Nortel Communication Server 1000

Nortel Communication Server 1000 Release 4.5

System Security Management

Document Number: 553-3001-302
Document Release: Standard 11.00
Date: June 2006

Produced in Canada

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Revision history

June 2006

Standard 11.00. This document is up-issued to support Communication Server 1000 Release 4.5.

August 2005

Standard 10.00. This document is up-issued to support Communication Server 1000 Release 4.5.

September 2004

Standard 9.00. This document is up-issued to support Communication Server 1000 Release 4.0.

October 2003

Standard 8.00. This document is issued to support Succession 3.0 Software.

January 2002

Standard 7.00. This document is up-issued to include content changes for the Meridian 1 Release 25.40 and Succession Communication Server for Enterprise 1000 systems.

April 2000

Standard 6.00. This is a global document and is up-issued for Release 25.0x.

June 1999

Standard 5.00. This document is updated for Release 24.2x.

October 1997

Standard 4.00. This document is updated for Release 23.0x.

July 1995

Standard 3.00. This document is issued to include Release 21 changes.

December 1994

Standard 2.00. Includes Release 20 changes, editorial changes, and indexing.

October 31, 1993

Standard 1.00.

Contents

Finding the latest updates on the Nortel Web site

The content of this documentation was current at the time the product was released. To check for updates to the latest documentation and software for Nortel Communication Server 1000 Release 4.5, click one of the following links:

Latest Software	Takes you directly to the Nortel page for Nortel Communication Server 1000 Release 4.5 software
Latest Documentation	Takes you directly to the Nortel page for Nortel Communication Server 1000 Release 4.5 documentation

How to get help

This chapter explains how to get help for Nortel products and services.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the telephone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the telephone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

List of procedures

About this document

This document is a global document. Contact your system supplier or your Nortel representative to verify that the hardware and software described are supported in your area.

Subject

The subject of this document is the detection of possible unauthorized access to the system and Meridian Mail, and the implementation of system-wide security features. This document describes how to:

- plan and implement security options for a new system
- audit an existing system's security
- upgrade an existing system's security features where necessary

This document also describes how to verify that security features are in place and how to use built-in system monitoring and reporting facilities to discover fraudulent and unauthorized use of telecommunication facilities.

This document addresses the security issues that are system-specific, such as toll fraud, unauthorized use of features, and unauthorized access to the system. It does not address non-system specific security issues. It is assumed that LAN/WAN administrators have implemented their own network security policies.

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 4.5

software. For more information on legacy products and releases, click the **Technical Documentation** link under **Support** on the Nortel home page:

www.nortel.com

Applicable systems

This document applies to the following systems:

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)
- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet
- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 81
- Meridian 1 PBX 81C

  Note: When upgrading software, memory upgrades may be required on the Signaling Server, the Call Server, or both.

System migration

When particular Meridian 1 systems are upgraded to run CS 1000 Release 4.5 software and configured to include a Signaling Server, they become

CS 1000M systems. Table 1 lists each Meridian 1 system that supports an upgrade path to a CS 1000M system.

Table 1
Meridian 1 systems to CS 1000M systems

This Meridian 1 system...	Maps to this CS 1000M system
Meridian 1 PBX 11C Chassis	CS 1000M Chassis
Meridian 1 PBX 11C Cabinet	CS 1000M Cabinet
Meridian 1 PBX 51C	CS 1000M Half Group
Meridian 1 PBX 61C	CS 1000M Single Group
Meridian 1 PBX 81	CS 1000M Multi Group
Meridian 1 PBX 81C	CS 1000M Multi Group

For more information, see one or more of the following NTPs:

- *Communication Server 1000M and Meridian 1: Small System Upgrade Procedures* (553-3011-258)
- *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures* (553-3021-258)
- *Communication Server 1000S: Upgrade Procedures* (553-3031-258)

Intended audience

This document is intended for individuals responsible for helping distributors and system administrators who are installing new systems and upgrading and maintaining existing systems. It is assumed that the reader has a thorough knowledge of system software and Meridian Mail software operations and has the ability to configure and maintain systems using configuration and maintenance programs.

Conventions

Terminology

In this document, the following systems are referred to generically as "system":

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M (CS 1000M)
- Communication Server 1000E (CS 1000E)
- Meridian 1

The following systems are referred to generically as "Small System":

- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet

The following systems are referred to generically as "Large System":

- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 81
- Meridian 1 PBX 81C

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *System Management* (553-3001-300)
- *Features and Services* (553-3001-306)
- *Software Input/Output: Administration* (553-3001-311)
- *Call Detail Recording: Description and Formats* (553-3001-350)
- *Traffic Measurement: Formats and Output* (553-3001-450)
- *Meridian Mail General Description* (553-7001-100)
- *Meridian Mail System Administration Guide* (553-7001-302)
- *Meridian Mail System Administration Tools* (553-7001-305)
- *Meridian Mail Fax on Demand Application Guide* (553-7001-327)
- *Meridian Mail Maintenance Messages* (553-7001-510)

Online

To access Nortel documentation online, click the **Technical Documentation** link under **Support** on the Nortel home page:

www.nortel.com

CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

Introduction

Contents

This section contains information on the following topics:

Introduction

This chapter provides an overview of how to control unauthorized access and provide security for the system. It describes the reason for implementing system security and provides recommendations for preventing abuse and damage to the telecommunications facilities.

System security overview

Each telecommunications system must be protected from unauthorized and fraudulent use. The system can be vulnerable to abuse by employees as well as outside sources, and individual calls can be vulnerable to disruption or intrusions against privacy. Security requirements for each system are unique and are based on the system configuration, functions, and features it supports.

Access to the functions and features supported by your system must be controlled by safeguards implemented in the system. Exercise caution when handling and disposing of information that can compromise system security. Inadequate control of calling privileges and unprotected physical access to switching systems are the main reasons companies incur fraudulent expenses through use of their telecommunications facilities.

One of the most serious sources of toll fraud is unauthorized remote access to a second dial tone through the system. This feature is called Direct Inward System Access (DISA). DISA privileges are intended for traveling employees who call into their company's system, enter an access code, and then use the company's long-distance calling services instead of using a credit card or letting the operator handle the call. Telecommunications managers must strictly monitor and control access privileges.

Voicemail and automated attendant services are also major targets. If proper safeguards are not in place, callers accessing a voicemail system can easily place toll calls once they know long-distance access codes or trunk access codes. They can also take over a mailbox for use as a bulletin board.

Remote system administration can be vulnerable to unauthorized access. Remote system administration allows system technicians to access, configure, and troubleshoot both the system and Meridian Mail software and hardware problems remotely.

If maintenance ports lack proper safeguards, an unauthorized person can access the system, change the system configuration, degrade system performance, and fraudulently use services.

An intruder can dial into a remote access port and, once the password is determined, access the system, change the customer database configuration to allow international calls, enable the DISA feature, turn off Call Detail Recording (CDR), and defeat any safeguards already in place.

By activating traffic and call detail reports, checking calling patterns, and looking for variations, system fraud, which occurs mostly at night, on weekends, and on holidays, can usually be detected.

Typical patterns for outgoing call fraud are:

- calls to unusual locations
- high call volume
- long call duration
- international calls
- unexplained 900 number calls

The primary call destinations for toll fraud are international and the 809 area code.

Incoming call patterns that must be investigated are long holding times, an unexplained surge in traffic, and higher than usual traffic after business hours. If no traffic is being reported when some traffic is expected, this can indicate that the CDR reporting was deactivated and a maintenance port has been compromised.

Secure the system by knowing the current system software configuration, knowing which security features are active, and monitoring calling patterns to detect unauthorized activity.

Protect calls by activating SRTP protection, and add a Secure Media Controller (SMC) to the system to protect UNIStim signaling.

General security practices

Each telecommunications facility must be protected by a security program to prevent unauthorized and fraudulent use. Failure to implement a security program when the system is first installed, neglecting to carefully monitor system traffic patterns and system messages, and neglecting to improve system security as additional services are added can make the system vulnerable.

To protect the privacy and integrity of calls, enable SRTP on each terminal connected to the system.

In addition, practice the following system security recommendations to minimize the possibility of fraud:

- Deny unauthorized access to long-distance trunk facilities (such as thru-dial) when using voicemail. This can be accomplished by requiring a password to access voicemail or by blocking its activation.
- Require outside callers to use authorization codes when making incoming calls to DISA lines. Never publish DISA numbers. For greater security, use maximum length authorization codes that do not include an employee identification number, home telephone number, or social security number as part of the authorization code.
- Safeguard system configuration printouts, call detail records, and authorization code printouts. Dispose of this information in the same way as you would any other confidential information.
- Change all authorization codes as often as is practical. A maximum interval of 60 days is recommended. Delete codes used by former employees. Treat authorization codes like credit card numbers. Do not allow employees to share authorization codes.
- Restrict DISA calls at night and on holidays, if possible. Unauthorized calls are usually placed during these times.
- Monitor traffic patterns and call detail records to detect unusual traffic patterns and unauthorized calls.
- Provide international calling privileges only to users who require them. Restrict international calls only to countries that authorized users normally call; otherwise, block international calls completely.
- Restrict call forwarding so that telephones cannot forward calls to long-distance numbers or trunk facilities.
- Do not allow employees to post access codes, authorization codes, and passwords in plain view.
- Restrict switchroom access to authorized personnel.
- Implement a system security policy that includes the following:
  - password management
  - program access control
  - Problems Determination Tool (PDT) access control

- — administration port security
- — Audit Trail review
- — History File review

Follow these recommendations, analyze the existing security plan regularly, and upgrade that plan when required to minimize the opportunity for unauthorized persons to abuse and damage the telecommunications facilities.

The following chapters describe system security planning, and implementing and verifying procedures to provide better telecommunications system security.

Controlling call privileges

Contents

This section contains information on the following topics:

Introduction

This chapter describes the system call processing security features and how to implement these features. System call processing security is done by limiting and controlling call privileges and restricting access to the system facilities and features. Call processing privileges and restrictions are implemented by the following:

- Defining basic access restrictions (see page 29)
- Modifying basic access restrictions (see page 36)
- System Access Enhancements (see page 66)
- Using system management features (see page 70)
- Controlling Call Forward access (see page 72)
- Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS) (see page 78)
- Controlling Direct Inward System Access (see page 87)
- Controlling Multi-Tenant Services (see page 89

Defining basic access restrictions

Basic access restrictions allow internal and external users to be assigned access to only the facilities and calling privileges their jobs require. In this way, internal abuse can be deterred and external access to toll facilities can be restricted. The following features control access restrictions:

- Class of Service (CLS)
- Trunk Group Access Restrictions (TGAR)

CLS and TGAR work together to control specific trunk groups to which telephones, DISA directory numbers, TIE trunks, and Authorization Codes (Authcodes) have direct access. They determine whether users can make local, TIE, or long-distance calls over these trunks.

Class of Service

Class of Service (CLS) provides the flexibility to group telephones, DISA directory numbers, TIE trunks, and Authcodes. CLS assigns to these groups the calling privilege levels that suit the groups' communication needs. CLS can help protect the system from internal abuse by preventing internal users from placing unauthorized toll calls.

Assign any one of the following Classes of Service to each telephone, DISA directory number (DN), TIE trunk, and Authcode to control the degree of access to the exchange network:

- **Unrestricted Service (UNR)** – Allowed to originate and receive calls to and from the exchange network.
- **Conditionally Unrestricted (CUN)** – Allowed to receive calls from the exchange network. Toll-denied for calls placed using direct access to trunks, but unrestricted for toll calls placed through Automatic Number Identification (ANI).
- **Conditionally Toll-Denied (CTD)** – Allowed to receive calls from the exchange network. Toll-denied for calls placed using direct access to the Central Office (CO), Foreign Exchange (FEX), and two-way Direct Inward Dial (DID) trunks, but unrestricted for toll calls placed through Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS) using Network Class of Service (NCOS). CTD is most effective when used in conjunction with Trunk Group Access Restrictions (TGAR).
- **Toll-Denied Service (TLD)** – Allowed to receive calls from the exchange network and to dial local exchanges. Calling privileges of toll-denied telephones can be modified using Code Restriction (CRB) or New Flexible Code Restriction (NFCR) or Forced Charge Account (FCA) to allow or deny certain dialing sequences using direct trunk access.
- **Semi-Restricted Service (SRE)** – Allowed to receive calls from the exchange network. Restricted from dial access to the exchange network but allowed access to TIE trunks. Allowed to access the exchange network through an attendant or an unrestricted telephone.

- **Fully Restricted Service** – The following classes of Fully Restricted Service are available:
  - **FRE** – Allowed to originate and receive internal calls. Allowed access to TIE and Controlled Class of Service Allowed (CCSA) networks, and to and from the exchange network using call modification from an unrestricted telephone. Denied access, either through dialing or through the attendant, to and from the exchange network.
  - **FR1** – Allowed to originate and receive internal calls. Allowed access to TIE and CCSA networks. Denied access to and from the exchange network.
  - **FR2** – Allowed to originate and receive internal calls. Denied access to TIE and CCSA networks and to the exchange network.

Table 2 outlines various call types and shows whether they are possible for each CLS assignment.

Table 2
CLS assignment (Part 1 of 2)

	UNR	CTD/ CUN	TLD	SRE	FRE	FR1	FR2
Incoming trunk call	Yes	Yes	Yes	Yes	Yes using call modification	No	No
Outgoing non-toll trunk call	Yes	Yes	Yes	Yes using attendant or UNR telephone	Yes using UNR telephone	No	No
Outgoing toll trunk call (0 or 1+ on COT or FX)	Yes	Yes using BARS/ NARS No direct access	Yes using attendant or UNR telephone No direct access	Yes using attendant or UNR telephone No direct access	Yes using UNR telephone No direct access	No	No
To/from TIE trunk	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 2
CLS assignment (Part 2 of 2)

	UNR	CTD/ CUN	TLD	SRE	FRE	FR1	FR2
To/from internal	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BARS/ NARS calls TGAR=No	Uses NCOS only	Uses NCOS only	Uses NCOS and CLS	Uses NCOS and CLS	Uses NCOS and CLS	Uses NCOS and CLS	Uses NCOS and CLS
BARS/ NARS calls TGAR=Yes	Uses NCOS and TGAR	Uses NCOS and TGAR	Uses NCOS, CLS, and TGAR	Uses NCOS, CLS, and TGAR	Uses NCOS, CLS, and TGAR	Uses NCOS, CLS, and TGAR	Uses CLS only

Table 3 lists the facilities that can be implemented using CLS, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 3
Implementing CLS

Facility	Overlay and prompt	Print program
Telephones	LD 10/11 – CLS	LD 10/11 by TN LD 81 by CLS
Authcodes	LD 88 – CLS	LD 88 by Authcode
DISA	LD 24 – TGAR	LD 24 by DN

Trunk Group Access Restrictions

Trunk Group Access Restrictions (TGAR) control access to trunks that interface with the exchange network, TIE and CCSA networks, and services such as paging, dictation, and recorded announcements.

Telephones, DISA directory numbers, TIE trunks, and Authcodes are assigned to TGAR groups. When users attempt to access trunk routes from telephones, TIE trunks, or Authcodes, the system uses their TGAR assignment to check whether they can access that trunk. All trunks are assigned to a Trunk Access Restriction Group (TARG).

- If the TGAR assignment of the telephone, DISA directory number, TIE trunk, or Authcode is the same as the TARG assigned to the trunk, direct access is blocked.
- If TARG and TGAR do not match, or either assignment is set to 0, then access is allowed. If access is permitted, the system uses the CLS assignment to determine call eligibility. The system always uses the most restrictive assignment (CLS or TGAR) to determine call eligibility when users try to access trunk facilities directly.

Limiting trunk access prevents users from generating unnecessary toll charges. It also limits long-distance calling capabilities of virtual voicemail agents and data ports.

> ***Note:*** The BARS/NARS Least Cost Routing software eliminates the need for direct access to outbound facilities for long-distance calls. TGARs can be used in conjunction with BARS/NARS, if required. Refer to “Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS)” on page 78.

Table 4 lists the facilities that can be implemented using TGAR, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 4
Implementing TGAR

Facility	Overlay and prompt	Print program
Telephones	LD 10/11 – TGAR	LD 10/11 by TN
Authcodes	LD 88 – TGAR	LD 88 by Authcode
TIE Trunks	LD 14 – TGAR	LD 20 by TN
Trunk Groups (Route)	LD 16 – TARG	LD 21 by route, access code
DISA	LD 24 – TGAR	LD 24 by DN

Table 5 lists the TGAR Routing.

Table 5
TGAR Routing

Route number	Rank type
0	COT
1	WATS
2	FX 1
3	FX 2
4	TIE 1
5	TIE 2
6	Paging

In the example shown in Table 6, assume the seven TGAR codes shown are required:

Table 6
TGAR Access Restriction Codes

TGAR	Access denied to routes
0	No restrictions
1	0, 1, 2, 3,4 , 5, 6 (default = 1)
2	2, 3, 4,5
3	3, 4, 5
4	2, 6
5	3, 4, 5, 6
6	5, 6

Modifying basic access restrictions

Occasionally, the basic access restrictions that have been implemented must be changed. The following features can be used to override CLS and TGAR when it is necessary to extend the normal calling capabilities of a DISA directory number, telephone, or TIE trunk:

- Outgoing Call Barring (see page 37)
- System Speed Call (see page 38)
- Network Speed Call (see page 39)
- Authorization Code (see page 40)
- Forced Charge Account (see page 44)
- Controlled Class of Service (see page 45)
- Enhanced Controlled Class of Service (see page 46)
- Electronic Lock (see page 47)
- Code Restriction Data Block (see page 48)
- New Flexible Code Restriction (see page 49)
- Called Party Disconnect Control (see page 50)
- Scheduled Access Restrictions (see page 51)
- Trunk Barring (see page 61)

Outgoing Call Barring

When a telephone with Outgoing Call Barring activates Customer Call Forward (CCFW) and is active (CFWAC) with a new CFW DN, the CFW DN is tested against the current barring level. If the DN is not allowed to be dialed, it can also not be used as a Call Forward DN. This restriction prevents a telephone from forwarding to a barred DN and then dialing its own DN to bypass the restrictions.

Digits dialed after an Authorization Code are checked against the active Outgoing Call Barring level.

Table 7 lists the facilities that can be implemented using Outgoing Call Barring, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 7
Implementing Outgoing Call Barring

Facility	Overlay and prompt	Print program
Telephones	LD 10/11 - OCBA/OCBD	LD 10/11 by TN LD 20 by TN
Customer	LD 15 - OCBA/OCBD/OCBV	LD 21 by CDB
Flexible Feature Codes	LD 57 - OCBA/OCBD/OCBV	LD 57 by FFC Data

System Speed Call

System Speed Call (SSC) extends the capabilities of Speed Call. In addition to providing abbreviated dialing, using entries in SSC lists allows internal users to temporarily override the NCOS assigned to telephones and to place calls to telephone numbers in the SSC list. With this feature, the most appropriate NCOS can be assigned to a telephone to limit the potential for unauthorized calling, and at the same time allow calls to approved destinations.

Telephones can be assigned to different SSC lists. These telephones can also be designated as either System Speed Call Users (SSUs) or as System Speed Call Users/Controllers (SSCs) on the list. A user/controller can add or delete telephone numbers from the list. Controller capabilities must be assigned only as the job function dictates, in order to minimize abuse. Usually, only one controller is assigned to each SSC list.

List controlling capabilities can be assigned to a key on the attendant console. However, this key does not override CLS and TGAR because the attendant is not subject to these restrictions.

> ***Note:*** An SSC list can also override the telephone restrictions imposed through BARS/NARS. See "Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS)" on page 78.

Table 8 lists the facilities that can be implemented using SSC, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 8
Implementing SSC (Part 1 of 2)

Facility	Overlay and prompts	Print programs
Telephones	LD 10 - FTR	LD 10 by TN
	LD 11- SSU, KEY	LD 81 by SSU, SSC, KEY, LD 11 by TN
Flexible Feature Code	LD 57 - SSPU	LD 57 by FFC Data

Table 8
Implementing SSC (Part 2 of 2)

Facility	Overlay and prompts	Print programs
Speed Call List	LD 18 - SSC, all prompts	LD 20 by List Number
Attendant	LD 12 - KEY	LD 20 by TN

Network Speed Call

Network Speed Call (NSC) expands the SSC capabilities by allowing users to access the NSC feature from public and private networks. This enables users who are normally restricted from making certain types of BARS/NARS calls to make these calls if the destination is a company-approved number defined in an NSC list.

Use this feature in conjunction with a restricted DISA directory number. The incoming DISA caller can gain access to approved destinations using the NSC list. This feature helps prevent abuse by allowing calls to be placed only to destinations on NSC lists.

Table 9 lists facilities that can be implemented using NSC, programs and prompts to implement the feature, and programs to print information about the feature.

Table 9
Implementing NSC (Part 1 of 2)

Facility	Overlay and prompts	Print programs
Network translation	LD 90 -TYPE = NSCL all prompts	LD 90 by NSC Access Code
SSC	LD 18 - TYPE = SSC all prompts	LD 20 by SSC list
Network Control	LD 87 FEAT = NCTL NSC, LIST	LD 87 by NCTL
Authcode	LD 88 TYPE = AUT, CODE, CLAS	LD 88 by Authcode

Table 9
Implementing NSC (Part 2 of 2)

Facility	Overlay and prompts	Print programs
Telephones	LD 10 and LD 11 - NCOS	LD 10/11 by TN LD 81 by NCOS
Trunk	LD 14 - NCOS	LD 20 by TN
Customer	LD 15 - NCOS, FCNC, NET	LD 21 by NET
SSC list	LD 18 - NCOS	LD 20 by Speed Call List
DISA	LD 24 - NCOS	LD 24 by DISA directory number

Authorization Code

Authorization Codes (Authcodes) enable users to temporarily override access restrictions assigned to telephones, DISA directory numbers, or TIE trunks. A user enters an Authcode that has an associated CLS, TGAR, and BARS/ NARS NCOS. The user has the calling privileges of the Authcode rather than those of the DISA directory number, telephone, or TIE trunk for the duration of the call.

Authcodes allow users to place calls from normally restricted telephones. These restricted telephones can be located in areas of public access where authorization codes are required or can be used without authorization codes by employees who do not require broader calling privileges.

The system offers Station Specific Authcodes, which allows the administrator to define the authorization code access level for each telephone. To verify the validity of the code, the system checks LDs 10, 11, and 88. To delete an Authcode, the administrator must delete it from LDs 10, 11, and 88.

There are three levels of Authcode access:

1 **Authcode Unrestricted (AUTU)** — allows a telephone to enter any authorization code without additional restrictions.

2 **Authcode Restricted (AUTR)** — requires that the entered authorization code must match one of the preassigned authorization codes. Any other Authcode is treated as invalid and an error message is generated at the TTY.

3 **Authcode Denied (AUTD)** — does not accept Authcode entries from a telephone as AUTD.

Authcode Alarm

The system offers an Authorization Code Security feature enhancement that enables a user to temporarily override access restrictions assigned to a station or trunk because of their assigned Network Class of Service (NCOS), Class of Service (CLS), and Trunk Group Access Restrictions (TGAR) codes. If a user requires access to system facilities in addition to those allowed on the telephone, the Authcode feature can be used to provide them.

In addition, the Authorization Code (Authcode) Alarm feature alerts the technician when an invalid Authcode is entered, by generating an Authcode Alarm. The alarm indicates to the technician that an unauthorized person may be trying to use an Authcode to access the switch illegally.

The Authcode alarm is generated upon detection of violation of all Authcode-related features (such as Basic, Network, Station Specific Authorization code features, and Security Administration [SECA]), except for calls originated by the attendant. The SECA alarm distinguishes security violations from other types of system messages. System messages are printed on the TTY.

The Authcode Alarm feature does not apply to calls originated by an attendant.

The Authcode alarm feature is enabled through the Authcode Data Block LD 88.

LD 88 – Enable the Authcode alarm feature.

Prompt	Response	Description
REQ	NEW CHG	Add. Change.
TYPE	AUB	Authcode Data Block.
CUST	xx	Customer number as defined in LD 15.
SPWD	xxx	Secure data password.
ALEN	1-14	Number of digits in Authcode.
ACDR	(NO) YES	(Do not) activate CDR for authcodes.
AUTHCOD_ALRM	(OFF) ON	(Disable) enable Authcode Alarm.

LD 17 – Configure the Alarm Filter table as per existing configuration procedures. The Authcode Alarm must be configured in this table in order for the messages to be displayed on the FIL TTY.

Authcodes can be recorded as part of Call Detail Records so that call patterns can be observed and calls billed back to the appropriate department or person.

> ***Note:*** Authcodes can be used to override telephone restrictions imposed through BARS/NARS. See “Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS)” on page 78.

Table 10 lists the facilities that can be implemented using the Authcode feature, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 10
Implementing Authcode

Facility	Overlay and prompts	Print programs
Authcodes	LD 88 – all prompts	LD 88 by Authcode
Secure Data Password	LD 15 – SPWD, PWD2 and LD 88 – SPWD	LD 22 Passwords
Authcodes by telephone	LD 10/11 – CLS: (AUTU), AUTR, AUTD MAUT: YES/NO SPWD: (if MAUT=YES) AUTH: x nnnn	LD 10/11 by TNB
Authcodes by feature	LD 81 – FEAT: AUTU, AUTR, AUTD	LD 81 by FEAT
Authcode Alarm (see Note)	LD88 – AUTHCOD_ALRM and LD17 – AUTHCOD_ALRM	
Note: For security reasons, the SECA00001 alarm must not be configured in the Exception Filter table.		

Forced Charge Account

Forced Charge Account (FCA) temporarily overrides toll-denied CLS restrictions when users enter account codes before placing toll calls. Account codes allow users to have a customer-defined FCA Network Class of Service for the duration of calls.

Call Detail Recording outputs a charge record that identifies the charge account used for the call.

> ***Note:*** FCA can also be used to override restrictions imposed through BARS/NARS. See "Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS)" on page 78.

Table 11 lists the facilities that can be implemented using FCA, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 11
Implementing FCA

Facility	Overlay and prompts	Print programs
Customer	LD 15 - CHLN, FCAF, CHMN, FCNC, CDR	LD 21 by CDR
Telephones	LD 10/11 - CLS = TLD, FCAR	LD 10/11 by TN
TIE Trunks	LD 14 - CLS = TLD, FCAR	LD 20 by TN

Controlled Class of Service

Controlled Class of Service (CCOS) allows the following users to temporarily alter telephone CLS:

- users of digital telephones designated as controllers
- users of TTYs designated as Background Terminals

When a telephone is in the controlled mode, its CLS is derived from the CLS restriction level defined for each customer. This prevents internal abuse by reducing the CLS for telephones in vacant areas.

Users of digital telephones designated as controllers can place telephones in a controlled mode one at a time and Background Terminals can alter individual, group, or all designated telephones at one time.

Table 12 lists the facilities that can be implemented using the CCOS feature, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 12
Implementing CCOS

Facility	Overlay and prompts	Print programs
Customer	LD 15 - CCRS, CCOS	LD 21 by CCOS
Telephones to be controlled	LD 10/11 - CLS	LD 20 by TN
Telephones to be controllers	LD 11 - KEY	LD 20 by TN
Background Terminal	LD 17 - ADAN, USER	LD 22 by ADAN

Enhanced Controlled Class of Service

Enhanced Controlled Class of Service (ECCS) extends the controller function of CCOS to attendant consoles and M3000 terminals equipped with a Controller Key. It also allows for two additional customer-defined levels of CCOS restrictions. This helps to further control calling privileges of telephones in unsecured areas and helps prevent unauthorized access to toll calls.

Table 13 lists the facilities that can be implemented using the ECCS feature, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 13
Implementing ECCS

Facility	Overlay and prompts	Print programs
Customer	LD 15 – CCRS, ECC1, ECC2, CCOS	LD 21 by Data group
Telephones to be controlled	LD 10/11 – CLS	LD 10/11 by TN
Telephones to be controllers	LD 11 – KEY	LD 11 by TN
Attendants to be controllers	LD 12 - KEY	LD 20 by TN
Background Terminal	LD 17 - USER	LD 22 by Data group

Electronic Lock

Electronic Lock (ELK) allows users to activate and deactivate CCOS mode from their telephones by entering the Station Control Password (SCPW) and the appropriate ELK code.

Define the Station Control Password Length (SCPL) for each customer. If SCPL is set to 0, ELK and Remote Call Forward (RCFW) are disabled. Use a unique four- to six-digit password for each telephone.

Telephone users can activate ELK to prevent unauthorized calls from their telephones when they are not able to restrict physical access to these telephones. This is particularly useful for evenings, weekends, vacations, and holidays.

