Nortel Communication Server 1000

Telephony Services Access Control Management

Release: 7.0
Document Revision: 04.01

www.nortel.com

NN43001-602

Nortel Communication Server 1000
Release: 7.0
Publication: NN43001-602
Document release date: 4 June 2010

Contents

New in this release

This section describes what's new in *Telephony Services Access Control Management* (NN43001-602) for Communication Server 1000 (CS 1000) Release 7.0.

Features

See the following section for information about feature changes:

RLI and DMI enhancement

For Communication Server Release 7.0, the range of allowable Route List Index (RLI) and Digit Manipulation Index (DMI) values is increased from 0–999 to 0–1999. For more information about RLI and DMI values, see "28. Route List Index (RLI)" (page 100).

Other changes

For a detailed revision history of this document, see Table 1 "Revision history" (page 9).

Table 1
Revision history

June 2010	Standard 04.01. This document is up-issued to support Communication Server 1000 (CS 1000) Release 7.0.
May 2009	Standard 03.01. This document is up-issued to support Communication Server 1000 (CS 1000) Release 6.0.
March 2008	Standard 02.02. This document is up-issued to add Mobile X - Security code and authorization information.
December 2007	Standard 02.01. This document is up-issued to support Communication Server 1000 (CS 1000) Release 5.5.
June 2007	Standard 01.02. This document is up-issued to remove the Nortel Networks Confidential statement.

May 2007	Standard 01.01. This document is up-issued to support CS 1000 Release 5.0 This document contains information previously contained in the following legacy document, now retired: System Security Management (553-3001-302). Some sections previously found in the legacy document are moved to the new document *Security Management Fundamentals* (NN43001-604).
August 2005	Standard 10.00. This document is up-issued for CS 1000 Release 4.5.
September 2004	Standard 9.00. This document is up-issued for CS 1000 Release 4.0.
October 2003	Standard 8.00. This document is issued for 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.

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.

Introduction

This chapter provides an overview of the document. The chapter is divided into the following sections:

Purpose

This document contains the information you need to avoid misuse or abuse of your Communication Server 1000 (CS 1000) system.

For information about security features in Communication Server 1000, including tools to manage accounts, protect signalling and media streams, and secure remote access, see *Security Management Fundamentals* (NN43001-604).

About this document

This section provides an overview of how you can 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.

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

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 7.0 software. For more information on legacy products and releases, click the Technical Documentation link under Support & Training on the Nortel home page: www.nortel.com.

The subject of this document is the implementation of system-wide security features.

Applicable systems

This document applies to the following systems:

- Communication Server 1000E (CS 1000E) CP PII, CP PIV and CP PM
- Communication Server 1000M Single Group (CS 1000M SG) CP PII, CP PIV
- Communication Server 1000M Multi Group (CS 1000M MG) CP PII, CP PIV
- Meridian 1 PBX 61C CP PII, CP PIV
- Meridian 1 PBX 81C CP PII, CP PIV

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 software and configured to include a Signaling Server, they become CS 1000 systems. Table 2 "Meridian 1 systems to CS 1000 systems" (page 14) lists each Meridian 1 system that supports an upgrade path to a CS 1000 system.

Table 2
Meridian 1 systems to CS 1000 systems

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

For more information, see the following NTPs:

- *CS 1000M and Meridian 1 Large System Upgrades Overview* (NN43021-458)

Intended audience

This document is intended for administrators responsible for configuring security features.

Terminology conventions

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

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

Access control overview

Your 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 that the system supports.

Toll Fraud

To secure the system against unauthorized use, you must become familiar with the current system software configuration, keep track of which security features are active, and monitor calling patterns to detect unauthorized activity. Inadequate control of calling privileges and unprotected physical access to switching systems are the main causes of toll fraud. Consider the following guidelines:

- Use the safeguards available in the system to limit access to the functions and features supported by your system.
- Exercise caution when handling and disposing of information that can compromise system security.

The following list describes some of the more common causes of toll fraud:

- Direct Inward System Access (DISA) poses a serious source of toll fraud because callers can use it to gain unauthorized remote access to a second dial tone. 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.
- Voice mail and automated attendant services pose a risk of toll fraud if proper safeguards are not in place. If a caller knows long-distance access codes or trunk access codes, they can access a voice mail

system and place toll calls. They can even take over a mailbox for use as a bulletin board.

- Remote system administration tools can pose a risk of toll fraud, if maintenance ports are not properly secured. Remote system administration allows system technicians to access, configure, and troubleshoot both the system and Call Pilot software and hardware problems remotely. An unauthorized person who gains access to the system can change the system configuration, degrade system performance, and fraudulently use services. If a caller knows the password, they can access the system by dialing in to a remote access port, where they can 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.

You can help to reduce the risk of toll fraud by carefully monitoring the system, 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 using these methods.

To detect outgoing call fraud, watch for:

- calls to unusual locations
- high call volume
- long call duration
- international calls
- unexplained calls to the 809 or 900 are code
- unexplained calls to international area codes

To detect incoming call fraud, watch for:

- long holding times
- unexplained surges in traffic
- 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.

General access control practices

Your telecommunications facility must be protected by a security plan to prevent unauthorized and fraudulent use. Failure to implement a security plan 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.

Consider including the following steps in your security plan:

- Deny unauthorized access to long-distance trunk facilities (such as thru-dial) when using voice mail. You can accomplish this by requiring a password to access voice mail, or by blocking the activation of voice mail.
- 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 dispose of 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 keep the plan up-to-date. This minimizes the opportunity for unauthorized persons to abuse and damage the telecommunications facilities.

The following chapters describe methods you can use to plan, implement, and verify procedures to protect the system from misuse.

Controlling call privileges

Navigation

This section contains information on the following topics:

Introduction

This chapter describes the steps you need to take to implement the system call processing security features. You can secure system call processing by limiting and controlling call privileges, and restricting access to the system facilities and features.

Restrict call processing privileges and restrictions are implemented by the following:

- "Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS)" (page 51))
- "Controlling Direct Inward System Access" (page 57)
- "Controlling Multi-Tenant Services" (page 59)

Defining basic access restrictions

You can use basic access restrictions to limit users' access to only the facilities and calling privileges their jobs require. In this way, you can deter abuse by internal users, and restrict access to toll facilities by external users. The following features control access restrictions:

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

Class of Service and TGAR work together to control whether long distance calls can be placed using specified telephones, DISA directory numbers, TIE trunks, and Authorization Codes (Authcodes).

Class of Service

Use Class of Service to prevent users from placing unauthorized toll calls. Using Class of Service, you can create groups of telephones, DISA directory numbers, TIE trunks, and Authcodes, and assign to these groups the calling privilege levels that suit the group's communication needs.

For each telephone, DISA directory number (DN), TIE trunk, and Authcode, assign one of the following Classes of Service:

- 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 3 "Class of Service assignment" (page 21) outlines various call types and shows whether they are possible for each Class of Service assignment.

