TNG-410

Security/User Authorization

1. GENERAL

1.1 This document provides a summary of the security mechanism provided by the 1603 SM Network Element (NE) to restrict either the intentional or inadvertent unauthorized use of input commands. Other security issues, such as physical security and the security mechanisms provided by the Operation Systems (OS) interfacing with the 1603 SM, are not covered here, but are assumed to be provided per local practices.

1.2 The main purpose of command entry security is to restrict the access to the NE databasem which stores the vital information concerning the operations and configuration of the NE. Inadvertent alterations to this database can disrupt the traffic-carrying and communications ability of the NE and, ultimately, interrupt service. Restricting access to and action on the information stored in the NE database to those who need this access privilege for the performance of their tasks is an effective security strategy to preserve the integrity of the NE database. This strategy is called the policy of least user privilege or, sometimes, the need-to-know policy, as it grants all users the smallest set of privileges necessary to perform their tasks.

1.3 The general security features provided by the 1603 SM are categorized as follows:

- Identification is the process of recognizing a session requester's unique and (audible) identity, such as the user ID. The user ID is not confidential; it is the name by which a valid user is recognized by the NE. A user ID aging mechanism is available to disable a user ID after some extended period of non-use time.
- Authentication is the process of verifying the claimed identity of the session requester. For a user login, this is done by the use of a password which must be entered after the user ID when logging in to the NE. This password is known only by the NE and the user. A password aging mechanism is available, which requires periodic changing of a user's password. In the case of OS network access channels such as X.25, a network-level security (i.e., not end-to-end connection security) is provided by verifying the calling address that is delivered to the NE via the call-setup packet.
- System Access Control authorizes establishment of a logon session and continuation of a session until logoff. System access (except for a limited set of commands) is allowed only to those users who are identified and authenticated. A session privilege level is established that is determined by the combination of the user and the channel (port) privilege levels.
- Command Access Control provides the capability of denying access to certain commands depending on the comparison of the session privilege level and the command privilege level. This subject is explained in greater detail in the remainder of this section.
- Data and System Integrity deal with the consistency and reliability issues associated with

the NE system and its data and software resources.

- Security Log (Audit) provides tools to establish an audit trail. If a security breach is suspected, an audit trail may be used to investigate the breach.
- Security Administration consists of proper activation, maintenance, and usage of the security features of the NE, conducted by the system administrator. It includes, among other things, overriding Alcatel-supplied defaults and managing the security database (i.e., keeping up-to-date user logins, privilege codes for users, commands and calling channels/ports).

2. CALLING CHANNEL IDENTIFIER (CID)

2.1 The Calling Channel Identifier (CID) describes what port or OS channel is used to access the NE. Two general classes of CIDs are available: user logon and OS.
2.2 Local and remote user logon access points are available. Local access consists of craft ports physically located at the NE. Remote logon capability is provided over the SONET overhead channels to allow logon capability at one NE, while physically being located at another.
2.3 Operations performed on an NE can be tendered from centralized operations centers (OCs), often via Operations Systems (OSs). An OC may have a number of work groups that provide technical expertise and clearly defined assignment of responsibilities in a central location for the best use of human resources. To accommodate the different work groups, OS-channel recognition is provided by the NE. The OS channels provided by the 1603 SM are for maintenance (MAINT), testing (TEST), and memory administration (PROV). A PEER CID channel also is provided for the 1301 NM network manager.
2.4 Certain security parameters are defined for each of the CIDs. A privilege code (described in more detail later) is assigned to each CID which is used for restricting access to commands that are outside of the CID domain of responsibility. Also, certain monitoring parameters can be set for each CID, such as: maximum number of invalid login attempts (MXINV), minimum time interval required between consecutive session setup attempts (MINT), inactivity time-out interval (TMOUT), and time interval over which the CID can be disabled due to an intrusion alert (DURAL).

3. PRIVILEGE CODES

3.1 The determination of whether a command can be executed is based on privilege codes. A privilege code can be associated with a command, a user, a port, or a (logon) session. The Command Privilege Code (COPC) specifies the minimum privilege requirements for all who will be able to execute a given command. Each command has an associated COPC, which is set up by a system default and maintained by the system administrator. The User Privilege Code (UPC) provides the user with a set of privileges, which eventually helps determine which commands he can execute and where he stands in the system user hierarchy. Each user has an associated UPC which is assigned when he is entered into the system, and is maintained by the system administrator. The Calling Address Identifier (CID, also known as port Privilege Code [CAPC]), is assigned to each network access point to provide a means of regulating the types of commands, which can be executed through a given port. Each network access point to the NE has an associated CAPC assigned to it. The CAPC is initially set up by a system default and is maintained by the system administrator. Finally, the Session Privilege Code (SPC) is defined by a combination of the UPC and CAPC, just as the user session itself is defined by both the user who is logged on and the port with which he is accessing the NE.

