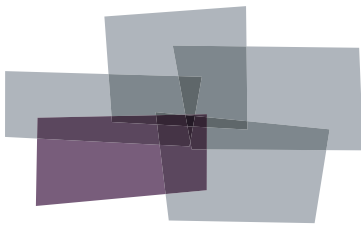# Security Audit

"How can I make my Communication Server more secure?"

Produced For
ABC Company

Customer Number: **12345**
Reflecting information from: **January 8, 2018**

Inventory
Configuration
Performance
Security
Backup

Communications Management with InfoPlus

Regardless of the size or type of organization, there are a few basic concerns of every communications manager. InfoPlus services help address those various concerns through an integrated suite of reports and analyses.

Inventory
Configuration
Performance
Security
Backup

Security – The increasing importance of communications security is met through the InfoPlus Communication Server Security Audit. Over 83 computerized analyses are performed listing the Description, the Security Concern and the Findings of each of the analyses. All violations of established security measures are highlighted with sufficient information to rectify the violation. More than just cost avoidance, the InfoPlus Communication Server Security Audit will ensure your communications system is not supporting unauthorized use.

A next logical step in gaining additional control over your telecommunications resources might be an InfoPlus Traffic Study. While the Security Audit will help you block all unintended usage, the Traffic Study will analyze usage, ensuring the most effective and efficient communications possible. Cost savings and/or service improving recommendations are clearly provided, easily justifying the expenditure.

Other services in the InfoPlus suite include:

Inventory – InfoPlus Site Survey
- Inventory of the major Communication Server hardware and software components
- Factory Support analysis pinpoints "End-of-Life" and other unsupported equipment
- Access to database for enterprise customers

Configuration – InfoPlus SourceBook
- Details a Communication Server's programming
- Graphics of each set and each button's feature or line assignment
- Lists of each defined group (Intercom, Call Pick-up, etc.)
- Clearly defines Trunking, Call Routing, and even Calling Privileges
- Service-improving Action Items are uniquely determined for your system

Performance – InfoPlus Traffic Study
- Consultative Report, not a "data dump"
- Supported by graphical representation of the "important" data
- Analyzes Networks, Trunks, Consoles and even Processors
- Clear recommendations for improving service

Backup – InfoPlus Backup Service
- Off-site backup of your Communication Server's configuration
- Available at any time for restoration through the Internet

Please contact your telecommunications vendor for additional information about these services.

Table of Contents

Introduction

We are pleased to provide you with the following Security Audit to help you identify and address areas of concern involved with the security of your telecommunications system.

Security of telecommunications services often involves the striking of a fine balance between business needs and the restrictive programming of various system features. As a result, the report can not tell us whether there is in fact a misuse of communications services taking place, but rather points out those areas where, and under what circumstances, abuse could take place. It is also intended to make you aware of the more mundane aspects of security practices and procedures as they relate to your telecommunication system.

The majority of this report is necessarily of a technical nature as it addresses the programming of sophisticated computerized systems. As a consequence, the report contains some mnemonics and Feature Names which may be unfamiliar to you. At the end of the report is a Glossary of Terms for your reference.

In the abstract, you would think that establishing calling privileges and capabilities would be rather straightforward. Unfortunately, as users and special services demanded more flexibility, a very interrelated set of features has been created. As such, care should be taken in making modifications as changes in one area may impact calling capabilities in another.

To derive the full benefits, this report should initially be reviewed with your vendor and/or in-house technical staff. During this review it is likely that several areas will require further internal investigation before making modifications. As such, a complete Security Audit process may require two reviews, with this document helping to focus attention on the more critical areas.

Conventions Used in This Report

This report contains a number of topics detailing a wide array of security issues, grouped into chapters of related topics. Each topic contains a Description section, which briefly describes the Communication Server feature(s) it analyzes, a Security Concerns section, which explains different ways the feature(s) and their settings could be exploited, and an Analysis section, a computerized examination of your system with respect to the options in question, complete with recommendations of how to make your system more secure, if applicable. Within the Analysis section, anything that we feel requires your further investigation is underlined and printed in red.