Table 14 lists the facilities that can be implemented using ELK, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 14
Implementing ELK

Facility	Overlay and prompts	Print programs
Customer	LD 15 - CCRS, SCPL, CCOS	LD 21 by Data group
Flexible Feature Code	LD 57 - FFCT, CODE, ELKA, ELKD	LD 57
Telephones	LD 10/11 - SCPW, CLS	LD 10/11 by TN

Code Restriction Data Block

Code Restriction Data Block (CRB) gives toll-denied telephones and TIE trunks limited access to the toll exchange network over CO and FEX trunks. For each CO and FEX trunk group, build a CRB that specifies the allowed area codes and/or exchange codes for toll-denied users accessing those facilities. This feature limits access to approved toll exchange networks and also limits the unauthorized use of toll facilities.

Table 15 lists the facilities that can be implemented using CRB, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 15
Implementing CRB

Facility	Overlay and prompts	Print programs
CRB	LD 19 all prompts	LD 21 by Route
Telephones	LD 10/11 - CLS = TLD	LD 81 by TLD LD 10/11 by TN

New Flexible Code Restriction

New Flexible Code Restriction (NFCR) enhances CRB by allowing toll-denied telephones, TIE trunks, and Authcodes to selectively make certain calls on outgoing trunk routes.

Assign toll-denied users a Network Class of Service (NCOS), and allow or deny calling privileges according to the Facility Restriction Level (FRL) of the NCOS.

Table 16 lists the facilities that can be implemented using NFCR, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 16
Implementing NFCR

Facility	Overlay and prompts	Print programs
Customer	LD 15 - NFCR, MAXT	LD 21 by NFCR
Network Control	LD 87 - NCOS, FRL	LD 87 by NCOS
NFCR Block	LD 49 - FCR all prompts	LD 49 by Table
Route	LD 16 - FRL	LD 21 by Route
Telephone	LD 10/11 - NCOS CLS=TLD	LD 10/11 by TN LD 81 by TLD, NCOS

Called Party Disconnect Control

Called Party Disconnect Control (CPDC) controls the disconnection of calls on CO, FEX, CCSA, DID, TIE, Wide Area Telephone Service (WATS), modem, and Central Automatic Message Accounting (CAMA) trunks.

Incoming trunk calls answered within the system are not disconnected until the called party hangs up. If the calling party hangs up, the connection is held allowing the call to be traced in emergency situations. If the calling party lifts the receiver again, the call is not reestablished.

CPDC prevents trunk-to-trunk transfers. A route assigned CPDC cannot be transferred to another route for outbound traffic.

Table 17 lists the facility that can be implemented using CPDC, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 17
Implementing CPDC

Facility	Overlay and prompts	Print programs
Trunk Group (Route)	LD 16 - CPDC	LD 21 by ROUT or ACOD

Scheduled Access Restrictions

The Scheduled Access Restrictions (SAR) feature allows a customer to define Trunk Group Access Restrictions (TGAR), Class of Service (CLS) restrictions, and Network Class of Service (NCOS) restrictions for different hours and days (typically off-hours and off-days).

These TGAR, CLS, and NCOS restrictions comprise SAR groups. Each customer can define up to 1000 SAR groups, and one of these groups can be assigned to each customer station or route. Up to eight time periods can be defined for each SAR group, and different restrictions can be applied to each time period.

SAR can be overridden on a single call basis for a station or route by using an authorization code or forced charge account. These restrictions can be changed on a more permanent basis by using the following Flexible Feature Codes (FFC):

- Scheduled Access Restrictions Disable (SARD)
- Scheduled Access Restrictions Enable (SARE)
- Scheduled Access Restrictions Lock (SARL)
- Scheduled Access Restrictions Unlock (SARU)

SARD returns the telephone/route to its normal restriction state. SARE cancels SARD, returning the telephone to its SAR state. SARL occurs automatically at a predefined period of time or when the Lock command is dialed by the user. Lock restrictions remain in effect until an SARU or SARD command is entered. The SARL command can be used on a customer basis or SAR group basis, depending on the Authcode used.

The Flexible Feature Codes can be used to do the following:

- extend off-hour restrictions for weekends or holidays (SARL)
- return to the schedule of access restrictions (SARU)
- extend normal restrictions into the off-hour period for after hour services (SARD)
- cancel after hour services (SARE)

- cause off-hour restrictions to start immediately (SARL followed by SARE)
- disallow any calls on an Attendant Console (SARL or SAR group containing the attendant(s).

Customer attendants that are included in SAR groups are placed in Position Busy when an off-hour or off-day period goes into effect. The restricted attendant can only release existing calls or dial the SAR Flexible Feature Codes. New calls cannot be made. Incoming calls are directed to any other attendants that are not included in SAR groups and that are not in Position Busy.

If the system is placed in Night Service by an attendant, or the system is automatically placed in Night Service because all attendants are in the Position Busy state, incoming calls are routed to the Night DN. Going into Night Service automatically places attendants who belong to a SAR group into SAR Locked and Enabled state. These attendants can only release existing calls or dial the SAR Flexible Feature codes; they cannot make new calls when restricted by SAR.

Operating parameters

The definition of authorization codes for SAR decreases the number of authorization codes available for non-SAR use.

SAR does not apply to Direct Inward System Access (DISA) DNs. DISA can be used to manually modify the SAR schedule using an FFC authorization code.

Telephones and trunks assigned to SAR groups have their Class of Service (CLS), Trunk Group Access Restriction (TGAR), and Network Class of Service (NCOS) defined by the SAR schedule of their SAR group.

During the periods that a SAR or SAR lock is in effect, the Controlled Class of Service (CCOS) for the station or trunk is overridden.

If a Facility Restriction Level (FRL) is changed in order to be associated with a different New Flexible Code Restriction (NFCR) tree, the NCOS using that FRL is affected. Also, different FRLs and, therefore, different NFCR trees are used at different times according to the NCOS assigned to the SAR group.

Feature interactions

The Scheduled Access Restrictions (SAR) feature has the following feature interactions:

- Basic Automatic Route Selection (BARS)

  If SAR is equipped when BARS is set up, an NCOS value between 0 and 99 must be defined for each time period.

- Coordinated Dialing Plan (CDP)

  If SAR is equipped when CDP is set up, an NCOS value between 0 and 99 must be defined for each time period.

- Call Detail Recording (CDR)

  If configured, CDR A-type records are printed for SAR Flexible Feature Code functions.

- Network Alternate Route Selection (NARS)

  If SAR is equipped when NARS is set up, an NCOS value between 0 and 99 must be defined for each time period.

- Speed Call and Network Speed Call

  The System Speed Call and Network Speed Call features ignore the Class of Service and TGAR access restrictions in a SAR schedule, using the Class of Service and NCOS defined in the Speed Call List.

- Office Data Administration System (ODAS)

  ODAS can be used to indicate that telephones have been assigned to a SAR group. ODAS must be equipped in order to print members of a SAR group in LD 81.

- Controlled Class of Service (CCOS)

  If SAR is active, it overrides CCOS whether activated by a controller or Electronic Lock.

- Multi-Tenant Service

  If a SAR is assigned to a tenant, any telephone belonging to the tenant follows this SAR schedule unless the telephone belongs to a SAR group. The telephone's Scheduled Access Restrictions override any SAR assigned to the tenant.

Feature packaging

This feature requires Scheduled Access Restrictions (SAR) package 162. SAR package 162 also requires the following:

- Flexible Feature Codes (FFC) package 139 and Basic Authorization Code (BAUT) package 25 add capability for manual modification of the schedules.
- Call Detail Recording (CDR) package 4, must be equipped if CDR is required.
- Network Class of Service (NCOS) package 32 must be equipped to make NCOS restrictions effective.
- Charge Account for CDR (CHG) package 23, Charge Account/ Authorization Code Base (CAB) package 24, and Forced Charge Account (FCA) package 52, can be equipped for additional billing information.

The following packages are also required:

- — Network Authorization Code (NAUT) package 63
- — Multi-Tenant Service (TENS) package 86

Feature implementation

LD 88 – Create or modify Schedule Access Restrictions. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW CHG	Add, or change.
TYPE	SAR	Scheduled Access Restrictions.
CUST	xx	Customer number as defined in LD 15.
SPWD	xxxx	Secure data password (same password as defined for DISA on a per-customer basis in LD 15). ***Note:*** The SPWD prompt does not appear to a user with an LAO password.
SGRP	0-999	SAR group number.
SCDR	(NO) YES	(Do not) activate CDR for the SAR FFC commands.
OFFP	1-8	Off-hour period number. Off-hour periods can overlap; the period that starts first has priority until that off-hour period is over.
	<cr>	Go to ICR prompt.
- STAR hh mm	hh mm	Start time. The current start time (hours and minutes) is printed individually after the prompt. Respond with the new start time.
	X	Remove value and return to OFFP prompt.
-STOP hh mm	hh mm	Stop time. The current stop time (hours and minutes) is printed individually after the prompt. Respond with the new stop time.

LD 88 – Create or modify Schedule Access Restrictions. (Part 2 of 2)

Prompt	Response	Description
	X	Remove value and return to OFFP prompt.
- DAYS	d...d	Respond with a new set of days to be used. Maximum of seven entries in the range of 1-7. For example, Day 1 = Sunday, Day 2 = Monday.
- COS		Off-hour period Class of Service.
	(UNR)	Unrestricted
	CTD	Conditionally Toll-Denied
	CUN	Conditionally Unrestricted
	FR1	Fully Restricted Class 1
	FR2	Fully Restricted Class 2
	FRE	Fully Restricted
	SRE	Semi-restricted
	TLD	Toll Denied
- TGAR	(0)-15	Trunk Group Access Restriction.
- NCOS	0-99	Network Class of Service.
- ICR	(NO) YES	Incoming Calls are Restricted.
LOCK	(1)-8	Lock period.

LD 88 – If the system is in an off-hour or locked period when a print command is issued, an asterisk appears following the restrictions being used. If lock is in effect, an additional asterisk appears following the lock prompt. The print command allows tenant number to be entered. The status of a tenant SAR group can be printed.

LD 88 – Print command.

Prompt	Response	Description
REQ	PRT	Print.
TYPE	SAR	Scheduled Access Restrictions.
CUST	xx	Customer number as defined in LD 15.
SPWD	xxxx	Secure data password.
SGRP	0-999	Prompted only if no tenant number is entered.

LD 88 – With SAR, configure the Authcode data block not to automatically generate Authcodes. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	New.
TYPE	AUB	Authcode data block.
CUST	xx	Customer number as defined in LD 15.
SPWD	xxxx	Secure data password (same password as defined for DISA on a per-customer basis in LD 15).
ALEN	1-14	Number of digits in Authcodes.
ACDR	YES NO	Activate CDR for Authcodes (there is no default response).

LD 88 – With SAR, configure the Authcode data block not to automatically generate Authcodes. (Part 2 of 2)

Prompt	Response	Description
RANR		RAN route number for "Authcode Last" prompt (NAUT).
	0-511	Range for Large System and CS 1000E system.
	0-127	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T
	x	Response for CS 1000M Small System.
CLAS	(0)-115	Classcode value assigned to Authcode.
AUTO	NO	Do not automatically generate Authcodes. The AUTO prompt appears when NAUT package 63 is equipped and REQ = NEW. The Authcode length must be a minimum of four digits.

LD 88 – Define SAR entries in the Authcode entries data block. (Part 1 of 2).

Prompt	Response	Description
REQ	NEW CHG	Add, or change.
TYPE	AUT	Authcode entries data block.
CUST	xx	Customer number as defined in LD 15.
SPWD	xxxx	Secure data password (same password as defined for DISA on a per-customer basis in LD 15).
CODE	xxxx...	Authcode (1-14 digits).

LD 88 – Define SAR entries in the Authcode entries data block. (Part 2 of 2).

Prompt	Response	Description
SARC	YES NO	Allow or deny Authcode to be used as the Scheduled Access Restriction (SAR) authorization code.
- SERV		SAR service functions for SARC (the SERV prompt appears if SARC = YES).
	(END) ENA	Enable (Denied) Allowed.
	(LKD) LKA	Lock (Denied) Allowed.
	(DSD) DSA	Disable (Denied) Allowed.
	(UND) UNA	Unlock (Denied) Allowed.
		Up to four entries can be made at once.
- SRGP	0-999	Number of SAR group to be defined or changed.
	ALL	Change all SAR groups.
CLAS	(0)-115	Class code value assigned to Authcode. Cycle continues with CODE.
		When type = AUT, enter X to configure the Authcode as an exempt code. When this data is printed, the month the Authcode was deactivated is output. The default is 0 when adding Authcode entries.
	X	Exempt Authcode.

LD 10 – For individual analog (500/2500-type) telephones, respond to the SGRP prompt with the SAR group number (0-999).

LD 11 – For individual display phones, or digital telephones, respond to the SCRP prompt with SAR group number (0-999).

LD 12 – For individual Attendant Consoles, respond to the SGRP prompt with the SAR group number (0-999).

LD 16 – For individual trunk routes, respond to the SGRP prompt with the SAR group number (0-999).

LD 57 – To define Flexible Feature Codes for the SAR disable, SAR enable, SAR lock, and SAR unlock functions, respond to the SADS, SAEN, SALK, and SAUN prompts, respectively, with the appropriate FFCs.

LD 93 – For a tenant, respond to the TYPE prompt with TGEN, Respond to the CUST prompt with the customer number. Respond to the TEN prompt with the tenant number. Respond to the SGRP prompt with the number of the SAR group to be assigned to the tenant.

Feature operation

Use Flexible Feature Codes to apply Scheduled Access Restrictions, as described earlier in this feature description.

Trunk Barring

The Trunk Barring feature provides the option of denying or allowing a direct or modified connection between customer-defined routes.

Trunk Barring works in conjunction with Route Access Restriction Tables (ARTs) defined in LD 16. Trunk Barring is applied on a route basis. Table 18 shows the four route categories that Trunk Barring recognizes, and the types of routes in each category.

Table 18
Trunk Barring route categories

Route category	Route types
Central Office Trunk (COT)	COT, FEX, WAT
Direct Inward Dialing	DID, DOD
TIE	ATVN, TIE, CAA, CAM, CSA
Other trunk types	ADM, AID, DIC, MDM, PAG, RCD

Operating parameters

When activated in conjunction with the Route Access Restriction Tables, Trunk Barring can prohibit previously allowed connections. Previously restricted connections cannot be lifted or circumvented by Trunk Barring.

Trunk Barring applies to all methods of connecting the trunks (for example, dialing route access, call modification, attendant extension). However, it does not apply to RAN, Music, AWU, or CAS trunks as it is inconsistent with their defined purpose.

Feature interactions

The Trunk Barring feature has the following feature interactions.

Access Restrictions

Trunk Barring is at the top of the hierarchy for access restrictions.

Attendant-extended calls

When an attendant attempts to extend an Originating Trunk Connection on a barred route, overflow tone is given.

Call Transfer

The originator of a call transfer, unless otherwise restricted, is able to connect to a denied party on a consultation basis. Operating the Transfer key on a Business Communication Set (BCS) telephone or going on hook on an analog (500/2500-type) telephone does not result in a call transfer if the Originating Trunk Connection is barred. The user of a BCS telephone remains connected to the denied party until releasing the connection and returning to the held Originating Trunk Connection. The user of an analog (500/2500-type) telephone is rerung by the Originating Trunk connection when a transfer is attempted and denied.

Call Forwarding

If an Originating Trunk Connection is forwarded to a barred route, it receives the intercept treatment specified in the customer data block.

Conference Calls

The originator of a conference call can connect to a barred route only on a consultation basis. A switchhook flash from an analog (500/2500-type) telephone results in a reestablished connection with the Originating Trunk Connection. The use of a BCS telephone must release the barred connection to return to the Originating Trunk connection or the conference containing the Originating Trunk connection; operating the Conference key on a BCS telephone has no effect. An attendant can return to the Originating Trunk Connection or the conference containing the Originating Trunk Connection by releasing the barred connection. This is done by pressing the RLS DEST key; pressing the Conference key has no effect.

Intercept Treatment/Direct Trunk Access

When an Originating Trunk Connection (OTC) attempts a trunk connection to a route that is restricted by its Access Restricted Table, the connection is not allowed. The intercept treatment specified in the customer data block is applied.

Enhanced Night Service

Any incoming trunk call that is routed by Enhanced Night Service to a telephone from which it is barred is not connected. Overflow tone (fast busy) is given to the incoming trunk instead.

Any incoming trunk call that is routed to an outgoing Public Network trunk is barred if Enhanced Night Service is active. Overflow tone (fast busy) is given to the incoming trunk instead. This restriction is in addition to the configured trunk barring for the system.

Toll Operator Break In

Trunk Barring results in intercept treatment for all route types that can be barred except Toll Operator Break In.

Feature packaging

This feature requires Trunk Barring (TBAR) package 132.

Feature implementation

In most cases that require barring, only one Access Restriction Table (ART) is necessary. When a new route is created (in LD 16), the default ART defined for that route type is assigned to the route. Use LD 56 to change the ART associated with a route or to handle other nondefault conditions.

LD 56 – Enter or change Trunk Barring parameters. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW CHG	Add or change Trunk Barring parameters.
TYPE	TBAR	Add or change Access Restriction Tables (s) (ARTs).
-ART	1-63	Select ART to add or change.
-DENY	yyy yyy	ART numbers denied originating trunk connection (OTC).
	ALL	Deny all ARTs to OTC.
	Xyyy Xyyy	ART numbers allowed to OTC.
TYPE	RART	Change ART number for the route.
-CUST	xx	Customer number as defined in LD 15.
-ROUT		Route number
	0-511	Range for Large System and CS 1000E system.
	0-127	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T.
-ART	0-63	ART to assign to route.
TYPE	RCDT	Change the route category default table.

LD 56 – Enter or change Trunk Barring parameters. (Part 2 of 2)

Prompt	Response	Description
-COT	(0)-63	COT,FEX, and WAT routes are assigned the entered number.
-DID	(0)-63	DID and DOD routes are assigned the entered number.
-TIE	(0)-63	ATVN, CAA, CAM, CSA, and TIE routes are assigned the entered number.
OTH	(0)-63	ADM, AID, DIC, MDM, PAG, and RCD routes are assigned the entered number.

Feature operation

No specific operating procedures are required to use this feature.

System Access Enhancements

System Access Enhancements (SAE) improve the Operations, Administration, and Maintenance (OA&M) for System Security and Toll Fraud prevention.

These enhancements strengthen the system security through changes to the following:

- Default Class of Service (CLS) (see page 67)
- Default Trunk Group Access Restriction (TGAR) and Trunk Access Restriction Group number (TARG) (see page 68)
- Call Forward Default Length and Range (see page 68)
- Security Banner at System Login (see page 69)
- Number of Invalid Attempts to LAPW Password in Overlays (Failed Login Attempt Threshold) (see page 69)
- PWD2/PWD1/LAPW Passwords and LAPW Login names (see page 70)
- Problems Determination Tool (PDT) Access Information (see page 70)

Default Class of Service (CLS)

System Access Enhancements provide highly restricted access by defaulting the Class of Service (CLS) to Conditionally Toll Denied (CTD) for all newly configured data. This Class of Service requires users to go through the Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS) to complete a call. Therefore, the possibility of unauthorized toll calls through the system is reduced.

Class of Service (CLS) is defaulted to Conditionally Toll Denied (CTD) in the following Overlays:

- LD 10 – Analog (500/2500-type) Telephone Administration
- LD 11 – Meridian Digital Telephone Administration
- LD 14 – Trunk Data Block (only TIE, CSA, ATVN, FGD, and IDA trunk types default to CLS of CTD)
- LD 16 – Route Data Block, Automatic Trunk Maintenance
- LD 24 – Direct Inward System Access
- LD 27 – ISDN Basic Rate Interface (BRI) Administration (only TIE trunk type defaults to Class of Service (CLS) of Conditionally Toll Denied (CTD))
- LD 88 – Authorization Code

The existing System Access functionality is not impacted by this default change.

Default Trunk Group Access Restriction (TGAR) and Trunk Access Restriction Group number (TARG)

The defaults for Trunk Group Access Restriction (TGAR) and Trunk Access Restriction Group number (TARG) were previously “0”. This provided unrestricted toll access after CLS had been checked. System Access Enhancements, however, change the default TGAR and TARG to “1” in order to automatically block direct access. TGAR is changed from “0” to “1” for the following Overlays:

- LD 10 – Analog (500/2500-type) Telephone Administration
- LD 11 – Meridian Digital Telephone Administration
- LD 14 – Trunk Data Block
- LD 24 – Direct Inward System Access
- LD 27 – ISDN Basic Rate Interface (BRI) Administration
- LD 88 – Authorization Code

TARG is changed from “0” to “1” in LD 16 – Route Data Block, Automatic Trunk Maintenance.

The existing System Access functionality is not impacted by this enhancement.

Call Forward Default Length and Range

System Access Enhancements lengthens the Call Forward Directory Number to any number of digits in the range of 4-23. The feature also changes the default length to four digits. The Call Forward All Calls/Internal Call Forward (CFW/ICF) feature functionality is modified to have not more than a single CFW/ICF key for a telephone.

Security Banner at System Login

System Access Enhancements (SAE) allow users the option of printing a security banner after login is attempted. To configure this option, the BANR prompt is set to “YES” in LD 17. When BANR is “YES”, a security banner, advising unauthorized users not to attempt login, is printed.

Failed Login Attempt Threshold

Based on the existing implementation of system login, when the Limited Access Password (LAPW) package 164 is equipped, the System Access Enhancements (SAE) strengthens the system security. This is accomplished by limiting the maximum number of invalid login attempts and by performing termination and lock if the number of invalid system password attempts exceeds the defined threshold.

With SAE, in the following overlays, the maximum number of invalid login attempts is limited to the value of the Failed Login Attempt Threshold (FLTH), defined in LD 17:

- LD 15 - Customer Data Block
- LD 17 - Configuration Record 1
- LD 21 - Print Routine 2
- LD 22 - Print Routine 3
- LD 97 - Configuration Record 2

When the number of invalid attempts exceeds the Failed Login Attempt Threshold (FLTH) value, the overlay access is terminated and the current TTY is locked for the LOCK duration, as defined in LD 17.

PWD2/PWD1/LAPW Passwords and LAPW Login names

PWD2, PWD1, and all LAPW passwords were previously stored contiguously in an unencrypted format. With this enhancement, security of PWD2, PWD1, and LAPW usages (if LAPW package 164 is enabled) is enforced by storing contiguously the above system passwords in an encrypted format. By storing passwords in an encrypted format, the random dumping of memory addresses is prevented from revealing passwords.

Problems Determination Tool (PDT) Access Information

System Access Enhancements (SAE) improves the Problems Determination Tool (PDT) by providing a reporting facility for recording this information. Records for valid login, invalid login, logout, PDT initialization, and PDT reboot are produced in a PDT access log file. This file is viewed by both PDT Level 2 and PDT Level 1 users by the new PDT command, RDAACCESS.

Using system management features

The System and Network Management program updates and improves Operations, Administration, and Maintenance (OA&M). Optivity Telephony Manager (OTM) is a Graphical User Interface (GUI) provided to perform a number of system administration functions.

Element Manager is a simple and user-friendly web-based interface that supports a broad range of system management tasks, including:

- configuration and maintenance of IP Peer and IP telephony features
- configuration and maintenance of traditional routes and trunks
- configuration and maintenance of numbering plans
- configuration of Call Server data blocks (such as configuration data, customer data, Common Equipment data, D-channels)
- maintenance commands, system status inquiries, backup and restore functions
- software download, patch download, patch activation

Element Manager has many features to help administrators manage systems with greater efficiency. Examples are as follows:

- Web pages provide a single point-of-access to parameters that were traditionally available through multiple overlays.
- Parameters are presented in logical groups to increase ease-of-use and speed-of-access.
- The “hide or show information” option enables administrators to see information that relates directly to the task at hand.
- Full-text descriptions of parameters and acronyms help administrators reduce configuration errors.
- Configuration screens offer pre-selected defaults, drop-down lists, check boxes, and range values to simplify response selection.

The Element Manager web server resides on the Signaling Server and can be accessed directly through a web browser or Optivity Telephony Manager (OTM). The OTM navigator includes integrated links to each network system and their respective instances of Element Manager.

Controlling Call Forward access

Call Forward All Calls (CFW) allows users who are going to be away from their desks to forward their calls to another telephone or location.

This feature is abused when telephones are forwarded to either long-distance telephone numbers or Trunk Access Codes, then off-site callers dial the DID extension numbers of these telephones. With the introduction of Remote Call Forward (RCFW), CFW can be abused by forwarding calls to a remote telephone if proper controls are not in place. The following features can help reduce the abuse of Call Forwarding:

- User Selectable Call Redirection (see page 72)
- Call Forward External Deny (see page 73)
- Internal Call Forward (see page 74)
- Call Forward All Calls (see page 75)
- Call Forward to Trunk Access Code (see page 75)
- Call Forward Originating or Forwarded Class of Service (see page 76)
- Remote Call Forward (see page 77)

User Selectable Call Redirection

User Selectable Call Redirection (USCR) allows a user to select the destination for Call Forward No Answer, Busy Hunt, External Call Forward No Answer, and External Hunt. USCR is controlled by Flexible Feature Code, Special Prefix Code, and/or a user key on the multi-line telephone. To use this feature, a Station Control Password is required to prevent abuse.

Since users can direct their calls to external numbers with this feature, this feature must be assigned very selectively to only those users who require the ability to control busy and no answer direction. Unique Station Control Passwords for each telephone are recommended.

Table 19 lists the facilities that can be implemented using USCR, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 19
Implementing USCR

Facility	Overlay and prompts	Print programs
Telephone	LD 10/11 - SETS, SCPW, CLS, USRA, KEY, USR	LD 10, LD 11 by TN or DN LD 22 by DN
Customer	LD 15 - CDB, SPCL, FFCS	LD 21 by CUST or by CFW
Flexible Feature Codes	LD 57 - CODE: USCR, USCR: XXXX	LD 57 by CODE LD 81 by CODE

Call Forward External Deny

Call Forward External Deny (CFXD) restricts call forward from a telephone to an external number, thus preventing unauthorized users from placing external calls.

The default value for this feature is Call Forward External Deny (CFXD).

Table 20 lists the facility that can be implemented using CFXD, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 20
Implementing CFXD

Facility	Overlay and prompts	Print programs
Telephone	LD 10/11 - CLS, CFXD	LD 10/11 by TN LD 81 by CFXA, CFXD

Internal Call Forward

Internal Call Forward (ICF) directs all internal calls to a specified location different from the call forward destination of external calls. An internal call is one of the following:

- a station call
- a DISA call
- a group call
- a call designated as internal over a trunk route
- an incoming trunk call using private numbering
- an attendant originated call

To prevent users from call forwarding their telephones to BARS/NARS access codes or trunk access codes and receiving a second dial tone when looping through private networks or accessing the system through DISA when ICF is active, you must disable Call Forward to Trunk Access Codes and Call Forward External must be denied.

Table 21 lists the facilities that can be implemented using ICF, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 21
Implementing ICF

Facility	Overlay and prompts	Print programs
Telephone	LD 10/11 - FTR, KEY, ICF	LD 10,11 by TN LD 81 by ICF
Customer	LD 15 - CFTA	LD 20 by CFW
Flexible Feature Codes	LD 57 - ICFA, ICFD, ICFV	LD 57 by CODE

Call Forward All Calls

Call Forward All Calls (CFW) allows users to forward all calls manually to an external or internal number. To call forward to an external telephone using the CFW feature, Call Forward External Allowed must be enabled on a telephone-by-telephone basis.

The default for CFW is 16 digits, allowing most international calls. However, telephones not requiring external call forward must be restricted to four digits to prevent abuse. Phones permitted external Call Forward must be limited to eight digits.

Table 22 lists the facility that can be implemented using CFW, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 22
Implementing CFW

Facility	Overlay and prompts	Print programs
Telephone	LD 10/11 - CFW	LD 10/11 by TN LD 81 by CFW

Call Forward to Trunk Access Code

Call Forward to Trunk Access Code (CFTA) restricts DID calls from being forwarded to a Trunk Access Code. This prevents incoming calls from being rerouted to trunking facilities through the system.

Trunk Access Codes must be a minimum of four (six if DN expansion is equipped) digits in length. CFW must be restricted to a smaller number of digits than the number of digits in the Trunk Access Code.

Post-dialing capabilities can be performed with AC1/AC2 but not with ACOD.