Table 3
Class of Service assignment

	UNR	CTD/ CUN	TLD	SRE	FRE	FR1	FR2
Incoming trunk call	Yes	Yes	Yes	Yes	Yes using call modific ation	No	No
Outgoing nontoll trunk call	Yes	Yes	Yes	Yes using attendant or UNR telephone	Yes using UNR teleph one	No	No
Outgoing toll trunk call (0 or 1+ on COT or FX)	Yes	Yes using BARS/NAR S No direct access	Yes using attendant or UNR telephone No direct access	Yes using attendant or UNR telephone No direct access	Yes using UNR teleph one No direct access	No	No

Table 3
Class of Service assignment (cont'd.)

	UNR	CTD/ CUN	TLD	SRE	FRE	FR1	FR2
To/from TIE trunk	Yes	Yes	Yes	Yes	Yes	Yes	Yes
To/from internal	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BARS/NARS calls TGAR = No	Uses NCOS only	Uses NCOS only	Uses NCOS and Class of Service	Uses NCOS and Class of Service	Uses NCOS and Class of Service	Uses NCOS and Cl ass of Service	Uses NCOS and Cl ass of Service
BARS/ NARS calls TGAR = Yes	Uses NCOS and TGAR	Uses NCOS and TGAR	Uses NCOS, Class of Service, and TGAR	Uses NCOS, Class of Service, and TGAR	Uses NCOS, Class of Service, and TGAR	Uses NCOS, Class of Servi ce, and TGAR	Uses Class of Ser vice only

Table 4 "Implementing Class of Service" (page 22) lists the facilities that can be implemented using Class of Service, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 4
Implementing Class of Service

Facility	Overlay and prompt	Print program
Telephones/Universal Extension	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

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

You can assign Telephones, DISA directory numbers, TIE trunks, and Authcodes to TGAR groups. When users attempt to access trunk routes from telephones, TIE trunks, or Authcodes, the system uses their TGAR

assignment to determine whether they can access that trunk. Each trunk must be assigned to a Trunk Access Restriction Group (TARG), and the system allows or denies access as follows:

- 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 allowed, the system uses the Class of Service assignment to determine call eligibility. The system always uses the most restrictive assignment (Class of Service 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 voice mail agents and data ports.

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. See “Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS)” (page 51).

Table 5 "Implementing TGAR" (page 23) 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 5
Implementing TGAR

Facility	Overlay and prompt	Print program
Telephones/Universal Extension	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 6 "TGAR Routing" (page 23) lists the TGAR Routing.

Table 6
TGAR Routing

Route number	Rank type
0	COT

Table 6
TGAR Routing (cont'd.)

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

In the example shown in Table 7 "TGAR Access Restriction Codes" (page 24), assume the seven TGAR codes shown are required.

Table 7
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. You can use the following features to override Class of Service 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 "Outgoing Call Barring" (page 25))
- System Speed Call (see "System Speed Call" (page 25))
- Network Speed Call (see "Network Speed Call" (page 26))
- Authorization Code (see "Authorization Code" (page 27))
- Forced Charge Account (see "Forced Charge Account" (page 29))
- Controlled Class of Service (see "Controlled Class of Service" (page 30))
- Enhanced Controlled Class of Service (see "Enhanced Controlled Class of Service" (page 31))

- Electronic Lock (see “Electronic Lock” (page 31))
- Code Restriction Data Block (see “Code Restriction Data Block” (page 32))
- New Flexible Code Restriction (see “New Flexible Code Restriction” (page 32))
- Called Party Disconnect Control (see “Called Party Disconnect Control” (page 33))
- Scheduled Access Restrictions (see “Scheduled Access Restrictions” (page 33))
- Trunk Barring (see “Trunk Barring” (page 40))

Outgoing Call Barring

You can configure Outgoing Call Barring to limit use of Customer Call Forward (CCFW). When Outgoing Call Barring is activated, the user can set up call forwarding only to DNs that are not barred. If the barring level denies calling a DN, that DN also cannot 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 8 "Implementing Outgoing Call Barring" (page 25) 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 8
Implementing Outgoing Call Barring

Facility	Overlay and prompt	Print program
Telephones/Universal Extension	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

You can configure System Speed Call (SSC) on a telephone to enable users to temporarily override the Network Class of Service (NCOS) assigned to the telephone. This allows users to place calls to approved destinations while limiting the potential for unauthorized calling to other numbers.

SSC extends the capabilities of Speed Call; allowing abbreviated dialing; the SSC list contains the telephone numbers that a user can dial using this feature. Telephones can be assigned to SSC lists, and can 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 Class of Service and TGAR because the attendant is not subject to these restrictions.

An SSC list can also override the telephone restrictions imposed through BARS/NARS. See “Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS)” (page 51).

Table 9 "Implementing SSC" (page 26) 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 9
Implementing SSC

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

Network Speed Call

You can configure Network Speed Call (NSC) to enable users to temporarily override calling restrictions and place calls to specific telephone numbers that are otherwise barred. 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 10 "Implementing NSC" (page 27) lists facilities that can be implemented using NSC, programs and prompts to implement the feature, and programs to print information about the feature.

Table 10
Implementing NSC

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
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

You can configure Authorization Codes (Authcodes) to enable users to temporarily override access restrictions assigned to telephones, DISA directory numbers, or TIE trunks. Use Authcodes to 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.

If a user enters an Authcode that has an associated Class of Service, TGAR, and BARS/NARS NCOS, they subsequently have the calling privileges of the Authcode rather than those of the DISA directory number, telephone, or TIE trunk for the duration of the call.

The system offers Station Specific Authcodes, which you can use 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, you 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 Authorization Code (Authcode) Alarm feature generates an alarm when an invalid Authcode is entered. The alarm indicates 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 any 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.

Table 11
Enable the Authcode alarm feature in LD 88

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.

Authcodes can be used to override telephone restrictions imposed through BARS/NARS. See “Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS)” (page 51).

Table 12 "Implementing Authcode" (page 29) 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 12
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

Configure Forced Charge Account (FCA) to allow users to temporarily override toll-denied Class of Service restrictions when by entering 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.

FCA can also be used to override restrictions imposed through BARS/NARS. See “Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS)” (page 51).

Table 13 "Implementing FCA" (page 30) 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 13
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

Configure Controlled Class of Service (CCOS) to allow the following users to temporarily alter telephone Class of Service:

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

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

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

Table 14 "Implementing CCOS" (page 30) 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 14
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

Use Enhanced Controlled Class of Service (ECCS) to extend the controller function of CCOS to attendant consoles and M3000 terminals equipped with a Controller Key. ECCS 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 15 "Implementing ECCS" (page 31) 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 15
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

Use Electronic Lock (ELK) to allow 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 16 "Implementing ELK" (page 32) 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 16
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

Use Code Restriction Data Block (CRB) to give 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 17 "Implementing CRB" (page 32) 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 17
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

You can use New Flexible Code Restriction (NFCR) to enhance CRB by allowing toll-denied telephones, TIE trunks, and Authcodes to selectively make certain calls on outgoing trunk routes. You can 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 18 "Implementing NFCR" (page 32) 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 18
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

Table 18
Implementing NFCR (cont'd.)

