NTP 297-3601-906

DMS-10 Family

600-Series Generics

DMS-10 Data Networks

06.01
For Generic 602.20 Standard August 2006

NORTEL

DMS-10 Family

600-Series Generics

DMS-10 Data Networks

Nortel Publications: NTP 297-3601-906
06.01
For Generic 602.20
Standard
August 2006

Publication history

Issue	Date	Rating	For generic
01.01	August 2000	Preliminary	501
01.02	October 2000	Standard	501
02.01	January 2001	Preliminary	502
02.02	April 2001	Preliminary	502.10
02.03	June 2001	Standard	502.10
03.01	July 2002	Preliminary	503.10
03.02	August 2002	Standard	503.10
03.03	July 2004	Preliminary	505.10
03.03	August 2004	Standard	505.10
04.01	July 2005	Preliminary	601.10
04.01	August 2005	Standard	601.10
05.01	February 2006	Preliminary	602.10
05.01	March 2006	Standard	602.10
06.01	July 2006	Preliminary	602.20
06.01	August 2006	Standard	602.20

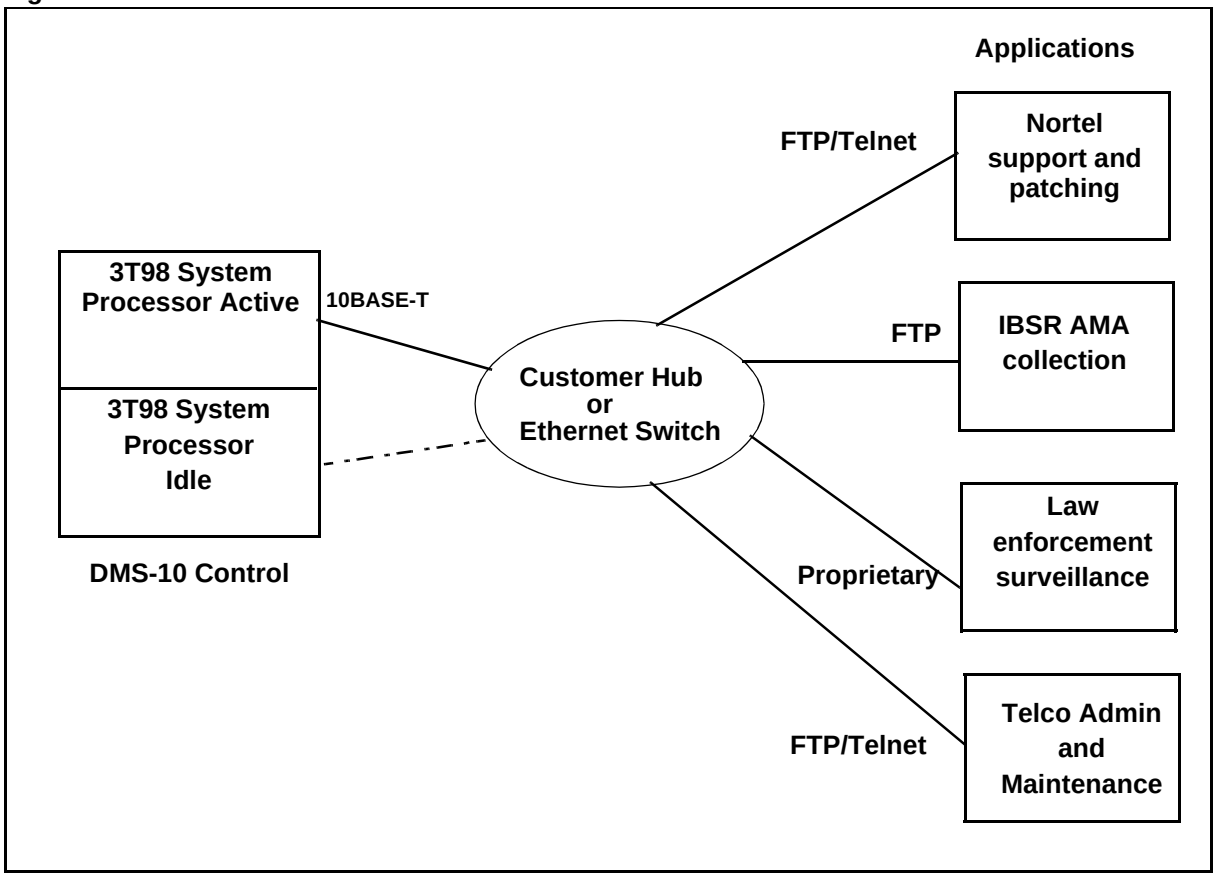
Contents

Section 1: DMS-10 Data Network

Data network architecture

The 500 Series DMS-10 introduced a Central Office (CO) Local Area Network (LAN) to support applications such as Telnet, IBSR AMA collection, CALEA and patch delivery. Collectively this group of applications is known as the Operation, Administration, Maintenance and Provisioning (OAM&P) LAN and it accesses the DMS-10 via 10 Base-T Ethernet ports on the NT3T98 System Processor. See Figure 1-1.