Table 23 on page 76 lists the facilities that can be implemented using CFTA, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 23
Implementing CFTA

Facility	Overlay and prompts	Print programs
Customer	LD 15 - CFTA	LD 21 by CUST
Route	LD 16 - ACOD	LD 21 by Route
Telephone	LD 10/11 - CFW4	LD 10/11 by TN

Call Forward Originating or Forwarded Class of Service

Call Forward Originating (CFO) or Forwarded Class of Service (CFF) uses the CLS access privileges of the telephone or trunk that originates the call or the telephone that forwards the call. By using the CLS that originates the call and prohibiting that source from making external calls, calls are prevented from being forwarded to an external telephone.

This feature is frequently used in restricting the capabilities of DID trunks in forwarding situations.

Table 24 lists the facilities that can be implemented using CFO or CFF, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 24
Implementing CFO or CFF

Facility	Overlay and prompts	Print programs
Customer	LD 15 – OPT = CFF or CFO CFW	LD 21 by CUST or CFW
Trunk	LD 14 – CLS	LD 20 by TN
Telephone	LD 10/11 – CLS	LD 10/11 by TN

Remote Call Forward

Remote Call Forward (RCFW) allows users to activate and deactivate call forwarding from remote telephones. Users enter codes to activate and deactivate the feature, and must also enter a telephone-specific password. This capability is given to users as required.

Table 25 lists the facilities that can be implemented using RCFW, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 25
Implementing RCFW

Facility	Overlay and prompts	Print programs
Customer	LD 15 - SCPL, FFC	LD 21 by FFC
Flexible Feature Code	LD 57 - CODE, RCFA, RCFD, RCFV	LD 57 by FFC
Telephone	LD 10/11 - SCPW, CFW	LD 10/11 by TN

Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS)

Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS) routes outgoing calls over the least expensive facility available at the time the user places a call. Use BARS/NARS features to prevent calls to a specific area code or exchange or to international locations. The following features restrict calling privileges for BARS/NARS:

- North American Numbering Plan (see page 78)
- Supplemental Digit Recognition/Restriction (see page 79)
- Network Class of Service and Facility Restriction Level (see page 80)
- Authorization Code Conditionally Last (see page 82)
- Time-of-Day Routing (see page 83)
- Routing Control (see page 84)
- Incoming Trunk Group Exclusion (see page 85)
- Free Calling Area Screening (see page 86)

North American Numbering Plan

The North American Numbering Plan (NANP) governs the telephone numbering system throughout Bermuda, Canada, the Caribbean, and the United States. Two components of the NANP are Interchangeable Numbering Plan Areas (INPAs) and Carrier Access Codes (CACs). NPAs are the three-digit prefixes commonly known as area codes. CACs permit telephone users to access any interexchange carrier or operator service provider. CACs must be supported by any entity, such as a hotel, motel, hospital, university, airport, gas station, or pay telephone owner, that makes telephone services available to the public.

Table 26 lists the facilities that can be implemented using North American Numbering Plan, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 26
Implementing NANP

Facility	Overlay and prompts	Print programs
Customer	LD 15 - HPNA	LD 21 by NET
Route	LD 16 - NPA	LD 21 by RDB
Code Restriction	LD 19 - NPA	LD 19 by FGD or ANI
ESN	LD 87 - NPA	LD 87 by REQ
	LD 90 - NPA, HNPA	LD 90 by REQ

Supplemental Digit Recognition/Restriction

Supplemental Digit Recognition causes the system to recognize dialing sequences associated with internal calls to prevent callers from using two trunks to complete an internal call. Internal telephones dial the BARS/NARS access code followed by the public telephone number of another internal telephone. This feature prevents callers from using outgoing COT and incoming DID trunks for internal calls by recognizing predefined dialing sequences.

Supplemental Digit Restriction blocks calls to certain telephone numbers within exchanges, area codes, or country codes. This allows calls to be blocked to prefixes typically associated with pay-per-call, such as 976.

Table 27 lists the facilities that can be implemented using Supplemental Digit Recognition/Restriction (SDRR), the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 27
Implementing SDRR

Facility	Overlay and prompts	Print programs
ESN	LD 86 - MXSD	LD 86 by FEAT = ESN
Network translation	LD 90 - DENY, LDID, LDDD	LD 90 by NPA, NXX or SPN

Network Class of Service and Facility Restriction Level

Network Class of Service (NCOS) determines calling privileges for telephones, TIE trunks, DISA directory numbers, and Authcodes for outgoing calls that use BARS/NARS. With NCOS, a Facility Restriction Level (FRL) from 0 to 7 can be assigned to determine access to a route. The FRL of the calling party must be equal to or greater than the FRL of the Route List entry in order to complete the call.

BARS/NARS can be configured to ignore or to use TGARs. When TGARs are ignored, BARS/NARS assesses the NCOS and the FRL to determine which call facilities are available for a particular call. This configuration allows flexibility in using a given trunk group while forcing users to place calls over less expensive facilities. Trunk availability for each call can be based on the FRL requirements for the number dialed rather than basing it on the TGAR assigned to the calling telephone.

BARS/NARS can be configured to include TGAR assignments in determining how the system can route a call. In this case, NCOS, TGAR, CLS, and FRL are used to determine which call facilities are available to process a particular call.

Table 28 lists the facilities restrictions that can be implemented using NCOS and FRL, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 28
Implementing NCOS and FRL

Facility	Overlay and prompts	Print programs
Network Control	LD 87 - FEAT = NCTL all prompts	LD 87 FEAT = NCTL by NCOS
Route List Index	LD 86 - FEAT = RLB FRL	LD 86 FEAT = RLB by Route List
Authcode	LD 88 - TYPE = AUT CODE, NCOS	LD 88 TYPE = AUT by Authcode
Telephones	LD 10 and LD 11 - NCOS	LD 10/11 by TN LD 81 by NCOS
Trunk	LD 14 - NCOS	LD 20 by TN
Customer	LD 15 - NET	LD 21 by NET
SSC list	LD 18 - NCOS	LD 20 by SCL
DISA	LD 24 - NCOS	LD 24 by DISA directory number

Network Authorization Codes

Network Authorization Codes (NAUT) can be configured to prompt users who fail to meet the minimum FRL requirement to enter an Authcode to complete a call. This control provides another level of security by requiring all callers placing calls to international locations or selected area codes, for example, to enter an Authcode.

Table 29 lists the facilities that can be implemented using NAUT, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 29
Implementing NAUT

Facility	Overlay and prompts	Print programs
Route List Index	LD 86 - FEAT = RLB, MFRL	LD 86 FEAT = RLB by Route List Index
Network Control	LD 87 - FEAT = NCTL, NCOS, FRL	LD 87 by NCOS
Authcode	LD 88 - TYPE = AUT, CODE, NCOS, RANR	LD 88 TYPE = AUT by Authcode
Telephones	LD 10 and LD 11 - NCOS	LD 10/11 by TN LD 81 by NCOS
Trunk	LD 14 - NCOS	LD 20 by TN
Customer	LD 15 - NET	LD 21 by NET
SSC list	LD 18 - NCOS	LD 20 by SCL
DISA	LD 24 - NCOS	LD 24 by DISA directory number

Time-of-Day Routing

Each entry in a route list is assigned to a Time of Day (TOD) schedule that specifies the hours that a particular entry can be accessed.

With this feature, employees can be restricted from calling locations they have no need to call for business purposes at certain hours. Because the majority of toll-fraud calls occur on holidays or after normal business hours, use this feature to deny access to routes supporting calls to international locations or to the 809 area code after hours.

Table 30 lists the facilities that can be implemented using TOD, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 30
Implementing TOD

Facility	Overlay and prompts	Print programs
ESN	LD 86 - FEAT = ESN, TODS	LD 86 FEAT = ESN
Route List Index	LD 86 - FEAT = RLB, TOD	LD 86 FEAT = RLB by Route List Index

Routing Control

Routing Control (RTCL) uses Time of Day (TOD) schedule 7 as an alternate TOD to modify a user’s network access capabilities automatically for a defined time frame each day and/or on weekends. In addition, a key can also be assigned on the attendant console that manually activates/deactivates RTCL.

Activating this feature prevents people from accessing unattended telephones after hours to place unauthorized calls. However, Authcodes are not subject to the alternate NCOS assignments imposed through RTCL. When users enter valid Authcodes, they are provided with the Network Classes of Service assigned to the Authcodes for the duration of the call.

Table 31 lists the facilities that can be implemented using RTCL, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 31
Implementing RTCL

Facility	Overlay and prompts	Print programs
ESN	LD 87 - FEAT = ESN, TODS 7, RTCL, NMAP, ETOD	LD 87 FEAT = ESN
Attendant	LD 12 - KEY = RTC	LD 20 by TN
Network Control	LD 87 - FEAT = NCTL NCOS	LD 87 by NCOS
Telephones	LD 10 and LD 11 - NCOS	LD 10/11 by TN
		LD 81 by NCOS
Trunk	LD 14 - NCOS	LD 20 by TN
Customer	LD 15 - NET	LD 21 by NET

Incoming Trunk Group Exclusion

Incoming Trunk Group Exclusion (ITGE) blocks network calls originating on TIE trunks from reaching certain destinations. Each TIE route is associated with a table that defines the dialing sequences allowed for calls originated on that TIE route.

ITGE prevents users from calling locations they do not need to reach for business purposes and keeps them from attempting to circumvent restrictions that are imposed at their local system. ITGE also helps prohibit a technique called "looping" that hackers use to cover their tracks when accessing a network for toll-fraud purposes.

Table 32 lists the facilities that can be implemented using ITGE, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 32
Implementing ITGE

Facility	Overlay and prompts	Print programs
ESN	LD 86 - FEAT = ESN, MXIX	LD 87 FEAT = ESN
ITGE	LD 86 - FEAT = ITGE all prompts	LD 86 FEAT = ITGE by ITGE Index
Network translation	LD 90 - FEAT = NET ITED, ITEI	LD 90 FEAT = NET by NPA, NXX, SPN, or LOC

Free Calling Area Screening

Free Calling Area Screening (FCAS) provides full six-digit screening to determine the route choice for completion of off-net calls. With FCAS, calls are allowed to certain area codes and restricted from other area codes within the free calling area surrounding a particular on-net location.

FCAS tables define the NPA codes and NXX codes used to screen calls. Each table is referenced by an FCI number that is assigned to a route; 0 indicates that the FCAS feature is not enabled for that route.

Table 33 lists the facilities that can be implemented using FCAS, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 33
Implementing FCAS

Facility	Overlay and prompts	Print programs
Route List Index	LD 86 - FCI	LD 88 FEAT = RLB by Route List Index
Free Calling Area Screening	LD87 - FCAS (allow, deny)	LD 87 - FEAT = FCAS
FNP		
Truncated CDR		

Controlling Direct Inward System Access

Direct Inward System Access (DISA) allows employees, when they are off-site, to place calls to internal extensions and to private and public network locations through the company system. Access to the system DISA feature is usually through dedicated trunks such as 1-800 service CO trunks. These trunks can be programmed to auto-terminate at a DISA directory number. DISA is not recommended for DID trunks.

Table 34 lists the facilities that can be implemented using DISA, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 34
Implementing DISA

Facility	Overlay and prompts	Print programs
Customer Data Block	LD 15 - SPWD	LD 21 by SDP, PWD2
DISA directory number	LD 24 - SPWD, DN, SCOD, AUTR, TGAR, NCOS, COS	LD 24 by DISA Block

A DISA directory number must be restricted by Authcodes and Security codes to protect access to the system. DISA can also be controlled using a combination of Routing Control (RTCL) and NCOS assignments to limit the weekend and evening access to this feature. Assigning unique NCOS levels to either the DISA directory number or Authcodes used by DISA reduces the access capability of the NCOS by lowering it to a more restricted level using RTCL. Refer to “Routing Control” on page 84 for configuration details.

To help prevent unauthorized persons from using DISA features, activate the following:

- Security Code (see page 88)
- Authorization Code (see page 88)
- Service restrictions (see page 89)

These features can be used alone or in combination with each other to provide the level of security that is necessary for that telecommunications facility.

Security Code

The system can be programmed to require a Security Code (SCOD) so that, when the system answers a DISA call, the caller must enter the SCOD assigned to the DISA directory number before gaining access to the system. This SCOD can be from 1 to 8 digits in length. The SCOD can be used in conjunction with an Authcode if desired.

Table 35 lists the facility that can be implemented using the SCOD feature, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 35
Implementing SCOD

Facility	Overlay and prompts	Print programs
DISA directory number	LD 24 - SCOD	LD 24 - DISA Block

Authorization Code

DISA callers can be required to enter an Authorization Code (Authcode) before they can gain access to system facilities. Assign Authcodes that are from 1 to 14 digits in length.

If DISA is not configured to require an Authcode, then users can still enter such a code by dialing SPRE + 6 followed by a valid Authcode. Either way, users take on the CLS, TGAR, and NCOS assigned to the Authcode entered. Users' calling capabilities are then based on the service restrictions assigned to the Authcode. Authcodes can be used in conjunction with Security Codes.

Refer to "Authorization Code" on page 40 for information about how to assign Authcodes to DISA.

Service restrictions

A CLS, TGAR, and NCOS can be assigned to a DISA directory number to restrict access through DISA. When the system accepts calls without requiring callers to enter Authcodes, they automatically receive the assigned DISA directory number calling privileges.

Refer to “Class of Service” on page 30, “Trunk Group Access Restrictions” on page 33, and “Network Class of Service and Facility Restriction Level” on page 80 for information about assigning these restrictions to the DISA directory number.

Controlling Multi-Tenant Services

Multi-Tenant Services (TENS) allow a customer to divide its services and resources into subgroups known as tenants. Access to tenants, attendant consoles, and trunk routes can be configured so that tenants have private use of some facilities, share some facilities, or are denied access to other facilities. All tenants share the numbering plan and features of the customer. TENS must be protected with security features to help prevent unauthorized use of these facilities. Restrictions must be implemented to control:

- Tenant-to-tenant access (see page 90)
- Tenant-to-route access (see page 90)
- Console Presentation Group assignment (see page 91)

Tenant-to-Tenant Access

A tenant's relationship with other tenants of the same customer is defined by Tenant-to-Tenant Access (TACC). A tenant can be configured to allow direct internal call access to some or all tenants of the same customer. Likewise, a tenant can be denied direct access to other tenants.

Table 36 lists the facility that can be implemented using TACC, the programs and prompts to implement them, and the programs to print information about the feature.

Table 36
Implementing TACC

Facility	Overlay and prompts	Print programs
Tenant-to-tenant access	LD 93 - TACC	LD 93 Define Tenant-to-Tenant access

Tenant-to-Route Access

Each customer can have a maximum of 128 trunk routes. Each tenant can share or have private access to any or all of these routes. Tenant-to-Route Access (RACC) applies only to outgoing calls.

Table 37 lists the facility that can be implemented using RACC, the programs and prompts used to implement them, and the programs to print information about the feature.

Table 37
Implementing RACC

Facility	Overlay and prompts	Print programs
Tenant-to-Route access	LD 93 - RACC	LD 93 Define Tenant-to-Route access

Console Presentation Group (CPG) assignment

Attendant consoles are placed into Console Presentation Groups (CPGs) that are associated with specific tenants and specific incoming trunk routes. The CPG range is from 0 to 63. All attendant consoles configured for a customer are automatically members of CPG 0. Other CPGs are defined to fit tenant requirements using the configuration program.

Table 38 lists the facility that can be implemented using CPG, the programs and prompts used to implement them, and the programs to print information about the feature.

Table 38
Implementing CPG

Facility	Overlay and prompts	Print programs
Console Presentation Group	LD 93 - CPG, NIT1 to NIT4	LD 93 CPG

Securing terminals

Contents

This section contains information on the following topics:

Introduction

This chapter describes measures that you can take to improve terminal security by encrypting traffic. The following two types of security are discussed:

- Secure UNIStim signaling
- Media security

While both of these options allow you to use encryption to protect the network, they serve two different purposes: Secure UNIStim signalling protects data exchanges between the IP Phones and the Signalling Server, while Media security protects the media stream between two IP Phones.

Secure UNISTIM signaling

Secure UNIStim signalling is designed to provide a means of encrypting data exchanges between the Signalling Server and the IP phones.

UNIStim signaling security is provided by the transparent UNIStim security proxy within the Secure Media Controller (SMC). Secure UNIStim signaling enables UNIStim IP phones to communicate with insecure UNIStim servers in a protected fashion, with encryption terminated at the SMC before the unencrypted traffic is passed to the back-end server.

To use UNIStim signaling security, you must have an SMC installed in the system. The SMC also allows you to create multimedia security zones (Secure Multimedia Zones (SMZ)), which protect the voice network from outside traffic. For more information about SMC, including accessing the CLI, see *Secure Multimedia Controller - Implementation Guide* (553-3001-225).

Media security

The SRTP feature is designed to provide a means of encrypting media exchanges between two phones.

Protecting the media stream using SRTP (PSK)

SRTP (Pre-Shared Key (PSK)) does not require call server support, and therefore is useful for telephony environments where the installed call server software does not offer SRTP support.

To use this feature, SRTP (PSK) must be supported on each telephone in a call, and you must enable it on each telephone using the manual configuration menu. For more information about enabling or disabling SRTP (PSK), see *IP Phones: Description, Installation, and Operation* (553-3001-368).

System security features verification

Contents

This section contains information on the following topics:

Introduction

This chapter describes how to verify that system security is operating properly after it is implemented in the system and Meridian Mail. It provides general **guidelines** to verify those system security features that most impact the telecommunications facilities. However, customers are encouraged to use their own system configuration scenarios to verify if their security features have been implemented correctly and are effective.

The most effective method of checking the security of the system is performing the following procedures:

- Verify system security features using the checklist.
- Verify Call Forward access restrictions.
- Verify DISA access restrictions.
- Verify BARS/NARS access restrictions.
- Verify administration program access restrictions.
- Verify Thru-dial restrictions for mailboxes and menus.

Verify system security features using the checklist

To make sure that the required system security has been correctly implemented, compare the system printouts after security features have been implemented with the appropriate checklist for the new or existing system security.

New system security verification

The security installation checklist is used together with new system configuration planning to properly coordinate system security features with the creation of the customer configuration database. Security features selected on this checklist must have been implemented using the system administration overlays.

Verify that all security features selected on the security installation checklist have been implemented by comparing new system printouts against the checklist.

Existing system security verification

The security audit checklist is used to check existing system security features and to specify changes to features that must be upgraded. Any security feature selected for upgrade on this checklist must have been implemented using system configuration programs.

Verify that all security features that were added or selected for upgrade on the security audit checklist have been implemented by comparing the new system printouts against the checklist.

Verify Call Forward access restrictions

Verify the operation of the following Call Forward access restrictions:

- Call Forward External Deny
- Call Forward to Trunk Access Code

Call Forward External (CFXA/D)

To verify the operation of this feature:

- Place an external call to a telephone forwarded to an external number and specified as CFXA. The call should go through.
- Place an external call to a telephone forwarded to an external number and specified as CFXD. The call should not go through.

Call Forward to Trunk Access Code (CFTA)

To verify the operation of this feature:

- Forward a telephone with a DID number to a Trunk Access Code. The telephone should be TGAR 0 or allow direct access to external trunking facilities. Call Forward must be set to a number larger than the ACOD. If CFTA in the customer data block is set to **Yes**, the call should go through.
- Forward the same telephone to the same Trunk Access Code. If CFTA in the customer data block is set to **No**, the call should not go through.

Verify DISA access restrictions

Depending on how security features are implemented for DISA calls, choose one of the following tests:

- DISA access using basic restrictions
- DISA access using a Security Code
- DISA access using an Authorization Code

DISA access using basic restrictions

To verify the operation of this security feature:

- Place a long-distance call to a DISA number whose NCOS/TGAR/FRL allows long-distance calling. The call should go through.
- Place a long-distance call to a DISA number whose NCOS/TGAR/FRL does not allow long-distance calling. The call should not go through.

DISA access using a Security Code (SCOD)

To verify the operation of this security feature:

- Place a long-distance call using an SCOD from a DISA number whose NCOS/TGAR/FRL allows DISA calling. The call should go through.
- Place a long-distance call using an SCOD from a DISA number whose NCOS/TGAR/FRL does not allow DISA calling. The call should not go through.

DISA access using an Authcode

To verify the operation of this security feature:

- Place a non-international long-distance DISA call using an Authcode allowed to access long-distance but not international calls. The call should go through if it is not an international call.
- Place an international long-distance DISA call using an Authcode allowed to access long distance but not international calls. The call should not go through.

Verify BARS/NARS access restrictions

The system provides many security features to prevent unauthorized BARS/NARS access. The most important of these features must be verified for proper operation. They are:

- Supplemental Digit Recognition/Restriction
- NCOS/FRL access restriction
- Authorization Code Conditionally Last
- Time-of-Day Routing
- Routing Control
- Incoming TIE Trunk Group Exclusion

Supplemental Digit Recognition/Restriction (SDRR)

To verify the operation of this security feature:

- Place a call to an internal telephone dialing the AC1/AC2 and full 7-digit public telephone number. The unnecessary digits are stripped and the extension number is used to reach the destination. The call should go through.
- Place a long-distance 976 call from a telephone to an area code denying 976 dialing. The call should not go through.

NCOS/FRL access restrictions

To verify the operation of this security feature:

- Place a call from a telephone by dialing the BARS/NARS access code. If the FRL of the telephone is equal to or greater than the minimum required FRL for the BARS/NARS trunk group, the call should go through.
- Place a call from a telephone by dialing the BARS/NARS access code. If the FRL of the telephone is less than the minimum required FRL for the BARS/NARS trunk group, the call should not go through.

- Place a call from a TIE trunk using an Authcode. If the FRL of the Authcode is equal to or greater than the minimum required FRL for the BARS/NARS trunk group, the call should go through.
- Place a call from a TIE trunk using an Authcode. If the FRL of the Authcode is less than the minimum required FRL for the BARS/NARS trunk group, the call should not go through.

Authorization Code Conditionally Last (NAUT)

To verify the operation of this feature:

- Place a toll call using a telephone that meets minimum FRL requirements for a route list. The call should go through without a request for an Authcode.
- Place a toll call using a telephone that does not meet minimum FRL requirements for a route list. The user should hear a tone or recorded message requesting that an Authcode be entered to complete the call.

Time-of-Day Routing (TOD)

To verify the operation of this feature:

- Place a call during regular business hours to a destination that is restricted during off hours. The call should go through.
- Place a call after regular business hours to a destination that is restricted during off hours. The call should not go through.

Routing Control (RTCL)

To verify the operation of this feature:

- Place a call during regular business hours from a telephone with a specified NCOS/FRL able to access WATS and CO trunks during normal business hours. The call should go through.
- Place a call from the same telephone after RTCL goes into effect. The call should not go through.

Incoming TIE Trunk Exclusion (ITGE)

To verify the operation of this feature:

- Place a call from a remote location by directly accessing a TIE route; dial a number that is not restricted in the remote PBX's translation table and in the local system's ITGE table. The call should go through.
- Place a call from a remote location by directly accessing a TIE route; dial a number that is restricted in the remote PBX's translation table and in the local system's ITGE table. The call should not go through.

Verify administration program access restrictions

To verify system and Application Processor administration passwords and user IDs, perform the following tests:

- Verify administration passwords.
- Verify Application Processor User ID.

Administration passwords

To verify the operation of this feature:

- Log on to the system console using the Level 1 password, access LD 17, and try to change the Level 2 password. The program should prompt for the Level 2 password, thus restricting access to the password change privilege.
- Log on to the system console using the Limited Access account and access LD 17. LD 17 should not load if the password is configured to restrict access to LD 17.
- Try to log on to the system console using an invalid password until the threshold value is reached. The port should lock out and the other maintenance TTYs on the system should receive a message detailing the logon attempts. Log on to another port using the Level 2 password. A special message should be displayed regarding invalid logon attempts. Access the Audit File to verify that there is a history of invalid logon attempts.

Application Processor User ID

To verify the operation of this feature:

- Log on to the Application Processor console using a valid Level 4 user ID. It should be possible to log on and run applications. However, it should not be possible to modify, install, or remove an application using this user ID.
- Log on to the Application Processor using the other three levels of user IDs and verify that the features accessible to each user ID can actually be accessed and those restricted cannot be accessed.
- Log on to the Application Processor console using an invalid user ID. It will not be possible to log on. Try to log on using an invalid user ID until the system refuses to display the logon prompt. The number of permitted unsuccessful logons can be set. This number is usually set at 3.

Verify Thru-dial restrictions for mailboxes and menus

To verify Meridian Mail security features, perform the following tests:

- Verify Thru-dial restrictions.
- Verify Thru-dial to Voice menus.
- Verify Express Messaging.
- Verify Outcalling.
- Verify Operator Revert.
- Verify Automated Attendant.

Thru-dial restrictions

To verify the operation of this feature:

- Place a call to a telephone that performs a Forward No Answer to Meridian Mail. When Meridian Mail answers, dial 0 followed by an extension number or an access code and telephone number that is permitted to Thru-dial followed by the # sign. The call should go through.
- Place a call to a telephone that performs a Forward No Answer to Meridian Mail. When Meridian Mail answers, dial 0 followed by an extension number or an access code and telephone number that is restricted to Thru-dial followed by the # sign. The call should not go through.

Thru-dial to Voice menus

To verify the operation of this feature:

- Using the **Voice Security Option** screen, specify the permission/ restriction table to define the numbers allowed to be accessed and those restricted from access.
- Dial 0 followed by an extension number or an access code and telephone number that is permitted to Thru-dial followed by the # sign. The call should go through.
- Dial 0 followed by an extension number or an access code and a telephone number that is restricted to Thru-dial followed by the # sign. The call should not go through.

Express Messaging

To verify the operation of this feature:

- Set a permission/restriction table for Meridian Mail access using the express messaging feature.
- Dial a number that is permitted to access Meridian Mail directly. The access should be direct and it should not be necessary to dial a user's directory number.
- Dial a number that is not permitted to access Meridian Mail directly. To access Meridian Mail, it is necessary to dial a user's directory number and then be forwarded to Meridian Mail.

Outcalling

To verify the operation of this feature:

- Define where the messages should be sent for non-user telephones.
- Access the Meridian Mail mailbox and enter the SEND command. Meridian Mail should dial the non-user telephone and deliver the messages when it detects voice, or when the non-user presses 2 if prompted.
- Listen to the message, record a reply, and forward it to the sender. The reply should automatically be deposited in the sender's mailbox.

Operator Revert

To verify the operation of this feature:

- Using the **Modify User** screen, define permission/restriction tables to specify an Operator Revert DN for each mailbox.
- Access a mailbox. Activate the Operator Revert feature, if configured for that mailbox, by dialing 0 while listening to the greeting or after leaving a message. The call is automatically forwarded to the predetermined Operator Revert DN.

Automated Attendant

To verify the operation of this feature:

- Define a permission/restriction table for DISA or self-terminating numbers that are allowed or denied access to the automated attendant.
- Dial a DISA or a self-terminating call to the automated attendant. If the number dialed is allowed, the call should be forwarded by the automated attendant; if the number is denied, the call terminates at the automated attendant.

Verify SRTP (PSK)

To verify the operation of SRTP (Pre-Shared Key (PSK)):

- Using a telephone that has the feature enabled, dial the DN of another phone that also has the feature enabled.
- A lock icon (🔒) appears on the display of both phones if the call is successfully encrypted.

Controlling OA&M access

Contents

This section contains information on the following topics:

Overview

Unauthorized access to programs can make the system vulnerable to abuse and performance degradation or failure. Administration programs (overlays) are used to configure the customer database and conduct day-to-day routine system administration functions.

Strict security must be implemented to help prevent unauthorized system access. This is accomplished with:

- Password management (see page 113)
- Program access control (see page 131)
- Audit Trail review (see page 133)
- History File review (see page 134)

CS 1000 Release 4.5 introduces OA&M security enhancements. OA&M security enhancements improve the security of the system access of the Call Server, Signaling Server, and Voice Gateway Media Card.

The following are OA&M security enhancements:

- encoding overlay, administration, and debugging passwords
- detecting and locking out external login attempts directed at cracking system passwords
- miscellaneous enhancements, such as Password Complexity Checking, and Force Password Change
- synchronizing passwords
- standardizing passwords
- Shell access control utility

Security enhancements are also in an improved CS 1000 Element Manager interface.

For further information on security enhancements in CS 1000 Element Manager, refer to "Security diagnostic commands in CS 1000 Element Manager", on page 143.

System passwords

Two modes of operation in the Call Server are system OAM (PWD) and Problem Determination Tool (PDT). Each mode provides two types of system passwords, which enable access to various database configuration and maintenance programs. Table 39 shows the system passwords.

