5. OPERATIONS, ADMINISTRATION, MAINTENANCE AND PROVISIONING (OAM&P)

Commands and Messages

5.1 The 1603 SM responds to commands entered by a user/Operating Systems (OS) by generating messages to acknowledge command input or an event. The 1603 SM supports a variety of local and remote User System Interface (USI) and OS interface options. The system software supports prompt, menu, and command modes that can be used to provision the 1603 SM, retrieve alarms/status, and for other maintenance activities.

5.2 All 1603 SM system commands consist of a command verb, up to two command modifiers, and multiple parameters. The commands and parameters form a command string that complies with the TL1 command protocol. The system commands can be divided into routine administration, no trouble maintenance, and trouble clearing commands. Depending on how the system administrator sets up security, all commands can be treated equally or specific commands can require a certain level of user privilege or command execution priority.

5.3 The 1603 SM receives and/or generates command response messages and autonomous messages. Command response messages are generated in response to a command execution and indicate acceptance. Autonomous messages are generated by alarm conditions, performance monitoring threshold crossings, status changes, error codes, common equipment events, DS1 events, EC1 events, optical carrier events, and provisioning changes.

User Access

5.4 The 1603 SM is designed to interact with ASCII terminals, the PC-based 1301 NMX, or an Operations System (OS). The ASCII terminal and 1301 NMX connect to the 1603 SM through either local USI connections on the front of the shelf or remote USI connections on the rear of the shelf.

Local USI Access

5.5 The primary local USI is a 9-pin D connector on the Craft, Orderwire and Alarm (COA) unit front panel. This USI port supports RS-232 Types D&E. In addition to autobaud, the USI port supports 1200, 2400, 4800, 9600 (default), and 19,200 baud rates.

Remote USI Access

5.6 Depending on the type of COA plug-in units, the 1603 SM rear USI port can be equipped/provisioned as a Telemetry Byte-Oriented Serial (TBOS) interface, a secondary USI port or an X.25 port. Electrical connections to this interface port are hard-wired to wire-wrap pins located on the rear of the 1603 SM shelf. If configured as a secondary USI, this interface port can be provisioned as either an alternate local RS-232 USI or an RS-232 modem interface port. ***NOTE:*** *A MODEM Overview is provided in Appendix E of this manual.*

Remote Logon Access

5.7 The previous paragraphs describe electrical connection ports on the 1603 SM. However, it is possible to gain access to the system without being physically connected by copper wire to the shelf. A user can access a 1603 SM remotely with optic carrier connections. To initiate a remote access session, connect to a local Network Element (NE) and enter the identification code of the remote NE, username, and password. After the password is verified by the remote NE, proceed as if logged on locally. Since logon security is checked on the remote NE only, the user must be authorized to use the remote NE, but not necessarily the local NE. Just as with a local logon session, the remote logon session is terminated by the logoff command.

OS Access

5.8 The 1603 SM supports a variety of Operations, Administration, Maintenance and Provisioning (OAM&P) functions that can be accessed by an Operation Systems (OS) site. These functions include: Telemetry Byte-Oriented Serial (TBOS) Parallel Telemetry Office Alarms, TCP/IP gateway interface, and an X.25 OS gateway interface. Details on these networking features are in the System Engineering section.

Security Management

5.9 The 1603 SM offers different levels of security management that can be provisioned using the 1301 NM APP1603SM. The levels are user security, channel security, and password security:

- User security deals with the access level assigned to specific users. The level of user security affects the type and number of commands an individual user may execute. This ability prevents unqualified user access to high level commands.
- Channel security deals with the access level assigned to specific channels or ports used to connect to the NE. The level of channel security affects the types of operations that may be performed over a particular service channel. Generally, front panel access using the NE Craft, Orderwire and Alarm (COA) plug-in unit is assigned the highest level of security. The 1301 NMX Port Access screen options include: Craft, Remote, Maintenance, Provisioning, Test and Peer.
- Password security is used to modify passwords by the individual user.

5.10 The 1603 SM security ensures that only authorized users have access to the system and its database. However, the level of security provided by this system depends on how thoroughly the security system/scheme is implemented and maintained by the system administrator(s).