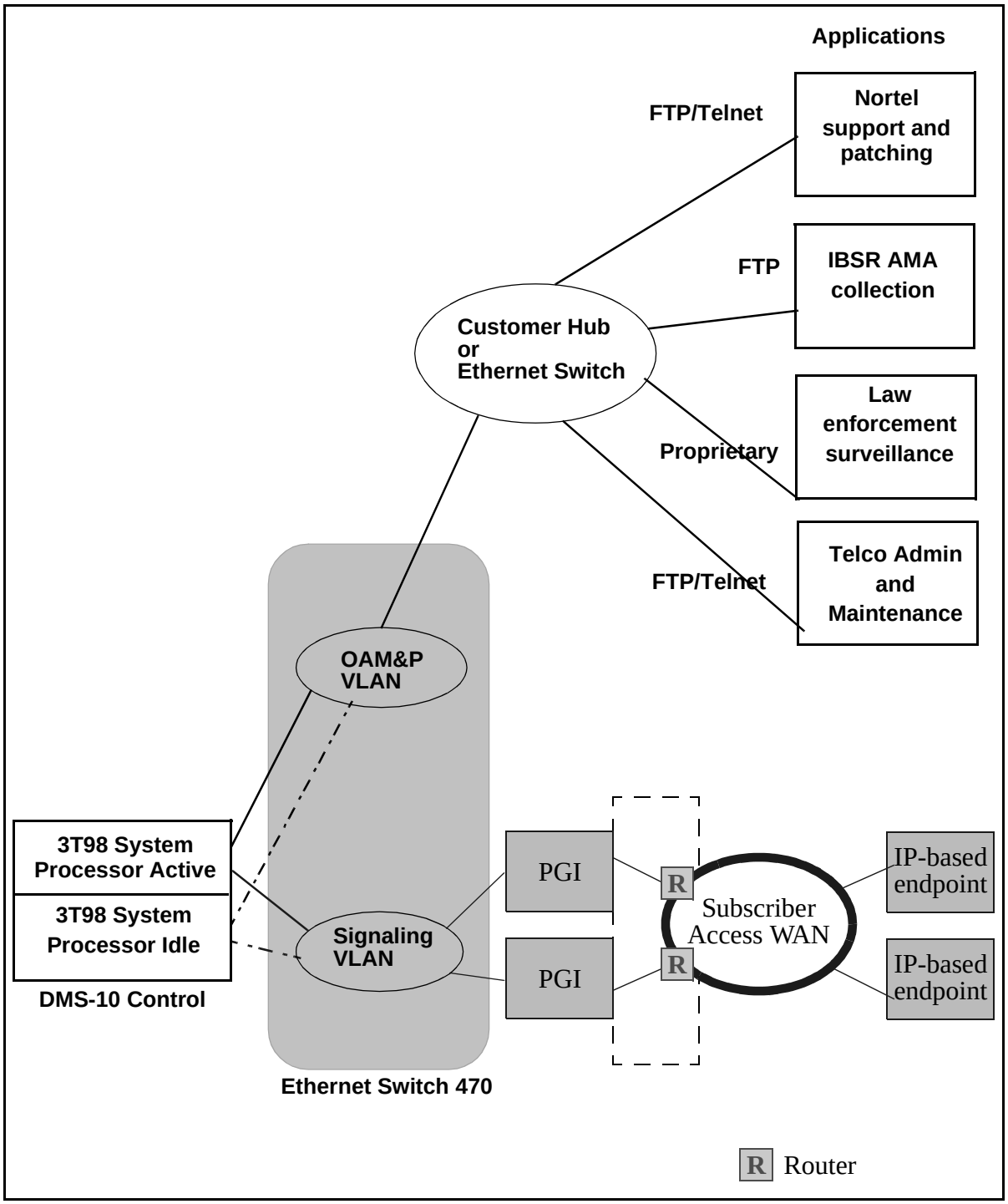
Figure 1-1: DMS-10 OAM&P Data Network



The 600 Series DMS-10 offers Voice over Internet Protocol (VoIP) capabilities that will enable the DMS-10 to support IP-based endpoint devices over a packet network. The VoIP capabilities require the introduction of a more complex CO LAN that is comprised of a Virtual LAN (VLAN) for the OAM&P function and a VLAN for the siganlling associated with the VoIP calls. See Figure 1-2. The Signalling VLAN will pass IP packets from Packet Gateway Interface (PGI) to the NT3T98 System Processor which will provide call control.

Characteristics of the OAM&P VLAN and the signalling VLAN will be discussed below. The characteristics of the OAM&P LAN are same whether it is a connected directly to the DMS-10 CPU or it is a OAM&P VLAN that is a partition on the Ethernet Switch used in VoIP applications.

Figure 1-2: DMS-10 VoIP Data Network



Ethernet Switch 470

In the DMS-10 packet network architecture, two Ethernet Switch 470 models will be used to implement the CO LAN. The dual Ethernet Switch configuration provides high speed (10/100 Mbps Ethernet) connectivity and power redundancy. The Ethernet Switch 470 provides 24 10/100 Base-T RJ-45 ports.

Packet Gateway Interface (PGI)

The PGI provides the circuit-to-packet interface between the DMS-10 Network Equipment and IP-based endpoint devices by converting G.711 Pulse Code Modulation (PCM) bearer packets used by the IP-based endpoint devices to TDM samples used by the DMS-10 Network Equipment.

Each PGI:

- Accommodates two (2) separate PGI controller (PGIC) packs for reliability
- Physical interface:
  - — RJ-45 100 base T-X full duplex
  - — 2 fixed MAC addresses per RJ-45
- Provides six (6) 10-BaseT/100-BaseT ethernet interfaces:
  - — Four (4) ports used for internal card control (one active and one standby per PGI controller pack).
  - — Four (4) ports used for external access (messaging and bearer for each PGIC).
  - — One (1) IP address per PGI for SIP signaling and two (2) bearer IP addresses per PGI for Real Time Protocol (RTP). All PGI IP addresses must be on the same subnet.
- provides protocol support for:
  - — VoIP over 10-BaseT/100-BaseT ethernet
  - — call control message filtering and forwarding
