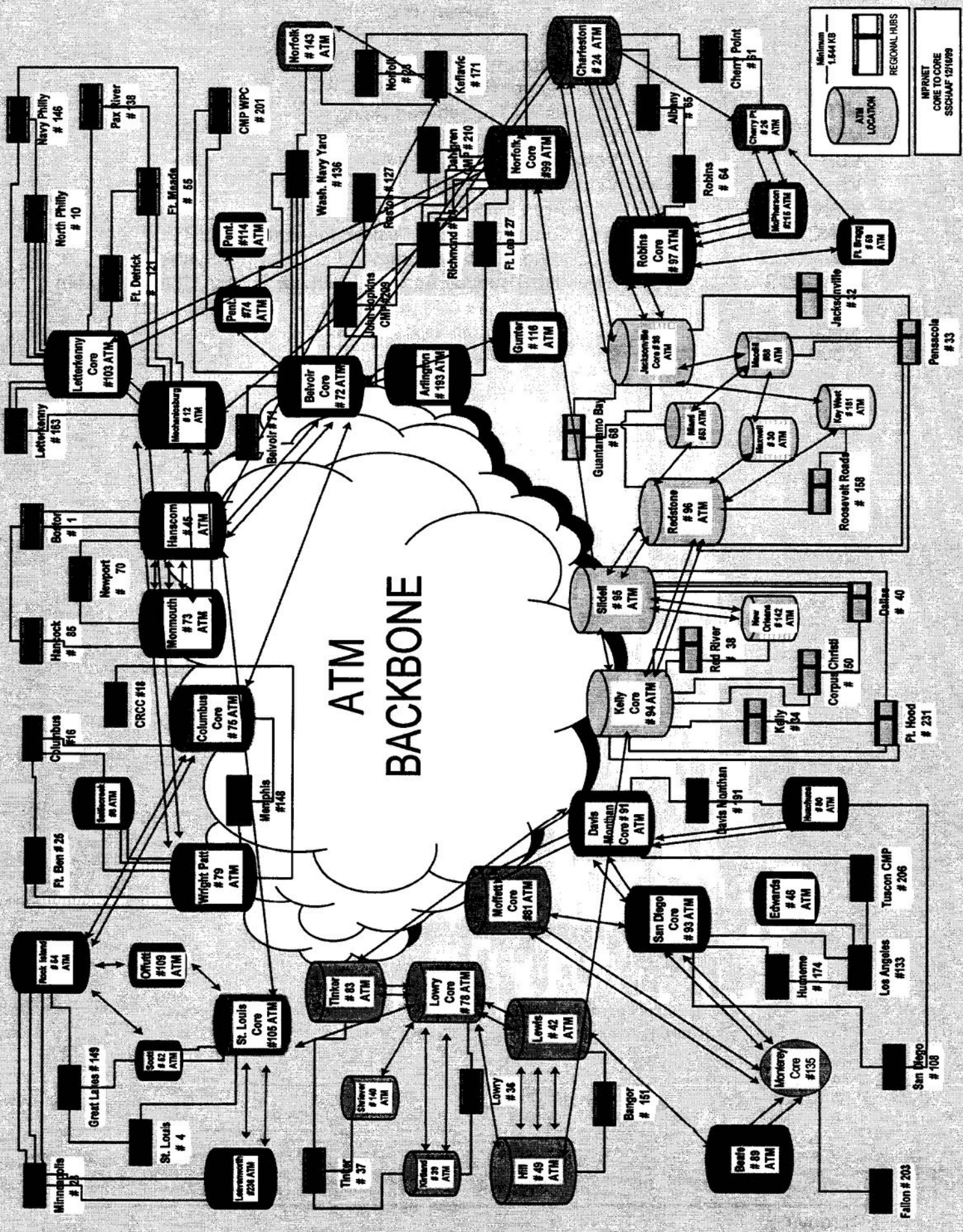
DS-3

E1

Existing

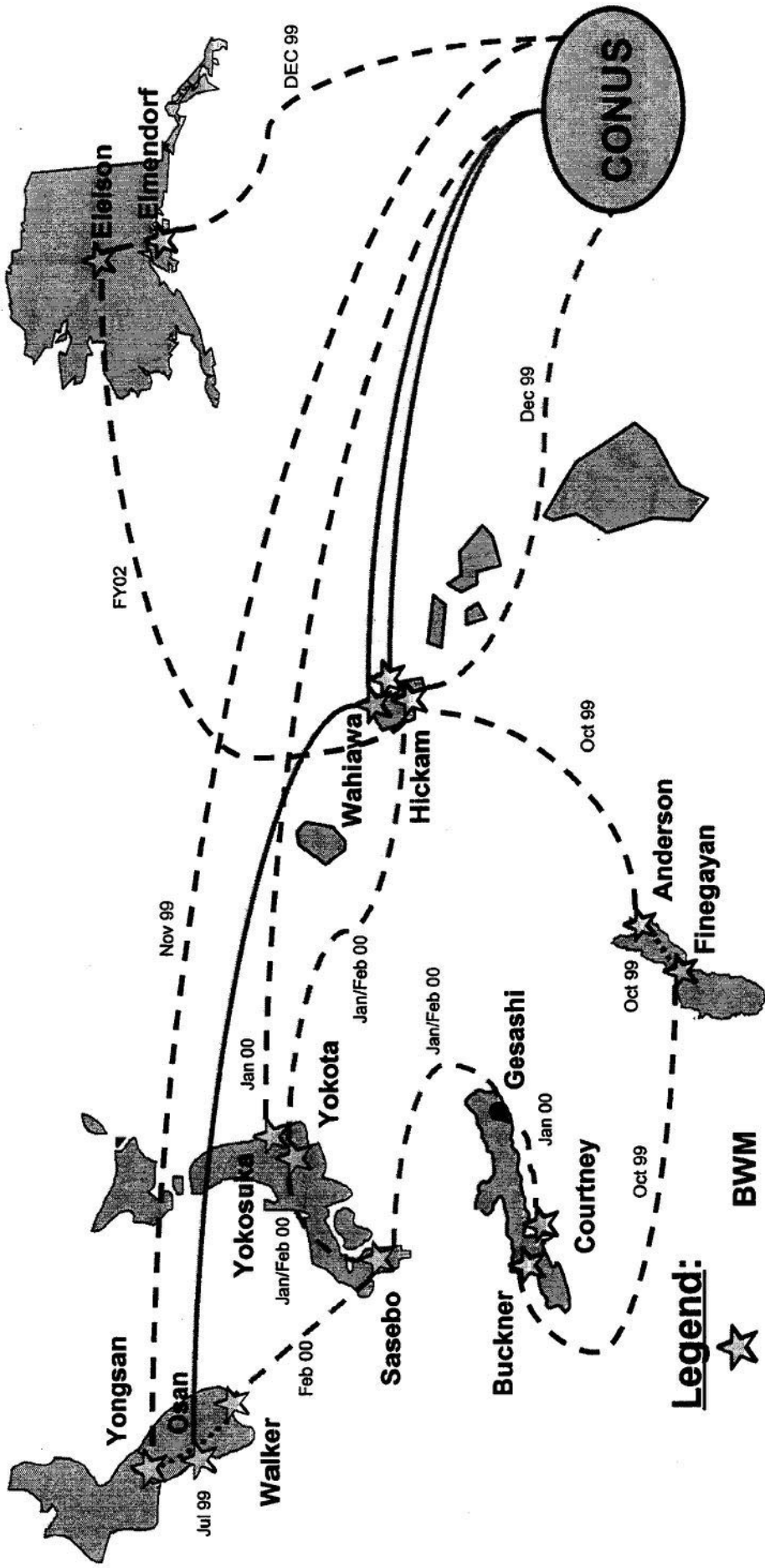
New

ATM BACKBONE





Planned ATM Transmission Connectivity



Legend:



BWM

— Current ATM DS3

- - - Non-ATM DS3 (Transition of Current Service)

- . - . - Planned DISN DS3

JIS NETWORK CONFIGURATION