Facility	Overlay and prompts	Print programs
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

You can use Called Party Disconnect Control (CPDC) to control 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 19 "Implementing CPDC" (page 33) 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 19
Implementing CPDC

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

Scheduled Access Restrictions

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

These TGAR, Class of Service, 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, 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 package 162 SAR Scheduled Access Restriction (X81). Package 162 also requires the following:

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

  The following packages are also required:

  — package 63 NAUT Network Authorization code

  — package 86 TENS Multi-Tenant Service

Feature implementation

Table 20
Create or modify Schedule Access Restrictions using LD 88

Prompt	Response	Description
REQ	NEW CHG	Add, or change.
TYPE	SAR	Scheduled Access Restrictions.
CUST	xx	Customer number as defined in LD 15.

Table 20
Create or modify Schedule Access Restrictions using LD 88 (cont'd.)

Prompt	Response	Description
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.
	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

Table 20
Create or modify Schedule Access Restrictions using LD 88 (cont'd.)

Prompt	Response	Description
- 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.

Table 21
Print command in LD 88

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.

Table 22
With SAR, configure the Authcode data block not to automatically generate Authcodes using LD 88

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).
RANR	0-511	RAN route number for "Authcode Last" prompt (NAUT).
CLAS	(0)-115	Classcode value assigned to Authcode.

Table 22
With SAR, configure the Authcode data block not to automatically generate Authcodes using LD 88 (cont'd.)

Prompt	Response	Description
AUTO	NO	Do not automatically generate Authcodes. The AUTO prompt appears when package 63 NAUT Network Authorization code is equipped and REQ = NEW. The Authcode length must be a minimum of four digits.

Table 23
Define SAR entries in the Authcode entries data block using LD 88

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).
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 24 "Trunk Barring route categories" (page 40) shows the four route categories that Trunk Barring recognizes, and the types of routes in each category.

Table 24
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 sounds.

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) sounds 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) sounds 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 package 132 TBAR Trunk Barring.

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.

Table 25
Enter or change Trunk Barring parameters using LD 56

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
-ART	0-63	ART to assign to route.
TYPE	RCDT	Change the route category default table.
-COT	(0)-63	COT, FEX, and WAT routes are assigned the entered number.

Table 25
Enter or change Trunk Barring parameters using LD 56 (cont'd.)

Prompt	Response	Description
-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 (see "Default Class of Service" (page 43))
- Default Trunk Group Access Restriction (TGAR) and Trunk Access Restriction Group number (TARG) (see "Default Trunk Group Access Restriction (TGAR) and Trunk Access Restriction Group number (TARG)" (page 44))
- Call Forward Default Length and Range (see "Call Forward Default Length and Range" (page 45))
- Security Banner at System Login (see "Security Banner at System Login" (page 45))
- Number of Invalid Attempts to LAPW Password in Overlays (Failed Login Attempt Threshold) (see "Failed Login Attempt Threshold" (page 45))
- PWD2/PWD1/LAPW Passwords and LAPW Login names (see "PWD2/PWD1/LAPW Passwords and LAPW Login names" (page 45))
- Problems Determination Tool (PDT) Access Information (see "Problems Determination Tool (PDT) Access Information" (page 46))

Default Class of Service

System Access Enhancements provide highly restricted access by configuring the default Class of Service 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 has a default value of 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 have a default Class of Service 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 has a default Class of Service 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 default values for Trunk Group Access Restriction (TGAR) and Trunk Access Restriction Group number (TARG) were previously "0". This provided unrestricted toll access after Class of Service 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 package 164 LAPW Limited Access to Overlays 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 package 164 LAPW Limited Access to Overlays 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).

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 preselected default values, 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 Telephony Manager (TM). The TM 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 “User Selectable Call Redirection” (page 47))
- Call Forward External Deny (see “Call Forward External Deny” (page 48))
- Internal Call Forward (see “Internal Call Forward” (page 48))
- Call Forward All Calls (see “Call Forward All Calls” (page 49))
- Call Forward to Trunk Access Code (see “Call Forward to Trunk Access Code” (page 49))
- Call Forward Originating or Forwarded Class of Service (see “Call Forward Originating or Forwarded Class of Service” (page 50))
- Remote Call Forward (see “Remote Call Forward” (page 51))

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 multiline 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 26 "Implementing USCR" (page 48) 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 26
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 27 "Implementing CFXD" (page 48) 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 27
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 28 "Implementing ICF" (page 49) 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 28
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 29 "Implementing CFW" (page 49) 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 29
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 30 "Implementing CFTA" (page 50) 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 30
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 Class of Service access privileges of the telephone or trunk that originates the call or the telephone that forwards the call. By using the Class of Service 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 31 "Implementing CFO or CFF" (page 50) 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 31
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 32 "Implementing RCFW" (page 51) 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 32
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 “North American Numbering Plan” (page 52))
- Supplemental Digit Recognition/Restriction (see “Supplemental Digit Recognition/Restriction” (page 52))
- Network Class of Service and Facility Restriction Level (see “Network Class of Service and Facility Restriction Level” (page 53))
- Authorization Code Conditionally Last (see “Network Authorization Codes” (page 54))
- Time-of-Day Routing (see “Time-of-Day Routing” (page 54))
- Routing Control (see “Routing Control” (page 55))
- Incoming Trunk Group Exclusion (see “Incoming Trunk Group Exclusion” (page 56))
- Free Calling Area Screening (see “Free Calling Area Screening” (page 56))

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 (INPA) and Carrier Access Codes (CAC). 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 33 "Implementing NANP" (page 52) 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 33
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 34 "Implementing SDRR" (page 53) 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 34
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, Class of Service, and FRL are used to determine which call facilities are available to process a particular call.

Table 35 "Implementing NCOS and FRL" (page 53) 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 35
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

Table 35
Implementing NCOS and FRL (cont'd.)

Facility	Overlay and prompts	Print programs
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 36 "Implementing NAUT" (page 54) 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 36
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 37 "Implementing TOD" (page 55) 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 37
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 38 "Implementing RTCL" (page 55) 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 38
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

Table 38
Implementing RTCL (cont'd.)

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 - 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 39 "Implementing ITGE" (page 56) 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 39
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 40 "Implementing FCAS" (page 57) 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 40
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 41 "Implementing DISA" (page 57) 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 41
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. See “Routing Control” (page 55) for configuration details.

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

- Security Code (see “Security Code” (page 58))
- Authorization Code (see “Authorization Code” (page 58))
- Service restrictions (see “Service restrictions” (page 58))

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 42 "Implementing SCOD" (page 58) 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 42
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 Class of Service, 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.

See “Authorization Code” (page 27) for information about how to assign Authcodes to DISA.

Service restrictions

A Class of Service, 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.

See "Class of Service" (page 20), "Trunk Group Access Restrictions" (page 22), and "Network Class of Service and Facility Restriction Level" (page 53) for information about assigning these restrictions to the DISA directory number.