  - — G.711 bearer channel encoding
  - — T.38 fax relay
  - — G.168 echo cancellation

Subscriber Access WAN

The DMS-10 Subscriber access WAN interface is the connection between the PGI and the network edge device. The network edge device must support 100 Base-T Ethernet (full duplex) on the access side of the PGI.

- Visible services:
  - — NAP-T/FW detection and traversal
  - — SIP over User Datagram Protocol (UDP) packet filtering
  - — RTP over UDP packet filtering
  - — Internet Control Message Protocol (ICMP) accepted
  - — Address Resolution Protocol (ARP) accepted

Network performance requirements

Network performance in IP-based packet networks is essential because of IP's connectionless nature. With the introduction of delay-sensitive and packet-loss-sensitive applications, such as telephony, fax, and video services transported over packet networks, today's network planners are focusing on traffic prioritization and QoS strategies as a new, mission-critical priority.

There are three key parameters that define performance in a packet network: latency, jitter and packet loss. For VoIP call control messages (e.g., SIP protocol), packet loss must absolutely be minimized. A lost SIP data packet, for example, can result in a lost call or a "hung" connection. Jitter is not relevant for call control packets. For VoIP bearer packets (RTP protocol), latency and jitter are critical for achieving carrier grade voice.

The following combinations will provide acceptable network performance.

0.5% packet loss	137 msec network delay
0.75% packet loss	127 msec network delay
1.0% packet loss	117 msec network delay
1.5% packet loss	112 msec network delay
2.0% packet loss	102 msec network delay

Security

The PGI acts as a firewall to protect the DMS-10 from attacks from the subscriber WAN by allowing only SIP packets to be passed through to the DMS-10. The DMS-10 IP address should never be exposed to the WAN.

Reliability

The packet network must be configured in a way that prevents any single failure from isolating nodes. Packet networks must be engineered to offer 'carrier-grade' quality with 99.999% availability. Packet networks should be engineered to make delay-sensitive or jitter-sensitive applications successful over an IP-based packet network.