5.11 The 1603 SM offers the following security features:

- Verification of the User Identifier (UID), Private Identifier (PID), and Calling Address Identifier (CID) when a user logs on to a Network Element.
- Encrypted internal storage of the PID.

- Temporary lockout of users (by UID) after a provisionable number of unsuccessful logon attempts. Lockout duration time is provisionable.
- Temporary lockout of CIDs after a provisionable number of unsuccessful logon attempts by a remote user. Lockout duration time is provisionable.
- Inactivity time-out for users who remain logged on to an NE, but do not interact with the system for a provisionable duration of time.

NOTE: *Because of the special requirements of Operations System entities, the inactivity time-out function is disabled for maintenance, provisioning and test entities. The inactivity time-out function only applies to USI (craft), remote and peer. This change was introduced in Release 04.00.*

- Limitation on the number of consecutive logon attempts over a period of time to discourage automated intrusion attempts. Attempt limitation is provisionable.
- PID aging to force the user to modify user password routinely. An expired PID requires system administrator intervention to reinstate user. The PID aging is provisionable; use any number less than or equal to 999 days.
- UID aging to disable those who do not use the system for long periods of time. An expired UID requires system administrator intervention to reinstate user. The UID aging is provisionable; use any number less than or equal to 999 days.
- Assigning User, Command and CID privileges to partition specific users to specific commands.
- Generation of audit reports by the system administrator to indicate all logon activity for users over a period of time,
- Displaying an advisory warning message upon system entry to warn unauthorized users.
- Autonomous message generation as events.

Database Management

5.12 The 1603 SM maintains a working database on the NEP plug-in unit and a primary backup database on the COA plug-in unit. The working database resides on volatile memory circuitry, and the primary backup database resides on nonvolatile memory circuitry. Both databases contain the following parameters:

- System security accounts and logs
- System synchronization settings
- Performance threshold settings
- Communications settings
- Alarm reporting attributes
- Provisioning for all plug-in units and external facilities (i.e., optical and electrical interfaces)
- VP/VT/STS1/STS3c cross-connections
- Customer-provisionable defaults

NOTE: *Performance threshold settings are maintained in protected database memory, but actual accumulated performance monitoring data is not. Various plug-in units throughout the system collect performance monitoring data at various time increments. The NEP does the final accumulation on an 8-hour incremental basis. If the NEP is removed or it fails, all accumulated reporting is lost; however, the customer-specified performance threshold settings are retained.*

5.13 When the 1603 SM is shipped from the factory, plug-in units are programmed with bootcode. The system requires an initial download of software designed to support the various plug-in units. This download enables the user to provision the system so it can accept and process traffic, as well as support the various OAM&P functions.

5.14 After the system software load is downloaded, the data is stored in nonvolatile memory on the COA plug-in unit and the NE Processor (NEP) plug-in unit. Software upgrades can be done while the system is in-service. Changes to database information can be provisioned to result in database change notification.

5.15 Certain COA plug-in units have a special memory expansion module that stores the entire system program load in a compressed form for programming a replacement card or for remote download. The units are: COA315, COA316, COA603/604, COA505/605, COA506/606, COA607/608, and COA609/610. Remote download is when a user at a remote NE requests the entire load from a neighbor NE. In this case, the entire system program load is copied across the net from one NE to the other NE using the DCC. The system program can also be downloaded through the LAN.

5.16 Several prvisionable features require a COA unit with expanded storage capability for the user's database. Table K identifies the COA requirement for those features.

Table K. COA Required for Provisioned Options

PROVISIONED OPTION *	WEIGHT	COA REQUIRED
Customer defined defaults/EMG	2	COAxx5, COAxx6, or any COA6xx
ATM routing (any STS1/STS3c in ATM mode)	9	COAxx5, COAxx6, or any COA6xx
LIF901	3	COAxx5, COAxx6, or any COA6xx
LIFB01	26	COA607, COA608, COA609, or COA610
HIFG0x	4	COAxx5, COAxx6, or any COA6xx
** A COA608,COA608, COA609, or COA610 is required if more than one option is provisioned and the sum of the option weights is greater than 14.*		

Remote Inventory

5.17 The 1603 SM system has local and remote inventory capability (Figure 24). Periodically, the NEP requests inventory data from the common equipment units and the drop modules that are installed in the system. The DMI plug-in units, in turn, request and accumulate inventory information from the VTG plug-in units. Each unit has an EEPROM that contains the hardware inventory data. Another address within the software load is used to describe the software version. All the system inventory data is stored in an NEP database. When the OS or craft person (by way of user system interface) issues the remote inventory request, the NEP transmits the current information in the database.