> ***Note:*** Use digits from 0 to 9 and alphabetic characters A through Z to form a password. Passwords are case-sensitive.

The OA&M modes are:

- PWD Level 1 user ID and password (PWD1)
- PWD Level 2 user ID and password (PWD2)

The PDT modes are:

- PDT Level 1 user ID and password (PDT1)
- PDT Level 2 user ID and password (PDT2)

Table 39
System passwords (Part 1 of 2)

	Passwords		
User	**Call Server**	**Signaling Server**	**Voice Gateway Media Card**
ADMIN 1: PWD1	Default password (set by the system)	Synchronized from the Call Server	Synchronized from the Call Server
ADMIN 2: PWD2	Default password (set by the system)	Synchronized from the Call Server	Synchronized from the Call Server
PDT Level 1	Default password (set by the system)	Not applicable	Not applicable

Table 39
System passwords (Part 2 of 2)

	Passwords		
User	**Call Server**	**Signaling Server**	**Voice Gateway Media Card**
PDT Level 2	Default password (set by the system)	Synchronized from the Call Server	Synchronized from the Call Server
LAPW	Default password (set by the system)	Not applicable	Not applicable
IP Phone Installer Password	Not applicable	No default password	No default password

The Call Server's Level 1 password (PWD1), Level 2 password (PWD2), and PDT Level 2 password (PDT2) become the system passwords for the Signaling Server and Voice Gateway Media Card. This change occurs when the Signaling Server and Voice Gateway Media Cards communicate directly with the Call Server and synchronize their passwords with the Call Server.

IMPORTANT!

Passwords or account changes made on the Call Server are not distributed or made permanent until the user performs a datadump (EDD). When a user upgrades to CS 1000 Release 4.5 or later, the system goes through account conversion, which is not made permanent until the user performs a datadump (EDD) at which time the accounts are distributed to all the attached devices.

Level 1 password

The administrator can use the Level 1 password to log on to the system to change the configuration database. Level 1 passwords cannot change Level 1 passwords, Level 2 passwords, or the secure data password associated with assigning Authorization Codes (Authcodes) and DISA parameters (if defined). Refer to LD 17 on page 140 to create or change a PWD1 password. To print all accounts, or to display all accounts with insecure passwords or expired passwords, refer to LD 22 on page 141.

Level 2 password

The Level 2 password provides all privileges of the Level 1 password, as well provides the ability to administer accounts. Refer to LD 17 on page 140 to create or change a Level 1, Level 2, and LAPW passwords. To print all accounts, or to display all accounts with insecure passwords or expired passwords, refer to LD 22 on page 141.

Limited Access Password (LAPW)

When accessing the system using a Limited Access Password, the Limited Access to Overlays feature can be configured to require a user name to be entered with up to 11 alphanumeric characters. The user name can be configured only by the administrator using the Level 2 password.

Password management

Proper password selection and frequent password changes provide an important safeguard against unauthorized system access. The following features enhance password security:

- Default Password Change — enhances the security of the system
- Password complexity checking — applies complexity criteria to a new password

Default Password Change

The Default Password Change feature enhances security of the system (including the Call Server, Signaling Server, and Voice Gateway Media Card) by forcing the user to change their system passwords.

The Default Password Change feature provides the following:

- A default password security warning message is provided to a user whenever the user logs in to a system and the system passwords are at predefined default values.

- A Force Password Change (FPC) prompt activated through LD 17 or through Element Manager is available to force the system passwords to be changed. For further information on activating FPC, see “Force Password Change (FPC) prompts”, on page 117 and “Security features in Element Manager”, on page 146.

IMPORTANT!

Nortel recommends that the default passwords be changed. The Default Password Change feature is used to enhance the security of a system by providing a default system password warning message and a Force Password Change (FPC) prompt.

Default Password Change applies to the following system passwords:

- PWD1
- PWD1
- PDT1
- PDT2
- Limited Access Password (LAPW)

  Note: Default Password Change does not apply to the IP Phone Installers Passwords. These passwords are assigned by a system administrator, and the system gives no default values.

Feature requirements

The Default Password Change feature requires the Limited Access Password (LAPW) package 164.

Warning message for default passwords

The five system user passwords (PWD1, PWD2, PDT1, PDT2, and LAPW) are set to predefined default values. To increase system security, a general security warning is displayed when a PWD (PWD1 or PWD2), PDT (PDT1 or PDT2), or an LAPW user logs in. The warning message is displayed if any of the five passwords is at the default value. The security warnings are also displayed if a system password is changed from a non-default value back to a default value.

The warning message is:

```
SEC0029 SECURITY WARNING: THIS SYSTEM CONTAINS
INSECURE PASSWORDS. NOTIFY THE SYSTEM ADMINISTRATOR.
```

An `SEC0029` message is also generated to record the event of the warning message. The `SEC0029` message is recorded in the log file and in a Simple Network Management Protocol (SNMP) trap. The location of the log file is c:/u/rpt/rpt.log.

Feature functionality

When a user logs in with a stale password, the user receives a warning message that their password needs to be changed. The user is prompted to change their password. If the user clicks Yes, the password change process is initiated so long as the user has the ability to change their password.

Example of PWD1 and PWD2 users

The following example illustrates a user's attempt to access the Call Server with a password that is at the default value and all the system passwords are in a stale condition.

```
logi
USERID? ADMIN2
PASS?

WARNING: THE PROGRAMS AND DATA STORED ON THIS SYSTEM
ARE LICENSED TO OR ARE THE PROPERTY OF NORTEL NETWORKS
AND ARE LAWFULLY AVAILABLE ONLY TO AUTHORIZED USERS FOR
APPROVED PURPOSES. UNAUTHORIZED ACCESS TO ANY PROGRAM
OR DATA ON THIS SYSTEM IS NOT PERMITTED. THIS SYSTEM
MAY BE MONITORED AT ANY TIME FOR OPERATIONAL REASONS.
THEREFORE, IF YOU ARE NOT AN AUTHORIZED USER, DO NOT
ATTEMPT TO LOGIN.

SEC0029 SECURITY WARNING: THIS SYSTEM CONTAINS
INSECURE PASSWORDS. NOTIFY YOUR SYSTEM ADMINISTRATOR.

PASSWORD(S) MUST BE CHANGED.
DO YOU WANT TO CONTINUE (Y/N)? [N]
```

If the user enters **N** (for No [default]), the user is automatically logged out of the system.

If the user enters **Y** (for Yes), the user is prompted to enter the new Level 1 and new Level 2 passwords.

```
PWD
PSWD_COMP
LOUT
FLTH
LOCK
FLTA
AUDT
LLID
INIT
REQ
...
```

IMPORTANT!

Passwords must be 4 to 16 alphanumeric characters in length.

If you change the PWD1, PWD2, PDT1, or PDT2 login name or password, they you must perform a datadump (EDD) to synchronize the new login name and password with the Signaling Server and Voice Gateway Media Cards. Otherwise, the new login name and password are synchronized when the PBX link goes down and is reestablished.

Example of PDT1 and PDT2 users

If a PDT user logs in with a stale password, the user is prompted to change the password.

The following example illustrates a Level 2 user login sequence.

```
PDT: login on /sio/0
Password:

The software and data stored on this system are the
property of, or licensed to Nortel Networks and are
lawfully available only to authorized users for
approved purposes. Unauthorized access to any software
```

```
or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not any
authorized user, then log out immediately. This system
may be monitored for operational purposes at any time.

Your password has expired. To login you must change
your password of have your System Administrator change
your password.

**Changing PDT passwords

Enter old PDT Level 2 password:
```

Force Password Change (FPC) prompts

During a new system installation or a system upgrade, a system installer can configure the FPC prompt to YES in LD 17 (for TYPE = PWD) and perform a datadump (EDD) in LD 43 before logging out of the system. As a result, the customer receiving the system gets the system with the predefined default passwords; however, the customer must change the passwords before using the system.

> ***Note 1:*** The FPC = YES value is not retained in the database and must be set to YES each time you want to force a change.

> ***Note 2:*** Setting FPC = YES must be done only by the Level 2 user.

By setting the FPC = YES, the passwords become stale. Users trying to access the system are warned about their expired passwords and are asked to change the passwords. The user is warned that the user IDs and passwords are still at the default values and the user is required to change them. If the users do not change their user identifications and passwords, they are denied access to the system.

Warning message for Force Password Change

When FPC = YES, a warning message is prompted to the user.

The warning message is:

```
WARNING: PASSWORDS HAVE TO BE CHANGED ON NEXT LOGIN
```

An SRPT195 message is also generated to record the event of the warning message. The SRPT195 message is recorded in the log file (c:/u/rpt/rpt.log) and in an SNMP trap.

The format of the SRPT195 message is:

```
SRPT195 Force Password Change Activated
```

Example

The following ia an example of the SRPT195 event log.

```
pdt> rdtail

RPT: ...rd : 95 new reports arrived since last command
RPT: ...rd : showing 16 records up to the newest record
(rec 435)
...

435 :(1/4/04 16:13:13.570) SRPT195 FORCE PASSWORD
CHANGE ACTIVATED
```

Problem Determination Tool (PDT) access

This section provides information about how to change, reset, or override PDT passwords, and provides an explanation of System Report messages for PDT.

Password Reset Mechanism

For CS 1000 Release 4.5, the Password Reset Mechanism for CP PIV, CS 1000S, Meridian 1 PBX 11C Cabinet, and Meridian 1 PBX 11C Chassis is introduced. On the Call Server, log in using the PDT2 account. Place the system in password override mode and enter one of the following commands:

- `resetPWD` (to reset PDT2 and Admin2 passwords to default)
- `resetACCT` (to set the accounts to default users and default passwords)

Placing the system in Password Override mode

Choose one of the following:

- To put a Large System into the PDT2 password reset mode, you must insert an install disk in the floppy drive. On a CP PII system, you must use the drive on the active side. On a CP PIV system, a faceplate Compact Flash is required.
- To put a Small System into the PDT2 password reset mode, use the Small System Controller (SSC) faceplate DIP switch. Turn on the switch that corresponds to the next baud rate lower than is currently activated, and do not turn off the current switch. The two switches directly beside each other on the faceplate will be on.

  Note: Ensure that only two switches are on at any one time. Turning three or more switches on causes an invalid condition, and communication with the switch halts.

CAUTION
As soon as the PDT2 password reset mode is no longer required, remove the install tool floppy disk (Large Systems), or return faceplate DIP switches to the original position (Small Systems). If a warm or cold restart occurs while the system is in the password reset mode, large switches can boot up in install mode. A Small System can boot up in an error state. If this occurs, remove the install tool floppy disk (Large Systems) or reset the faceplate DIP switches to the original position (Small Systems) and perform an INI.

Changing the passwords

After you have placed the system in Password Override Mode (the disk is inserted, or the DIP switch is turned on), use one of the following:

- Procedure 1 to reset the passwords for all systems except CP PIV.
- Procedure 2 to reset the passwords on CP PIV.
- Procedure 3 to override the passwords.
- Procedure 4 to change the passwords when you know the old password.

Procedure 1
Using the Password Reset Mechanism

1 At the PDT prompt, type `resetPWD`.

The following message appears:

```
Warning: All attempts to use the Password Reset
Mechanism are logged. In order to proceed, you will
need physical access to the Call Server.
```

Note: If the installation disk is present in the CF2 drive, the Password Reset Mechanism cannot start and the following message appears:

```
There is an installation flash card present in the
CF2: Drive CF2. Drive must be empty to start the
Password Reset Mechanism. Remove any media in the
CF2: Drive and restart the procedure.
Password Reset Mechanism failed.

Invalid Login Attempt. Try again.
```

2 Ensure the CF2: Drive CF2 is empty. Press **<Enter>**.

The following message appears:

```
You have 60 seconds to put some media into the CF2:
Drive and press ENTER:
Checking the drive, please wait…
```

If a disk is detected in the drive, the following message appears:

```
/cf2/  - Volume is OK
```

3 Enter the new PDT2 password.

The password is checked against existing password rules.

4 Reenter the new PDT2 password.

The following message appears:

```
### New PWD2 account (newuser) created with
    specific password.

### PDT2 password successfully changed.

### Perform EDD to synchronize passwords to all
    elements.

**************************************************
```

```
REMINDER: Remove any media in the CF2: Drive and
          replace the backup media if necessary.

*************************************************
```

Note: For CS 1000 Release 4.5, only PWD2 and PDT2 passwords are affected by the Password Reset Mechanism.

End of Procedure

Use Procedure 2 to reset the passwords on a CP PIV.

Procedure 2
Using the Password Reset Mechanism on CP PIV

1 If a Compact Flash card is inserted in the faceplate, remove it.

2 Log in to PDT. When prompted for the password, enter `resetPWD`

The following message appears:

```
Warning: All attempts to use the Password Reset
Mechanism are logged. In order to proceed, you will
need physical access to the Call Server.
```

Note: If a Compact Flash card is present, the Password Reset Mechanism cannot start and the following message appears:

```
There is an installation flash card present in the
CF2: Drive CF2. Drive must be empty to start the
Password Reset Mechanism. Remove any media in the
CF2: Drive and restart the procedure.
Password Reset Mechanism failed.
```

3 Choose one of the following:

- If you do not wish to continue, enter the word QUIT,
- To continue, enter the following:

```
PDW2/Admin2 userID:  admin2
```

The following message appears:

```
You have 60 seconds to put some media into the CF2:
Drive and press ENTER:
Checking the drive, please wait…
```

If a disk is detected in the drive, the following message appears:

```
/cf2/  - Volume is OK
```

4 Enter the new PWD2 password.

5 Reenter the new PWD2 password to confirm.

6 Enter the new PDT2 password.

7 Reenter the new PDT2 password.

The following message appears:

```
### PWD2 password successfully changed.

### PDT2 password successfully changed.

### Perform EDD to synchronize passwords to all
   elements.

**************************************************

REMINDER: Don't forget to remove any media in the
          CF2: Drive and replace the backup media if
          necessary.

**************************************************
```

End of Procedure

Use Procedure 3 to override the PDT passwords.

Procedure 3
Overriding the PDT passwords

1 Log in to PDT. When prompted for the password, choose one of the following:

- Large Systems: use the site ID (LD 22 TID) as the password.
- Small Systems, use the security ID as the password.
- For the CPP PIV, enter resetPWD as the password.

2 At the PDT prompt, type `passwd`.

3 When prompted for the current Level 2 password, enter the tape ID. For the Small System, enter the security ID. For the CP PIV, use resetPWD. PDT passwords are case-sensitive, must be 6 to 16 characters in length, and the Level 1 and Level 2 passwords must be different.

To accept a password without changing it, press the **<Enter>** key when prompted to enter a new password.

4 Enter the new Level 2 and Level 1 PDT passwords when prompted.

5 For Large System, remove the install tool floppy disk.
For Small Systems, restore the DIP switch for the password reset mode to the off position.

6 Exit PDT.

7 Verify the passwords by entering PDT with the current passwords.

End of Procedure

Changing the PDT password if the existing password is known

For CPP machines
Passwords can be changed only on the active side when the system is joined. If the system is split, the passwords on either side can be changed. However, when the system is joined, the active side overwrites the inactive-side PDT passwords with the active-side PDT passwords.

For Small Systems with IP Expansion
The PDT passwords can be modified only on the main cabinet. All expansion cabinets use the main cabinet's PDT passwords.

Use Procedure 4 to change one or both of the PDT passwords.

Procedure 4
Changing one or both PDT passwords

1 Log in to PDT using the current Level 2 password.

Note: If the Force Password Change (FPC) flag has been changed to YES in LD 17 (see “Force Password Change (FPC) prompts”, on page 117, then you are prompted to the PDT passwords and step 2 is not necessary.

2 At the PDT prompt, type `passwd`.

3 Enter the current Level 2 password when prompted.

4 Enter the new Level 2 and Level 1 PDT passwords when prompted. PDT passwords are case-sensitive, must be 6 to 16 characters in length, and the Level 1 and Level 2 passwords must be different.

To accept a password without changing it, press the **<Enter>** key when prompted to enter a new password.

5 Exit PDT.

Verify the changes by logging in with the new passwords..

IMPORTANT!

Password or account changes made on the Call Server and system software upgrades are not distributed or made permanent until a user performs a datadump (EDD).

System Report messages for PDT

Table 40 shows selected System Report (SRPT) messages for the PDT. For further System Report (SRPT) messages, refer to *Software Input/Output: System Messages* (553-3001-411).

Table 40
System Report messages for PDT (Part 1 of 3)

Report	Description / Action required	Severity
SRPT0051	PDT: PDT passwords set to default	Info
SRPT0052	PDT: Could not create PDT password file Try resetting the PDT passwords using the PASSWD command. If the PASSWD command fails or cannot be executed then: • For the Small System, enable the faceplate DIP switch. Enter PDT using the systems SECURITY ID. Enter the PASSWD command and use the SECURITY ID as the Old PDT Level 2 Password. • For all other systems, enter the install disk in the floppy drive of the active core. Enter PDT using the systems TAPE ID. Enter the PASSWD command and use the TAPE ID as the Old PDT Level 2 Password. If this fails, contact the system technical support group.	Minor

Table 40
System Report messages for PDT (Part 2 of 3)

Report	Description / Action required	Severity
SRPT0053	PDT: Could not save PDT passwords Try resetting the PDT passwords using the PASSWD command. If the PASSWD command fails or cannot be executed then: • For the Small System, enable the faceplate DIP switch. Enter PDT using the systems SECURITY ID. Enter the PASSWD command and use the SECURITY ID as the Old PDT Level 2 Password. • For all other systems, enter the install disk in the floppy drive of the active core. Enter PDT using the systems TAPE ID. Enter the PASSWD command and use the TAPE ID as the Old PDT Level 2 Password. If this fails, contact the system technical support group.	Minor
SRPT0054	PDT: Passwords cannot be changed from a remote cabinet	Info
SRPT0055	PDT: Password changes have been stored	Info
SRPT0056	PDT: Passwords can only be changed from the active side Check the core state using LD 135 stat CPU. Ensure the core is the active core. Try to change the passwords using the PASSWD command again. If this fails, contact the system technical support group.	Info
SRPT0057	PDT: Problem detected with password synchronize • For Small Systems: check the connection between the main cabinet and the remote cabinets. Ensure that the main cabinet and remote cabinets have completed their boot cycle. Try to change the passwords using the PASSWD command again. • For CP PII systems, check that the HSP is up, the systems are joined and the disks are synchronized. Try to change the passwords using the PASSWD command. If these actions fail, contact the system technical support group.	Minor

Table 40
System Report messages for PDT (Part 3 of 3)

Report	Description / Action required	Severity
SRPT0058	PDT: Corrupt password detected Try resetting the PDT passwords using the PASSWD command. If the PASSWD command fails or cannot be executed then: • For Small Systems, enable the faceplate DIP switch. Enter PDT using the systems SECURITY ID. Enter the PASSWD command and use the SECURITY ID as the Old PDT Level 2 Password. • For all other systems, enter the install disk in the floppy drive of the active core. Enter PDT using the systems TAPE ID. Enter the PASSWD command and use the TAPE ID as the Old PDT Level 2 Password. If these actions fail, contact the system technical support group.	Minor
SRPT0059	PDT: Invalid password entered	Info
SRPT0060	PDT: Unexpected error occurred during PDT password changes Try to change the passwords using the PASSWD command. If the PASSWD command fails or cannot be executed then: • For Small Systems, enable the faceplate DIP switch. Enter PDT using the systems SECURITY ID. Enter the PASSWD command and use the SECURITY ID as the Old PDT Level 2 Password. • For all other systems, enter the install disk in the floppy drive of the active core. Enter PDT using the systems TAPE ID. Enter the PASSWD command and use the TAPE ID as the Old PDT Level 2 Password. If these actions fail, contact the system technical support group.	Minor

Multi-user login

Multi-user login allows up to five users to simultaneously log into a system to load and execute overlays. A sixth overlay can be running at midnight or in the background. This feature supports only the following:

- sets administration
- maintenance
- midnight routines
- background routines
- attendant administration

The History File includes separate Log Files for each configured TTY port to record each technician's maintenance and administration activities.

A user can be forced to log off a terminal if a Level 2 or Limited Access Password user logs in to the system. A monitor command allows a logged-in user to monitor the input/output activities of a different local or remote terminal.

Table 41 lists the facility that can be implemented using a Level 2 password and multi-user login, the programs and prompts to implement the password, and the programs to print information about the password.

Table 41
Implementing Level 2 password and multi-user login

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - PWD2, LAPW, TLOG, SIZE MULTI-USER ON(OFF)	LD 22 by CFN or LAPW

Single Terminal Access

The Single Terminal Access (STA) feature uses Multi-purpose Serial Data Link (MSDL) cards to reduce the number of physical devices needed to administer and maintain a system and its associated subsystems.

Note: For remote access over IP networks, a terminal server provides a more cost-effective method of switching between EIA232 serial port devices.

When the user intends to switch to another system, a mechanism for ending the original session is provided in the STA application through a user-determined logout sequence. This sequence is specified in the database with each STA port. This sequence is automatically sent to the destination system by the application to prevent users from leaving a session open in the background without logging out.

If the logout sequence is not programmed, or is programmed incorrectly, the user could leave a program open in the background, and the system could be subject to unauthorized access.

The STA master terminal uses the configured logout sequences to automatically exit from the active and existing background sessions when the modem connection for the terminal experiences carrier drop out.

A password is required before the user can enter NEW or CHANGE to configure an STA port. This process is designed to protect the STA port from unauthorized alteration.

Table 42 lists the facility that can be implemented to configure STA, the programs and prompts to implement single terminal access, and the programs to print information about single terminal access.

Table 42
Implementing single terminal access

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - ADAN, STA, TTY, CTYP, GRP, DNUM, ADMIN_PORT, LANGUAGE, ADDITIONAL_PORT	LD 22 by CFN or ADAN

Password Complexity Checking

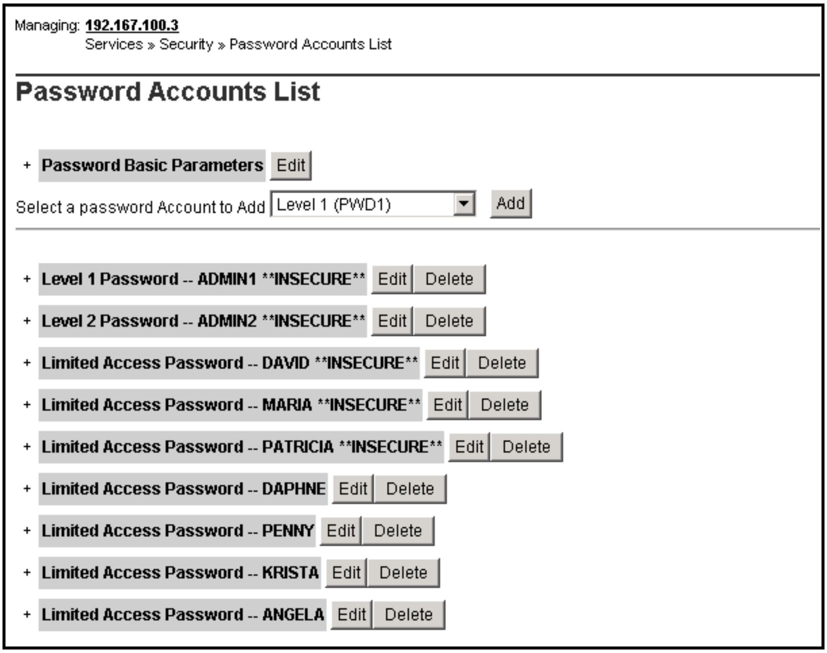
Level 2 users can turn Password Complexity Checking feature to ON in LD 17 or in Element Manager. For further information on implementing LD 17, see page 140.

Procedure 5
Turn Password Complexity Check to ON

1 Navigate to **Services** > **Security** > **System Password**.

The Password Accounts List web page opens. Figure 1 shows the Password Accounts List web page.

Figure 1
Password Accounts List web page



Managing: 192.167.100.3
Services » Security » Password Accounts List

Password Accounts List

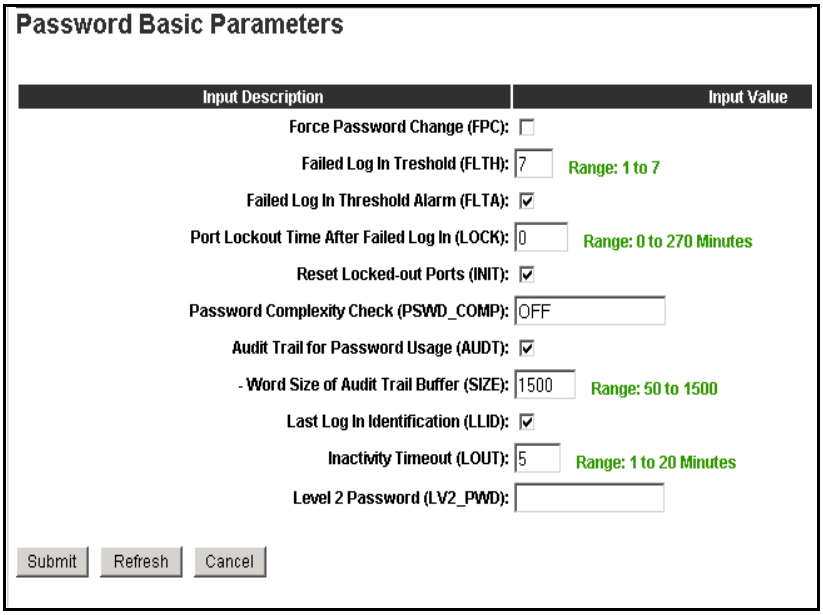
+ Password Basic Parameters Edit

Select a password Account to Add Level 1 (PWD1) Add

+ Level 1 Password -- ADMIN1 **INSECURE** Edit Delete
+ Level 2 Password -- ADMIN2 **INSECURE** Edit Delete
+ Limited Access Password -- DAVID **INSECURE** Edit Delete
+ Limited Access Password -- MARIA **INSECURE** Edit Delete
+ Limited Access Password -- PATRICIA **INSECURE** Edit Delete
+ Limited Access Password -- DAPHNE Edit Delete
+ Limited Access Password -- PENNY Edit Delete
+ Limited Access Password -- KRISTA Edit Delete
+ Limited Access Password -- ANGELA Edit Delete

2 Select **Edit** option for **Password Basic Parameters**.
The Password Basic Parameters web page opens. Figure 2 on page 130 shows the Password Basic Parameters web page.

Figure 2
Password Basic Parameters



Password Basic Parameters

Input Description	Input Value
Force Password Change (FPC):	□
Failed Log In Treshold (FLTH):	7 Range: 1 to 7
Failed Log In Threshold Alarm (FLTA):	☑
Port Lockout Time After Failed Log In (LOCK):	0 Range: 0 to 270 Minutes
Reset Locked-out Ports (INIT):	☑
Password Complexity Check (PSWD_COMP):	OFF
Audit Trail for Password Usage (AUDT):	☑
- Word Size of Audit Trail Buffer (SIZE):	1500 Range: 50 to 1500
Last Log In Identification (LLID):	☑
Inactivity Timeout (LOUT):	5 Range: 1 to 20 Minutes
Level 2 Password (LV2_PWD):	

3 Enter **ON** in the Password Complexity Check (PSWD_COMP) text box.

4 Click **Submit**.

End of Procedure

When Password Complexity Checking is turned to ON, all new passwords entered by the user are validated against the password rules. The user is prompted to enter the new password twice. If the two entries do not match, a warning message is displayed and the transaction is cancelled.

The following section lists the password rules:

- must be at least eight characters long
- must not contain the user name in forward or reverse order
- must not have a keyboard trail
- must not repeat

- must not have four or more consecutive characters of the same type (lower case alpha, upper case alpha, and numeric)
- must not have five or more consecutive alpha characters

Recommended password management practices

- Nortel recommends that you use Password Complexity Checking feature to avoid or minimize unauthorized access to the administration terminal.
- Avoid simple passwords or those that are derived from personal information such as social security number, home telephone number, birth dates, and family names.
- Change the default password and change the password every 60 to 290 days.
- Do not use a password you have used before.
- Use a longer password to provide greater security.
- The password should be changed following the system installation and configuration.
- Invalid login thresholds should be set to 3; manual initialization overrides the lock-out time limit defined for invalid attempts. This must be programmed. The default = NO.
- Change the system password when anyone knowing a system password leaves the company.

After changing their password, a user’s password will not be synchronized with the rest of the system until the Call Server performs an datadump (EDD).

Login names are required when changing passwords and cannot be left blank.