Table 43
LD 24- Configure a Mobile Service DN with Security Code

Prompt	Response	Description
REQ:	CHG NEW PRT	Change route, create a new route, print Mobile Service DN information.
TYPE:	MSA	Mobile Service Access
CUST	x...x	Customer number
SPWD	x.....x	Security Data Password
DN	x...x	Mobile Service DN, the DN can be up to 7 digits.
SCOD	x...x	Security Code (1-8 digit DISA security access code)
AUTR	YES	Enable Authorization Code Required
CCBA	YES	Enable Allow Collect Call Blocking Answer Signal to be sent

Controlling Multi-Tenant Services

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

- Tenant-to-tenant access (see "Tenant-to-Tenant Access" (page 59))
- Tenant-to-route access (see "Tenant-to-Route Access" (page 60))
- Console Presentation Group assignment (see "Console Presentation Group (CPG) assignment" (page 60))

Tenant-to-Tenant Access

A tenant's relationship with other tenants in the system is defined by Tenant-to-Tenant Access (TACC). You can configure a tenant to allow or deny it direct internal call access to some or all tenants.

Table 44 "Implementing TACC" (page 60) 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 44
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 45 "Implementing RACC" (page 60) lists the facilities that can be implemented using RACC, the programs and prompts used to implement them, and the programs to print information about the feature.

Table 45
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 are automatically configured to be members of CPG 0. You can create other CPGs using the configuration program.

Table 46 "Implementing CPG" (page 60) 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 46
Implementing CPG

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

System security features verification

Navigation

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 Call Pilot. It provides general guidelines to help you verify those system security features that most impact the telecommunications facilities. However, Nortel recommends that you use your own system configuration scenarios to verify if security features have been implemented correctly and are effective.

Use the following procedures to verify security:

- 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 new or existing system security.

New system security verification

Use the security installation checklist together with new system configuration planning to properly coordinate system security features with the creation of the customer configuration database. Security features you select from this checklist must be implemented using the system administration overlays.

Compare new system printouts against the security installation checklist.

Existing system security verification

Use the security audit checklist 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 be implemented using system configuration programs.

Compare the new system printouts against the security audit 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. If this feature is correctly configured, the call connects.
- Place an external call to a telephone forwarded to an external number and specified as CFXD. If this feature is correctly configured, the does not connect.

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 must 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 connects.
- If CFTA in the customer data block is set to No, the call does not connect.

Verify DISA access restrictions

In the following list, choose the method your system uses to implement security for DISA calls:

- 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 that has NCOS/TGAR/FRL configured to allow long-distance calling. If the feature is correctly configured, the call connects.
- Place a long-distance call to a DISA number that has NCOS/TGAR/FRL configured to disallow long-distance calling. If this feature is correctly configured, the call does not connect.

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 that has NCOS/TGAR/FRL configured to allow DISA calling. If this feature is correctly configured, the call connects.
- Place a long-distance call using an SCOD from a DISA number that has NCOS/TGAR/FRL configured to disallow DISA calling. If this feature is correctly configured, the call does not connect.

DISA access using an Authcode

To verify the operation of this security feature:

- Place a noninternational long-distance DISA call using an Authcode that is configured to allow long-distance but not international calls. If

this feature is correctly configured, the call connects normally, unless it is an international call.

- Place an international long-distance DISA call using an Authcode that is configured to allow long distance but not international calls. If this feature is correctly configured, the call does not connect.

Verify BARS/NARS access restrictions

The system provides many security features to prevent unauthorized BARS/NARS access. Verify that the following features are configured to provide secure operation:

- 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. If this feature is correctly configured, the call connects.
- Place a long-distance 976 call from a telephone to an area code denying 976 dialing. If this feature is correctly configured, the call does not connect.

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 connects.
- 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 does not connect.

- 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 connects.
- 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 does not connect.

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 connects without a request for an Authcode.
- Place a toll call using a telephone that does not meet minimum FRL requirements for a route list. If this feature is correctly configured, a tone or recorded message sounds, 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. If this feature is correctly configured, the call connects.
- Place a call after regular business hours to a destination that is restricted during off hours. If this feature is correctly configured, the does not connect.

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. If this feature is correctly configured, the call connects.
- Place a call from the same telephone after RTCL goes into effect. If this feature is correctly configured, the call does not connect.

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. If this feature is correctly configured, the call connects.

- 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. If this feature is correctly configured, the call does not connect.

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:

- To verify that Level 1 users cannot change Level 2 passwords, log on to the system console using the Level 1 password, access LD 17, and try to change the Level 2 password. If configured correctly, the program prompts for the Level 2 password, thus restricting access to the password change privilege.
- To verify that Limited Access password (LAPW) users cannot access LD 17, log on to the system console using the Limited Access account. Access LD 17. If the password is configured to restrict access to LD 17, LD 17 does not load.
- To verify that the invalid login threshold is configured, make repeated attempts to log on to the system console using an invalid password. When the threshold value is reached; the port is locked out and the other maintenance TTYs on the system receive a message detailing the logon attempts. To verify that a message is sent to other maintenance terminals, log on to another port using the Level 2 password. A special message is 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. If this feature is correctly configured, you can log on and run

applications, but you cannot 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.
- Attempt to log on to the Application Processor console using an invalid user ID. After a number of attempts to log on using an invalid user ID, the system no longer displays the logon prompt. You can configure the number of permitted unsuccessful logon attempts; the default value is 3.

Verify Thru-dial restrictions for mailboxes and menus

To verify Call Pilot 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 Call Pilot. When Call Pilot 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. If this feature is correctly configured, the call connects.
- Place a call to a telephone that performs a Forward No Answer to Call Pilot. When Call Pilot 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. If this feature is correctly configured, the call does not connect.

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. If this feature is correctly configured, the call connects.
- 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. If this feature is correctly configured, the call does not connect.

Express Messaging

To verify the operation of this feature:

- Set a permission/restriction table for Call Pilot access using the express messaging feature.
- Dial a number that is permitted to access Call Pilot directly. You can access Call Pilot directly without having to dial a user's directory number.
- Dial a number that is not permitted to access Call Pilot directly. To access Call Pilot, it is necessary to dial a user's directory number and then be forwarded to Call Pilot.

Outcalling

To verify the operation of this feature:

- Define where the messages are sent for nonuser telephones.
- Access the Call Pilot mailbox and enter the SEND command. If correctly configured, Call Pilot dials the nonuser telephone and deliver the messages when it detects voice, or when the nonuser presses 2 if prompted.
- Listen to the message, record a reply, and forward it to the sender. If this feature is configured correctly, the reply is automatically 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 is forwarded by the automated attendant; if the number is denied, the call terminates at the automated attendant.

New system security planning

Navigation

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 Call Pilot 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 you install a new system, you must activate security features that protect call processing and administrative functions from unauthorized access.

It is most efficient to plan and implement system security procedures when the system is initially installed. Making changes that affect the day-to-day operation of a system is disruptive to users and incoming callers alike.