Figure 24. Remote Inventory Subsystem

Provisioning

5.18 The 1603 SM plug-in units have certain operational characteristic parameters that can be modified, depending on specific requirements of the application and system configuration. Provisioning refers to the act or process of defining the operational characteristic states and/or conditions for equipment, facilities, and data paths. All 1603 SM provisioning is software-controlled and implemented by entering commands using the User System Interface (USI). The individual command syntax contains the applicable parameter fields and option state fields that the user can specify.

5.19 The 1603 SM supports four types of provisioning services: defaults provisioning, start-up provisioning, on-request provisioning, and background provisioning (refer to Table L).

Table L. 1603 SM Provisioning Services

PROVISIONING TYPE*	DESCRIPTION
Defaults Provisioning	Applied in place of either the customer's provisioning or factory defaults to return the system to a known state (usually when the equipment and facilities are first provisioned or when a site problem is difficult to troubleshoot)
Start-up Provisioning	Cold start initialization process; it is nondisruptive to service
On-request Provisioning	Changes or updates only one provisionable unit at a time
Background Provisioning	Low priority process for provisioning refresh or reprovisioning in a sequential manner

** Regardless of the type used, all four are applied to all equipment and facilities.*

5.20 Depending on the plug-in unit, the provisioning data is stored in either the nonvolatile or volatile memories. The Network Element Processor (NEP) plug-in unit stores the working provisioning data in on-board (volatile) database circuitry. The Craft, Orderwire and Alarm (COA) plug-in unit stores the backup provisioning data in on-board (nonvolatile) database circuitry.

5.21 Alcatel SONET products are designed to be flexible and permit both local and remote provisioning of system options. Provisioning of individual NEs addresses turn-up considerations for common equipment, OAM&P functions, and traffic-carrying (external) interfaces. Appendix B contains tables summarizing the types of parameters that can be provisioned using the system TL1 commands.

Maintenance Functions

5.22 In this context, maintenance refers to features, functions, facilities, and procedures routinely used to ensure the system operates properly. Maintenance also addresses trouble detection/sectionalization and trouble or repair verification. Trouble detection/sectionalization deals with identifying a failure to one of the terminating network elements or the facility that connects them. Trouble or repair verification is the process of verifying the continued existence or nonexistence of a problem before beginning or closing out work on that problem. The following paragraphs describe 1603 SM features designed to simplify and optimize maintenance functions.

Plug-in Unit Status Indicators

5.23 Each of the 1603 SM plug-in units is equipped with status and alarm LED indicators, except the VSCC20x units. The HIF, VSCC, NEP, DMI, LIF(except LIF901), and LDR plug-in units also have an active (ACT) LED indicator. The HIF, LDR, and VTG plug-in units have signal

failure (SF) LED indicators, as does the LIF40x and LIF901. The NEP plug-in unit has an abnormal (ABN) LED indicator, and the COA plug-in unit has an alarm cutoff (ACO) LED indicator. The COA also has far-end alarm reporting LED indicators (see *Far-End Alarm Reporting* for details).
NOTE: *The VSCC20x fixed-path cross-connect plug-in units are passive (no active circuitry) and, as such, do not have LED indicators.*

Performance Monitoring

5.24 The 1603 SM offers various performance monitoring functions that monitor all incoming (traffic) signals, detect and count errors, and report any counts that exceed system defaults or customer-specified thresholds. Performance monitoring data can be used to analyze the impact and severity of intermittent or recurring conditions. The following functions are supported on all facilities and equipment installed and provisioned:

- Periodic performance monitoring reports
- Collecting and storing performance monitoring data
- Initializing performance monitoring registers
- Reporting performance monitoring data upon request
- Inhibiting performance monitoring during failure conditions
- Establishing thresholds, detecting and signaling events where the threshold is achieved or exceeded