3.2 Once all of these privilege codes have been established, the question of command execution versus denial is answered by a comparison of the command privilege code (COPC) and the session privilege code (SPC). In general, if the SPC is greater-than or equal-to the COPC, the command is executed. If not, the command is denied. Before more details of the comparison can be made, a detailed look at the privilege code is in order.

4. PRIVILEGE CATEGORIES

4.1 Each privilege code is made up of four categories, and each category contains a one-digit privilege level. The categories are defined as Maintenance (M), Provisioning (P), Security (S), and Test (T). These categories reflect the four basic categories of system TL1 commands. The privilege levels for the four categories are concatenated into a single Privilege Code (PC):

PC = (M, P, S, T)

where: M, P, S, and T are the privilege levels for the respective categories.

5. PRIVILEGE LEVELS

5.1 Each privilege category (M, P, S, and T) is assigned a privilege level that ranges from 0 to 7. Privilege levels from 0 to 7 can be assigned by the system administrator to user privilege codes (UPC), CID privilege codes (CAPC) and command privilege codes (COPC). The privilege levels (0 - 7) are defined as follows:

- Level 7 is reserved for the system administrator and commands which can alter the integrity of the system.
- Levels 3-6 are open and can be used by the system administrator to organize the user hierarchy as required by the application (e.g., supervisor, clerk).
- Level 2 is the base level of a user who is considered logged into the system. This level includes basic commands, which, for security purposes, should be executable by anyone who is allowed to logon (includes most of the RTRV commands).
- Level 1 is the lowest level and it is applied to all users who are connected to the system, but have not yet logged on. This level allows the user to execute the most basic commands, such as RTRV-HDR (to retrieve the system header), ACT-USER (to activate a user), and LOGOFF.
- Level 0 is assigned to a privilege category when it is not to be considered during the process of deciding whether to allow a user to execute a command.

6. COMMAND EXECUTION

6.1 When a user enters a command, the NE command processor must first decide whether the user has the proper privilege levels before allowing or denying the execution of the command. This is done by comparing each privilege category (M, P, S, and T) of the Session Privilege Code (SPC) and Command Privilege Code (COPC). When an SPC and a COPC are being compared, only the common categories are considered. A common category is one in which both the SPC and COPC have a non-zero privilege level. In this way, a zero privilege level disables or disqualifies a category from the comparison. A zero value in the category for either the SPC or COPC causes the comparison process to skip to the next category with no immediate effect on the outcome. If a common category is found and the SPC privilege level is greater-than or equal-to the COPC privilege level, the comparison is considered successful and the next category is compared. The comparison is done for each privilege category until a comparison fails or all categories have been compared. In the case of a comparison failure, the comparison process is halted and the command execution is denied.

6.2 At least one successful comparison must be found before the command can be executed. It is possible that a command could be denied execution even though none of the comparisons failed. This is possible if no common categories are found. For example, if a session user with an SPC = 5500 tries to execute a command with a COPC = 0003, the command would be denied, since the two privilege codes contain no common categories to be compared. Likewise, if a session user with an SPC = 5500 tries to execute a command with a COPC = 7003, the command would also be denied, since in its only common category, MAINT, the COPC (7) is greater than the SPC (5). On the other hand, if a session user with an SPC = 0500 tries to execute a command with a COPC = 6406, the command would be executed, since in the only common category, PROV, the SPC (5) is greater than the COPC (4).

6.3 Commands and users can be grouped by category. In the case of the COPC, the privilege level associated with each category determines to which categories the command belongs (e.g., COPC = 0005 would indicate this command is strictly a T command and the session user trying to execute it must have a minimum T privilege of 5). In the case of an SPC, the privilege level associated with each category determines which types of commands the session user can execute (e.g., SPC = 0070 implies that this session will be able to execute S commands of privilege levels up to 7). Table A lists the 1603 SM system TL1 commands, their functional category and their default COPC levels.