Multi-service requirements

The packet network must be designed to handle different types of network traffic, such as voice, video and data traffic, as well as call control signaling.

Bandwidth

To support flexibility in moving traffic from one network element to another in a packet network, each node must have sufficient bandwidth available to handle all current and planned VoIP traffic. For voice and voice-band services, a 64 kbps bearer payload is required; however, packet overheads increase this figure to approximately 83.2 kbps (assuming 20 ms packet size and G.711 codec) per VoIP call.

OAM&P VLAN

Network performance requirements

In a 500 Series switch, the DMS-10 CO LAN will consist of a hub or Ethernet switch connected to the 3T98 CPU.

In a 600 Series switch with VoIP, the existing DMS-10 CO LAN infrastructure will be relocated off of a port on the new Ethernet Switch. OAM&P traffic is low priority and will have its throughput limited at the ingress port to the Ethernet Switch.

Security

Security is an important consideration in the implementation of the data network. A malicious user on the network could disrupt the operation of the DMS-10 functions and cause an outage or compromise privacy by allowing AMA data or law enforcement surveillance information to fall into the wrong hands. It is imperative that appropriate measures be taken to ensure the security of the data network.

Reliability

Reliability is another consideration in the data network. The data network may be configured for various levels of reliability by engineering redundant elements within the network. Routers and Remote Access Servers can be configured in redundant pairs and there are routing protocols to support redundancy. The data network should be engineered for high availability but the degree of redundancy to incorporate is dependent upon Telco practices and the ability of the Telco to work around periods of downtime. The DMS-10 will continue to operate if the OAM&P VLAN fails and the IBSR application will continue to store AMA files on the local hard drives. Remote maintenance and support are inhibited during periods of data network outage.

Bandwidth

The bandwidth requirement of the data network is determined by the applications that use the network. The application that will place the most consistent demands on bandwidth is IBSR. The IBSR collection is performed by FTP so it is not a real time function. FTP has no inherent bandwidth requirements; it will use the available bandwidth and continue until all data is transferred. A general rule for estimating bandwidth requirements for AMA collection is that every billable call will generate 70 bytes of data transferred across the data network.

Signaling VLAN

The Signaling VLAN is the means of signaling between the System Processor pack (NT3T98) and the PGIs. The Signaling VLAN will provide secure, carrier-grade, fully redundant routing of call processing, signaling, and management messages between the communications server function on the DMS-10 and the IP-based endpoint devices.

Security

The PGI acts as a firewall to protect the DMS-10 from attacks from the subscriber WAN by allowing only SIP packets to be passed through to the DMS-10. The DMS-10 IP address should never be exposed to the WAN.

Reliability

The Signaling VLAN is configured to prevent any single failure from isolating nodes. This configuration includes redundent Ethernet Switches with independent power suplies.

Bandwidth

The Signaling VLAN is used to pass call control messages between the PGI and the NT3T98 System Processor. This requires a 10 Base-T port on each Ethernet Switch.

Data network implementations

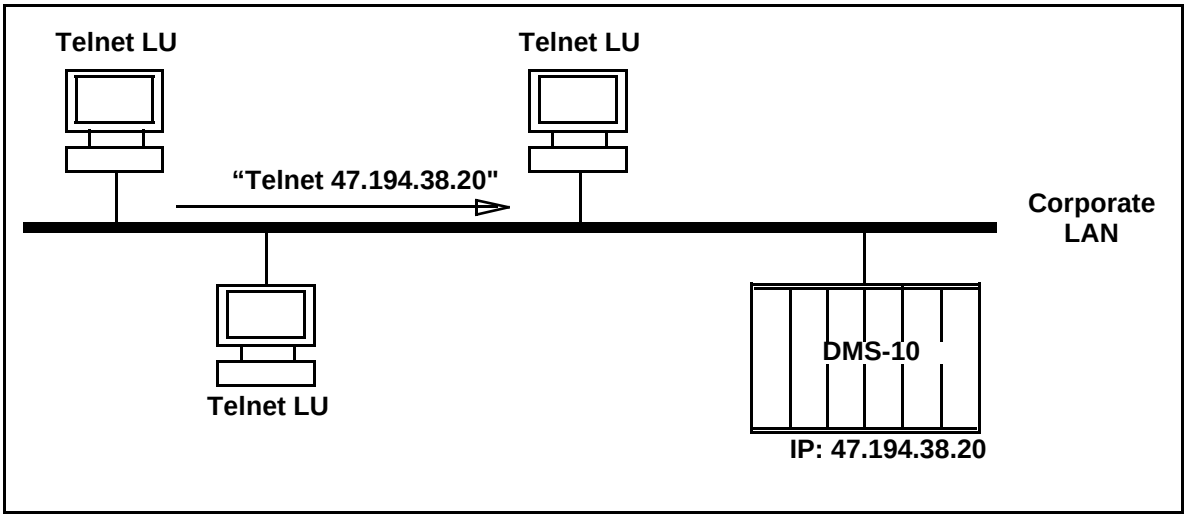
Data networking equipment evolves rapidly so any descriptions of specific implementations will likely become obsolete with time.