Definitions

Throughout the report, we make references to dialing sequences that could direct calls outside of your Communication Server network onto the public telephone network. We call these dialing sequences "external numbers," and define them as any sequence that is longer than seven digits or begins with a BARS/NARS Access Code, a Trunk Route Access Code, a Trunk Steering Code, or a Distant Steering Code that could be routed over the public network. (These Distant Steering Codes are listed in Section 11.12, Coordinated Dialing Plan.)

References to area codes with high toll abuse are based on the reports of the LincMad website as of November, 2001, and can be viewed at <http://www.lincmad.com/telesleaze.html>.

Passwords and Security Codes

There are several topics in this report that reference and/or analyze various passwords and security codes programmed in your Communication Server or related telecommunications equipment. For increased security, we do not display in this report the actual passwords, but rather only show the results of analyzing the password for sufficient complexity. Your telecommunications vendor will have the details needed to perform any of the recommended changes presented in this report.

Communication Server Programming

1. Administrative Access

One of the most important aspects of Communication Server security is controlling the ability to change the programming of the switch. A Communication Server in which unauthorized users can make changes is equivalent to using no security measures at all. While the Communication Server does have some features to help control this administrative access, there are other points to consider. You must still guard both physical access to the switch and the passwords themselves. Managing password knowledge when employees change, and giving individuals only the access they require are also important. The following is an explanation of how the Communication Server helps you manage these administrative responsibilities.

1.1. External Security

Description

The first line of defense against remote access to your Communication Server may not be part of the Communication Server at all. Modern Communication Servers allow full administrative access through a LAN interface. When combined with a corporate VPN, highly secure remote access becomes possible without the use of a modem. On older systems or in situations where employing a VPN is not possible, advanced modems can be used to provide an added layer of security. Advanced modems can use one-time challenge/response combinations or require separate passwords be entered before any access to the Communication Server is granted.

Security Concerns

When using a VPN to access your Communication Server, the possibility that an unauthorized individual will gain access to your switch is extremely remote. It is recommended that any modem is disconnected, and a VPN is employed to increase security. If this is not possible, a Secure Modem is preferred over a standard modem to protect your Communication Server.

Analysis

You are currently using a secure modem.

Your secure modem password is unacceptable for the following reason(s):

- shorter than 6 characters
- does not contain both alpha and numeric characters
- contains a run of 3 or more ascending/descending characters

1.2. Passwords: Level 1 & 2

Description

The data in your Communication Server is protected from modification by two passwords which provide different levels of access. The Level 1 Password allows changes to be made to the database configuration, with the exception of data pertaining to the passwords themselves, Authorization Codes, and DISA settings. The Level 2 Password allows you all of the capabilities of the Level 1 Password, and in addition, allows you to modify both passwords and data pertaining to Authorization Codes and DISA. It is vital that you know both of these passwords and are informed if either password is modified.

Security Concerns

Since they are the key to the main gate of the Communication Server, the Level 1 and 2 Passwords should be difficult to guess, protected as sensitive data, and changed frequently. In Release 16 and later, they should be at least 6 characters long, and contain both alpha and numeric characters. In earlier releases, they are limited to four characters from the range '0' through '9' and 'A' through 'F'. With Succession 4.5 and later, a password complexity checking feature is available to ensure only secure passwords are selected.

Analysis

The Level 1 Password is unacceptable for the following reason(s):

- shorter than 6 characters

You should change your Level 1 password for increased security.

The Level 2 Password is unacceptable for the following reason(s):

- shorter than 6 characters

You should change your Level 2 password for increased security.

Upgrading to at least Communication Server 1000 Release 4.5 would provide increased security features, including a Password Complexity check.

1.3. Limited Access Passwords

Description

For a greater degree of control, you can assign up to 100 Limited Access Passwords and increase security by defining reduced access permissions to them. Using this feature also increases the ability to track who made modifications to the database, and when.

Security Concerns

Any access to the database, no matter how limited, is a potential security risk. These passwords should be protected just like the Level 1 and 2 Passwords, and managed to ensure that individuals have only the access they need. Please note that in Succession 5.0 and later users with Limited Access Passwords can change their own passwords.