Before installing security features, you must generate and install a configuration database. Based on this configuration database, you can implement system security features 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. See "Access Restriction features" (page 135) 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 Call Pilot. See "System checklist" (page 73) and "Call Pilot checklist" (page 82).

Use the checklist during the system configuration planning stage. For each function and feature in the configuration database, specify an equivalent security feature using the checklist. You can also use the completed checklist 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" (page 19) to understand the system and Call Pilot security features. For more information about OAM access, see *Security Management Fundamentals* (NN43001-604).

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

Print program — Terminal Number Block Program LD 20

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

Single-line/multiline telephones	_____
DISA	_____
Authcodes	_____
TIE Trunks	_____
Call Pilot Agents	_____

See "Class of Service" (page 20).

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/multiline telephones	_____
DISA	_____
Authcodes	_____
Call Pilot 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" (page 22)

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" (page 25).

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" (page 26).

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" (page 27).

4. Forced Charge Account (FCA)

Print program — Customer Data Block Program LD 21

Guidelines — Select Yes to temporarily override toll-denied Class of Service 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" (page 29).

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" (page 30) and "Enhanced Controlled Class of Service" (page 31).

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" (page 31).

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)

ALLOW _____ DENY _____

See "Code Restriction Data Block" (page 32).

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" (page 32).

9. Called Party Disconnect Control (CPDC)

Print program — Route Data Program LD 21

Guidelines — Specify routes from 0 to 127 or check No to allow trunk-to-trunk transfers.

Route _____ _____ _____ _____ _____

No _____

See "Called Party Disconnect Control" (page 33).

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" (page 47).

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" (page 48).

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" (page 48).

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" (page 49).

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" (page 49).

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" (page 51).

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 Class of Service 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" (page 50).

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" (page 52).

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	_____	NCOS	_____
FRL	_____	FRL	_____
Calling area	_____	Calling area	_____
NCOS	_____	NCOS	_____
FRL	_____	FRL	_____
Calling area	_____	Calling area	_____
NCOS	_____	NCOS	_____
FRL	_____	FRL	_____
Calling area	_____	Calling area	_____
NCOS	_____	NCOS	_____
FRL	_____	FRL	_____
Calling area	_____	Calling area	_____
NCOS	_____	NCOS	_____
FRL	_____	FRL	_____
Calling area	_____	Calling area	_____

See "Network Class of Service and Facility Restriction Level" (page 53).

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" (page 54).

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" (page 54).

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" (page 55).

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" (page 56).

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 1999 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" (page 56)

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" (page 22).

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" (page 57)

Multi-Tenant (TENS)

Print program — Define Multi-Tenant Program LD 93

Guidelines — Specify a tenant from 1 to 511, a route from 0 to 1999, 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" (page 59).

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 1999 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" (page 117).

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" (page 120).

Call Pilot checklist

Define all entries in the checklist that are configured for Call Pilot. 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. Default names 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 _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

See “Thru-dial to Voice menus” (page 68).

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 _____ _____ _____ _____ _____

	_____	_____	_____	_____	_____
Name	_____				
Restrict	_____	_____	_____	_____	_____
	_____	_____	_____	_____	_____
Permit	_____	_____	_____	_____	_____
	_____	_____	_____	_____	_____

See "Thru-dial to Voice menus" (page 68).

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)

See "Thru-dial to Voice menus" (page 68).

4. Password Parameters

Print program — Voice Security Option screen

Guidelines — Used to limit unauthorized access to voice mail.

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

Naviation

This section contains information on the following topics:

Introduction

This chapter describes how to plan 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
- Call Pilot 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 Call Pilot software.

Before filling out the checklist, read "Controlling call privileges" (page 19) and"Auditing Call Pilot security features" (page 107) to understand the system and Call Pilot security features. For more information about OAM, see *Security Management Fundamentals* (NN43001-604).

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. See “Access Restriction features” (page 135) 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 *Security Management Fundamentals* (NN43001-604) for more information about configuring LAPW Audit Trail.

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" (page 58).

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" (page 117).

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" (page 49).

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 Class of Service when the called telephone is in Call Forward All Calls. If OPT = CFO, check the Class of Service, 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 Class of Service 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	If CFO, CLS, TGAR and
NCOS on DID trunks = _____	NCOS on DID trunks = _____

See "Controlling Call Forward access" (page 47).

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” (page 52) and “Incoming Trunk Group Exclusion” (page 56).

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 voice mail 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" (page 32).

9. Console Presentation Group (CPG)

Print program — Multi-Tenant Service Program LD 93

Guidelines — Indicate if any night numbers for any CPGs are Call Pilot DNs.

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

See "Controlling Multi-Tenant Services" (page 59).

10. Controlled Class of Service (CCOS)

Print program — Customer Data Block Program LD 21

Guidelines — Identify the three (maximum) Class of Service 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" (page 30) and "Enhanced Controlled Class of Service" (page 31).

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” (page 52) and “Incoming Trunk Group Exclusion” (page 56).

12. Customer Night Numbers

Print program — Customer Data Block Program LD 21

Guidelines — Identify the night numbers and determine if any NITE DNs are Call Pilot ACD-DNs. Indicate those that are Call Pilot 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” (page 52).

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 Class of Service.

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” (page 57).

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	_____	_____

Parameter	Current value	Proposed value
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” (page 52), “Network Authorization Codes” (page 54), “Time-of-Day Routing” (page 54), and “Incoming Trunk Group Exclusion” (page 56).

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	_____	_____

Parameter	Current value	Proposed value
SCPC	_____	_____
SSPU	_____	_____

See "Electronic Lock" (page 31).

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" (page 29).

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 *Security Management Fundamentals* (NN43001-604) for more information about the History File.

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” (page 56).

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. Call Pilot Virtual Agent data

Print program — Terminal Number Block Program LD 11.

Guidelines — Identify the ACD-DNs associated with Call Pilot. List the system software for each virtual agent position ID and review to ensure that each is the lowest NCOS, FRL, Class of Service 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	_____	_____
Call Pilot	Yes No (circle one)	Yes No (circle one)

Virtual Agent Position IDs and Associated Class of Service, NCOS, TGAR

Current value		Proposed value	
_____	_____	_____	_____

Current value		Proposed value	
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

See ACD Directory Number Program LD 23.

22. Multiline telephones

Print program — Terminal Number Blocks Program LD 20

Guidelines — Make note of all virtual ports that are used for access to a voice mail 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 multiline telephones. All multiline 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 multiline 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. Avoid 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 multiline 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 Multiline Telephone Administration Program LD 11. These new telephone configuration parameters are in effect when implementing multiline 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" (page 32), "Network Speed Call" (page 26), "Network Authorization Codes" (page 54), and "Routing Control" (page 55).

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" (page 26).

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 voice mail 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” (page 32).

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” (page 52), “Incoming Trunk Group Exclusion” (page 56), and “Free Calling Area Screening” (page 56).

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	_____	_____

For more information about program access see *Security Management Fundamentals* (NN43001-604).