Password management for the standalone

Program access control

The Limited Access to Overlays feature, controlled through Limited Access Password (LAPW), provides a greater degree of control of password assignment and program access. The feature also enhances tracking of system access. This feature provides additional security by allowing up to 100 LAPW passwords to be defined for each system. The LAPW passwords can be 4 to 16 alphanumeric characters in length.

In addition to the login time, name, and password, the LAPW Audit Trail provides a time stamp indicating when the user logged out. When accessing the system using LAPW, the Limited Access to Overlays feature can be configured to require a user to enter a user name with up to 11 alphanumeric characters.

Access to specific programs can be defined for each password and a Print Only capability specified. An Audit Trail can be configured to record the date, time, password used, and programs accessed. The system performs the following actions:

- monitors failed logon attempts
- compares the number of attempts with a predefined threshold
- locks the entry port if the threshold is exceeded

The system reports lock-out conditions on all terminals and provides a special report to the next administrator who logs on.

Table 43 lists the facility that can be implemented using Limited Access to Overlays programs, the prompts used to implement the feature, and the programs to print information about the feature.

Table 43
Implementing the Limited Access to Overlays feature

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - LAPW, PWnn, OVLA, CUST, TEN, OPT = CFPD(A), LLCA(D), PROA(D), PSCD(A), HOST, FLTH, LOCK, AUDT, SIZE, INIT	LD 22 by CFN or LAPW

Audit Trail review

The Audit Trail stores system activities messages in memory. The stored information can be accessed using a system terminal or a remote device. The information can be printed.

Make sure that the file is large enough to hold all possible entries. Increase the size if necessary.

INIT = YES indicates that a manual initialization is allowed to reset a port locked out due to invalid logon attempts. If ACD reports are run, this INIT feature interrupts reports and provides incomplete statistics.

The Audit Trail for Limited Access Password (LAPW) includes time stamps that indicate when users logged out.

Table 44 lists the facility used to implement the Audit Trail feature, and the programs used to print information about the feature.

Table 44
Implementing the Audit Trail

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - AUDT, SIZE, INIT	LD 22 by AUDT or LD 22 by CFN

History File review

The History File stores system messages in memory. The stored information is accessed by using a system terminal or a remote device. The information can be printed.

Specify the types of information to be stored in the History File. This information includes the following:

- maintenance messages (MTC)
- service change activity (SCH)
- customer service change activity (CSC)
- software error messages (BUG)

Selectively view the History File using the VHST command. This command permits the following actions:

- search forward
- repeat the last search
- go up or down
- define the next or previous number of lines to display
- display lines from the current location to the bottom of the file
- search on a string of up to 12 characters

A Traffic Log file can be created separate from the History File.

Table 45 lists the facility that can be implemented using the History File, programs and prompts to implement the feature, and programs to print information about the feature.

Table 45
Implementing the History File

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - IOTB, HIST, USER ADAN, SIZE	LD 22 CFN or ADAN

Diagnostic commands

Level 2 user can use diagnostic commands to enable, disable, or view the access status of secured and unsecured shells in the system.

LD 117 — Shell Login commands

Command	Description
ENL SHELLS INSECURE	Enables all insecure shells in the system. This includes TELNET and RLOGIN sessions.
DIS SHELLS INSECURE	Disables all insecure shells in the system. This include TELNET, RLOGIN sessions.
STAT SHELLS INSECURE	Indicates whether insecure shell access is enabled or disabled.

Table 46
Shell security CLI commands on Signalling Server and VGMC devices

Command	Description
disInsecureShells	Disables all insecure shells in the system. This includes TELNET and RLOGIN sessions.
enlInsecureShells	Enables all insecure shells in the system. This includes TELNET and RLOGIN sessions.
statInsecureShells	Displays the status of the insecure shell access.

Controlling access to the system

To limit unauthorized functional and physical access to the system and its network connections, provide the following:

- System administration port security (see page 136)
- Switchroom security (see page 136)
- Network facilities security (see page 137)

System administration port security

Remote system administration allows technicians to access the system using maintenance modems or the on-site terminal. This allows technicians to adjust and troubleshoot system hardware and software components; however, unauthorized users can also access the system remotely, alter the system configuration, steal services, and degrade system performance.

Unauthorized users have been known to dial into the remote access port, break the password, and reprogram system memory to allow international calls, enable the DISA feature, turn off Call Detail Recording (CDR), traffic, and history reports, and either eliminate the need for Authcodes or create new Authcodes.

Ports defined as TTY or PRT are controlled by counters monitoring invalid characters. Ports disabled due to invalid characters can be automatically enabled after four minutes. Disabled ports can be enabled a maximum of three times in 30 minutes. If a port is disabled four times in 30 minutes, it requires manual enabling.

Access to the system communication ports can be limited with passwords. Refer to "Password management", on page 113.

Switchroom security

If a switchroom is not secure, unauthorized users can access all system resources. The activities of unauthorized users can range from turning off printer and CDR processors to removing cards from the system and rendering it inoperable. Follow these security procedures to minimize this risk:

- Limit access to the switchroom to authorized personnel only.
- Require distributor and telephone company personnel to sign in and out and provide identification, if necessary.
- Control, document, and audit major changes to system configuration.
- Require personnel to sign out parts and equipment.
- Store printouts of system configurations and databases in a secure, locked area.

- Do not post passwords or Trunk Access Codes in the switchroom.
- Keep the switchroom and telephone equipment closets locked.

Network facilities security

Network security is just as important as switchroom security. For example, unsecured facilities can be accessed by a lineman using a test terminal to place unauthorized calls without these calls being detected by the system and recorded by the CDR.

Follow these security procedures to minimize this risk of abuse:

- Secure the telephone company access point, individual distribution frame location, and the Main Distribution Frame (MDF).
- Avoid locating Intermediate Distribution Frames (IDF) in janitorial, electrical, and supply closets whenever possible. Limit access when colocation is unavoidable.
- Document existing outside and inside cable plans and update these records as service changes are made.
- Where cable plan records do not exist, consider hiring an independent consultant to verify and document the cable plan.
- Maintain and document all moves and changes. Eliminate all out-of-service cross connects if not using the Automatic Set Relocation feature.
- Encase and lock building entry terminals and secure manholes.
- Avoid posting cable documentation in the IDF.
- Keep cable plant documentation in at least two separate secure locations.
- Verify terminal connections against cable plant/system records, and resolve all differences.
- Audit the entire system, ensuring that all cable, telephone company, telephone, and system records are accurate.

Controlling access to system Application Processors

Restrict access to Application Processors by requiring a user to enter a valid user ID and password on the Application Processor console. The user can then access and run applications, or configure operating characteristics of the Application Processor.

System access privileges are based on user IDs that are password-protected. Application Processors are Unix System V-based self-contained modules that interface with the system. They can also interface to local and remote peripheral devices such as terminals, personal computers, and printers. Access is restricted by the user ID, not by the terminal. A user can log on with a user ID from any terminal, including the system console.

These UNIX-based Application Processors use a hierarchy of four basic user identifications, where number 1 is the highest and number 4 is the lowest. These user IDs are as follows:

- **root**
  First-level user ID used by authorized engineering and development personnel only. The **root** user ID is set during the application installation and is chosen based on the ID of the system to which it is connected. The **root** ID is different for each application.

- **disttech**
  Second-level user ID used by qualified field technicians, emergency technical assistance and service, and distributors to configure the Application Processor according to the customer applications requirements. This is also the second-level default password. The administrator must change this password when the system is first placed in service.

- **maint** or **mlusr**
  Third-level user IDs used by the customer application and maintenance administrator to install, modify, and remove applications running on the Application Processor. These are also the third-level default passwords.

- **mlusr** and **ccrusr**
  Application access user IDs and fourth-level user IDs used by the application user to access the Application Processor console, local or remote terminals, and personal computers to run applications. These are also the fourth-level default passwords. **ccrusr** is present only if CCR is installed.

To protect the Application Processor facilities from unauthorized access, refer to “Recommended password management practices”, on page 131.

Implementation

Level 2 users can change passwords using LD 17 or CS 1000 Element Manager. Element Manager performs the same tasks as the PWD-related CLI commands traditionally configured in LD 17. Refer to “Security diagnostic commands in CS 1000 Element Manager”, on page 143 for information on Element Manager.

LD 17

The PWD2 prompt appears immediately following the TYPE = PWD entry, unless the LAPW password Multi User Logins are enabled. To view LAPW prompts, LAPW package 149 must be equipped. LAPW users can change their passwords by entering the current password at prompt LPWD and entering the new password at the NLPW prompt.

LD 17- Change password (Part 1 of 2)

Prompt	Response	Comment
REQ:	CHG	Change
TYPE:	PWD	Configuration Record
PWD2	a...a	Enter valid password
PSWD_COMP	(OFF) ON	Turns on or off the password complexity check for the ADMIN, LAPW and PDT passwords.
FPC	(NO) YES	Force Password Change
LOUT	1-(20) - 30	Logout, Inactive Session Logout Time in minutes
FLTH	0-(3)-7	Failed Log In Threshold
LOCK	0-(60)-270	Lockout time
FLTA	(NO) YES	Failed Log In Threshold Alarm
AUDT	(NO) YES	Audit Trail for password usage
- SIZE	(50)-1500	Word Size of Audit Trail buffer
LLID	(NO) YES	Last Log In Identification
INIT	(YES) NO	Initialize to reset locked-out ports
ACCOUNT_REQ	aaa	Account Request, where: aaa = (END), NEW, CHG, or OUT
PWD_TYPE	aaa	Specifies the user type being added to the system, where: aaa = PWD2, PWD1, LAPW
- PWTP	(OVLY) SBA	Type of LAPW account, where: (Overlay) Password Access Type Set-Based Administration Password Access Type

LD 17- Change password (Part 2 of 2)

USER_NAME	a...a	Unique user name - up to 11 characters
PASSWORD	a...a	Password for validating the users credentials on login, 4 to 16 characters
NEW_PASSWORD	a…a	Password for modifying the existing password.
CONFIRM	a...a	Confirm the typed in password
OVLA	xx xx ... xx	Overlays Allowed
LEVL	aaaa	Access Level for Set Based Administration password, where; aaaa = (INST) or ADMN
CUST	aaa	Customer to be accessible by way of PWnn
HOST	(NO) YES	Enable HOST mode Log In for password PWnn
MAT	(NO) YES	Enable MAT Log In for password PWnn
OPT	a...a	Options for password PWnn

LD 22 - Display all accounts with an insecure or expired password

Prompt	Response	Description
REQ	PRT	Print
TYPE	IPWD	
PWD2	x…x	Displays all accounts with insecure or expired passwords

```
PWD

   User_Name NORTEL2 **INSECURE**
   TYPE PWD2

   User_Name NORTEL1 **INSECURE**
   TYPE PWD1

   USER_NAME LAPW1 **INSECURE**
   TYPE LAPW_OVL

   USER_NAME LAP3  **EXPIRED**
   TYPE LAPW3_OVL
```

LD 22– Print all user accounts

Prompt	Response	Description
REQ	PRT	Print
TYPE	PWD	
PWD2	x…x	Displays detailed information about all user accounts. Note: For security reasons, passwords are not displayed.

```
PWD
PSWD_COMP ON
LOUT 20
FLTH 3
LOCK 30
FLTA NO
AUDT NO
LLID NO
INIT NO

USER_NAME NORTEL2 **INSECURE**
TYPE PWD2

USER_NAME NORTEL1 **INSECURE**
TYPE PWD1
```

```
USER_NAME LAPW1 **INSECURE**
TYPE LAPW)

OVLA  001   002   003   004   005   006   007   008   009   010
      011   012   013   014   015   016   017   018   019   020
      021   022   023   024   025   026   027   028   029   030
      031   032   033   034   035   036   037   038   039   040
      041   042   043   044   045   046   047   048   049   050
      051   052   053   054   055   056   057   058   029   060
      061   062   063   064   065   066   067   068   069   070
      071   073   073   074   075   076   077   078   079   080
      081   082   083   084   085   086   087   088   089   090
      091   092   093   094   095   096   097   098   099   117
      135   137   143

CUST
HOST NO
MAT NO
OPT PSCA RBBD CFPA LLCD PROD LOSD FORCD MOND

USER_NAME LAPW3 **INSECURE**
TYPE LAPW_OVL
OVLA 017 022
CUST
HOST NO
MAT NO
OPT PSCA RDBD DFPA LLCD PROD LOSE FORCD MOND

USER_NAME SBA2
PWTP SBA
LEVL ADMN
CUST
OPT FEAD NAMA TADD TOLD DTD TRKD INSD
```

Security diagnostic commands in CS 1000 Element Manager

Level 2 users can use Element Manager to navigate to **Services** > **Security** to access security diagnostic commands:

- System password
- PDT password

- Shell Login Options
- SSL/TLS

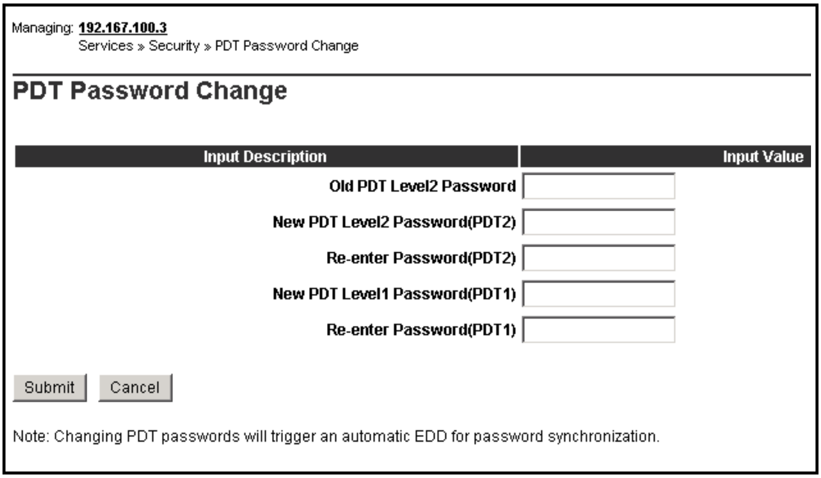
System password

System password access is password-protected. Level 2 users can use Password Account List web page to access Password Basic Parameters and all user accounts. Figure 1 on page 129 shows the Password Account List web page. Figure 5 on page 147 shows the Password Basic Parameters web page.

Problem Determination Tool (PDT) access

Problem Determination Tool (PDT) access is password-protected. Level 2 PDT users, usually administrators, can change Level 1 and Level 2 PDT passwords. Figure 3 shows the PDT Password Change web page in Element Manager.

Figure 3
PDT Password Change web page



Managing: 192.167.100.3
Services » Security » PDT Password Change

PDT Password Change

Input Description	Input Value
Old PDT Level2 Password	
New PDT Level2 Password(PDT2)	
Re-enter Password(PDT2)	
New PDT Level1 Password(PDT1)	
Re-enter Password(PDT1)	

Note: Changing PDT passwords will trigger an automatic EDD for password synchronization.

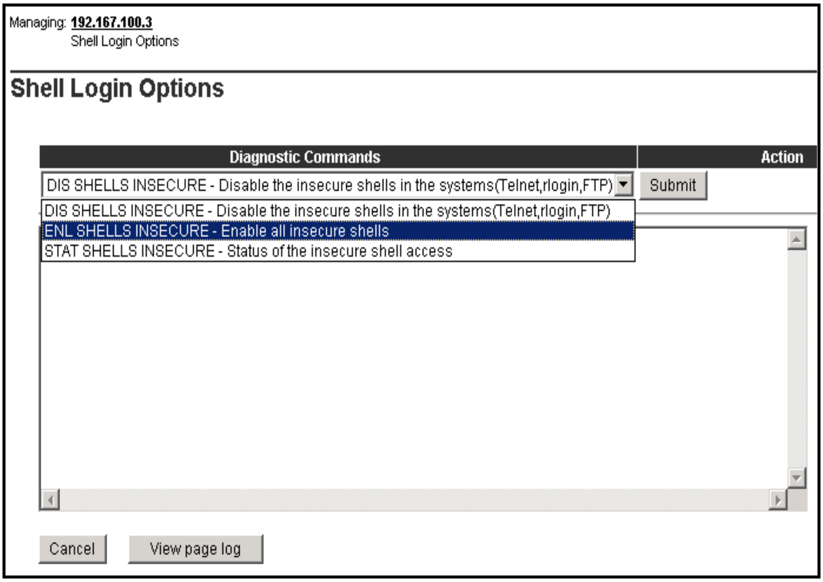
Shell access control utility

A Level 2 user can use Element Manager to enable, disable, or view the access status of secured and unsecured shells in the system using the following diagnostic commands:

- DIS SHELLES INSECURE – Disables all insecure shells in the system.
- SNL SHELLS INSECURE – Enables all insecure shells in the system.
- STAT SHELLS INSECURE – Displays the status of the insecure shell access.

Figure 4 shows the Diagnostics commands web page in Element Manager.

Figure 4
Diagnostic commands web page



Managing: **192.167.100.3**
Shell Login Options

Shell Login Options

Diagnostic Commands	Action
DIS SHELLS INSECURE - Disable the insecure shells in the systems(Telnet,rlogin,FTP)	Submit

DIS SHELLS INSECURE - Disable the insecure shells in the systems(Telnet,rlogin,FTP)
ENL SHELLS INSECURE - Enable all insecure shells
STAT SHELLS INSECURE - Status of the insecure shell access

SSL/TLS

A Level 2 user can use Element Manager to guide users through the certificate management and Transportation Layer Security (TLS) configuration process.

For information on configuring certificates in Element Manager, refer to *Element Manager: System Administration* (553-3001-332).

Security features in Element Manager

Only a Level 2 user has access to change the Password Basic Parameters. When the Force Password Change (FPC) feature is turned to On, PWD and PDT users logging in with default passwords must change their passwords before continuing.

Procedure 6
Enabling Force Password Change

1 Navigate to **Services** > **Security** > **System Password**.

Password Accounts List web page opens. See Figure 1 on page 129.

2 Select **Edit** option for **Password Basic Parameters**
The Password Basic Parameters web page opens.

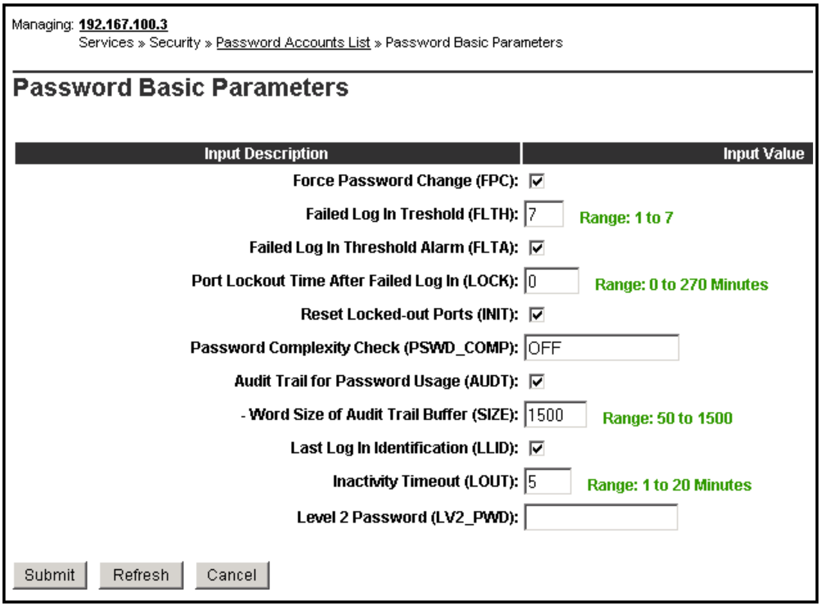
3 Check the **Force Password Change** (**FPC**) option. See Figure 5 on page 147.

4 Enter the Level 2 Password (LV2_PWD).

5 Select **Submit.**

During the next login, the user is prompted to change the system passwords.

Figure 5
Password Basic Parameters web page



Managing: **192.167.100.3**
Services » Security » Password Accounts List » Password Basic Parameters

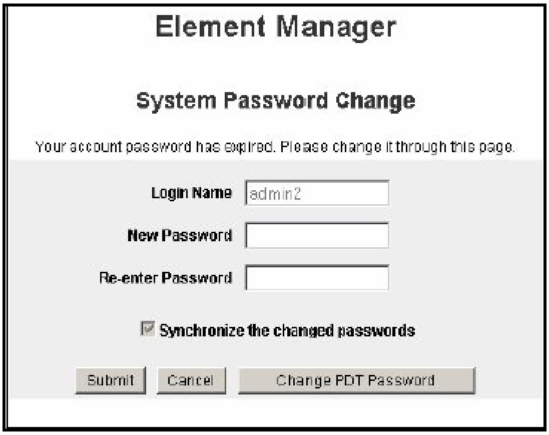
Password Basic Parameters

Input Description	Input Value	
Force Password Change (FPC):	☑	
Failed Log In Treshold (FLTH):	7	Range: 1 to 7
Failed Log In Threshold Alarm (FLTA):	☑	
Port Lockout Time After Failed Log In (LOCK):	0	Range: 0 to 270 Minutes
Reset Locked-out Ports (INIT):	☑	
Password Complexity Check (PSWD_COMP):	OFF	
Audit Trail for Password Usage (AUDT):	☑	
- Word Size of Audit Trail Buffer (SIZE):	1500	Range: 50 to 1500
Last Log In Identification (LLID):	☑	
Inactivity Timeout (LOUT):	5	Range: 1 to 20 Minutes
Level 2 Password (LV2_PWD):		

Expired passwords

When a user logs in with an expired password, they are directed immediately to the System Password Change facility of Element Manager, where the password must be changed before continuing. See Figure 6 on page 148.

Figure 6
System Password Change web page



Element Manager

System Password Change

Your account password has expired. Please change it through this page.

Login Name: admin2

New Password:

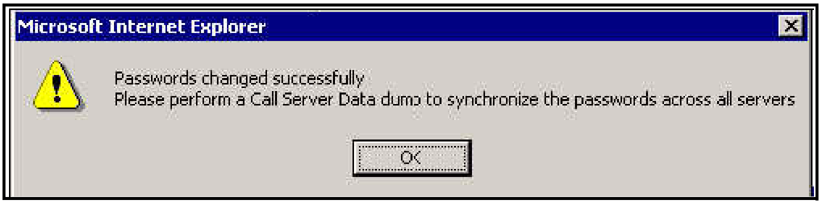
Re-enter Password:

☑ Synchronize the changed passwords

Synchronize changed Passwords

This option is selected by default and will perform a datadump (EDD) in the Call Server after the passwords are changed successfully. The a datadump (EDD) is required to synchronize the password across the servers linked to the Call Server. See Figure 7.

Figure 7
System password change



Microsoft Internet Explorer

Passwords changed successfully
Please perform a Call Server Data dump to synchronize the passwords across all servers

Password management for standalone Signaling Server

Level 2 (PWD2) users manage accounts and passwords on the standalone Signaling Server running Network Routing Service (NRS). The Level 2 (PWD2) user issues commands from the OA&M shell as shown in Table 47.

Table 47
Commands issued to manage accounts and passwords on the standalone NRS

Command	Description
adminUserPasswordChange [userID]	allows a user to change their own password or allows a Level 2 (PWD2) user to change any user password specified in the userID field
adminUserCreate [userID]	allows a Level 2 (PWD2) user to create an account specified in the userID field
adminUserDelete [userID]	allows a Level 2 (PWD2) user to delete an account specified in the userID field
adminAccountShow	allows a Level 2 (PWD2) user to display all configured accounts on the system

New system security planning

Contents

This section contains information on the following topics:

Introduction

This chapter describes how to evaluate new hardware and software security options for a new system using system software and Meridian Mail software. To plan security for a new system, do the following:

- Analyze the current system configuration
- Compare the current configuration to the new system
- Fill out the security installation checklist
- Evaluate the new hardware with the software security option

Analyzing the system configuration

When a new system is installed, security features necessary to protect call processing and administrative functions from unauthorized access must be activated.

It is easier for users to learn system security procedures once than to adjust to frequent changes later on. Making changes that affect the day-to-day operation of a company's system is disruptive to users and incoming callers alike.

Before installing security features, it is necessary to generate and install a configuration database. Based on this configuration, system security features can be designed to protect the system's call processing, administration, and maintenance functions.

To help define security for functions and features activated in the configuration database, use the security installation checklist. Refer to Appendix A on page 235 for a list of available security features.

Filling out the security installation checklist

The security installation checklist is designed to help provide the maximum protection for the system and its users. There is one checklist for the system and one for Meridian Mail. See "System checklist" on page 153 and "Meridian Mail checklist" on page 168.

The checklist is used by the customer and the distributor during the system configuration planning stage. For each function and feature in the customer configuration database, an equivalent security feature must be specified using the checklist. The checklist can also be used when installation is complete to verify that all planned security features have been implemented. To verify these features, use the print program listed for each feature in the checklist.

The checklist is organized by feature. Each feature is divided into the following:

- **Print program** — The name of the program used to print data about the feature.
- **Guidelines** — Instructions on filling out security feature parameters.
- **Parameter values** — Security feature parameter values.
- The chapter and section to go to or the program to use to implement any proposed values.

To fill out each feature in the checklist, do the following:

1 Fill in the security feature **parameter values**.

2 Refer to the **Implementation** information for each security feature to implement the parameter values.

Before filling out the checklist, read “Controlling call privileges” on page 27, and “Controlling OA&M access” on page 109 to understand the system and Meridian Mail security features.

System checklist

Define all entries on the checklist that are configured in the system database. Skip entries that are not active in the system.

Basic Access Restrictions

Class of Service (CLS)

Print program — Terminal Number Block Program LD 20

Guidelines — Eight CLS levels are available: UNR, CTD, CUN, TLD, SRE, FRE, FR1, and FR2. Specify one or more levels for each item.

Single-line/multi-line telephones ________________

DISA ________________

Authcodes ________________

TIE Trunks ________________

Meridian Mail Agents ________________

See “Class of Service” on page 30.

Trunk Group Access Restrictions (TARG/TGAR)

Print program — Terminal Number Block Program LD 20

Guidelines — Specify a TARG/TGAR from 0 to 31 for each item, where 0 indicates no restrictions.

Single-line/multi-line telephones ________________

DISA ________________

Authcodes ________________

Meridian Mail Agents ____________________

Trunks ____________________

COTS (TARG) ____________________

WATS (TARG) ____________________

DID (TARG) ____________________

FEX (TARG) ____________________

TIE (TARG on route) ____________________

TIE (TGAR on individual trunks) ____________________

PAG (TARG) ____________________

MUS (TARG) ____________________

See "Trunk Group Access Restrictions" on page 33

Modifying Basic Access Restrictions

1. System Speed Call (SSC)

Print program — Speed Call List Program LD 20.

Guidelines — Specify an NCOS from 0 to 99 for the SSC list.

NCOS ____________________

See "System Speed Call" on page 38.

2. Network Speed Call (NSC)

Print program — Speed Call List Program LD 20

Guidelines — Enter the NSC list number to be used for specified long-distance access.

NSC list number ____________________

See "Network Speed Call" on page 39.

3. Authorization Code (Authcode)

Print program — Authcode Data Block Program LD 88

Guidelines — Specify a CLAS from 1 to 115, a COS restriction level of UNR, CTD, CUN, TLD, SRE, FRE, FR1, or FR2, a TGAR from 0 to 31, and an NCOS restriction level from 0 to 99 for each Authcode in the system.

Authcode length ________ (4 to 16 digits)

CLAS ______ COS ______ TGAR ______ NCOS ______

CLAS ______ COS ______ TGAR ______ NCOS ______

CLAS ______ COS ______ TGAR ______ NCOS ______

CLAS ______ COS ______ TGAR ______ NCOS ______

CLAS ______ COS ______ TGAR ______ NCOS ______

CLAS ______ COS ______ TGAR ______ NCOS ______

See “Authorization Code” on page 40.

4. Forced Charge Account (FCA)

Print program — Customer Data Block Program LD 21

Guidelines — Select Yes to temporarily override toll-denied CLS restrictions. If Yes is selected, enter the length of the FCA.

FCC: Yes No (circle one)

FCC length ________ (4 to 5 digits)

See “Forced Charge Account” on page 44.

5. Enhanced and Controlled Class of Service (ECCS/CCOS)

Print program — Customer Data Block Program LD 21

Guidelines — Three different levels are available. Identify the class of service for the three parameters, CCRS with either ECC1 and/or ECC2, or just ECC1, ECC2, or CCRS alone.

CCRS ________ ECC1 ________ ECC2 ________

See “Controlled Class of Service” on page 45 and “Enhanced Controlled Class of Service” on page 46.