Section 2: Network Applications

DMS-10 Telnet interface

The DMS-10 Telnet Interface feature enables operating company personnel to establish a Telnet session with the DMS-10 switch through a 10BASE-T Ethernet port on the NT3T98 System Processor pack, as illustrated in Figure 2-1. In a Telnet session, operating company personnel are able to perform existing Operations, Administration, and Maintenance (OA&M) functions from a remote site just as such functions are performed on a teletype connected directly to the DMS-10 switch. Telnet logical units can be assigned to any of the 32 logical unit ports available on the DMS-10 switch, although the maximum number of serial devices, such as NT3T50 (Data Link Controller) packs or NT3T80 (Dual Serial Data Interface) packs, that can be assigned is reduced by one for each Telnet logical unit assigned.

Figure 2-1: Telnet Logical Unit (LU) Access to the DMS-10 Switch



A Telnet session is established through a DMS-10 Telnet port, using a Telnet client. When the session is established, a command shell is used to start the DMS-10 TTY I/O process and to connect to the desired logical unit. Solicited messages can then be exchanged between the DMS-10 switch and the Telnet client, allowing operating company personnel to enter DMS-10 TTY commands. Unsolicited messages from the DMS-10 switch (that is, messages not associated with any input by operating company personnel) are directed to the logical unit, based on the message class defined for the logical unit by the operating company.

The DMS-10 Telnet Interface feature is composed of two capabilities: Telnet Server and DMS-10 Terminal Server. Telnet Server, using standard RFC854 protocol, enables a remote machine to connect to the host switch. DMS-10 Terminal Server provides the interface between the DMS-10 I/O system logical units configured as Telnet TTYs and the Telnet client, enabling operating company personnel to perform OA& M functions using existing DMS-10 login/logout and man-machine interface routines.

The DMS-10 Telnet feature provides security in two ways: by standard DMS-10 passwords and by the permissions granted via the password command from within an established Telnet session. If more secure access is required, network equipment that can provide the required encryption or user authentication services must be provided by the operating company.

The following conditions pertain to DMS-10 Telnet Interface:

- In the event that a core switchover occurs while Overlay CED is being operated, the Telnet session is maintained through the switchover.
- Since a split system reload (SPLD) includes a warm restart (INIT), Telnet sessions will be dropped when performing a changeover to the maintenance active CPU.
- Up to 10 simultaneous Telnet sessions are permitted.
- The number of Telnet sessions that can be run simultaneously on a single terminal is dependent upon the limitations of the terminal.

Interaction of DMS-10 Telnet Interface with other Features

Cluster

Operating company personnel can access SSOs in a DMS-10 Cluster network through a Telnet session. If, however, a DMS-10 switch is configured as a Host Switching Office (HSO), logical unit number 14 cannot be assigned to a Telnet logical unit. Also, if a DMS-10 switch is configured as a Satellite Switching Office (SSO), logical unit numbers 11 through 14 cannot be assigned to Telnet logical units.

Emergency Input/Output (EIO) Operating company personnel are able to invoke EIO mode on Telnet logical units.

Switching Control Center System (SCCS) SCCS formatted output is available on Telnet logical units.

EADAS EADAS formatted output is available on Telnet logical units.