Table A. Commands and Default Command Privilege Codes (COPC)

COMMAND	FUNCTIONAL CATEGORY*	COPC (MPST)
ABT-CPY	M---	7000
ACT-USER	MPST	1111
ALW-AUTORST	M---	2000
ALW-CONT-VPL	M---	2000
ALW-DGN-EQPT	M---	2000
ALW-LPBK-T1	M---	2000
ALW-LPBK-T3	M---	2000
ALW-MSG-ALL	M---	2000
ALW-PMREPT-ALL	M---	2000
ALW-PMREPT-ATMPORT	M---	2000
ALW-PMREPT-ATMPROC	M---	2000
ALW-PMREPT-EC1	M---	2000
ALW-PMREPT-EQPT	M---	2000
ALW-PMREPT-OC3	M---	2000
ALW-PMREPT-OC12	M---	2000
ALW-PMREPT-STS1	M---	2000
ALW-PMREPT-STS3C	M---	2000
ALW-PMREPT-SYNCN	M---	2000
ALW-PMREPT-T1	M---	2000
ALW-PMREPT-T3	M---	2000
ALW-PMREPT-VPL	M---	2000

ALW-PMREPT-VT1	M---	2000
ALW-SWDX-EQPT	M---	2000
ALW-SWTOPROTN-EQPT	M---	2000
ALW-SWTOWKG-EQPT	M---	2000
CANC-USER	MPST	1111
CHG-ACCMD-T1	---T	2002
CONFIG-SYS	-P--	0700
CONN-TACC-T1	---T	2002
CONN-TEST-T1	---T	2002
CONN-TEST-T3	---T	2002
CPY-MEM	M---	7000
DGN-EC1	---T	2002
DGN-EQPT	---T	2002
DGN-OC3	---T	2002
DGN-OC12	---T	2002
DGN-STS1	---T	2002
DGN-STS3C	-P--	0200
DGN-VT1	---T	2002
DISC-TACC	---T	2002
DISC-TEST-T1	---T	2002
DISC-TEST-T3	---T	2002
DLT-BITS	-P--	0200
DLT-CRS-STS1	-P--	0200
DLT-CRS-STS3C	-P--	0200
DLT-CRS-VPL	-P--	0200
DLT-CRS-VT1	-P--	0200
DLT-DOMAIN	-P--	0200
DLT-E2AMAP	-P--	0200
DLT-EC1	-P--	0200
DLT-EQPT	-P--	0200
DLT-IP	-P--	0200
DLT-LAN	-P--	0200
DLT-LLSDCC	-P--	0200
DLT-LLSMLDCC	-P--	0200
DLT-MAADDR	-P--	0200
DLT-MEM	M---	7000
DLT-OC3	-P--	0200
DLT-OC12	-P--	0200
DLT-OSACMAP	-P--	0200
DLT-PORT	MP--	2200
DLT-RADMAP	-P--	0200
DLT-SECU-USER	--S-	0070
DLT-SML	-P--	0200
DLT-STS3C	-P--	0200
DLT-T1	-P--	0200

DLT-T3	-P--	0200
DLT-TADRMAP	-P--	0200
DLT-VPL	-P--	0200
ED-ATMPORT	-P--	0200
ED-ATMPROC	-P--	0200
ED-BITS	-P--	0200
ED-CRS-STS1	-P--	0200
ED-CRS-STS3C	-P--	0200
ED-CRS-VPL	-P--	0200
ED-CRS-VT1	-P--	0200
ED-EC1	-P--	0200
ED-EQPT	-P--	0200
ED-FFP-OC3	-P--	0200
ED-FFP-OC12	-P--	0200
ED-FFP-STS1	-P--	0200
ED-FFP-STS3C	-P--	0200
ED-FFP-VPL	MP--	0200
ED-FFP-VT1	-P--	0200
ED-IP	-P--	0200
ED-LAN	-P--	0200
ED-LLSDCC	-P--	0200
ED-LLSMLDCC	-P--	0200
ED-MAADDR	-P--	0200
ED-OC3	-P--	0200
ED-OC12	-P--	0200
ED-OSACMAP	-P--	0200
ED-PORT	MP--	2200
ED-RADMAP	-P--	0200
ED-SECU-CID	--S-	7777
ED-SECU-CMD	--S-	0070
ED-SECU-PID	--S-	2222
ED-SECU-USER	--S-	0070
ED-SML	-P--	0200
ED-STS1	-P--	0200
ED-STS3C	-P--	0200
ED-SYNCN	-P--	0200
ED-T1	-P--	0200
ED-T3	-P--	0200
ED-TADRMAP	-P--	0200
ED-TARP	-P--	0200
ED-ULSDCC	-P--	0200
ED-VPL	-P--	0200
ED-VT1	-P--	0200
ED-X25	-P--	0200
ENT-BITS	-P--	0200