5.25 Introduction of the DMI301 and VTG301 plug-in units provides enhancements to the DS1 path performance monitoring. SF and ESF mode support has been added, in addition to existing DS1 line performance monitoring. In ESF mode, monitoring of the Facility Data Link (FDL), in particular the Performance Report Message (PRM) for far-end PM information, is provided. In addition, both directions (receive from facility and from network) are monitored. Other enhancements include the DS1 Idle capability and loopback diagnostic commands. Error records are listed in 15-minute intervals, and totals can be compiled in intervals of 15 minutes, past 8-hour period, current day, and previous day.
NOTE: *To use enhanced performance monitoring, the Drop Module Interface slots on the 1603 SM shelf must be equipped with DMI301 plug-in units. Any DS1 ports in the drop group requiring enhanced performance monitoring must be equipped with the VTG301. However, the remainder of the drop group's VTG slots can be VTG10x plug-in units, provided the protection slot is equipped with a VTG301 unit.*

Embedded Operations Channel (EOC) Functions

5.26 The SONET optical carrier allocates a portion of its bandwidth for overhead information used for maintenance, control and test functions. Within this overhead are the Data Communications Channels (DCC) that provide Embedded Operations Channel functions, such as:

- Centralized Autonomous Message Reporting (CAMR)
- Concentrated Telemetry Byte-Oriented Serial (TBOS)
- Remote Logon
- Customer-Defined Alarms and Controls (CDAC)
- Far-End Alarm Reporting

Network Management Channel (for R03.00.02 only)

5.27 The 1603 SM supports network level features, such as remote craft logon, concentrated TBOS, CAMR, and CDAC. Communication between sites is carried through the SONET D1-D3 Data Communications Channel (DCC). The routing for the SONET subnetwork is controlled by routing tables provisioned into each 1603 SM (later releases provided IS-IS routing). Each 1603 SM reads the packet address and either processes or relays the packets. To control the routing of the network manager channel, each 1603 SM must be provisioned with data link routing tables (referred to as DLMAP).

ES-IS/IS-IS Routing (for R03.01 and Later)

5.28 R03.01 and later releases of the 1603 SM support routing protocols developed by the International Organization of Standardization (ISO), such as the End System to Intermediate System (ES-IS) and Intermediate System to Intermediate System (IS-IS). An intermediate system or intermediate NE (INE) has one or more subtending NEs and performs routing for tandem traffic. An INE must support IS-IS level 1 routing and the IS role of the ES-IS protocol. The End System or End NE (ENE) handles only its own traffic. The ENE must have direct access to either a DCC, an LAN, or an X.25 OS/NE interface. An ENE must support the ES role of the ES-IS protocol.
5.29 Figure 25 shows how ES-IS and IS-IS routing work. Site A and Site B are end systems, or ENEs. The routing between these ENEs and Site C is ES. However, Site C is an intermediate system, or INE, with respect to Site D. Therefore, the routing between Sites C and D is IS. Site E is another ENE and the routing between Sites D and E is ES. However, Site F is an INE with respect to Site D and some other remote NE. Therefore, the routing between Sites D and F is IS.
Figure 25. ES-IS and IS-IS Routing

Target Identifier Address Resolution Protocol (TARP) (for R03.01 and Later)

5.30 All Network Management and OAM&P applications on the 1603 SM use the Target Identifier Address Resolution Protocol (TARP). TARP translates the Target Identifier (TID) of a TL1 message by mapping the TID into a Network Service Access Point (NSAP) address of an NE. TARP is used in the following applications:

- When X.25 is used on the OS-to-NE interface, the Gateway NE needs to be able to map TIDs for subtending NEs to NSAP addresses of those subtending NEs.
- When Remote Logon is initiated by entering the TID of remote NE at the local workstation, the local NE needs to be able to map that TID to the NSAP address.
- When interacting with the 1301 NMX.

NOTE: *Other systems in the network must support TARP, or manual provisioning of TADRMAP is required.*

TID Address Resolution Map (TADRMAP) (for R03.01 and Later)

5.31 R03.01 and later releases of the 1603 SM provide the ability to communicate with NEs that do not support the TARP addressing scheme, but do support Target Identifier (TID) addressing. This is done by provisioning the TID Address Resolution Map (TADRMAP). The user can manually specify the NE TID, NE system ID, organization, and routing area address of neighbor NEs to define NSAP addresses.