6. Electronic Lock (ELK)

Print program — Customer Data Block Program LD 21

Guidelines — Select Yes to allow users to activate and deactivate CCOS mode from their telephones by entering the Station Control Password (SCPW) and the appropriate ELK code. If Yes is selected, enter the length of the SCPW.

ELK: Yes No (circle one)

SCPW length ________ (1 to 8 digits)

See “Electronic Lock” on page 47.

7. Code Restriction Blocks (CRB)

Print program — Route Data Program LD 21

Guidelines — Select Yes to allow toll-denied telephones and TIE trunks limited access to the toll exchange network over CO and FX trunks.

CRB: Yes No (circle one)

ALOW ________ DENY ________

See “Code Restriction Data Block” on page 48.

8. New Flexible Code Restriction (NFCR)

Print program — Customer Data Block Program LD 21

Guidelines — Select Yes to allow toll-denied telephones, TIE trunks, and Authcodes to selectively make certain calls on outgoing trunk routes.

NFCR: Yes No (circle one)

See “New Flexible Code Restriction” on page 49.

9. Called Party Disconnect Control (CPDC)

Print program — Route Data Program LD 21

Guidelines — Specify routes from 0 to 127 or check No if trunk-to-trunk transfers will not be prevented.

Route ________ ________ ________ ________ ________

No _________

See “Called Party Disconnect Control” on page 50.

Call Forward (CFW)

1. User Selectable Call Redirection (USCR)

Print program — Terminal Number Block Program LD 20 and Station Administration Program LD 10/11

Guidelines — Select USCR to restrict call forward destinations to external telephones.

IUSR Yes No (circle one)

SCPW length_________ (0 to 8 digits)

USR, FFC, SPCL (circle one or more)

See “User Selectable Call Redirection” on page 72.

2. Call Forward External (CFXA/D)

Print program — Customer Data Block Program LD 21

Guidelines — Select CFXD to restrict call forward from a telephone to an external DN.

CFXA CFXD (circle one)

See "Call Forward External Deny" on page 73.

3. Internal Call Forward (ICF)

Print program — Customer Data Block Program LD 21

Guidelines — Select ICF to allow user to route internal calls to a different location other than external calls.

ICF Yes No (circle one)
ICF length ______ 4 to 23 digits

See "Internal Call Forward" on page 74.

4. Call Forward All Calls (CFW)

Print program — Terminal Number Block Program LD 20 and Features and Station Print LD 81

Guidelines — Select CFW to allow call forward from a telephone to another location (internal or external).

CFW Yes No (circle one)
CFW length ________ (4 to 23 digits)

See "Call Forward All Calls" on page 75.

5. Call Forward to Trunk Access Code (CFTA)

Print program — Customer Data Block Program LD 21

Guidelines — Select No to restrict DID calls from being forwarded to a Trunk Access Code.

Trunk access code length ________ (1 to 4 digits – 7 with DN expansion)

CFTA: Yes No (circle one)

See “Call Forward to Trunk Access Code” on page 75.

6. Remote Call Forward (RCFW)

Print program — Customer Data Block Program LD 21

Guidelines — Select Yes to allow users to activate or deactivate call forwarding from remote telephones.

RCFW: Yes No (circle one)
RCFW Flexible Feature Code ________

See “Remote Call Forward” on page 77.

7. Call Forward Originating (CFO) or Forwarded (CFF) Class of Service

Print program — Customer Data Block Program LD 21

Guidelines — Select CFO or CFF to use CLS access privileges of the telephone that originates the call or the telephone that forwards the call.

CFF CFO (circle one)

See “Call Forward Originating or Forwarded Class of Service” on page 76.

Basic/Network Automatic Route Selection

1. Supplemental Digit Recognition/Restriction (SDRR)

Print program — ESN Data Block Program LD 86

Guidelines — Select Yes or No to allow or deny access to specific number sequences following NPAs, NXXs, or SPNs.

SDRR blocking 976 and 976 look alikes: Yes No (circle one)

SDRR blocking International "976-type" numbers: Yes No (circle one)

SDRR blocking 800/900 numbers: Yes No (circle one)

See "Supplemental Digit Recognition/Restriction" on page 79.

2. Network Class of Service (NCOS) and Facility Restriction Level (FRL)

Print program — Customer Data Block Program LD 21

Guidelines — Specify an NCOS from 0 to 99, a corresponding FRL from 0 to 7, and the calling area they are allowed to access, which can be area codes, geographic locations, exchanges, or special numbers.

NCOS ________
FRL ________
Calling area ________
NCOS ________
FRL ________

NCOS ________
FRL ________
Calling area ________
NCOS ________
FRL ________

Calling area __________

NCOS __________

FRL __________

Calling area __________

NCOS __________

FRL __________

Calling area __________

NCOS __________

FRL __________

Calling area __________

Calling area __________

NCOS __________

FRL __________

Calling area __________

NCOS __________

FRL __________

Calling area __________

NCOS __________

FRL __________

Calling area __________

See “Network Class of Service and Facility Restriction Level” on page 80.

3. Authorization Code Conditionally Last Network Authorization Code (NAUT)

Print program — Authcode Data Block Program LD 88.

Guidelines — Select Yes to prompt users who fail to meet the minimum FRL requirement assigned to a route to enter an Authcode to complete a call.

NAUT: Yes No (circle one)

See “Network Authorization Codes” on page 82.

4. Time of Day Schedule (TODS)

Print program — Route List Index Program LD 86

Guidelines — There are eight time spans when routes are available for call processing. Each span is three hours in duration, from 12:00 a.m. and ending at 11:59 p.m. Check the time spans covered by BARS/NARS.

0 __________ 1 __________ 2 __________ 3 __________

4 __________ 5 __________ 6 __________ 7 __________

See “Time-of-Day Routing” on page 83.

5. Routing Control (RTCL)

Print program — Route Data Program LD 21

Guidelines — Select Yes to reduce NCOS to lower levels when the attendant console is in night mode or when the attendant activates the key that controls routing. If Yes for RTCL was circled, specify NMAP by entering the current NCOS and the NCOS value when the Extended Time of Day (ETOD) schedule is in effect. Enter a value of 1 to 7 for ETOD to specify the days of the week when RTCL is in effect, where 1 is Sunday and 7 is Saturday. One or more ETOD can be entered.

RTCL: Yes No (circle one)

NMAP ________ ETOD ________

See "Routing Control" on page 84.

6. Incoming Trunk Group Exclusion (ITGE)

Print program — ITGE Index Program LD 86

Guidelines — Specify routes from 0 to 511 and the area codes to be blocked on these routes.

Route ________ Block ________

Route ________ Block ________

Route ________ Block ________

Route ________ Block ________

Route ________ Block ________

Route ________ Block ________

See "Incoming Trunk Group Exclusion" on page 85.

7. Free Calling Area Screening (FCAS)

Print program — Route List Index Program LD 86

Guidelines — For each Route List Index (RLI), specify a number from 0 to 999 to define the Free Calling Index (FCI) 1 to 255 for each RLI entry. Specify 0 for the FCI if FCAS is not required.

Route List ________
Route List Entry ________ FCI ________
Route List Entry ________ FCI ________
Route List Entry ________ FCI ________
Route List Entry ________ FCI ________
Route List Entry ________ FCI ________
Route List Entry ________ FCI ________

See "Free Calling Area Screening" on page 86

8. TGAR Control (TGAR)

Print program — ESN Data Block Program LD 86

Guidelines — Select Yes to add TGAR access privileges to BARS/NARS as a qualification for call completion.

BARS/NARS TGAR: Yes No (circle one)

See "Trunk Group Access Restrictions" on page 33.

Direct Inward System Access (DISA)

Print program — Print DISA Block Program LD 24

Guidelines — Select the following parameters to define public access into the system for placing long-distance calls over system facilities.

SCOD: Yes No (circle one) Length______________
Authcodes: Yes No (circle one) Length______________

DISA DN TGAR ________ CLS ________ NCOS ________

See “Controlling Direct Inward System Access” on page 87

Multi-Tenant (TENS)

Print program — Define Multi-Tenant Program LD 93

Guidelines — Specify a tenant from 1 to 511, a route from 0 to 999, and a Console Presentation Group (CPG) from 1 to 63.

Tenant-to-Tenant Access (TACC): Yes No (circle one)

Tenant ________ to Tenant ________

Tenant ________ to Tenant ________

Tenant ________ to Tenant ________

Tenant ________ to Tenant ________

Tenant ________ to Tenant ________

Tenant-to-Route Access (RACC): Yes No (circle one)

Tenant ________ to Route ________

Tenant ________ to Route ________

Tenant ________ to Route ________

Tenant ________ to Route ________

Tenant ________ to Route ________

Console Presentation Groups (CPG): Yes No (circle one)

CPG ________ for Tenants ________

CPG ________ for Tenants ________

CPG ________ for Tenants ________

CPG ________ for Tenants ________

CPG ________ for Tenants ________

See "Controlling Multi-Tenant Services" on page 89.

SDI ports

1. Call Detail Recording (CDR)

Print program — Configuration Record Program LD 22

Guidelines — Specify the CDR port that connects the CDR terminal to the system, and enter routes programmed to output CDR from 0 to 999 and if they are incoming, outgoing, two-way, and so on.

CDR Port number ________

Route ______ Type ______ Route ______ Type ______

Route ______ Type ______ Route ______ Type ______

Route ______ Type ______ Route ______ Type ______

See “Analyzing Call Detail Recording reports” on page 212.

Traffic Reporting (TFC)

Print program — Configuration Record Program LD 22.

Guidelines — Specify the port that connects the traffic terminal to the system and specify traffic parameters required to collect and report traffic statistics.

Traffic Port number ________
Schedule ________
Which reports are scheduled ________
Traffic Log Yes No (circle one)

See “Analyzing Traffic Measurement reports” on page 216.

Meridian Mail checklist

Define all entries in the checklist that are configured for Meridian Mail. Skip entries that are not active. Note why the feature is not active.

1. Call Answering/Express Messaging Thru-dial Restriction/ Permission Code Tables

Print program — Voice Security Option screen

Guidelines — Specify 1- to 5-digit extension numbers, trunk access codes, special prefix codes, or BARS/NARS access codes that callers are permitted to use, or restricted from using. Ten permission and ten restriction codes are allowed for each table. Name defaults are On-Switch, Local, Long Distance 1, or Long Distance 2. Users can select their own table names.

Name ____

Restrict _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

Permit _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

Name ____

Restrict _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

Permit _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

Name ____

Restrict _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

Permit _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

Name ____

Restrict _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

Permit _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

2. Custom Voice Menu/Thru-dial Restriction/Permission Code Tables

Print program — Voice Menu Thru Dialers

Guidelines — Specify 1- to 5-digit extension numbers or area codes that callers are permitted to use or restricted from using. Ten permission and ten restriction codes are allowed for each table.

Menu Name ________________________________
Restrict _____ _____ _____ _____ _____
_____ _____ _____ _____ _____
Permit _____ _____ _____ _____ _____
_____ _____ _____ _____ _____
Menu Name ________________________________
Restrict _____ _____ _____ _____ _____
_____ _____ _____ _____ _____
Permit _____ _____ _____ _____ _____
_____ _____ _____ _____ _____
Menu Name ________________________________
Restrict _____ _____ _____ _____ _____
_____ _____ _____ _____ _____
Permit _____ _____ _____ _____ _____
_____ _____ _____ _____ _____
Menu Name ________________________________
Restrict _____ _____ _____ _____ _____
_____ _____ _____ _____ _____
Permit _____ _____ _____ _____ _____
_____ _____ _____ _____ _____

3. Mailbox Password Assignment

Print program — Voice Security Option screen

Guidelines — Specify if the mailbox password is to be a default or an administrator-assigned password.

Default _____ Administrator Assigned _____ (check one)

Password prefix Yes No (circle one)

4. Password Parameters

Print program — Voice Security Option screen

Guidelines — Used to limit unauthorized access to voicemail.

Invalid login attempts per session ________
Invalid login attempts per mailbox ________
Minimum password length ________
Forced password change ________
Number of days between changes ________
Number of changes before password repeats ________
Expiration warning Yes No (circle one)
Expiration warning schedule ________

Existing system security upgrade

Contents

This section contains information on the following topics:

Introduction

This chapter describes how to plan an a security upgrade for an existing system. The chapter also describes the security audit procedures used to analyze existing system security and define additional security features as required. The following security features are audited:

- system security features
- Meridian Mail security features
- system Application Processor security features

Note: Auditing an existing system assumes an in-depth working knowledge of system software, including prompts and responses. Users must contact their Nortel distributor for assistance in conducting this audit if they are not trained and certified in system software and/or Meridian Mail software.

Before filling out the checklist, read "Controlling call privileges" on page 27, and "Controlling OA&M access" on page 109 to understand the system and Meridian Mail security features.

Auditing system security features

System security includes call processing security features, system administration, and maintenance security features. To audit existing security, use the system audit checklist. Refer to Appendix A on page 235 for a list of available security features.

System audit checklist

The checklist is organized by feature. Each feature is divided into:

- **Print program** — The name of the program used to print data about the feature.
- **Guidelines** — Instructions on filling out proposed values.
- **Parameter values** — Current feature values and proposed feature values.
- The chapter and section to review, or the program to use, to implement any proposed values.

To fill out each feature in the checklist, do the following:

1. Print out data about the feature using the **Print program** information.
2. Fill in the **Current values** column using the information generated by the **Print program**.
3. Use the **Guidelines** to fill out the **Proposed value** column. If retaining the current value, enter a check mark in this column.
4. Refer to the **Implementation** information to change current values to **Proposed values**.

1. Audit Trail

Print program — Audit Trail Program LD 22. Only the administrator with a Level 2 password is allowed to print the contents of the Audit Trail.

Guidelines — Determine if an Audit File exists. If no file exists, activate one. Ensure that the file is large enough to hold all possible entries. Increase the size if necessary. To allow manual initialization of a port locked out due to invalid logon attempts, set INIT = YES.

Parameter	Current value	Proposed value
AUDT	Yes No (circle one)	Yes No (circle one)
SIZE	______________	______________
INIT	Yes No (circle one)	Yes No (circle one)

See “Audit Trail review” on page 133.

2. Authorization Code (Authcode)

Print program — Authcode Data Block Program LD 88

Guidelines — Ensure that CDR is recording the Authcodes. Determine the COS, TGAR, and NCOS for each CLAS. There must be no duplicate CLAS.

Parameter	Current value	Proposed value
SPWD	______________	______________
ALEN	______________	______________
ACDR	______________	______________
CLAS	______________	______________
COS	______________	______________
TGAR	______________	______________
NCOS	______________	______________

Verify the following for each Authcode:

Parameter	Current value	Proposed value
SPWD	______________	______________
CODE	______________	______________
CLAS	______________	______________

See “Authorization Code” on page 88.

3. Background Terminal

Print program — Configuration Record Program LD 22

Guidelines — Identify if a Background Terminal exists and is used for Controlled Class of Service.

Parameter	Current value	Proposed value
ADAN	TTY__________	TTY__________
USER	BGD	BGD
CUST	______________	______________
MANU	______________	______________

See Configuration Record Program LD 17.

4. Call Detail Recording

Print program — Configuration Record Program LD 22

Guidelines — Identify which port is assigned CDR output. Check to ensure activity. If there is no CDR, disregard all other references to CDR.

Parameter	Current value	Proposed value
ADAN	TTY__________	TTY__________
USER	CTY	CTY
CDR port assigned	______________	______________
CDPR	Yes No (circle one)	Yes No (circle one)
CLID	Yes No (circle one)	Yes No (circle one)

See “Analyzing Call Detail Recording reports” on page 212.

5. Call Forward to Trunk Access Codes (CFTA)

Print program — Customer Data Block Program LD 21

Guidelines — This prompt must be set to No. If forwarding to Trunk Access Codes is allowed, users can forward incoming calls to outbound trunks. If the telephone's TGAR does not allow direct access, this feature is not active even if allowed.

Parameter	Current value	Proposed value
CFTA	Yes No (circle one)	Yes No (circle one)

See "Call Forward to Trunk Access Code" on page 75.

6. Call Forwarding: Forwarding (CFF) or Originating (CFO) Control

Print program — Customer Data Block Program LD 21

Guidelines — Note if OPT = CFF or CFO. CFO indicates that the originator of the call has the controlling CLS when the called telephone is in Call Forward All Calls. If OPT = CFO, check the CLS, TGAR, and NCOS of the DID trunk and Route Data Blocks. DID trunks must be restricted from external calling or long-distance calling through BARS/NARS and denied direct access to other trunk groups. The option CFF indicates that the telephone being called carries the controlling CLS for call processing in Call Forward All Calls.

Current value	Proposed value
OPT = CFF or CFO (Circle one)	OPT = CFF or CFO (Circle one)
If CFO, CLS, TGAR and NCOS on DID trunks =_____	If CFO, CLS, TGAR and NCOS on DID trunks =_____

See "Controlling Call Forward access" on page 72.

7. Central Office Translation (NXX)

Print program — Central Office Translation Program LD 90

Guidelines — Eliminate NXX 976 if programmed. Highlight any numbers with inconsistent routing and/or digit manipulation.

Parameter	Current value	Proposed value
TRAN		
NXX		
RLI		
SDRR		
DMI		
DENY		
LDID		
LDDD		
DID		
DDD		
ITED		
ITEI		

See Central Office Translation Program LD 90. New NXX configuration parameters are in effect when implementing NXX-related security features in “Supplemental Digit Recognition/Restriction” on page 79 and “Incoming Trunk Group Exclusion” on page 85.

8. Code Restriction (CRB)

Print program — Code Restriction Data Program LD 21

Guidelines — Review the ALOW and DENY entries for each CRB on each route. Indicate those routes that permit long-distance dialing and have no BARS/NARS access to control call routing.

Parameter	Current value	Proposed value
ROUT		
CLR	ALOW or DENY	ALOW or DENY
ALOW or DENY		

If the system is required to permit equal-access capability, verify that only operator-assisted or credit-card calls are accessible. Allowing direct-dialed equal-access capabilities affects all telephones, DISA DNs, Authcodes, TIE trunks, and voicemail virtual agent ports.

Identify all programming for Feature Group D:

Parameter	Current value	Proposed value
FGNO	______________	______________
LDAC	AC1 or AC2	AC1 or AC2
LAAC	AC1 or AC2	AC1 or AC2
OPER	______________	______________
INIT	______________	______________

See “Code Restriction Data Block” on page 48.

9. Console Presentation Group (CPG)

Print program — Multi-Tenant Service Program LD 93

Guidelines — Indicate if any night numbers for any CPGs are Meridian Mail DNs.

Parameter	Current value	Proposed value
CPG	______________	______________
NIT1	______________	______________
NIT2	______________	______________
NIT3	______________	______________
NIT4	______________	______________

See “Controlling Multi-Tenant Services” on page 89.

10. Controlled Class of Service (CCOS)

Print program — Customer Data Block Program LD 21

Guidelines — Identify the three (maximum) CLS assignments.

Parameter	Current value	Proposed value
CCRS (Rel. 7 or later)	______________	______________
ECC1 (Rel. 15 or later)	______________	______________
ECC2 (Rel. 15 or later)	______________	______________

See “Controlled Class of Service” on page 45 and “Enhanced Controlled Class of Service” on page 46.

11. Coordinated Dialing Plan (CDP)

Print program — Coordinated Dialing Plan Program LD 87

Guidelines — Provide the following information for each Distant Steering Code (DSC), Local Steering Code (LSC), and Trunk Steering Code (TSC).

Parameter	Current value	Proposed value
LSC, DSC, or TSC	______________	______________
DEL (LSC)	______________	______________
RLI (DSC, TSC)	______________	______________

See Coordinated Dialing Plan Program LD 87. New CDP configuration parameters are in effect when implementing CDP-related security features in “Supplemental Digit Recognition/Restriction” on page 79 and “Incoming Trunk Group Exclusion” on page 85.

12. Customer Night Numbers

Print program — Customer Data Block Program LD 21

Guidelines — Identify the night numbers and determine if any NITE DNs are Meridian Mail ACD-DNs. Indicate those that are Meridian Mail ACD-DNs by an “M” after the number.

Parameter	Current value	Proposed value
NITE	______________	______________
NIT1	______________	______________
TIM1	______________	______________
NIT2	______________	______________
TIM2	______________	______________
NIT3	______________	______________
TIM3	______________	______________
NIT4	______________	______________
TIM4	______________	______________

See Customer Data Block Program LD 15. These parameters are in effect for customer-related security features.

13. Digit Manipulation Index (DGT)

Print program — Digit Manipulation Index Program LD 86

Guidelines — Note any DGTs that delete internal numbers, and insert complete external numbers. Verify that these numbers are valid, especially if they are routed to another area code.

Parameter	Current value	Proposed value
DMI	______________	______________
DEL	______________	______________
INST	______________	______________

See Digit Manipulation Index Program LD 86. New DGT configuration parameters are in effect when implementing DGT-related security features in “Supplemental Digit Recognition/Restriction” on page 79.

14. Direct Inward System Access (DISA)

Print program — Print DISA Block Program LD 24

Guidelines — If no DISA DNs are active on the system, no plans exist to activate DISA, and the DISA software is resident on PKG, consider having DISA removed from the base software of the diskettes or tapes. Eliminate the possibility of database abuse whenever possible.

Determine if SCODs and Authcodes are required. DISA directory numbers must not directly access trunks by using access codes. DISA DNs requiring Authcodes must carry a low COS and NCOS. The Authcode is the mechanism that overrides the DISA directory number CLS.

Parameter	**Current value**	**Proposed value**
SPWD	______________	______________
DN	______________	______________
SCOD	______________	______________
AUTR	Yes No (circle one)	Yes No (circle one)
TGAR	______________	______________
NCOS	______________	______________
CLS	______________	______________

See "Controlling Direct Inward System Access" on page 87.

15. ESN Data Block (ESN)

Print program — ESN Data Block Program LD 86

Guidelines — Verify if the system uses CDP and how many digits are in a steering code. List codes for AC1 and AC2 and list time schedules for TODS. Indicate if RTCL is used and when it is effective. State if TGAR is used in addition to the standard BARS/NARS controls for access to trunk routes. TGAR control is commonly used in Multi-tenant environments.

Parameter	Current value	Proposed value
CDP	Yes No (circle one)	Yes No (circle one)
MXSC	______________	______________
NCDP	______________	______________
AC1	______________	______________
AC2	______________	______________
TODS	______________	______________
	______________	______________
	______________	______________
	______________	______________
	______________	______________
	______________	______________
	______________	______________
RTCL	Yes No (circle one)	Yes No (circle one)
NMAP	______________	______________
ETOD	______________	______________
TGAR	Yes No (circle one)	Yes No (circle one)

See ESN Data Block Program LD 86. New ESN block configuration parameters are in effect when implementing ESN-related security features in “Supplemental Digit Recognition/Restriction” on page 79, “Network Authorization Codes” on page 82, “Time-of-Day Routing” on page 83, and “Incoming Trunk Group Exclusion” on page 85.

16. Flexible Feature Code (FFC)

Print program — Print FFC Data Program LD 57

Guidelines — These features allow activation of access features such as Call Forward, ELK, SSC, and SCPD change.

Parameter	Current value	Proposed value
ASRC		
AUTH		
CDRC		
CFWA		
CFWD		
CFWV		
DEAF		
ELKA		
ELKD		
RCFA		
RCFD		
RCFV		
SCPC		
SSPU		

See “Electronic Lock” on page 47.

17. Forced Charge Account (FCA)

Print program — Customer Data Block Program LD 21

Guidelines — If FCAF = Yes, identify the number length of the FCA, the minimum number of digits, and the NCOS for network FCA.

Parameter	Current value	Proposed value
CHLN		
FCAF	Yes No (circle one)	Yes No (circle one)
CHMN		
FCNC		

See “Forced Charge Account” on page 44.

18. History File

Print program — History File Program LD 22

Guidelines — Verify that a History File exists. Make certain that the file is large enough to hold the activity directed to it. Review the type of messages being sent to the history file. Print the history file to verify the content. Eliminate outputting all unnecessary messages.

Parameter	Current value	Proposed value
HIST		
ADAN	HST	
USER		

See “History File review” on page 134.

19. Incoming Trunk Group Exclusion (ITGE)

Print program — Incoming Trunk Group Exclusion Index Program LD 86

Guidelines — Determine what numbers ITGEs are blocking. Decide if they are programmed effectively and test to ensure correct application.

Parameter	Current value	Proposed value
ITEI	______________	______________
RTNO	______________	______________

See Incoming Trunk Group Exclusion Index Program LD 86. New ITGE configuration parameters are in effect when implementing ITGE-related security features in “Incoming Trunk Group Exclusion” on page 85.

20. Location Code (LOC)

Print program — Location Code Program LD 90

Guidelines — Determine DGT for each entry on the RLI. Indicate if DGT modifies calls to a specific external location. Validate location and telephone number.

Parameter	Current value	Proposed value
TRAN	______________	______________
LOC	______________	______________
RLI	______________	______________
ITEG	______________	______________
LDN	______________	______________
DID	Yes No (circle one)	Yes No (circle one)
MNXX	Yes No (circle one)	Yes No (circle one)
SAVE	______________	______________
OFFC	______________	______________
RNGE	______________	______________

See Location Code Program LD 90. New LOC configuration parameters are in effect when implementing LOC-related security features.

21. Meridian Mail – Virtual Agent data

Print program — Terminal Number Block Program LD 11.

Guidelines — Identify the ACD-DNs associated with Meridian Mail. List the system software for each virtual agent position ID and review to ensure that each is the lowest NCOS, FRL, CLS possible and cannot directly access any outbound trunk route. Flag any exceptions.

Parameter	**Current value**	**Proposed value**
ACDN	______________	______________
Voicemail DN	Yes No (circle one)	Yes No (circle one)
NCFW	______________	______________
Meridian Mail	Yes No (circle one)	Yes No (circle one)

Virtual Agent Position IDs and Associated CLS, NCOS, TGAR

Current value		**Proposed value**	
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________

See ACD Directory Number Program LD 23.

22. Multi-line telephones

Print program — Terminal Number Blocks Program LD 20

Guidelines — Make note of all virtual ports that are used for access to a voicemail system. Ensure that they are as restricted as possible to prohibit calls from transferring out of the mail system to the PBX and making unauthorized toll calls.

Enter the TGAR definitions on the TGAR matrix. The matrix shows direct-access capabilities of multi-line telephones. All multi-line telephones must be restricted from direct access of outbound facilities unless BARS/NARS is not programmed to process calls. If direct access is the only method of making outbound calls from multi-line telephones, review CRB and NFCR data blocks to ensure authorized access of facilities.

SCPW must be as long as possible; codes up to eight digits are allowed. Each SCPW must be unique.

Verify that the number of Call Forward digits is no greater than necessary. If the system has 4-digit extensions, CFW4 is sufficient. All telephones must be programmed as CFXD. This prohibits call forwarding to access codes such as AC1 and AC2, Trunk Access Codes, and numbers external to the system. There should be very rare exceptions allowing external Call Forward.

UNR allows unrestricted calls. CTD is recommended. Use TLD, SRE, FRE, FR1, and FR2 whenever possible.

Indicate telephones that are assigned CCSA, SSU, FCA, and/or TENA. When active, these features affect access restrictions and controls.

For each multi-line telephone, identify the following:

Parameter	**Current value**	**Proposed value**
TGAR	______________	______________
NCOS	______________	______________
SSU	______________	______________
SCPW	______________	______________
CLS	______________	______________
(UNR - CFXA, CCSA, TENA, ICDA, AUTR, AUTU, AUTD)		
EFD	______________	______________
EHT	______________	______________
TEN	______________	______________
FCAR	Yes No (circle one)	Yes No (circle one)
KEY		
CFW (no. of digits)	______________	______________
CHG	______________	______________

See Multi-line Telephone Administration Program LD 11. These new telephone configuration parameters are in effect when implementing multi-line telephone-related security features.

23. Network Control (NTCL)

Print program — Network Control Program LD 87

Guidelines — Each NCOS is defined to restrict calls to specific calling patterns. NCOSs are traditionally built with increasing call capabilities. Lower numbered NCOSs are usually most restrictive and higher numbered NCOSs are least restrictive. One NCOS must not duplicate another. Print out the entire NCOS database to ensure that a rogue code is not built at the end of the database.

Parameter	Current value	Proposed value
NCOS	______________	______________
EQA	______________	______________
FRL	______________	______________
RWTA	Yes No (circle one)	Yes No (circle one)
NSC	Yes No (circle one)	Yes No (circle one)
LIST	Yes No (circle one)	Yes No (circle one)

See Network Control Program LD 87. New NTCL configuration parameters are in effect when implementing NTCL-related security features in "New Flexible Code Restriction" on page 49, "Network Speed Call" on page 39, "Network Authorization Codes" on page 82, and "Routing Control" on page 84.