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	_____	_____

Parameter	Current value	Proposed value
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” (page 54), “Time-of-Day Routing” (page 54), and “Free Calling Area Screening” (page 56).

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” (page 58).

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 voice mail 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. Avoid allowing external Call Forward.

UNR Class of Service 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” (page 52) and “Incoming Trunk Group Exclusion” (page 56).

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” (page 25).

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” (page 31).

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" (page 59).

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" (page 59).

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” (page 120).

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 system wide 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 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. Use the form in the following table to configure the routes, referring to the TGAR worksheet form in Appendix B.

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)

Parameter	Current value	Proposed value
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 Call Pilot Voice Menu DNs, ensure that the Call Pilot Voice Menu table for Voice Security Options blocks all unauthorized access. Ensure that the NCOS, TGAR, and Class of Service 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)	_____	_____

Parameter	Current value	Proposed value
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 Call Pilot security features

Call Pilot security features include features that access Call Pilot mailboxes, voice menus, or automated attendants. To audit an existing Call Pilot security system, use the Call Pilot audit checklist.

Call Pilot 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**
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

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 voice mail. 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	_____	_____

Parameter	Current value	Proposed value
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

Navigation

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 47 "System reports summary" (page 116) provides a summary of these messages and reports. Table 47

"System reports summary" (page 116) 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 47
System reports summary

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.
All Trunks Busy conditions viol ating 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.

Table 47
System reports summary (cont'd.)

Information required	Report	Statistics provided	Output
NCOS call activity through BARS/NARS.	TFN002	The number of call attempts each NCOS group generated and other statistics.	According to schedule.
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 outside of normal business 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 48 "Configuring and printing CDR reports" (page 117) shows how to configure CDR and print reports for customers, routes, Authcodes, and telephones.

Table 48
Configuring and printing CDR reports

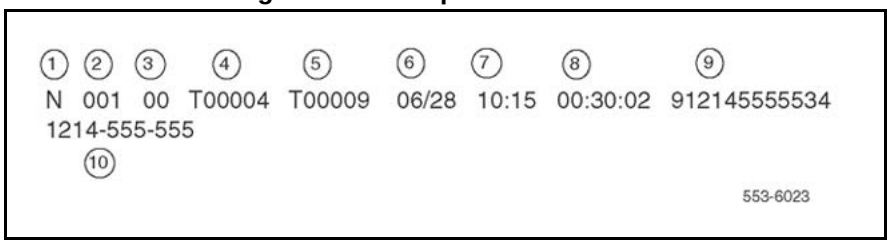
Facility	Overlay and prompts	Print programs
Configuration	LD 17 - IOTB, ADAN, USER = CTY	LD 22 CFN or LD 22 ADAN

Table 48
Configuring and printing CDR reports (cont'd.)

Facility	Overlay and prompts	Print programs
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 1 "Call Detail Recording record example" (page 118) shows an example of the CDR report. The circled numbers correspond to the description of fields below Figure 1 "Call Detail Recording record example" (page 118). For other CDR report examples, see *Call Detail Recording Fundamentals* (NN43001-550).

Figure 1
Call Detail Recording record example



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
CFlIln	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 49 "Configuring traffic output ports and schedule" (page 120) shows how to configure traffic output ports and set up an automatic report printing schedule.

Table 49
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.

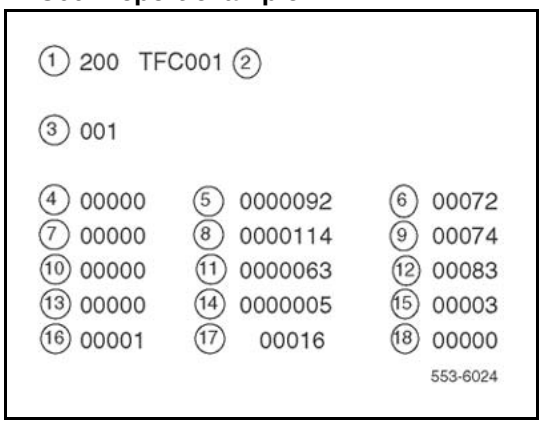
Table 50 "Configuring and printing the TFC001 report" (page 121) shows prompts in Traffic Program LD 2 to configure and print the TFC001 report.

Table 50
Configuring and printing the TFC001 report

Facility	Overlay and prompts	Print programs
Traffic	LD 2 SOPS	LD 2 TOPS

Figure 2 "TFC001 report example" (page 121) 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 2 "TFC001 report example" (page 121).

Figure 2
TFC001 report example



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 trunks.

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. See *Traffic Measurement: Formats and Outputs Reference* (NN43001-750) for more information.

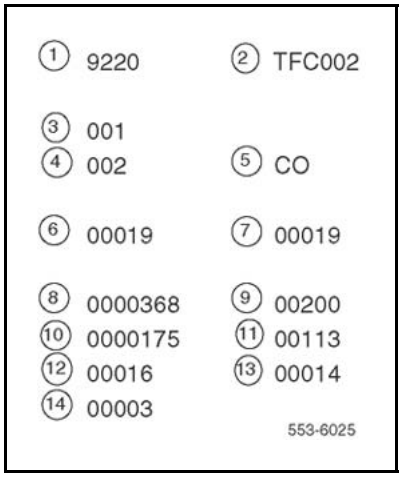
Table 51 "Configuring and printing the TFC002 report" (page 122) shows the prompts in Traffic Program LD 2 to configure and print the TFC002 report.

Table 51
Configuring and printing the TFC002 report

Facility	Overlay and prompts	Print programs
Traffic	LD 2 SOPC	LD 2 TOPC

Figure 3 "TFC002 report example" (page 123) 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 3
TFC002 report example



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.

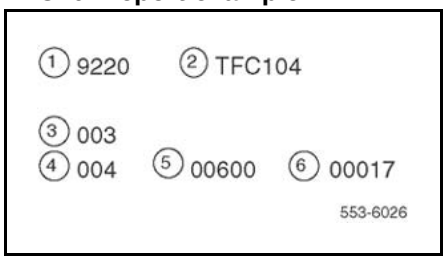
Table 52 "Configuring and printing the TFC104 report" (page 124) shows Traffic Program LD 2 prompts used to configure and print the TFC104 report.

Table 52
Configuring and printing the TFC104 report

Facility	Overlay and prompts	Print programs
Traffic	LD 2 STHC	LD 2 TTHC

Figure 4 "TFC104 report example" (page 124) 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 4 "TFC104 report example" (page 124).

Figure 4
TFC104 report example



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 53 "Configuring and printing TFS40X messages" (page 126) specifies Traffic Program LD 2 prompts used to configure and print the TFS40X messages.

Table 53
Configuring and printing TFS40X messages

Facility	Overlay and prompts	Print programs
Traffic	LD 2 SOPC	LD 2 TOPC

Figure 5 "TFS411 and TFS412 messages example" (page 126) is an example of the TFS411 and TFS412 reports. The circled numbers correspond to the description of fields below Figure 5 "TFS411 and TFS412 messages example" (page 126).