CALEA (Communications Assistance for Law Enforcement Agencies)

CALEA requires telecommunications equipment manufacturers to provide the technical capability to support lawfully authorized electronic surveillance. From the telecommunications equipment manufacturers' perspective, electronic surveillance refers to the capability to isolate and intercept all wireline, wireless, and electronic communications, to deliver call content and call identifying information to an authorized Law Enforcement Agency (LEA) for a given switch-based subject, and to perform the interception unobtrusively and with minimal interference. Electronic surveillance also refers to the capacity for simultaneous interceptions a switch must be capable of performing during a 24-hour period. The CALEA feature on the DMS-10 switch provides the functionality, capability, and capacity required to ensure compliance with these requirements. For a complete description of the CALEA feature, see Section 10 in NTP 297-3601-105, *Features and Services Description*, entitled, “CALEA.”

DMS-10 FTP application

File Transfer Protocol (FTP) is a well-known method of transferring files across a TCP/IP connection. FTP is fully described in the Internet Engineering Task Force (IETF) document RFC 765. The DMS-10 provides an FTP server application that is based on the BSD UNIX implementation. The DMS-10 FTP server listens to TCP port 21, which is the well-known port for FTP. DMS-10 FTP supports passive and active modes of operation and transfer restarts. Any FTP client that is compatible with RFC 765 may be used for file transfer access to the DMS-10.

There is also an FTP client application that is hosted on the DMS-10 for the IBSR feature. This client mode of operation is not for general usage; the IBSR feature uses the client mode when FTP is configured for the Push mode of transferring AMA files.

Section 3: DMS-10 Operating System Commands

The DMS-10 Telnet Interface feature enables operating company personnel to establish a Telnet session with the DMS-10 operating system, in order to perform OA&M functions for the switch from a Windows PC, HPUX workstation, or Sun workstation.

To initiate a Telnet session, perform the steps in DMS-10 Data Network Procedure 2, in Section 4 of this NTP.

General use commands

The commands shown below can be entered in response to a Telnet command prompt by all users:

dmstty [*tty number*] | ?

Provides access to DMS-10 logical units and displays the connection status and accessibility of all of the configured logical units.

The variable, *tty number* must be configured as a Telnet logical unit through Overlay CNFG (LOGU) on the DMS-10 switch. The user may enter the command, “dmstty ?” to determine which logical unit(s) are available for Telnet use. Note also that a carriage return (<CR>) must be entered after “!!!!”. The login and password are checked against security files to determine access rights and privileges. If the login and password are accepted, the user can access the DMS-10 overlays through the Telnet window as if the commands were being entered at a regular DMS-10 TTY window, although a carriage return must then be entered after each four-character sequence (that is, ****, !!!!, ####, ((((,)))), %%%%).

help

Displays the command syntax for all commands.

password

Adds, modifies, and deletes passwords.

Note: Root-level access has the ability to use the password command on all passwords, while all other users may use the password command only for their individual passwords.

quit

Exits a Telnet session.

Nortel support commands

The commands shown below can be entered in response to a Telnet command prompt only by Nortel support or customer support personnel:

akill <actor-ID>

Kills the specified c_actor on the target system. This command is restricted for use by trusted users.

CAUTION: Any **akill** command that results in killing the telephony user or telephony superuser will result in a switch outage.

aps

Displays a list of all c_actors running on the target system. For each c_actor, the following information is displayed: UID (the uid of the c_actor), AID (the actor_id), NAME (the name (argv[0]) of the c_actor), and DBG (1, if the c_actor is being debugged)

arun [-S | -U] [-k] [-T] [-d] *actor_name*

Actor C_INIT starts *actor_name* running on the target system and reports the actor-id (aid) of the new c_actor, where:

-S specifies that the new c_actor is to be started as a supervisor c_actor.
-U specifies that the new c_actor is to be started as a user c_actor.
-k specifies that the new c_actor's symbol table will be accessible to the kernel debugger.
-T specifies that the new c_actor will be started as a trusted-user c_actor.
-d causes the new c_actor to be created in a stopped state, typically so that a debugger may attach to the c_actor before it starts.

cd

Changes the current directory.

chmod

Changes the permissions associated with a file. (Wildcards, such as an asterisk (*), are not supported.)

chown

Changes the ownership associated with a file. (Wildcards, such as an asterisk (*), are not supported.)

echo
Echoes arguments to the standard output.

env
Displays the current environment.

memstat
Displays information about current memory usage, including total memory size, current free memory, and current locked memory, in bytes.

mount
Mounts the designated file system on the file identified by the indicated path.