ENT-CRS-STS1	-P--	0200
ENT-CRS-STS3C	-P--	0200
ENT-CRS-VPL	-P--	0200
ENT-CRS-VT1	-P--	0200
ENT-DOMAIN	-P--	0200
ENT-E2AMAP	-P--	0200
ENT-EC1	-P--	0200
ENT-EQPT	-P--	0200
ENT-IP	-P--	0200
ENT-LAN	-P--	0200
ENT-LLSDCC	-P--	0200
ENT-LLSMLDCC	-P--	0200
ENT-MAADDR	-P--	0200
ENT-OC3	-P--	0200
ENT-OC12	-P--	0200
ENT-OSACMAP	-P--	0200
ENT-PORT	MP--	2200
ENT-RADMAP	-P--	0200
ENT-SECU-USER	--S-	0070
ENT-SML	-P--	0200
ENT-STS3C	-P--	0200
ENT-T1	-P--	0200
ENT-T3	-P--	0200
ENT-TADRMAP	-P--	0200
ENT-VPL	-P--	0200
INH-AUTORST	M---	2000
INH-CONT-VPL	M---	2000
INH-DGN-EQPT	M---	2000
INH-LPBK-T1	M---	2000
INH-LPBK-T3	M---	2000
INH-MSG-ALL	M---	2000
INH-PMREPT-ALL	M---	2000
INH-PMREPT-ATMPORT	M---	2000
INH-PMREPT-ATMPROC	M---	2000
INH-PMREPT-EC1	M---	2000
INH-PMREPT-EQPT	M---	2000
INH-PMREPT-OC3	M---	2000
INH-PMREPT-OC12	M---	2000
INH-PMREPT-STS1	M---	2000
INH-PMREPT-STS3C	M---	2000
INH-PMREPT-SYNCN	M---	2000
INH-PMREPT-T1	M---	2000
INH-PMREPT-T3	M---	2000
INH-PMREPT-VPL	M---	2000
INH-PMREPT-VT1	M---	2000

INH-SWDX-EQPT	M---	2000
INH-SWTOPROTN-EQPT	M---	2000
INH-SWTOWKG-EQPT	M---	2000
INIT-LOG	M-S-	7070
INIT-LOLOG-ATMPORT	M---	2000
INIT-REG-ALL	M---	2000
INIT-REG-ATMPORT	M---	2000
INIT-REG-ATMPROC	M---	2000
INIT-REG-EC1	M---	2000
INIT-REG-EQPT	M---	2000
INIT-REG-OC3	M---	2000
INIT-REG-OC12	M---	2000
INIT-REG-STS1	M---	2000
INIT-REG-STS3C	M---	2000
INIT-REG-SYNCN	M---	2000
INIT-REG-T1	M---	2000
INIT-REG-T3	M---	2000
INIT-REG-VPL	M---	2000
INIT-REG-VT1	M---	2000
INIT-SYS	M---	7000
LOGOFF	MPST	1111
OPR-ACO-COM	M---	2000
OPR-CONT-VPL	M---	2000
OPR-EXT-CONT	M---	2000
OPR-LPBK-EC1	---T	2002
OPR-LPBK-OC3	---T	2002
OPR-LPBK-OC12	---T	2002
OPR-LPBK-T1	---T	2002
OPR-LPBK-T3	---T	2002
OPR-LSR	M---	2000
OPR-PROTNSW-OC3	M---	2000
OPR-PROTNSW-OC12	M---	2000
OPR-PROTNSW-STS1	M---	2000
OPR-PROTNSW-STS3C	M---	2000
OPR-PROTNSW-VPL	M---	2000
OPR-PROTNSW-VT1	M---	2000
OPR-SYNCNSW	M---	2000
RD-MEM-ADRS	M---	2000
RD-SYNCN	M---	2000
RLS-CONT-VPL	M---	2000
RLS-EXT-CONT	M---	2000
RLS-LPBK-EC1	---T	2002
RLS-LPBK-OC3	---T	2002
RLS-LPBK-OC12	---T	2002
RLS-LPBK-T1	---T	2002