Analysis

You have 2 Limited Access Password(s) defined in your system which have access to your data. The following list explains the capabilities of each of these passwords. Those passwords which are considered insecure should be changed to be longer and/or more complex.

Limited Access Password 0 (MMAIL)

This password is considered too simple for adequate security.

This is a Limited Access to Overlays password.

Overlays Allowed: 2, 48

Users cannot Log-In to MAT with this password.

Password Options Allowed
• Allowed to make changes in general (not Print-Only)

Limited Access Password 1 (OTM)

This password is considered too simple for adequate security.

This is a Limited Access to Overlays password.

Overlays Allowed: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 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, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 117, 135, 137, 143

Users can Log-In to MAT and make changes with this password.

Password Options Allowed
• Printing of Speed Call Lists allowed
• Allowed access to Configuration Prompts
• Allowed to make changes in general (not Print-Only)

1.4. Log-In Name Option

Description

You can require administrators to enter a Log-In name before and in addition to using the Level 1 and 2 Passwords, or any Limited Access Passwords. Each password can be assigned a unique Log-In name. This feature is always enabled in Succession 4.5 and later.

Security Concerns

Requiring Log-In names in addition to passwords decreases the possibility of unauthorized access to your Communication Server. It essentially lengthens the passwords already in use, making them more complex.

Analysis

The Log-In Name option is currently enabled on your Communication Server. Below is a table of the Log-In Names defined for each Password. Names that are too simple, or that are the default Log-In Name for the password, are highlighted in red and underlined. These names should be changed to be more difficult or complex.

Password Type	Log-In Name
Level 1	ADMIN1
Level 2	ADMIN2
LAPW 0	MMAIL
LAPW 1	OTM

1.5. Failed Log-In Threshold & Lockout Time

Description

You can specify how many incorrect Log-In attempts can be made from an access port before the Communication Server enters 'Lockout mode,' during which no Log-Ins are accepted from the port for a defined amount of time. The next port logging in during the lockout time receives a message that the port with excessive invalid log-in attempts has been locked out. However, manual initialization of the Communication Server can override this time limit, and allow immediate re-access to the system.

Security Concerns

The combination of these features protects your Communication Server against password hacking. The simplest way to guess a password is to try all of the various combinations. The Failed Log-In Threshold and Lockout Time features make this process unattractive by limiting the 'guesses' that can be made in a given time period. It is recommended that the threshold be set to 3 or less, and the Lockout Time be set to 30 minutes or more to deter password guessing. However, if the hacker has physical access to the switch, it is possible to initialize the Communication Server to circumvent this obstacle. Therefore, it is recommended that the Lockout Time should not be reset during initialization.

Analysis

Your current Failed Log-In Threshold is set to 3. This meets or exceeds recommendations for this feature.

Your Lockout Time is currently set for 5 minutes. This is less than recommended, and should be increased to at least 30.

However, one cannot Initialize the Communication Server to circumvent this Lockout time. This is the recommended setting.

1.6. Security Banner

Description

With the introduction of System Access Enhancements in Release 22, users have the option of printing a Security Banner after log-in is attempted. If programmed, the banner will provide a warning that unauthorized users should not be accessing the Communication Server.

Security Concerns

The Security Banner is intended to deter individuals from changing the programming of the Communication Server by reminding them that unauthorized access is punishable by law.

Analysis

You have 5 Maintenance/Service Change TTY port(s) which are not displaying the Security Banner. The following is a list of the ports which should be modified to activate the Security Banner feature:

TTY 0, TTY 1, TTY 3, TTY 4, TTY 5

1.7. Secure Data Password

Description

This password allows access to the database that controls Authorization Codes and the Direct Inward System Access (or DISA) feature.

Security Concerns

DISA is a powerful feature and also a common entry point for Communication Server abuse. If the DISA programming can be altered by an unauthorized individual, it could open the Communication Server to significant toll fraud. Similarly, the ability to create and modify Authorization Codes could have toll fraud impact as well. See the sections on DISA and Authorization Codes for more information. It is recommended this password be at least 4 digits, and difficult to guess.