> ***Note:*** *This command is restricted for use by Nortel support or customer support users whenever arguments to the command are specified. This command is available to all users when no arguments are specified, in which case only information is displayed.*

ping
Elicits an ICMP ECHO_RESPONSE from the specified host (Internet dot notation address). If the host responds, the ping command indicates that the host is alive on the standard output and then exits. If the host does not respond within 20 seconds, the ping command indicates that no answer has been received from the host.

route [add | delete [net | host] *destination gateway metrics*]
Allows the user to operate directly on the routing table for the specific host or network indicated by *destination*. The *gateway* argument specifies the network gateway to which packets are to be addressed. The *metric* argument indicates the number of "hops" to the destination, and is required for "add" commands. *Metric* must be zero if the destination is on a directly-attached network and non-zero if the route utilizes one or more gateways.

The "add" command instructs the route command to add a route to the destination. The "delete" command instructs the route command to delete a route. Since routes to a host must be distinguished from routes to a network, the optional keywords, "host" and "net," enable the user to specify the appropriate destination. If a destination type is not specified and the destination has a "local address part" of INADDR_ANY, the route is assumed to be to a network; otherwise, the destination is assumed to be a route to a host.

If the route is to a destination connected by a gateway, the *metric* parameter should be greater than 0. If a route with a metric 0 is added, the *gateway* given is the address of this host on the common network, indicating the interface to be used directly for transmission. The destination and gateway parameters are Internet addresses given in the standard dot notation. "Default" is also a valid destination used for all routes when there is no specific host or network route.

When no parameters are entered with the command, the routing tables are displayed. Each route consists of a destination host or network, and a gateway to be used in forwarding packets. The “flags” field shows a collection of information about the route stored as binary choices. The mapping between letters and flags is:

1	RTF_PROTO2	protocol-specific routing flag #1
2	RTF_PROTO1	protocol-specific routing flag #2
B	RTG_BLACKHOLE	only discard packets (during updates)
C	RTF_CLONING	generate new routes on use
D	RTF_DYNAMIC	created dynamically (by redirect)
G	RTF_GATEWAY	destination requires forwarding by intermediary
H	RTF_HOST	host entry (net otherwise)
L	RTF_LLINFO	valid protocol to link address translation
M	RTF_MODIFIED	modified dynamically (by redirect)
R	RTF_REJECT	host or net unreachable
S	RTF_STATIC	manually added
U	RTF_UP	route usable
X	RTF_XRESOLVE	external daemon translates proto to link address

Direct routes are created for each interface attached to the local host; the gateway field for such entries shows the address of the outgoing interface. The REFCNT field shows the current number of active uses of the route. Connection-oriented protocols normally retain a single route for the duration of a connection while connectionless protocols obtain a route while sending to the same destination. The USE field provides a count of the number of packets sent using that route. The interface entry indicates the network interface utilized for that route.

> ***Note:*** *This command is restricted for use by Nortel support or customer support users whenever arguments to the command are specified. This command is available to all users when no arguments are specified, in which case only information is displayed.*

setenv

Sets the environment.

source

Reads commands from the *file-name* and executes them. (This command may not be nested.) An ampersand (&) character must be added at the end of an arun command if the actor doesn't terminate (daemon actors).

traceroute

Print the route used for packet transmission to the network host.

umount

Unmounts the designated file system contained on the block special device identified by name.

Section 4: DMS-10 Data Network Procedures

The DMS-10 Data Network Procedures are used for setting up the appropriate interface to support the administration of the DMS-10 Data Network applications described in Section 1 of this NTP. These procedures include:

- DMS-10 Data Network Procedure 1 - Initiate an FTP session
- DMS-10 Data Network Procedure 2 - Initiate a Telnet session
- DMS-10 Data Network Procedure 3 - Set up connection to a switching application TTY port through DMS-10 Telnet Interface
- DMS-10 Data Network Procedure 4 - Add a DMS-10 Telnet Interface user account
- DMS-10 Data Network Procedure 5 - Modify a DMS-10 Telnet Interface user account
- DMS-10 Data Network Procedure 6 - Delete a DMS-10 Telnet Interface user account
- DMS-10 Data Network Procedure 7 - Change a DMS-10 Telnet Interface user password

DMS-10 Data Network Procedure 1
Initiate an FTP session

To initiate an FTP session from a PC or workstation FTP client:

1) Enter: ftp *<ip address of the DMS-10 switch>*

The following response displays:

Connected to *<ip address of the DMS-10 switch>*
Name *<ip address of the DMS-10 switch>:<username>*

2) Enter the user name.

The following response displays:

331 - Password required for *<username>*
331 Login ok
Password:

3) Enter the password.