RLS-LPBK-T3	---T	2002
RLS-PROTNSW-OC3	M---	2000
RLS-PROTNSW-OC12	M---	2000
RLS-PROTNSW-STS1	M---	2000
RLS-PROTNSW-STS3C	M---	2000
RLS-PROTNSW-VPL	M---	2000
RLS-PROTNSW-VT1	M---	2000
RLS-SYNCNSW	M---	2000
RMV-BITS	M---	2000
RMV-EC1	M---	2000
RMV-EQPT	M---	2000
RMV-OC3	M---	2000
RMV-OC12	M---	2000
RMV-SML	M---	2000
RMV-T1	M---	2000
RMV-T3	M---	2000
RST-BITS	M---	2000
RST-EC1	M---	2000
RST-EQPT	M---	2000
RST-OC3	M---	2000
RST-OC12	M---	2000
RST-SML	M---	2000
RST-T1	M---	2000
RST-T3	M---	2000
RTRV-ALM-ALL	M---	1111
RTRV-ALM-ATMPORT	M---	1111
RTRV-ALM-ATMPROC	M---	1111
RTRV-ALM-BITS	M---	1111
RTRV-ALM-COM	M---	1111
RTRV-ALM-EC1	M---	1111
RTRV-ALM-ENV	M---	1111
RTRV-ALM-EQPT	M---	1111
RTRV-ALM-LAN	M---	1111
RTRV-ALM-LLSDCC	M---	1111
RTRV-ALM-LLSMLDCC	M---	1111
RTRV-ALM-NETWORK	M---	1111
RTRV-ALM-OC3	M---	1111
RTRV-ALM-OC12	M---	1111
RTRV-ALM-PORT	M---	1111
RTRV-ALM-RMT	M---	1111
RTRV-ALM-SML	M---	1111
RTRV-ALM-STS1	M---	1111
RTRV-ALM-STS3C	M---	1111
RTRV-ALM-SYNCN	M---	1111
RTRV-ALM-T1	M---	1111

RTRV-ALM-T3	M---	1111
RTRV-ALM-TADRMAP	M---	1111
RTRV-ALM-VPL	M---	1111
RTRV-ALM-VT1	M---	1111
RTRV-ALM-X25	M---	1111
RTRV-AO	M---	2000
RTRV-ATMPORT	-P--	0200
RTRV-ATMPROC	-P--	0200
RTRV-ATTR-ATMPORT	M---	2000
RTRV-ATTR-ATMPROC	M---	2000
RTRV-ATTR-BITS	M---	2000
RTRV-ATTR-COM	M---	2000
RTRV-ATTR-CONT	M---	2000
RTRV-ATTR-EC1	M---	2000
RTRV-ATTR-ENV	M---	2000
RTRV-ATTR-EQPT	M---	2000
RTRV-ATTR-LAN	M---	2000
RTRV-ATTR-LLSDCC	M---	2000
RTRV-ATTR-LLSMLDCC	M---	2000
RTRV-ATTR-NETWORK	M---	2000
RTRV-ATTR-OC3	M---	2000
RTRV-ATTR-OC12	M---	2000
RTRV-ATTR-PORT	M---	2000
RTRV-ATTR-RMT	M---	2000
RTRV-ATTR-SML	M---	2000
RTRV-ATTR-STS1	M---	2000
RTRV-ATTR-STS3C	M---	2000
RTRV-ATTR-SYNCN	M---	2000
RTRV-ATTR-T1	M---	2000
RTRV-ATTR-T3	M---	2000
RTRV-ATTR-TADRMAP	M---	2000
RTRV-ATTR-VPL	M---	2000
RTRV-ATTR-VT1	M---	2000
RTRV-ATTR-X25	M---	2000
RTRV-BITS	-P--	0200
RTRV-CMD-STAT	M---	1111
RTRV-CNFGRN	M---	2000
RTRV-COND-ATMPORT	M---	2000
RTRV-COND-ATMPROC	M---	2000
RTRV-COND-BITS	M---	2000
RTRV-COND-COM	M---	2000
RTRV-COND-EC1	M---	2000
RTRV-COND-ENV	M---	2000
RTRV-COND-EQPT	M---	2000
RTRV-COND-LAN	M---	2000