Centralized Autonomous Message Reporting (CAMR)

5.32 The CAMR feature provides the ability to route autonomous messages to a remote NE (known as the concentrator NE). Autonomous messages are displayed at the concentrator NE similar to the local craft feature, except the source identification in the message header indicates the remote NE. Autonomous messages are alarm messages, threshold crossing events, automatic state change messages, and switchover notification messages.

5.33 There can be any number of concentrator NEs in a network, and any NE in the network can be provisioned as a concentrator NE. However, each NE in the network can only be provisioned to communicate with up to two concentrator NEs. The concentrator NE can be provisioned to receive autonomous messages from up to 32 remote NEs. Although autonomous messages are reported to a concentrator NE, the concentrator NE cannot retrieve the remote NE alarms locally without logging on to the remote NE. The concentrator NE declares a remote alarm when at least one critical, major, or minor alarm is active at a provisioned remote NE, on a per NE basis.

NOTE: *If a network consists of 20 or more NEs, distribute functions (such as CAMR concentrator and X.25 gateway NE) to individual NEs in the network so no one NE has more than one function. This avoids overloading the memory capability of an NE. However, if the network consists of 10 to 20 NEs, combining functions on a single NE should not impair performance.*

5.34 If 1301 NMX systems are not being used to monitor the network, terminals or PCs running terminal emulation software can be connected to each CAMR/Far-End Alarm concentrator NE (Figure 26). This arrangement provides some network monitoring redundancy in the event of a cable break in a linear network.

Figure 26. Redundant Terminal Arrangement

System Alarms

5.35 The 1603 SM provides three types of alarm indicators depending on the severity of the event. These alarm indicators are: autonomous messages, plug-in unit status LED indicators, and system notification codes.

5.36 Autonomous messages are generated by alarm conditions, threshold crossings, state changes, common equipment events, facility events, switchovers, and performance monitoring reports. Each alarm event is associated with a system notification code. The possible notification codes are Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), and Not Reported (NR). The effect on the plug-in unit alarm LED(s) and autonomous message generation depends on the notification code associated with the alarm event. The CR, MJ and MN notification codes generate an autonomous message and can activate alarm LED(s). The NA notification code results in a lesser severity autonomous message, but no alarm LED activation. The NR notification code silences alarms and messages.

5.37 The 1603 SM provides an active centralized alarm reporting process responsible for:

- Collecting, storing and maintaining all declared alarm conditions from all subsystems
- Generating autonomous events and alarm reports
- Processing all periodic performance monitoring reports
- Distributing alarms, conditions, events, and reports to their appropriate destinations (e.g.,

the user, CAMR, or the log)

- Activating and/or deactivating requests to the alarm display process for LED and audible alarms
- Processing alarms, conditions, and events retrieval requests (typically, TL1 commands)

Far-End Alarm Reporting

5.38 The Far-End Alarm Reporting feature determines NE states without requiring special external equipment (such as an ASCII terminal or a 1301 NMX), having to log on to an NE or the network, or having to know the appropriate TL1 commands. Simply press a button to select NEs in the network and display individual NE status. The Far-End Alarms feature is designed so using the function cannot affect traffic, provisioning, or system programming.

5.39 Far-End Alarm Reporting controls and displays are mounted on the front panel of the COA50x/60x plug-in units (see Figure 27). At the top of the COA50x/60x plug-in unit's front panel are four LEDs. The red LED labeled CRI represents a Critical alarm. The red LED labeled MAJ represents a Major alarm. The yellow LED labeled MIN represents a Minor alarm. The yellow LED labeled REM ALM indicates the presence of an alarm on a remote NE in the network.

Figure 27. COA50x/60x Front Panel Far-End Alarm Functions

5.40 In the middle of the COA50x/60x plug-in unit front panel are two seven-segment LEDs and a pushbutton labeled ID SEL. When the pushbutton is pressed and held, the two seven-segment LEDs display the assigned two-digit NE number for every NE in the network, including the local NE, in ascending numerical sequence. The three LEDs at the top of the COA50x/60x front panel indicate the status of the NE being selected/displayed. The REM ALM LED is ON (lighted) when a remote NE status is being displayed and OFF when indicating the local NE status.