The following response displays:

230 - Logging in with home=/
230 User root logged in from *<IP address of the client>*
Remote system type is DMS-10.
ftp>

Note: *This session is based upon a specific instance of a UNIX FTP client. FTP clients vary in their user interface.*

DMS-10 Data Network Procedure 2
Initiate a Telnet session

To initiate a Telnet session from a PC or workstation Telnet client:

1) At a command prompt, enter: telnet *<ip address of the selected DMS-10 switch>* In response, a new input window opens and a command prompt displays.

2) At the command prompt, enter a user ID (see DMS-10 Data Network Procedure 4).

3) At the password prompt, enter a valid password.

Note: *This session is based upon a specific instance of a UNIX Telnet client. Telnet clients vary in their user interface.*

DMS-10 Data Network Procedure 3
Set up connection to a switching application TTY port through DMS-10 Telnet interface

1) Establish a telnet session by performing DMS-10 Data Network Procedure 2.
2) To determine accessibility of the TTY port, at the command prompt enter: dmstty ? <CR>
3) To select the TTY port, at the command prompt enter: dmstty <*tty number*> <CR>
4) Log in to the DMS-10 switch.

DMS-10 Data Network Procedure 4
Add a DMS-10 Telnet Interface user account

1) Establish a telnet session by performing DMS-10 Data Network Procedure 2.
2) Log in as Root.
3) To launch the password utility, at the shell "$" prompt enter: password
4) At the "Choice:" prompt, select "A" from the menu.
5) At the "Enter username:" prompt, enter the new username. (The username must contain at least two alphanumeric characters.)
6) At the "Trusted user?" prompt, enter the appropriate response, either Y or N.
7) At the "Enter user id:" prompt, enter the new user ID. (Valid numbers are between 0 and 32767.)
8) At the "Enter group id:" prompt, enter the new group ID. (Valid numbers are between 0 and 32767.)
9) At the "Enter additional group ids:" prompt, enter either additional group IDs, or leave blank. (If additional IDs are entered, separate the IDs (valid numbers are between 0 and 32767), one from another, with commas (,).
10) At the "Enter remote hosts list:" prompt, press Enter.
11) At the "Enter password:" prompt, enter the new password. Valid passwords consist of at least four alphanumeric characters.
12) At the "Repeat password:" prompt, enter the password entered in the previous step.

DMS-10 Data Network Procedure 5
Modify a DMS-10 Telnet Interface user account

1) Establish a telnet session by performing DMS-10 Data Network Procedure 2.
2) Log in as Root.
3) To launch the password utility, at the shell "$" prompt, enter: password.
4) At the “Choice:” prompt, select “M” from the menu.
5) At the “Choice:” prompt, enter the number associated with the user whose account is to be changed.
6) At the “Choice:” prompt, enter the number associated with the item to be changed.
7) Make the appropriate changes by using “Add” commands described in Data Network Procedure 4.
8) At the “Enter group id:” prompt, enter the new group ID. (Valid numbers are between 0 and 32767.)
9) To save the changes that have been made, at the “Choice:” prompt select “S” from the menu.

DMS-10 Data Network Procedure 6
Modify a DMS-10 Telnet Interface user account

1) Establish a telnet session by performing DMS-10 Data Network Procedure 2.
2) Log in as Root.
3) To launch the password utility, at the shell "$" prompt, enter: password.
4) At the “Choice:” prompt, select “D” from the menu.
5) At the “Choice:” prompt, enter the number associated with the user whose account is to be deleted.
6) To save the changes that have been made, at the “Choice:” prompt select “S” from the menu.

DMS-10 Data Network Procedure 6
Modify a DMS-10 Telnet Interface user account

1) Establish a telnet session by performing DMS-10 Data Network Procedure 2.
2) Log in as Root.
3) To launch the password utility, at the shell "$" prompt, enter: password.
4) At the “Choice:” prompt, select “P” from the menu.
5) At the “Choice:” prompt, enter the number associated with the user whose password is to be changed.
6) At the “Enter password:” prompt, enter the new password. Valid passwords consist of at least four alphanumeric characters.
7) At the “Repeat password:” prompt, enter the password entered in the previous step.

Section 5: Index

D

DMS-10 Family

600-Series Generics

DMS-10 Data Networks

NTP number: NTP 297-3601-906
Release: 06.01
For Generic 602.20
Status: Standard
Date: August 2006