RTRV-COND-LLSDCC	M---	2000
RTRV-COND-LLSMLDCC	M---	2000
RTRV-COND-NETWORK	M---	2000
RTRV-COND-OC3	M---	2000
RTRV-COND-OC12	M---	2000
RTRV-COND-PORT	M---	2000
RTRV-COND-RMT	M---	1111
RTRV-COND-SML	M---	2000
RTRV-COND-STS1	M---	2000
RTRV-COND-STS3C	M---	2000
RTRV-COND-SYNCN	M---	2000
RTRV-COND-T1	M---	2000
RTRV-COND-T3	M---	2000
RTRV-COND-TADRMAP	M---	2000
RTRV-COND-VPL	M---	2000
RTRV-COND-VT1	M---	2000
RTRV-COND-X25	M---	2000
RTRV-CPY-STAT	M---	7000
RTRV-CRS-STS1	-P--	0200
RTRV-CRS-STS3C	-P--	0200
RTRV-CRS-VPL	-P--	0200
RTRV-CRS-VT1	-P--	0200
RTRV-DOMAIN	-P--	1111
RTRV-E2AMAP	-P--	0200
RTRV-EC1	-P--	0200
RTRV-EQPT	-P--	0200
RTRV-EXT-CONT	M---	2000
RTRV-FFP-OC3	MP--	2200
RTRV-FFP-OC12	MP--	2200
RTRV-FFP-STS1	MP--	2200
RTRV-FFP-STS3C	MP--	2200
RTRV-FFP-VPL	MP--	2200
RTRV-FFP-VT1	MP--	2200
RTRV-HDR	MPST	1111
RTRV-INV-EQPT	MP--	2200
RTRV-IP	-P--	0200
RTRV-LAN	-P--	2000
RTRV-LED	M---	2000
RTRV-LLSDCC	-P--	2000
RTRV-LLSMLDCC	-P--	2000
RTRV-LOG	M---	2000
RTRV-LOLOG-ATMPORT	M---	2000
RTRV-MAADDR	-P--	2000
RTRV-MEM	M---	7000
RTRV-NE-ALL	M---	2000

RTRV-NSAP	M---	1111
RTRV-OC3	-P--	0200
RTRV-OC12	-P--	0200
RTRV-OSACMAP	-P--	0200
RTRV-PM-ATMPORT	M---	2000
RTRV-PM-ATMPROC	M---	2000
RTRV-PM-EC1	M---	2000
RTRV-PM-EQPT	M---	2000
RTRV-PM-OC3	M---	2000
RTRV-PM-OC12	M---	2000
RTRV-PM-STS1	M---	2000
RTRV-PM-STS3C	M---	2000
RTRV-PM-SYNCN	M---	2000
RTRV-PM-T1	M---	2000
RTRV-PM-T3	M---	2000
RTRV-PM-VPL	M---	2000
RTRV-PM-VT1	M---	2000
RTRV-PMNODE-ATMPORT	M---	2000
RTRV-PMMODE-ATMPROC	M---	2000
RTRV-PMMODE-EC1	M---	2000
RTRV-PMMODE-EQPT	M---	2000
RTRV-PMMODE-OC3	M---	2000
RTRV-PMMODE-OC12	M---	2000
RTRV-PMMODE-SYNCN	M---	2000
RTRV-PMMODE-T1	M---	2000
RTRV-PMMODE-T3	M---	2000
RTRV-PMMODE-VPL	M---	2000
RTRV-PORT	MP-	2200
RTRV-PTHTRC-STS1	M---	2000
RTRV-PTHTRC-STS3C	M---	2000
RTRV-RADMAP	-P--	0200
RTRV-SCNTRC-EC1	M---	2000
RTRV-SCNTRC-OC3	M---	2000
RTRV-SCNTRC-OC12	M---	2000
RTRV-SECU-CID	--S-	2222
RTRV-SECU-CMD	--S-	2222
RTRV-SECU-UPC	--S-	2222
RTRV-SECU-USER	--S-	2222
RTRV-SML	-P--	0200
RTRV-STATS-ATMPROC	M---	2000
RTRV-STATUS	MPST	2222
RTRV-STS1	-P--	0200
RTRV-STS3C	-P--	0200
RTRV-SWVER-EQPT	M---	2000
RTRV-SYNCN	M---	2000