Figure 5
TFS411 and TFS412 messages example

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.

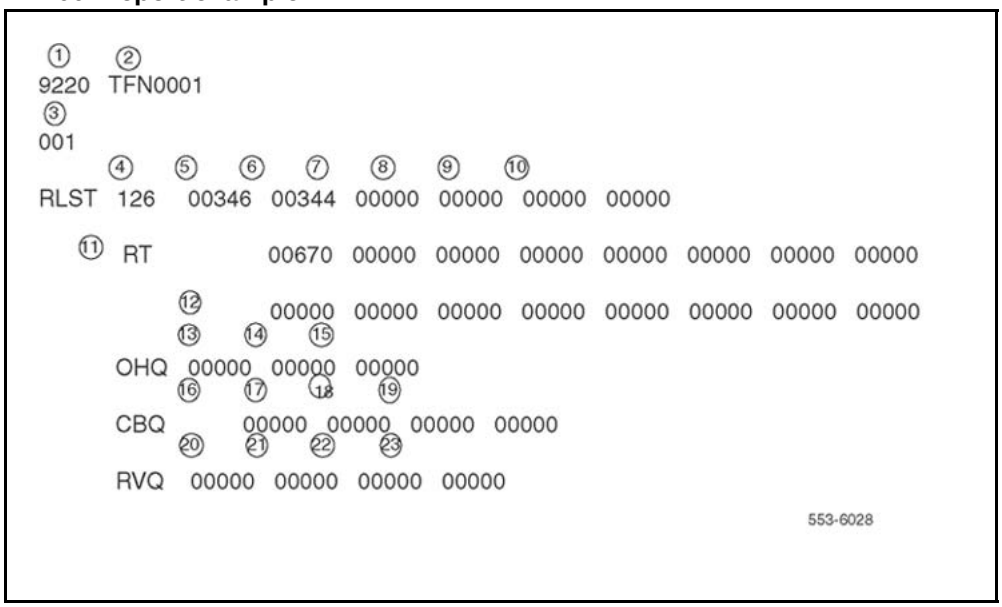
Table 54 "Configuring and printing the TFN001 report" (page 126) shows Traffic Program LD 2 prompts to configure and print routing measurement reports.

Table 54
Configuring and printing the TFN001 report

Facility	Overlay and prompts	Print programs
Traffic	LD 2 SOPN	LD 2 TOPN

Figure 6 "TFN001 report example" (page 127) 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 6 "TFN001 report example" (page 127).

Figure 6
TFN001 report example



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.

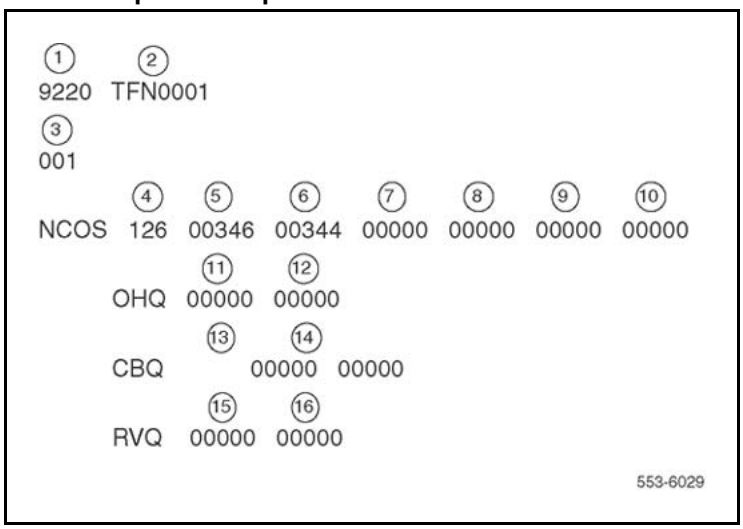
Table 55 "Configuring and printing the TFN002 report" (page 129) specifies Traffic Program LD 2 prompts used to configure and print the TFN002 report.

Table 55
Configuring and printing the TFN002 report

Facility	Overlay and prompts	Print programs
Traffic	LD 2 SOPN	LD 2 TOPN

Figure 7 "TFN002 report example" (page 129) 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 7 "TFN002 report example" (page 129).

Figure 7
TFN002 report example



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 56 "Configuring and printing the History File" (page 130) shows Traffic Program LD 2 prompts used to configure and print specific messages for the History File.

Table 56
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 Call Pilot 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 57 "Voice Service Summary report example" (page 131) is an example of the Voice Service Summary report.

Table 57
Voice Service Summary report example

Operational Measurement Voice Service Summary				
Interval Start-End	**Service Name**	**Number of Accesses**	**Average Length (in sec)**	**Call Pilot 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.
- **Call Pilot Usage** — the amount of time in CCS Call Pilot 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 57 "Voice Service Summary report example" (page 131) 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 58 "Outcalling Detail report example" (page 132) is an example of the Outcalling Detail report.

Table 58
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

Table 58
Outcalling Detail report example (cont'd.)

Operational Measurement										
Outcalling Detail (Remote Notification and Delivery to Non-users)										
	Number of New Requests		Number of Attempts --- 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	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 nonuser.
- **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
Access Restriction features

Use Table 59 "Feature Assessment" (page 135) 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 59
Feature Assessment

Security Features	DISA	voice mail	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	
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		