5.41 The manner in which the seven-segment LEDs display an NE number is also significant. If the two-digit number is flashing, the NE was not accessible when the NE was last polled and the database was updated. This could mean a fiber cut between two NEs in a linear network configuration or a complete power failure. If the two-digit number is not flashing, the NE was accessible when polled.

5.42 Far-End Alarm Reporting requires that one NE in the network be assigned as the Far-End Alarm concentrator. The CAMR function permits multiple concentrators in the network. However, there can only be one Far-End Alarm concentrator in a network. This concentrator can monitor up to 32 NEs in the network. Figure 28 shows a four-NE network where the NE at Site D is the Far-End Alarm concentrator. Typically, a Far-End Alarm concentrator NE is at a central office.

Figure 28. Far-End Alarm Reporting Concentrator

5.43 Any NE in the network can display the individual NE alarm status of all NEs in the network. When the COA50x/60x plug-in unit ID SEL pushbutton is pressed, the COA50x/60x displays information from the local NE database. The Far-End Concentrator NE routinely polls other NEs in the network and updates the concentrator NE database; the concentrator NE updates the other NEs. The delay before NEs are updated depends on the number of NEs in the network. In addition, there is a slight delay between removing an alarm state and updating the Far-End Alarm Reporting displays.

5.44 If Site A is also a central office and there are more than 32 NEs in the network, the customer may want to make the NE at Site A a Far-End Alarm concentrator, too. If there are two Far-End Alarm concentrator NEs in a network, specific NEs in the network are assigned to each concentrator that establishes separate domains or alarm reporting networks. None of the NEs are assigned to both concentrators. Establishing separate domains is also ideal for ring networks as shown in Figure 29.

NOTE: *Far-End Alarm Reporting only provides an indication of NE status. Once a problem is detected, comprehensive diagnostic procedures are needed to isolate and correct the problem; e.g., connecting an ASCII terminal or 1301 NM to the 1603 SM COA50x/60x USI port, logging on to the NE, and obtaining detailed information about the problem.*

Figure 29. Separate Domains Far-End Alarm Reporting in a UPPS Ring Network

Remote Alarm Display Map (RADMAP) for R03.01 and Later

5.45 The Remote Alarm Display Map (RADMAP) is used to provision the Centralized Alarm Message Reporting (CAMR) feature and either enable or disable the Far-End Alarm (FEA) feature. These features allow up to 32 remote NEs to send autonomous messages to two distinct concentrator NEs.

PC Domain (for R03.01 and Later)

5.46 PC Domain is a way of organizing, presenting and monitoring groupings of SONET NEs in a network map configuration. PC Domain is a 1301 NMX function supported by the 1603 SM. PC Domain does not work without a 1301 NMX. For more information, refer to the 1301 NMX General System Description section in this manual.

Trouble Clearing

Overview

5.47 Trouble clearing is the isolation of failures and the restoration of the system. Trouble isolation is narrowing failures down to a replaceable plug-in unit or a fiber. Trouble clearing requirements include test access, loopbacks, access to performance data, and diagnostics available in the SONET network element. Restoration permits service restoration even though the failure may not have been repaired. Protection switching and traffic rerouting are examples of achieving network restoration without fully repairing the NE.

5.48 As of R06.00 and later, both the 1603 SM Maintenance and Trouble Clearing manual and the optional Online Troubleshooting Guide (OTG) contain trouble clearing procedures that address both hardware and software system failures. For more information on the OTG, refer to the 1301 NMX General System Description and the 1301 NM OTG1603 unit data sheet in this manual.

Testing

5.49 The test process includes equipment diagnostics and facility tests in the network element. Test requests may be received by TL1 request, maintenance background diagnostics, maintenance fault isolation diagnostics, or external inband facility test requests. Upon test completion, an appropriate test result is returned to the originator of the test request.

5.50 Diagnostics are broken down in two types of tests: facility and equipment. Facility tests provide test access support or a loopback state for external test set verification of the actual facility. Equipment diagnostics pertain to the actual plug-in unit, backplane, or cable hardware tests.