RTRV-T1	-P--	0200
RTRV-T3	-P--	0200
RTRV-TADRMAP	M---	2000
RTRV-TARP	M---	2000
RTRV-TH-ATMPORT	M---	2000
RTRV-TH-ATMPROC	M---	2000
RTRV-TH-EC1	M---	2000
RTRV-TH-OC3	M---	2000
RTRV-TH-OC12	M---	2000
RTRV-TH-STS1	M---	2000
RTRV-TH-STS3C	M---	2000
RTRV-TH-T1	M---	2000
RTRV-TH-T3	M---	2000
RTRV-TH-VT1	M---	2000
RTRV-ULSDCC	-P--	0200
RTRV-VPL	-P--	0200
RTRV-VT1	-P--	0200
RTRV-X25	-P--	0200
SET-ACO-COM	M---	2000
SET-ATTR-ATMPORT	M---	2000
SET-ATTR-ATMPROC	M---	2000
SET-ATTR-BITS	M---	2000
SET-ATTR-COM	M---	2000
SET-ATTR-CONT	M---	2000
SET-ATTR-EC1	M---	2000
SET-ATTR-ENV	M---	2000
SET-ATTR-EQPT	M---	2000
SET-ATTR-LAN	M---	2000
SET-ATTR-LLSDCC	M---	2000
SET-ATTR-LLSMLDCC	M---	2000
SET-ATTR-NETWORK	M---	2000
SET-ATTR-OC3	M---	2000
SET-ATTR-OC12	M---	2000
SET-ATTR-PORT	M---	2000
SET-ATTR-RMT	M---	2000
SET-ATTR-SML	M---	2000
SET-ATTR-STS1	M---	2000
SET-ATTR-STS3C	M---	2000
SET-ATTR-SYNCN	M---	2000
SET-ATTR-T1	M---	2000
SET-ATTR-T3	M---	2000
SET-ATTR-TADRMAP	M---	2000
SET-ATTR-VPL	M---	2000
SET-ATTR-VT1	M---	2000
SET-ATTR-X25	M---	2000

SET-DAT	-P--	7777
SET-NE-ALL	-P--	2202
SET-PMMODE-ATMPORT	M---	2000
SET-PMMODE-ATMPROC	M---	2000
SET-PMMODE-EC1	M---	2000
SET-PMMODE-EQPT	M---	2000
SET-PMMODE-OC3	M---	2000
SET-PMMODE-OC12	M---	2000
SET-PMMODE-SYNCN	M---	2000
SET-PMMODE-T1	M---	2000
SET-PMMODE-T3	M---	2000
SET-PMMODE-VPL	M---	2000
SET-PTHTRC-NE	M---	2000
SET-SID	-P--	2000
SET-SYNCN	M---	2000
SET-TH-ATMPORT	M---	2000
SET-TH-ATMPROC	M---	2000
SET-TH-EC1	M---	2000
SET-TH-OC3	M---	2000
SET-TH-OC12	M---	2000
SET-TH-STS1	M---	2000
SET-TH-STS3C	M---	2000
SET-TH-T1	M---	2000
SET-TH-T3	M---	2000
SET-TH-VT1	M---	2000
SW-DX-EQPT	M---	2000
SW-RING-ALL	M---	2000
SW-TOPROTN-EQPT	M---	2000
SW-TOWKG-EQPT	M---	2000
TS-LPBK-VPL	M---	2000
** For Functional Category and Default COPC columns: M = Maintenance, P = Provisioning, S = Security, and T = Testing.*		

7. THE SUPERUSER AND A SUPERUSER

7.1 The SUPERUSER is the system administrator who has a security privilege level of 7 for all privilege categories. To distinguish between the two, they are referenced as the SUPERUSER (all upper case) and a Superuser. When logging on to a 1603 SM network element as the SUPERUSER, the user ID is literally SUPERUSER (all uppercase). No user in the system is able to delete the SUPERUSER. The SUPERUSER can create another user, with privilege levels equal to his own, who may also be considered a superuser. The difference is that The SUPERUSER can modify and delete a Superuser, but a Superuser cannot modify the SUPERUSER or any other created Superuser (there can be more than one created). The SUPERUSER's user ID and password are provided by Alcatel and are programmed into the NE factory-default software. The SUPERUSER's password can be changed but not its user ID. A superuser is simply a user ID with a user privilege code set to 7777.