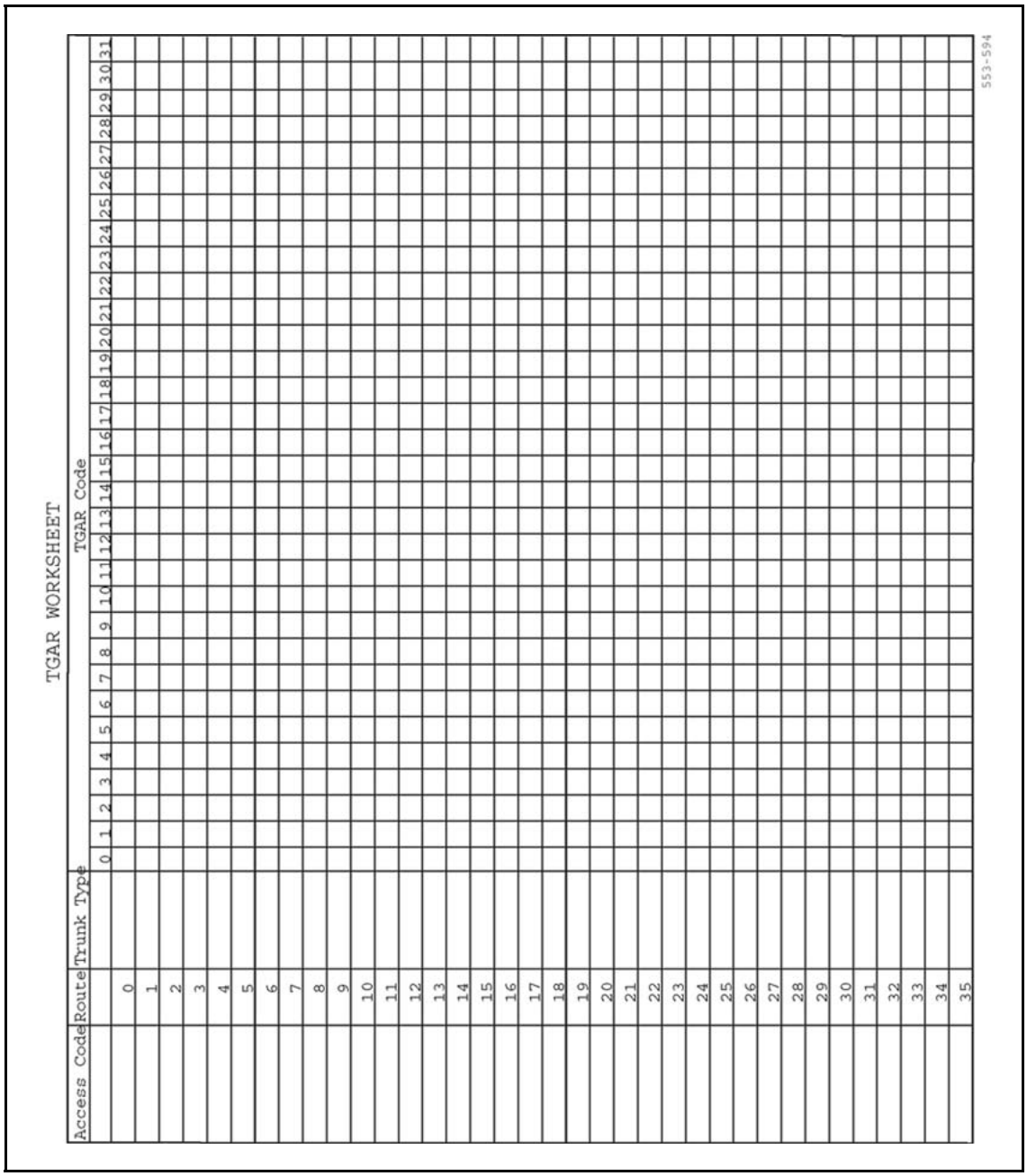
Table 59
Feature Assessment (cont'd.)

Security Features	DISA	voice mail	Internal	Network	System
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	
Call Pilot System Options Voice Security		X			
Call Pilot User Options		X			
Call Pilot Voice Menus Thru-dial Security		X			
Level 1 Password					X
Level 2 Password					X
Limited Access to Passwords					X
Trunk barring					
Scheduled Access Restrictions					
Restricted Call Transfer					
User Selectable Call Redirection					
Multiuser 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 Trunk Group Access Restrictions worksheet

Use Table 60 "Trunk Group Access Restrictions worksheet" (page 137) to specify Trunk Group Access Restrictions (TGAR) for each route. Also, specify the trunk type and access code required to access that route.

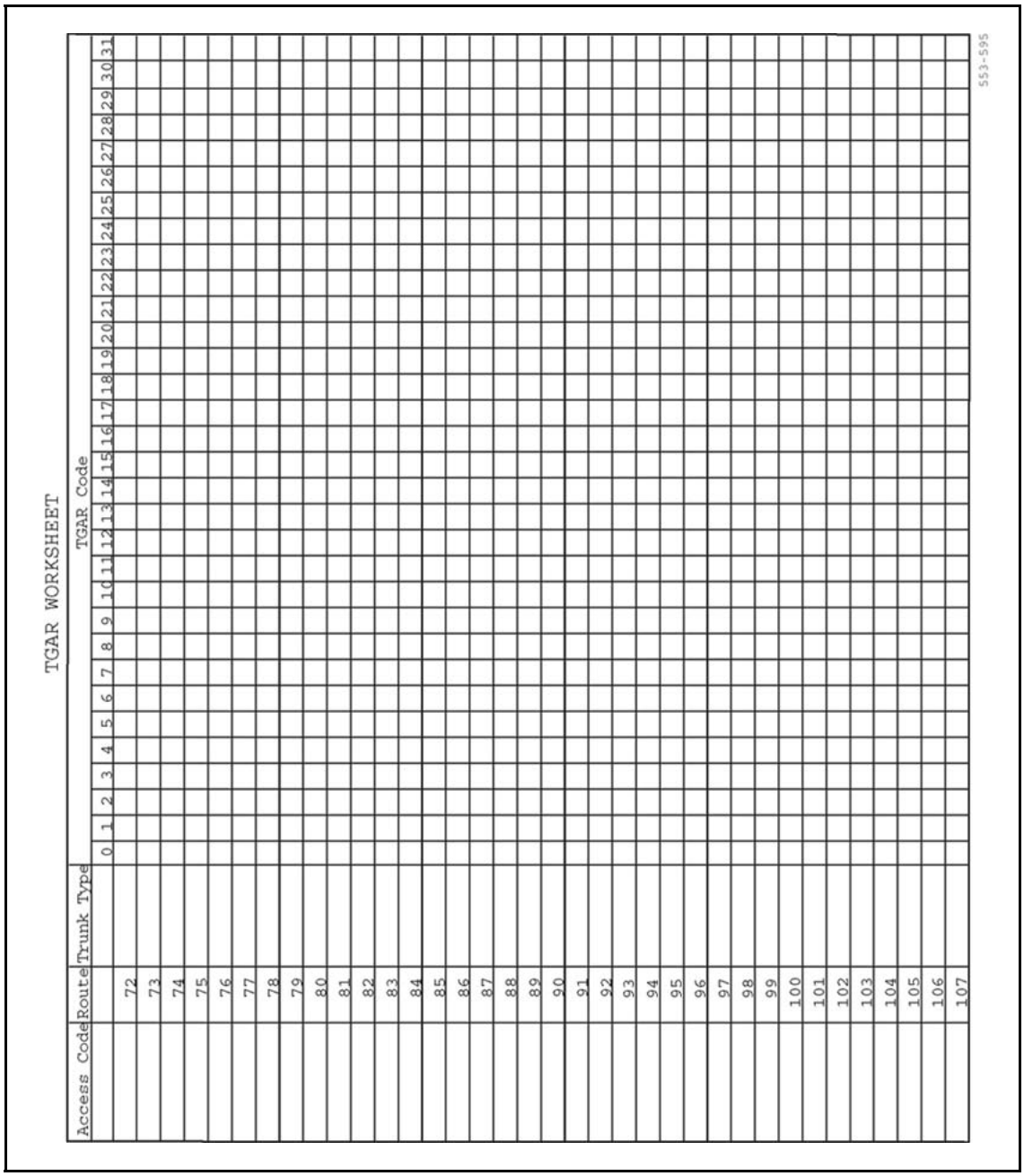
Table 60
Trunk Group Access Restrictions worksheet



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



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																																

553-595

Index

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Nortel Communication Server 1000

Telephony Services Access Control Management

Release: 7.0
Publication: NN43001-602
Document revision: 04.01
Document release date: 4 June 2010

Sourced in Canada

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com