24. Network Speed Call (NSC)

Print program — Network Translation Program LD 90

Guidelines — Select a BARS/NARS access code and specify a 1- to 3-digit Network Speed Call Access Code (NSCC) and a 0 to 4095 System Speed Call List (SSCL) number.

Parameter	Current value	Proposed value
TRAN	AC1 or AC2	AC1 or AC2
NSCC	______________	______________
SSCL	______________	______________

See "Network Speed Call" on page 39.

25. New Flexible Code Restriction (NFCR)

Print program — Print Data Program LD 49

Guidelines — Identify trees used for Feature Group D, all trees allowing long-distance calls, and operator-assisted calls.

If selecting Yes for NFCR, specify MAXT from 1 to 255 to define the maximum number of NFCR trees.

If the system is required to permit equal-access capability, verify that only operator-assisted or credit-card calls are accessible. Allowing direct-dialed equal-access capabilities affects all telephones, DISA DNs, Authcodes, TIE trunks, and voicemail virtual agent ports.

Verify if the Central Office provides a service that prohibits bill-back to the telephone placing an equal-access call. This prohibits callers who dial 010XXX from using the listed directory number (DN) as a bill number instead of a credit-card number.

Parameter	**Current value**	**Proposed value**
NFCR	Yes No (circle one)	Yes No (circle one)
MAXT	______________	______________
CRNO	______________	______________
ALOW and/or DENY	______________	______________
BYPS	______________	______________

See “New Flexible Code Restriction” on page 49.

26. Numbering Plan Area Code (NPA)

Print program — Numbering Plan Area Code Program LD 90

Guidelines — Indicate area codes to international locations and if they are sent to a route different from U.S. long-distance calling. The route must be different to indicate special status; it must carry a higher NCOS and have an FCAS table to permit calling to specific business numbers within a high-fraud area code such as 809. If a company doesn't call the 809 area, remove it from the translation tables.

Parameter	**Current value**	**Proposed value**
TRAN	______________	______________
NPA	______________	______________
RLI	______________	______________
SDRR	______________	______________
DMI	______________	______________
DENY	______________	______________
LDID	______________	______________
LDDD	______________	______________
DID	______________	______________
DDD	______________	______________
ITED	______________	______________
ITEI	______________	______________

See Numbering Plan Area Code Program LD 90. New NPA configuration parameters are in effect when implementing NPA-related security features in "Supplemental Digit Recognition/Restriction" on page 79, "Incoming Trunk Group Exclusion" on page 85, and "Free Calling Area Screening" on page 86.

27. Passwords

Print program — Passwords Program LD 22

Guidelines — Verify all passwords. Ensure that all passwords have been changed from the default value. Passwords must be a maximum of eight characters in length. Make all passwords complex alphanumeric entries and nonrepetitive. Change all passwords that are obvious.

Limit access to administration and maintenance programs (overlays) by allowing a specific password to access only selected programs and restricting access to all other programs. Where necessary, allow users to change their own passwords.

Parameter	Current value	Proposed value
LAPW	______________	______________
PWnn	______________	______________
LOGIN_NAME	______________	______________
OVLA	______________	______________
CUST	______________	______________
TEN	______________	______________
HOST	Yes No (circle one)	Yes No (circle one)
OPT (Circle A or D):		
	CFPD (A)	CFPD (A)
	LLCA (D)	LLCA (D)
	PROA (D)	PROA (D)
	PSCD (A)	PSCD (A)
LPWD	______________	______________
FLTH	______________	______________
LOCK	______________	______________
Multi-User	______________	______________

See “Program access control” on page 131.

28. Route List Index (RLI)

Print program — Route List Index Program LD 86

Guidelines — Note any RLIs that deviate from consistent programming: no TODs, DGTs to external numbers, low FRLs, FCAS tables for long-distance routing, or unusual route patterns. Make note of which NPAs, NXXs, SPNs, DSCs, TSCs, or LOCs are routed to these RLIs.

Parameter	Current value	Proposed value
RLI	______________	______________
ENTR	______________	______________
ROUT	______________	______________
TOD	______________	______________
CNV	Yes No (circle one)	Yes No (circle one)
EXP	Yes No (circle one)	Yes No (circle one)
FRL	______________	______________
DMI	______________	______________
FCI	______________	______________
MFRL	______________	______________

See Route List Index Program LD 86. New RLI configuration parameters are in effect when implementing RLI-related security features in “Network Authorization Codes” on page 82, “Time-of-Day Routing” on page 83, and “Free Calling Area Screening” on page 86.

29. Secure Data Password (SPWD)

Print program — Customer Data Block Program LD 21 to display passwords

Guidelines — Verify that a password exists to change Authcodes and DISA information. Activate a password when DISA and Authcodes are used.

Parameter	Current value	Proposed value
SPWD	_____________	_____________

See “Authorization Code” on page 88.

30. Single-line telephones

Print program — Terminal Number Block Program LD 20

Guidelines — Make note of all virtual ports that are used for access to a voicemail system. Ensure ports are as restricted as possible to prohibit calls from transferring out of the mail system to the PBX and making unauthorized toll calls.

Enter the TGAR definitions on the TGAR matrix. The matrix shows direct-access capabilities of single-line telephones. All single-line telephones must be restricted from direct access of outbound facilities unless no BARS/NARS is programmed to process calls. If direct access is the only method of making outbound calls from single-line telephones, review CRB and NFCR data blocks to ensure authorized access to facilities.

SCPWs must be as long as possible; codes up to eight digits are permissible. Each SCPW must be unique.

Verify that the number of Call Forward digits is no greater than necessary. If the system has 4-digit extensions, CFW4 is sufficient. All telephones must be programmed as CFXD. This prohibits call forwarding to access codes such as AC1 and AC2, Trunk Access Codes, and numbers external to the PBX. There should be very rare exceptions allowing external Call Forward.

UNR CLS allows unrestricted calls. CTD is recommended. Use TLD, SRE, FRE, FR1, and FR2 whenever possible.

Identify all telephones that Hunt or Forward No Answer out of the system and their hunt or no answer location. Restrict this ability whenever possible.

Indicate telephones that are assigned CCSA, SSU, FCA, and/or TENA. When active, these features indicate possible access restrictions and controls.

For each single-line telephone, identify the following:

Parameter	**Current value**	**Proposed value**
TGAR	______________	______________
NCOS	______________	______________
SCPW	______________	______________
CLS	______________	______________
(UNR - CFXA, CCSA, TENA, ICDA, AUTR, AUTU, AUTD)		
TEN	______________	______________
FCAR	Yes No (circle one)	Yes No (circle one)
FTR		
CFW (no. of digits)	______________	______________
EHT	______________	______________
EFD	______________	______________
SSU	______________	______________

See Single-line Set Administration Program LD 10. These new telephone configuration parameters are in effect when implementing telephone-related security features.

31. Special Number Translation (SPN)

Print program — Network Translation Program LD 90

Guidelines — Check for entries permitting equal-access calls. Ensure these entries do not override entries in CRB or NFCR databases. Check for entries of country codes. If there is no international dialing, eliminate any entries for international dialing from the table. If international calls are permitted, define levels to the country code if possible. Restrict using flexible ESN routing for 0, 00, 01, 011, and Supplemental Digit Recognition/Restriction (SDRR).

Parameter	**Current value**	**Proposed value**
TRAN		
SPN		
RLI		
SDRR		
DMI		
DENY		
LDID		
LDDD		
DID		
DDD		
ITED		
ITEI		

See Network Translation Program LD 90. New SPN configuration parameters are in effect when implementing SPN-related security features in “Supplemental Digit Recognition/Restriction” on page 79 and “Incoming Trunk Group Exclusion” on page 85.

32. System Speed Call (SSC)

Print program — Speed Call List Program LD 20

Guidelines — Verify SSC lists and entries.

Parameter	**Current value**	**Proposed value**
LNSO	______________	______________
NCOS	______________	______________
STOR	______________	______________

See “System Speed Call” on page 38.

33. Telephone Control Password Length

Print program — Customer Data Block Program LD 21

Guidelines — Indicate the number of digits allowed for a telephone control password. The recommended minimum is six.

Parameter	**Current value**	**Proposed value**
SCPL	______________	______________

See “Electronic Lock” on page 47.

34. Tenant-to-Route Access (RACC)

Print program — Multi-Tenant Service Program LD 93

Guidelines — Identify any RACC restrictions.

Parameter	**Current value**	**Proposed value**
ROUT	______________	______________
ACC	ALOW or DENY	ALOW or DENY
DENY	______________	______________
ALOW	______________	______________

See “Controlling Multi-Tenant Services” on page 89.

35. Tenant-to-Tenant Access (TACC)

Print program — Multi-Tenant Service Program LD 93

Guidelines — Identify any TACC restrictions.

Parameter	Current value	Proposed value
TEN	______________	______________
ACC	ALOW or DENY	ALOW or DENY
DENY	______________	______________
ALOW	______________	______________

See “Controlling Multi-Tenant Services” on page 89.

36. Traffic Log

Print program — Configuration Record LD 22

Guidelines — Identify the size of the traffic log. Determine from Traffic LD2 when traffic reports are scheduled. Verify which reports are scheduled, when they are scheduled, and how often they are checked. If there is a third-party device that captures and processes traffic information, identify the hardware and software.

Parameter	Current value	Proposed value
ADAN	TRF_________	TRF_________
SIZE	_____________	_____________

37. Traffic Terminal

Print program — Configuration Record Program LD 22

Guidelines — Identify the traffic terminal. Determine from Traffic Program LD 2 when traffic programs are scheduled. Verify which reports are scheduled and how often they are checked. If there is a third-party device that captures and processes traffic information, identify the hardware and software.

Parameter	Current value	Proposed value
ADAN	TTY_________	TTY_________
USER	TRF	TRF
CUST	_____________	_____________
Third-Party Device	_____________	_____________

See “Analyzing Traffic Measurement reports” on page 216.

38. Trunk Route and CDR control

Print program — Route Data Block Program LD 21

Guidelines — Highlight all AUTO routes. Label any routes that are DISA or auto-terminating to the automated attendant.

Verify that all routes configured as Incoming Trunks (ICT) or Outgoing Trunks (OGT) are sent one way from the CO. The caution here is that some trunks are two way from the CO and configured as one way at the PBX, inadvertently allowing access to or from the public network.

Routes configured as CPDC = Yes are unable to be transferred to another route for outbound traffic. This is a systemwide parameter and is effective for any call using the route. There is no override.

Ensure that all routes carrying outbound traffic are configured to output CDR, and identify the types of CDR they will output.

If the route uses NFCR, note the FRL and tree number.

Using the **TGAR worksheet** form, which is a TARG/TGAR matrix, enter the trunk type access code and TARG of each route as a horizontal entry. Refer to the TGAR worksheet form in Appendix Band use this form to configure the routes.

Parameter	**Current value**	**Proposed value**
ROUT	______________	______________
TKTP	______________	______________
PRIV	______________	______________
ISDN	______________	______________
AUTO	Yes No (circle one)	Yes No (circle one)
ICOG	______________	______________
ACOD	______________	______________
TARG	______________	______________
CPDC	Yes No (circle one)	Yes No (circle one)
CDR	Yes No (circle one)	Yes No (circle one)
INC	Yes No (circle one)	Yes No (circle one)
QREC	Yes No (circle one)	Yes No (circle one)
QAL	Yes No (circle one)	Yes No (circle one)
QTL	Yes No (circle one)	Yes No (circle one)
AIA	Yes No (circle one)	Yes No (circle one)
OAN	Yes No (circle one)	Yes No (circle one)
OPD	Yes No (circle one)	Yes No (circle one)
NATL	Yes No (circle one)	Yes No (circle one)
TDG	_____________	_____________
FRL	_____________	_____________

For trunks where TYPE = TIE, ISDN = YES, and ISAR = YES, record the following:

Parameter	**Current value**	**Proposed value**
NCOS	______________	______________
CLS	______________	______________
TGAR	______________	______________

See system security features Trunk Route and CDR control.

39. Trunks

Print program — Terminal Number Block Program LD 20

Guidelines — Enter the TGAR information on the TGAR matrix for trunks, DISA DNs, Authcodes, and telephones. If night numbers are Meridian Mail Voice Menu DNs, ensure that the Meridian Mail Voice Menu table for Voice Security Options blocks all unauthorized access. Ensure that the NCOS, TGAR, and CLS are sufficiently restrictive to prohibit direct access to other outbound trunks and long-distance calling. Unless trunks tandem through the system for either a network hop-off application or on-net ESN call, the trunks must not have the ability to direct access to other outbound facilities.

Parameter	Current value	Proposed value
NCOS	______________	______________
NITE	______________	______________
ATDN	______________	______________
TGAR (TIE trunks)	______________	______________
FCAR	Yes No (circle one)	Yes No (circle one)
CLS	______________	______________

See Trunk Administration Program LD 14. These new trunk configuration parameters are in effect when implementing trunk-related security features.

Auditing Meridian Mail security features

Meridian Mail security features include features that access Meridian Mail mailboxes, voice menus, or automated attendants. To audit an existing Meridian Mail security system, use the Meridian Mail audit checklist.

Meridian Mail audit checklist

The checklist is organized first by software release and then by feature. Each feature is divided into:

- **Print program/print screen** — The name of the program used to print data about the feature. Mailbox information is obtained by using the print screen routine for each mailbox screen of information.
- **Guidelines** — Instructions on filling out proposed values.
- **Parameter values** — Current feature values and proposed feature values.
- The chapter to go to or the program to use to implement any proposed values.

See Voice Security Option screen.

To fill out each feature in the checklist, do the following:

1. Identify the software release.
2. Print out data about the feature using the **Print screen** information.
3. Fill in the **Current values** column using the information generated by the **Print screen**.
4. Use the **Guidelines** to fill out the **Proposed value** column. If keeping the current value, enter a check mark in this column.
5. Refer to the **Implementation** information to implement the **Proposed values**.

1. Call Answering/Express Message Outcalling Thru-dial

Print — Voice Security Option screen

Guidelines — Ensure that all direct Trunk Access Codes, Special Prefix Codes, and AC1 and AC2 codes on system printouts are included in the restriction tables.

On-Switch

Current value		**Proposed value**	
Permission	**Restriction**	**Permission**	**Restriction**
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________

Local

Current value		**Proposed value**	
Permission	**Restriction**	**Permission**	**Restriction**
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________

Long Distance 1

Current value		Proposed value	
Permission	**Restriction**	**Permission**	**Restriction**
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________

Long Distance 2

Permission	Restriction	Permission	Restriction
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________

See Voice Security Option screen.

2. Directory Number Table

Print — Voice System Administration screen

Guidelines — List all Voice Menu DNs. Compare to the ACD-DNs on the system printouts. Be certain to identify all possible accesses to voicemail. Ensure that Voice Menu Thru-dial restrictions control access to Trunk Access Codes, and SPRE and AC1 and AC2 codes.

See Voice System Administration screen.

3. Express Messaging Thru-dial

Print — Voice Security Option screen

Guidelines — Review permission/restriction tables for each Voice Menu. Ensure that the restriction table for Voice Menus includes blocking of Trunk Access Codes and SPRE and AC1 and AC2 codes.

Menu Name_____________

Current value		**Proposed value**	
Permission	**Restriction**	**Permission**	**Restriction**
_________	_________	_________	_________
_________	_________	_________	_________
_________	_________	_________	_________
_________	_________	_________	_________
_________	_________	_________	_________
_________	_________	_________	_________
_________	_________	_________	_________
_________	_________	_________	_________
_________	_________	_________	_________
_________	_________	_________	_________

See Voice Security Option screen.

4. Passwords

Print — Voice Security Option screen

Parameter	**Current value**	**Proposed value**
Invalid logon attempts	____________	____________
Minimum password length	____________	____________
Forced password change	____________	____________
Number of entries before repeat password	____________	____________
Expiration warning message parameters	____________	____________

See Voice Security Option screen.

5. Password parameters

Print — Voice Security Option screen

Guidelines — When configuring new mailboxes, it is preferable not to use the default password. Nortel recommends using the custom password that can be assigned for each mailbox by the system administrator. Users frequently do not change default passwords. Unauthorized persons try the obvious first (default passwords) and then common choices such as 123456, 654321, 222222, 333333 as well as telephone numbers, addresses, and so on.

Parameter	**Current value**	**Proposed value**
Invalid logon attempts per mailbox	____________	____________
Invalid logon attempts per session	____________	____________
Minimum password length	____________	____________
Forced password change	____________	____________
Number of entries before repeat password	____________	____________
Expiration warning message parameters	____________	____________

See Voice Security Option screen.

6. Thru-dial

Print — Voice Security Option screen

Guidelines — Ensure that all access codes on the system printouts are included in this table. Verify that all direct Trunk Access Codes, Special Prefix Codes, and AC1 and AC2 codes are covered in this table.

Parameter	**Current value**	**Proposed value**
Thru-dial restrictions	____________	____________
Thru-dial restrictions	____________	____________
Thru-dial restrictions	____________	____________
Thru-dial restrictions	____________	____________
Thru-dial restrictions	____________	____________
Thru-dial restrictions	____________	____________
Thru-dial restrictions	____________	____________
Thru-dial restrictions	____________	____________
Thru-dial restrictions	____________	____________
Thru-dial restrictions	____________	____________

See Voice Security Option screen.

7. Voice Menu Thru-dial

Print — Voice Security Option screen

Guidelines — Review permission/restriction tables for each Voice Menu. Ensure that the restriction table for Voice Menus includes blocking of Trunk Access Codes and SPRE and AC1 and AC2 codes.

Menu Name_____________

Current value		**Proposed value**	
Permission	**Restriction**	**Permission**	**Restriction**
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________
__________	__________	__________	__________

See Voice Security Option screen.

Auditing Application Processor security features

System Application Processor security features prevent unauthorized access to the Application Processor console and any terminals and personal computers that could be linked to the Application Processor. This is primarily accomplished through proper password management at the Application Processor and peripheral devices connected to it. Nortel Application Processors are UNIX V-based modules, which follow the UNIX basic user ID convention. It supports four user ID levels. These are:

- **root** — First-level user ID used by authorized engineering and development personnel only. The **root** user ID is set during an application installation and is chosen based on the ID of the system to which it is connected. The **root** ID is different for each application.
- **disttech** — Second-level user ID used by qualified field technicians, emergency technical assistance and service, and distributors to configure the Application Processor according to the customer applications requirements. This is also the second-level default password. The administrator must change this password when the system is first placed in service.
- **maint** or **mlusr** — Third-level user ID used by the customer application and maintenance administrator to install, modify, and remove applications running on the Application Processor. This is also the third-level default password.
- **mlusr** and **ccrusr** — Application access user ID. Fourth-level user ID used by the application user to access the Application Processor console or local or remote terminals and personal computers to run applications. This is also the fourth-level default password. **ccrusr** is present only if CCR is installed**.**

Obtain a list of all passwords accessing an Application Processor from the first to the fourth level. Make sure that default passwords are not being used. This is especially critical for the first-level password, which has access to all Application Processor functions.

System security analysis

Contents

This section contains information on the following topics:

Introduction

This chapter describes how to analyze system security to detect unauthorized access and fraud, using system reporting capabilities. The most effective method of detecting fraud is by doing the following:

- using the system reports summary
- analyzing Call Detail Recording reports
- analyzing Traffic Measurement reports
- checking the History File
- analyzing Operational Measurement reports

The information in this chapter must be used as part of routine system maintenance after security has been implemented and security features are operating correctly. It can reveal unauthorized call placements, unusual traffic patterns, and past events and system messages that can reveal unauthorized or attempted access to the system.

Using the system reports summary

There are a number of messages and reports that can be used to analyze security for the system. Table 48 provides a summary of these messages and reports. Table 48 shows how they can help analyze fraud using the statistics they provide, and how they are obtained. Use this summary to find the reports that produce the needed information. These reports are discussed in detail in this chapter.

The History File includes a separate file dedicated to traffic. Reports can be sent to that file instead of to the online printer.

Table 48
System reports summary (Part 1 of 3)

Information required	Report	Statistics provided	Output
Call placement statistics per telephone.	CDR	Identifies the calling party, trunk group used, destination called, the time, date, and duration of the call, and the Authcode or account code used to place the call.	To devices as defined.
Trunk-to-trunk call activity.	TFC001	The tandem peg count and usage.	According to schedule.
Individual trunk group activity including All Trunks Busy conditions.	TFC002	The peg count and usage for both incoming and outgoing calls, and peg count of All Trunks Busy conditions.	According to schedule.

Table 48
System reports summary (Part 2 of 3)

Information required	Report	Statistics provided	Output
All Trunks Busy conditions violating specified threshold.	TFC104	All Trunks Busy conditions on a per-route basis if established threshold is exceeded.	Automatically to a maintenance TTY if All Trunks Busy conditions exceed threshold. Associated trunk group report is also output according to its schedule.
Long call duration information.	TFS401 and TFS402	TFS401 and TFS402 identify the terminal numbers (TNs) involved in connections 36 to 49 CCS and 50 CCS or higher, respectively.	According to schedule.
	TFS411 and TFS412	TFS411 and TFS412 provide a peg count and total CCS of connections 36 to 49 CCS and 50 CCS or higher, respectively.	According to schedule.
Call activity by Route List NCOS using BARS/NARS.	TFN001	The peg count by Route List of how often the Route List was accessed and the number of calls that were successfully completed.	According to schedule.
NCOS call activity through BARS/NARS.	TFN002	The number of call attempts each NCOS group generated and other statistics.	According to schedule.

Table 48
System reports summary (Part 3 of 3)

Information required	Report	Statistics provided	Output
How often a service such as Thru-dial and Outcalling is used.	Voice Service Summary	The number of times callers used a service and the average length of each call.	On demand.
Outcalling activity for incoming and outgoing calls.	Outcalling Detail	The number of requests, attempts, retries, and the average wait time Outcalling was used.	On demand.

Analyzing Call Detail Recording reports

Call Detail Recording (CDR) reports show the details of a call, such as called and calling parties, time and duration of the call, and access codes used to place the call. Among the signs of fraudulent use are calls placed to international or unauthorized locations, calls of unusually long duration, and calls placed during nonbusiness hours.

The system outputs a record when a call terminates, when a user enters a valid Authcode or charge account code, or when a call is modified. The following types of trunk and telephone calls can be selected to appear in the CDR report:

- Incoming trunk calls
- Outgoing trunk calls
- Outgoing toll trunk calls
- Internal telephone-to-telephone calls

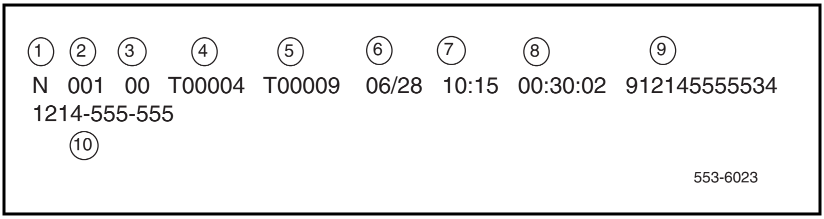
Table 49 on page 213 shows how to configure CDR and print reports for customers, routes, Authcodes, and telephones.

Table 49
Configuring and printing CDR reports

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - IOTB, ADAN, USER = CTY	LD 22 CFN or LD 22 ADAN
Customer	LD 15 - CDR = YES, AXID, TRCR, CDPR, PORT	LD 21 by CUST or LD 21 Data groups
Route - enabled on a per route basis	LD 16 - CDR = YES, INC, OAL, QREC, OTL, AIA, OAN, NATL, TDG, OPD	LD 21 by Route
Authcode	LD 88 - ACDR = YES	LD 88 by AUB
Telephones	LD 10 and LD 11 - CLS	LD 20 by TN LD 10/11 by TN
		LD 81 by FEAT = ICDA, ICDD

Figure 8 shows an example of the CDR report. The circled numbers correspond to the description of fields below Figure 8. For other CDR report examples, see *Call Detail Recording: Description and Formats* (553-3001-350).

Figure 8
Call Detail Recording record example



```
N   001   00  T00004  T00009   06/28   10:15   00:30:02   912145555534
1214-555-555
```

1
2
3
4
5
6
7
8
9
10
553-6023

1 **Record Type** — The type of call record being output. This field consists of a letter identifying the type of record:

N Normal — Generated when a user places a regular call and does not activate other telephone features.

S Start — Generated when one of the following features affects a call: Call Transfer, Conference, Call Forward, Barge-In, Busy Verify, Privacy Release, or Override.

E End — Generated when a call terminates, which is associated with a specific start record.

A Authorization Code — Generated when a user enters an Authcode and does one of the following:

— makes a trunk call

— calls a local telephone to make a DISA call

— activates Ring Again

This code must be set in the Authcode data block to appear on the CDR report.

C Charge Account — Generated when a user enters a charge account code and makes a trunk call or has already established a call.

M Charge for Conference — Generated when a user enters a charge account code during a conference call. This record allows for each conference party to be charged with a different charge account code, if necessary.

Q Initial Connection — Generated when an ACD agent makes or receives a trunk call.

R Transfer Connection — Generated when an ACD agent transfers a call.

F Conference Connection — Generated when an ACD agent sets up a conference call.

L Internal Call Record — Generated when a telephone completes an internal call.

2 **Record Number** — The number of the current record in the CDR sequence.

3 **Customer Number** — The customer associated with the call.

4 **Originator Identification** — The facility that originated the call:

DNxxxx	Telephone
ATTNxx	Attendant
CFlllnn	Conference
Txxxxxx	Trunk without answer supervision
Axxxxxx	Trunk with answer supervision

5 **Terminator Identification** — The facility on which a call terminated:

DNxxxx	Telephone
ATTNxx	Attendant
CFllln	Conference
Txxxxxx	Trunk without answer supervision
Axxxxxx	Trunk with answer supervision

6 **Timestamp (Date and Time)** — The date and time of a call. Its exact definition depends on the type of record:

N For a normal record, it shows when a call ends.

I For an internal record without call modification, it shows when the call ends.

I For an internal record with call modification, it shows when the call has been modified.

S For a start record, it shows when the call begins.

E For an end record, it shows when the call ends.

Q, R, F For a connection record, it shows when the call is connected.

7 **Call Duration** — The length of time the call lasted.

8 **Digits Dialed** — The telephone number dialed.

9 **CLI/ANI Digits** — The telephone number of the calling party, which appears in the report only if this option is installed.

Analyzing Traffic Measurement reports

Traffic Measurement reports are used to monitor the traffic volume and variations in the traffic volume that can indicate possible unauthorized use. These reports can be printed on-demand or according to a schedule. Among the signs of fraudulent use are increased trunk-to-trunk activity, long call durations, and calls to unusual locations.

Table 50 shows how to configure traffic output ports and set up an automatic report printing schedule.

Table 50
Configuring traffic output ports and schedule

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - IOTB = YES, ADAN, USER = TRF	LD 22 by CFN or LD 22 by ADAN
Traffic	LD 2 - SSHC	LD 2 - TSHC

Network traffic reporting (TFC001)

Traffic measurements provided by the TFC001 report include a cumulative peg count and information about incoming, outgoing, and tandem trunk activity. Of particular value in identifying possible fraudulent activity are the tandem (trunk-to-trunk) CCS and peg count.

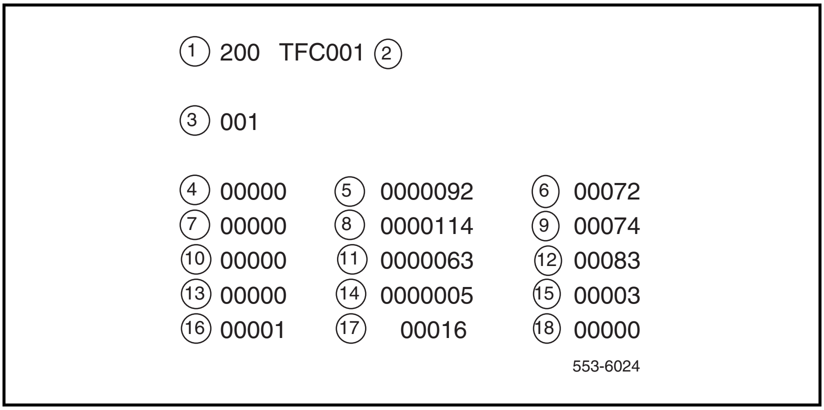
Table 51 shows prompts in Traffic Program LD 2 to configure and print the TFC001 report.

Table 51
Configuring and printing the TFC001 report

Facility	Overlay and prompts	Print programs
Traffic	LD 2 SOPS	LD 2 TOPS

Figure 9 is an example of the TFC002 report showing trunk-to-trunk CCS and peg count for tandem calls processed during the reported period. The circled numbers correspond to the description of fields below Figure 9.