8. SECURITY TL1 COMMANDS

8.1 Described in this section are the TL1 commands associated with security administration.

- **ACT-USER** This is the command for logging on to the NE. It has a fairly low security privilege code since it must be executed by users who, prior to logon, are provided only a default low level (connected) privilege. The security code is always 1111.
- **CANC-USER** This is the command executed by the user to logoff the NE. This command can also be used by A superuser or The superuser to log another user off the NE. Since this command must be executed by all users, its security code is always 1111.
- **DLT-SECU-USER** This command deletes a user from the system and can only be executed by the SUPERUSER or A superuser. The SUPERUSER can delete a superuser. The SUPERUSER cannot be deleted. This command allows deletion of one or a combination (by grouping) of users at the same time. Even if this command security level is lowered, it can only be executed successfully by a Superuser and the SUPERUSER. The recommended security code is 0070.
- **ED-SECU-CID** This command is used to edit or change the privilege code (CAPC) associated with a single or combination (grouping) of CIDs. Also, certain monitoring parameters can be set for each CID, such as maximum number of invalid login attempts (MXINV), minimum time interval required between consecutive session setup attempts (MINT), inactivity time-out interval (TMOUT), and time interval over which the CID can be disabled due to an intrusion alert (DURAL). This command should have a high security privilege code which only allows a/the superuser to execute it. If the command privilege level is lowered, an internal mechanism prohibits a user from modifying the CID if his security privilege is lower than that of the CID. The recommended security code is 7777.
- **ED-SECU-CMD** This command is used to edit the privilege code (COPC) associated with a single or combination of commands. This command should have a high security privilege code which only allows the/a superuser to execute it. But, if the command privilege level is lowered, an internal mechanism prohibits a user from modifying the command if his security privilege is lower than that of the command. The recommended security code is 0070.
- **ED-SECU-PID** This command is used by a user to edit his own password (private identifier). The user must enter his old password before he can change it. The recommended security code is 2222.
- **ED-SECU-USER** This command is used to edit the security parameters associated with a single or combination of users. This command permits changing a user privilege code (UPC), user ID, and password. Parameters also can be set for password aging as well as user ID aging. This command should have a high security privilege code, which only allows The/A superuser to execute it. If the command privilege level is lowered, an internal mechanism prohibits a user from modifying another user of equal or greater privilege. The superuser can modify A superuser, but The superuser cannot be modified by any other user. The recommended security code is 0070.
- **ENT-SECU-USER** This command is used to enter a new user and all associated parameters listed for the ED-SECU-USER command. This command should have a high security privilege code which only allows The/A superuser to execute it. If the command privilege level is lowered, an internal mechanism prohibits a user from creating another

user with higher privileges than his own. The recommended security code is 0070.

- **RTRV-SECU-CID** This command is used to retrieve the security parameters associated with a single or combination of CIDs. This command should have a low security privilege code which allows all users to execute it. Although a user may have sufficient privilege to execute the command, he may not have sufficient privilege to view all the requested database information. An internal mechanism prohibits a user with a lower security privilege than that of the CID from actually retrieving it. For example, a user with a security privilege sufficient to execute this command, yet lower than all the CIDs, would receive the completed message (verifying his execution privilege), but he would still not be able to see any CID data in output. The recommended security code is 2222.
- **RTRV-SECU-CMD** This command is used to retrieve the privilege code associated with a single or combination of commands. This command should have a low security privilege code that allows all users to execute it. An internal mechanism prohibits a user from retrieving information for a command that has a higher security privilege level than his own. In this case, provided a user has sufficient command privilege, he could execute the command, but would only see data pertaining to those commands that he is sufficiently privileged to see. The recommended security code is 2222.
- **RTRV-SECU-UPC** This command is executed by a user to retrieve his own User Privilege Code (UPC). The recommended security code is 2222.
- **RTRV-SECU-USER** This command is used to retrieve the security parameters associated with a single or combination of users. This command should have a low security privilege code that allows all users to execute it. An internal mechanism prohibits a user from retrieving database information on users who have a higher security privilege than his own. For example, a user with a security privilege sufficient to execute this command, yet lower than some of the other users, would get the completed message (verifying his execution privilege), but he would still not be able to see any information on users with a security privilege higher than his own; he would only see information for users of equal or lower security privilege. The recommended security code is 2222.
- **LOGOFF** This is another command for logging off the NE. The security code is always 1111.