Figure 9
TFC001 report example



```
①  200  TFC001 ②

③  001

④  00000    ⑤  0000092    ⑥  00072
⑦  00000    ⑧  0000114    ⑨  00074
⑩  00000    ⑪  0000063    ⑫  00083
⑬  00000    ⑭  0000005    ⑮  00003
⑯  00001    ⑰    00016    ⑱  00000
                              553-6024
```

1 **System ID** — the number assigned to the system for a specific site.

2 **Report Name** — the name of the report.

3 **Customer Number** — the customer associated with the call.

4 **Incoming FTM** — the number of incoming FTMs.

5 **Incoming CCS** — the amount of time in hundred call seconds (CCS) for incoming trunk calls.

6 **Incoming PC** — the number of incoming trunk calls processed.

7 **Outgoing FTM** — the number of outgoing FTMs.

8 **Outgoing CCS** — the amount of time in hundred call seconds (CCS) for outgoing trunk calls.

9 **Outgoing PC** — the number of outgoing trunk calls processed.

10 **Intra-Customer FTM** — the number of internal FTMs processed.

11 **Intra-Customer CCS** — the amount of time in hundred call seconds (CCS) for internal calls.

12 **Intra-customer PC** — the number of internal calls processed.

13 **Tandem FTM** — the number of tandem FTMs processed.

14 **Tandem CCS** — the amount of time in hundred call seconds (CCS) that trunk-to-trunk connections were held.

15 **Tandem PC** — the number of trunk-to-trunk calls processed.

Note: Tandem CCS and Tandem PC are of particular value in identifying possible fraudulent activity.

16 **Permanent Signal** — the number of trunks that are in permanent signal mode.

17 **Abandon** — the number of calls that were not completed.

18 **Partial Dial** — the number of calls that did not complete the dialing sequence.

Trunk traffic reporting (TFC002)

TFC002 provides information about use, overflow, and All Trunks Busy (ATB) conditions for each trunk group. Signs of fraud include All Trunks Busy conditions, a higher than normal amount of call activity, and high usage occurring outside of normal business hours.

TFC002 can be a scheduled report, but the system generates the TFC002 report automatically when an All Trunks Busy threshold violation occurs during the reporting period, regardless of whether the report is scheduled or not.

TFC002 includes a Traffic Period Option and a Trunk Seizure Option. These options can be selected in the Configuration Data Block. Refer to *Traffic Measurement: Formats and Output* (553-3001-450) for more information.

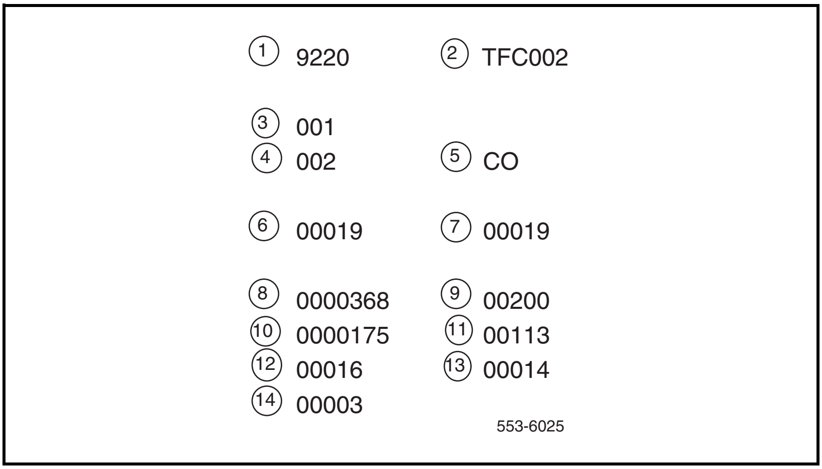
Table 52 shows the prompts in Traffic Program LD 2 to configure and print the TFC002 report.

Table 52
Configuring and printing the TFC002 report

Facility	Overlay and prompts	Print programs
Traffic	LD 2 SOPC	LD 2 TOPC

Figure 10 is an example of the TFC002 report that is automatically generated when an All Trunks Busy condition is reached. The circled numbers correspond to the description of fields.

Figure 10
TFC002 report example



```
① 9220        ② TFC002

③ 001
④ 002         ⑤ CO

⑥ 00019       ⑦ 00019

⑧ 0000368     ⑨ 00200
⑩ 0000175     ⑪ 00113
⑫ 00016       ⑬ 00014
⑭ 00003
```

553-6025

1 **System ID** — the number assigned to the system for a specific site.

2 **Report Name** — the name of the report.

3 **Customer Number** — the customer associated with the call.

4 **Route Number** — the Route Number that is the subject of the report.

5 **Trunk Type** — the type of trunk group, which can be CO = Central Office, WATS = Wide Area Telephone Service, DID = Direct Inward Dial, TIE = TIE Line, FEX = Foreign Exchange.

6 **Trunks Equipped** — the number of trunks in the system.

7 **Trunks Working** — the number of trunks that are operating in the system.

8 **Incoming Usage** — the total time in hundred call seconds (CCS) that incoming calls lasted on trunks in the trunk group.

Note: Look for and investigate a higher than normal amount of incoming trunk traffic.

9 **Incoming PC** — the number of incoming calls processed on the trunk group.

10 **Outgoing Usage** — the total time in CCS that outgoing calls lasted on trunks in the trunk group.

11 **Outgoing PC** — the number of outgoing calls processed on the trunk group.

Note: Look for and investigate a higher than normal amount of outgoing trunk traffic.

12 **Outgoing Overflow** — the number of times all trunks in this trunk group were busy when a user tried to gain access to the route and the system blocked the attempt or routed the call over an alternate route.

13 **All Trunks Busy** — the number of times all trunks in this route were busy, whether a user tried to gain access or not.

Note: Look for and investigate a higher than normal number of overflows and All Trunks Busy conditions.

14 **Toll PC** — the number of times that toll calls (0+ or 1+ calls) were established on Central Office (CO) and Foreign Exchange (FX) trunk routes.

Note: Look for and investigate a higher than normal number of toll calls.

Percent All Trunks Busy reporting (TFC104)

TFC104 is an All Trunks Busy report that allows the percent of time an All Trunks Busy condition occurs for a customer to be set. When call activity exceeds the percentage threshold during the reporting period, the system automatically outputs the report.

This report identifies the trunk group, the All Trunks Busy percentage for the trunk group, and the percentage threshold value.

The associated trunk group report (TFC002) is also automatically output at its scheduled report time.

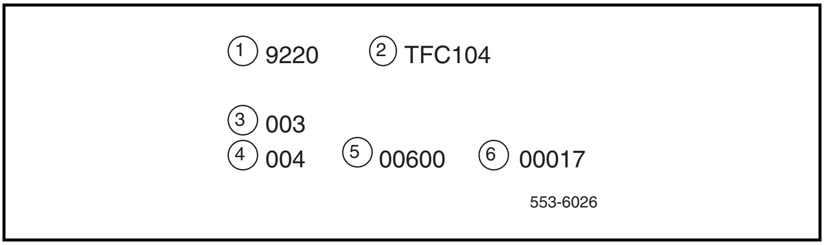
Table 53 shows Traffic Program LD 2 prompts used to configure and print the TFC104 report.

Table 53
Configuring and printing the TFC104 report

Facility	Overlay and prompts	Print programs
Traffic	LD 2 STHC	LD 2 TTHC

Figure 11 is an example of the TFC104 report that is automatically generated when an All Trunks Busy condition is reached. The circled numbers correspond to the description of fields following Figure 11.

Figure 11
TFC104 report example



```
①9220      ②TFC104

③003
④004    ⑤00600    ⑥00017
```

553-6026

1 **System ID** — the number assigned to the system for a specific site.

2 **Report Name** — the name of the report.

3 **Customer Number** — the customer number to which the trunk group belongs.

4 **Trunk Group** — Trunk Group Number that is the subject of the report.

5 **Busy** — indicates the All Trunks Busy percentage that occurred, in units of 0.1 percent.

   Note: Look for and investigate a higher than normal number of All Trunks Busy conditions.

6 **Threshold** — indicates the All Trunks Busy threshold for this customer, in units of 0.1 percent.

Long-duration call reporting (TFS40X and TFS41X)

TFS40X messages are output to the traffic terminal at regularly scheduled intervals showing long-holding connections.

Messages such as TFS401 and TFS402 are displayed to show the number of calls that exceeded the specified call duration threshold.

TFS411 and TFS412 are output at regularly scheduled intervals showing the total number of calls that exceeded the specified call duration threshold. These messages help you to monitor calls of unusually long duration.

TFS401 output automatically identifies the Terminal Numbers (TNs) of connections held for at least 36 hundred call seconds (CCS) but less than 50 CCS.

TFS411 provides a peg count of the number of connections held for at least 36 CCS but less than 50 CCS, together with total use on the connections.

TFS402 output automatically identifies the TNs of connections that were held for 50 CCS or longer.

TFS412 provides a peg count of the number of connections that were held for 50 CCS or longer, together with the total use on the connections.

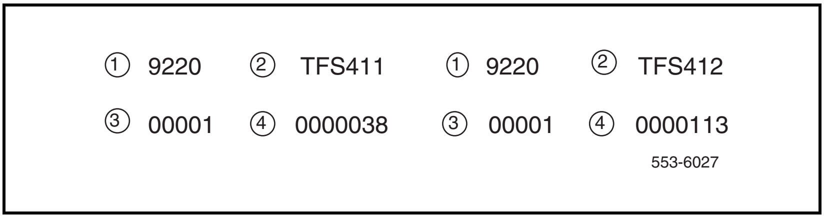
Table 54 specifies Traffic Program LD 2 prompts used to configure and print the TFS40X messages.

Table 54
Configuring and printing TFS40X messages

Facility	Overlay and prompts	Print programs
Traffic	LD 2 SOPC	LD 2 TOPC

Figure 12 is an example of the TFS411 and TFS412 reports. The circled numbers correspond to the description of fields below Figure 12.

Figure 12
TFS411 and TFS412 messages example



```
① 9220    ② TFS411     ① 9220    ② TFS412
③ 00001   ④ 0000038    ③ 00001   ④ 0000113
```

1 **System ID** — the number assigned to the system for a specific site.

2 **Message Name** — the name of the message.

3 **Number of Connections** — the number of calls that were held for the peg count of the report.

4 **Total Usage (CCS)** — the total amount of time all calls were held.

Note: Look for and investigate a higher than normal number of long call durations on trunk-to-trunk calls.

Routing measurements (TFN001)

TFN001 provides data related to individual Route List use. For each Least Cost Route List, the report shows how often the list was accessed, which entries in the list were used, and whether callers were successful in completing a selection.

By partitioning “high fraud” numbers into unique route list indexes, activity can be tracked more effectively. The report can show calls to international locations and 900 numbers, indicating possible unauthorized access.

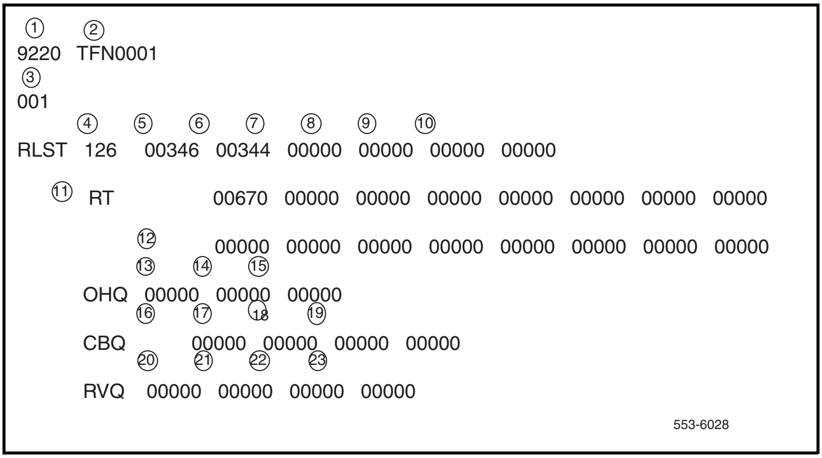
Table 55 shows Traffic Program LD 2 prompts to configure and print routing measurement reports.

Table 55
Configuring and printing the TFN001 report

Facility	Overlay and prompts	Print programs
Traffic	LD 2 SOPN	LD 2 TOPN

Figure 13 is an example of the TFN001 showing Route List information that indicates the usage of BARS/NARS and calls blocked by the Route List. The circled numbers correspond to the description of fields following Figure 13.

Figure 13
TFN001 report example



```
9220  TFN0001
001
RLST  126   00346  00344  00000  00000  00000  00000

        RT            00670  00000  00000  00000  00000  00000  00000  00000

                      00000  00000  00000  00000  00000  00000  00000  00000

         OHQ  00000  00000  00000

         CBQ         00000  00000  00000  00000

         RVQ  00000  00000  00000  00000
```

①
②
③
④
⑤
⑥
⑦
⑧
⑨
⑩
⑪
⑫
⑬
⑭
⑮
⑯
⑰
⑱
⑲
⑳
㉑
㉒
㉓
553-6028

1 **System ID** — the number assigned to the system for a specific site.

2 **Report Name** — the name of the report.

3 **Customer Number** — the customer number to which the trunk group belongs.

4 **Route List Number** — the Route List number for which the report was generated.

5 **Route List Requests** — the number of times the Route List was chosen to process a call.

6 **Route List Requests Served Without Delay** — the number of calls routed using the Route List that did not encounter any delay.

7 **Expensive Route Acceptances** — the number of times users allowed calls to be completed over expensive routes.

Note: Look for and investigate traffic using expensive routes.

8 **Route List Requests Standard Blocking** — the number of calls blocked at the Route List because routes or queues were not available.

Note: Look for and investigate callers attempting to call specific locations that are blocked.

9 **Not Used**

10 **Not Used**

11 **Route List Entry Usage** — the number of times each entry in the Route List was used.

12 **TD Calls** — the number of long-distance calls that used a tone detector dial tone to complete the call.

13 **OHQ Calls** — the number of calls placed in the Off-Hook Queue.

14 **OHQ Average Time** — the average time calls stayed in the Off-Hook Queue, in 0.1 seconds.

15 **OHQ Cancellations** — the number of calls that were canceled while waiting in the Off-Hook Queue.

16 **CHQ Calls** — the number of calls placed in the Call-Back Queue.

17 **CBQ Average Time** — the average time calls stayed in the Call-Back Queue in 0.1 seconds.

18 **CBQ Offerings** — the number of calls that were offered Call-Back Queuing.

19 **CBQ Cancellations** — the number of calls that were canceled by the user while waiting in the Call-Back Queue.

20 **RVQ Quantity** — the number of calls placed in the Remote Virtual Queue.

21 **RVQ Average Time** — the average time calls stayed in the Remote Virtual Queue, in 0.1 seconds.

22 **RVQ Offerings** — the number of calls that were offered Remote Virtual Queuing.

23 **RVQ Cancellations** — the number of calls that were canceled by the user while waiting in the Remote Virtual Queue.

Network Class of Service measurements (TFN002)

TFN002 provides information about outgoing BARS/NARS activity for each defined NCOS group. The report includes a count of the total number of call attempts each NCOS group generates.

By partitioning users, TIE trunks, and Authcodes into easily identified NCOS groups, normal calling patterns associated with each group can be monitored. Variations in normal calling patterns can be readily noticed.

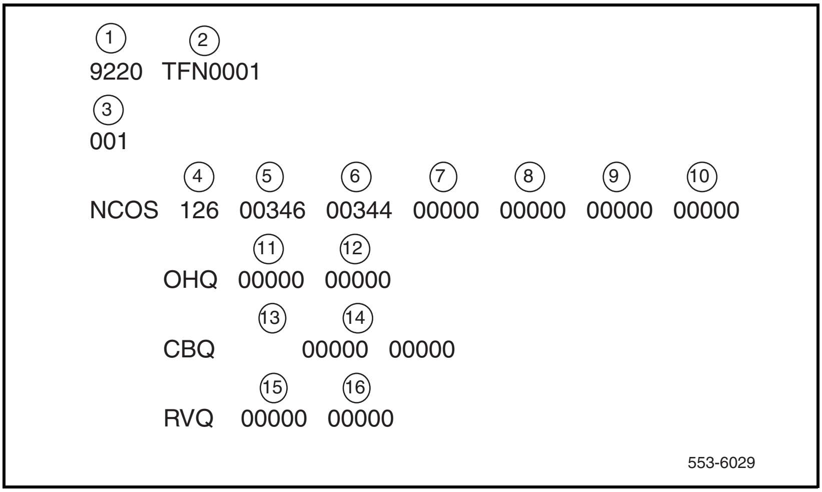
Table 56 specifies Traffic Program LD 2 prompts used to configure and print the TFN002 report.

Table 56
Configuring and printing the TFN002 report

Facility	Overlay and prompts	Print programs
Traffic	LD 2 SOPN	LD 2 TOPN

Figure 14 is an example of the TFN002 report showing the number of attempts a caller with a specific NCOS made during the specified reporting period. The circled numbers correspond to the description of fields following Figure 14.

Figure 14
TFN002 report example



```
9220  TFN0001
001
NCOS  126  00346  00344  00000  00000  00000  00000
        OHQ  00000  00000
        CBQ        00000  00000
        RVQ  00000  00000
```

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
553-6029

1 **System ID —** the number assigned to the system for a specific site.

2 **Report Name —** the name of the report.

3 **Customer Number —** the customer number to which the trunk group belongs.

4 **NCOS —** the NCOS group shown in the report.

5 **Call Attempts —** the number of calls attempted by the NCOS group.

Note: Look for and investigate excessive number of calls attempted to a specific destination.

6 **Routing Requests Served Without Delay —** the number of calls routed by the network that did not encounter any delay.

7 **Expensive Route Acceptances —** the number of times users allowed calls to be completed over expensive routes.

Note: Look for and investigate traffic using expensive routes.

8 **Network Call Standard Blocking —** the number of calls blocked by the network because routes or queues were not available.

Note: Look for and investigate callers attempting to call specific locations that are being blocked.

9 **Not Used**

10 **Expensive Route Refusals** — the number of calls refusing the use of expensive routes.

11 **OHQ Calls —** the number of calls placed in the Off-Hook Queue.

12 **OHQ Average Time —** the average time calls stayed in the Off-Hook Queue, in 0.1 seconds.

13 **CHQ Calls** — the number of calls placed in the Call-Back Queue.

14 **CBQ Average Time —** the average time calls stayed in the Call-Back Queue, in 0.1 seconds.

15 **CHQ Calls —** the number of calls placed in the Remote Virtual Queue.

16 **CBQ Average Time —** the average time calls stayed in the Remote Virtual Queue, in 0.1 seconds.

Checking the History File

Certain system messages or activities can be tracked and printed as required. The History File stores system messages in memory. The stored information can be accessed from a local or remote terminal and printed.

The type of information to be stored in the History File can be specified. This can include Maintenance messages (MTC), Service Change activity (SCH), Customer Service Change activity (CSC), Traffic outputs (TRF), and software error messages (BUG). By storing SCH activity and TRF output messages, information associated with traffic patterns that can reveal unauthorized access to the system can be retrieved.

Table 57 shows Traffic Program LD 2 prompts used to configure and print specific messages for the History File.

Table 57
Configuring and printing the History File

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - IOTB, HIST, ADAN USER	LD 22 by CFN or LD 22 by ADAN

Analyzing Operational Measurement reports

Operational Measurement reports are generated at the Meridian Mail administration terminal. They provide information about Thru-dial and Outcalling activities that can help locate and prevent fraud.

Monitoring Thru-dial activities

Assess how callers use Thru-dial by reviewing the Operational Measurement Reports Voice Service Summary. This report lists the number of times callers used a service such as Thru-dial, and the average length of each call. Use this report to determine whether Thru-dial traffic is unusually high for your system. A high amount of Thru-dial tandem traffic could indicate unauthorized use.

Table 58 on page 231 is an example of the Voice Service Summary report.

Table 58
Voice Service Summary report example

Operational Measurement				
Voice Service Summary				
Interval Start-End	**Service Name**	**Number of Accesses**	**Average Length (in sec)**	**Meridian Mail Usage (in CCS)**
2/08 9:00 - 10:00	Thru-dial	5	60	3
2/08 9:00 - 10:00	Voice Menu	10	30	3
2/08 9:00 - 10:00	VM Logon	10	30	3
2/08 9:00 - 10:00	Call Answering	60	30	18
2/08 9:00 - 10:00	Express Messaging	10	60	6
2/08 9:00 - 10:00	Voice Announcements	5	60	3
2/08 9:00 - 10:00	Networking	10	60	6
2/08 9:00 - 10:00	Voice Administration	0	0	0
2/08 9:00 - 10:00	Time of Day Control	0	0	0
2/08 9:00 - 10:00	Delivery to Non-users	5	0	0
2/08 9:00 - 10:00	Remote Notification	0	0	3
2/08 9:00 - 10:00	Remote Activation	0	0	0

The following describes the fields in the report. Some of these fields differ slightly, depending on the release of software:

- **Interval Start-End** — the start and end time of each reporting interval.
- **Service Name** — the name of the service.
- **Number of Accesses** — the number of direct calls made to each service.
- **Average Length** — the average length of a call in seconds.
- **Meridian Mail Usage** — the amount of time in CCS Meridian Mail service was active.

Monitoring Outcalling activities

Assess the use of the Outcalling features Delivery to Non-users and Remote Notification through the Operational Measurement Reports Voice Service Summary and Outcalling Detail. These reports must be used together to detect excessive use of these features.

The Voice Service Summary lists the number of times a service was used and the average length of service. Use this report to determine if your system is experiencing excessive use of Message Delivery to Non-users and Remote Notification. Such an increase could indicate an unauthorized access problem.

Table 58 on page 231 shows an example of the Voice Service Summary report.

The Outcalling Detail report gives detailed statistics on Outcalling activity for incoming and outgoing calls. This report shows the number of requests, attempts, retries, and the average wait time. Use this report to determine if there is higher than normal Message Delivery to Non-users and Remote Notification tandem traffic for the system. An increase in such traffic could indicate a problem with unauthorized access.

Table 59 on page 233 is an example of the Outcalling Detail report.

Table 59
Outcalling Detail report example

Operational Measurement										
Outcalling Detail (Remote Notification and Delivery to Non-users)										
			Number of Attempts							
	Number of New Requests		New Requests		Retries		Number of Successes		Wait Avg	Time Max
Interval Start-End	RN	DNU	RN	DNU	RN	DNU	RN	DNU	(sec)	(sec)
2/08 9:00 - 10:00	0	0	0	0	0	0	0	0	0	0
2/08 9:00 - 10:00	1	0	0	0	0	0	1	0	259	259
2/08 9:00 - 10:00	4	0	1	0	0	0	0	0	0	0
2/08 9:00 - 10:00	1	1	0	1	0	0	0	0	0	0

The following describes the fields in the report:

- **Interval Start/End** — the start and end time of the report.
- **Number of New Requests** — the total number of requests the Remote Notification user made to deliver a message to a non-user.
- **Number of Attempts** — the total number of attempts made at Remote Notification and Delivery to Non-users.
- **New Requests** — the number of new requests attempted.
- **Retries** — the number of times the system had to retry Remote Notification or Delivery to Non-users calls because the number was busy or not answered.
- **Number of Successes** — the number of successful Remote Notification and Message Delivery to Non-users calls.
- **Wait Time** — the average time an Outcalling agent took to acquire the necessary resources to call out to the specified DN.

Appendix A: Access Restriction features

Use Table 60 to assess the available features that can be used to restrict access. **X** indicates features that can be used to control each area of access. **Test** indicates features that can be used to assess potential abuse in the areas of access. **Optional** indicates features that may or may not be used to control their area of access.

Table 60
Feature Assessment (Part 1 of 3)

Security Features	DISA	Voicemail	Internal	Network	System
Class of Service	X	X	X	X	
Trunk Group Access Restrictions	X	X	X	X	
System Speed Call			X		
Authorization Codes	X		X	X	
Sta Spec Authcode			X		X
Forced Charge Account			X	X	
Controlled Class of Service			X		
Enhanced Controlled Class of Service			X		
Flexible Feature Code			X		
Code Restriction			X	X	

Table 60
Feature Assessment (Part 2 of 3)

Security Features	DISA	Voicemail	Internal	Network	System
New Flexible Code Restriction			X	X	
Call Forward External Deny			X		
Flexible Feature Code - Remote Call Forward			X		
Internal Call FWD			X		X
Call Detail Recording	Test	Test	Test	Test	
Internal Call Detail Recording			Test		
Traffic Measurement	Test	Test	Test	Test	
Supplemental Digit Restriction and Recognition	X		X		
Network Class of Service	X	X	X	X	
Network Speed Call	Optional		Optional	Optional	
Network Authorization Code - Authorization Code Conditionally Last	Optional		Optional	Optional	
Routing Control			X	X	
Incoming Trunk Group Exclusion				X	
Meridian Mail System Options Voice Security		X			
Meridian Mail User Options		X			
Meridian Mail Voice Menus Thru-dial Security		X			
Level 1 Password					X

Table 60
Feature Assessment (Part 3 of 3)

Security Features	DISA	Voicemail	Internal	Network	System
Level 2 Password					X
Limited Access to Passwords					X
Trunk barring					
Scheduled Access Restrictions					
Restricted Call Transfer					
User Selectable Call Redirection					
Multi-user User Name					Test
Attendant Administration					X
Automatic Set Relocation					X
History File					Test
Password Protection		X			
A/B Switch to Restrict External Access to Administration		X			
Authorization Code					
Alarms					

Appendix B: Trunk Group Access Restrictions worksheet

Use Table 61 on page 240 to specify Trunk Group Access Restrictions (TGAR) for each route. Also, specify the trunk type and access code required to access that route.

Table 61
Trunk Group Access Restrictions worksheet (Part 1 of 4)

TGAR WORKSHEET

Access Code	Route	Trunk Type	TGAR Code																															
			0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	0																																	
	1																																	
	2																																	
	3																																	
	4																																	
	5																																	
	6																																	
	7																																	
	8																																	
	9																																	
	10																																	
	11																																	
	12																																	
	13																																	
	14																																	
	15																																	
	16																																	
	17																																	
	18																																	
	19																																	
	20																																	
	21																																	
	22																																	
	23																																	
	24																																	
	25																																	
	26																																	
	27																																	
	28																																	
	29																																	
	30																																	
	31																																	
	32																																	
	33																																	
	34																																	
	35																																	

553-5948

Table 61
Trunk Group Access Restrictions worksheet (Part 2 of 4)

TGAR WORKSHEET

Access Code	Route	Trunk Type	TGAR Code																															
			0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	36																																	
	37																																	
	38																																	
	39																																	
	40																																	
	41																																	
	42																																	
	43																																	
	44																																	
	45																																	
	46																																	
	47																																	
	48																																	
	49																																	
	50																																	
	51																																	
	52																																	
	53																																	
	54																																	
	55																																	
	56																																	
	57																																	
	58																																	
	59																																	
	60																																	
	61																																	
	62																																	
	63																																	
	64																																	
	65																																	
	66																																	
	67																																	
	68																																	
	69																																	
	70																																	
	71																																	

553-5949

Table 61
Trunk Group Access Restrictions worksheet (Part 3 of 4)

TGAR WORKSHEET

Access Code	Route	Trunk Type	TGAR Code																															
			0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	72																																	
	73																																	
	74																																	
	75																																	
	76																																	
	77																																	
	78																																	
	79																																	
	80																																	
	81																																	
	82																																	
	83																																	
	84																																	
	85																																	
	86																																	
	87																																	
	88																																	
	89																																	
	90																																	
	91																																	
	92																																	
	93																																	
	94																																	
	95																																	
	96																																	
	97																																	
	98																																	
	99																																	
	100																																	
	101																																	
	102																																	
	103																																	
	104																																	
	105																																	
	106																																	
	107																																	

553-5950

Table 61
Trunk Group Access Restrictions worksheet (Part 4 of 4)

TGAR WORKSHEET

Access Code	Route	Trunk Type	TGAR Code																															
			0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	108																																	
	109																																	
	110																																	
	111																																	
	112																																	
	113																																	
	114																																	
	115																																	
	116																																	
	117																																	
	118																																	
	119																																	
	120																																	
	121																																	
	122																																	
	123																																	
	124																																	
	125																																	
	126																																	
	127																																	
	128																																	

553-5951

Index

Nortel Communication Server 1000

System Security Management

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Publication number: 553-3001-302
Document release: Standard 11.00
Date: June 2006

Produced in Canada

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.