Analysis

The Secure Data Password has not been assigned a non-default value, although DISA and/or Authorization Code software is installed. The Secure Data password should be assigned a random, non-default value to protect these features if they are activated.

1.8. Attendant Administration Access Code

Description

The Attendant Administration feature allows the attendant to modify features assigned to telephones by using the attendant console as the programming device, instead of a system terminal. To enter the programming mode in this manner, the Attendant must first use the program key and a four-digit access code.

Security Concerns

Any modification to the Communication Server database, whether through a TTY terminal or other device, can have significant effect on the overall vulnerability of your telecommunications system. This access code should be treated like the terminal passwords: only given to authorized personnel and significantly difficult to guess.

Analysis

You do not have an Attendant Administration Access Code defined. This disables the Attendant Administration feature.

1.9. Set Relocation Security Code

Description

Automatic Set Relocation and Modular Telephone Relocation are features that allow a user to move a telephone from one location to another without the involvement of a technician. However, prior to moving a telephone, the user must enter a security code.

Security Concerns

Moving a set from a 'secure' location to an 'insecure' location can incur toll abuse. For example, phones with international calling capability should not be located in a lobby or other public space. This security code is intended to ensure that only those personnel with authorization can move the physical location of sets.

Analysis

The Set Relocation Security Code is unacceptable because it has not been changed from the default.

2. System Configuration

Certain aspects of your Communication Server's programming and configuration have system wide influences. In this section, we present some of these high-level settings. While some of the information in the following topics is purely informational, they paint a broad picture of your Communication Server to increase your familiarity with the system.

2.1. Serial Number

Description

A unique serial number is assigned to each Communication Server, and is located on the back of the Common Equipment cabinet and on the software storage media of the Communication Server.

Security Concerns

The serial number of the software loaded on your Communication Server should always match the Communication Server's serial number. If this is not the case, you may have incorrect software loaded which can corrupt your system data.

Analysis

Your serial number is 01234567.

2.2. Software Release

Description

A software Release number is assigned by the manufacturer for all enhancements that have been made since the introduction of the SL1, Meridian 1 and Communication Server 1000 systems. With a particular Release of software, there may be several Issues distributed for more frequent updates. In addition, software Patches are released to fix bugs or security holes quickly, without waiting for the next major Issue or Release.

Security Concerns

As with any software, problems and bugs found in older versions are fixed in later versions. For this reason, it is recommended to keep your software Release current. Also, older software Releases no longer fully supported by the manufacturer can present problems when assistance is required. Any software Patches that fix security-related issues should be installed as needed.

Analysis

Your current software is Release 25, Issue 40 B +.

Your software Release is classified as 'End of Manufacturer Support' or 'End of Services Support', and Avaya will provide only very limited support. You should consider upgrading to a newer Release of software.

2.3. Multiple Customer

Description

Up to 100 individual customers can be supported on a Communication Server, each having their own features, trunks, numbering plans, restrictions, and other special services.

Security Concerns

If this is not a shared Communication Server, you want to ensure that no other customers are defined in the switch. The presence of an additional customer could indicate use of the Communication Server by unauthorized personnel.

Analysis

There is only one Customer defined in this Communication Server, although the Multi-Customer software option is installed.

2.4. Input/Output Devices

Description

Input/Output Devices are required for communications with the Communication Server. These devices can either be on-site (local) or at a remote location, and are typically a TTY/VDT terminal.

Security Concerns

The proper configuration of your Input/Output devices can help control and log the information generated by the Communication Server, as well as access to its programming. Each TTY device can capture a log of its activity, which can be used to assess unauthorized access. It is recommended that these logs be able to store at least 1,000 words. It is also recommended that at least one device output Maintenance messages.

Analysis

The following 5 TTY device(s) have no log defined: 0, 1, 3, 4, 5

You should increase the log size of these TTY ports to at least 1,000 words.

You have at least one TTY device outputting Maintenance messages. This is the recommended configuration.

2.5. Error Messages

Description

Your Maintenance ports output Error Messages to help alert you to hardware and software problems within the Communication Server. The selected messages are defined in the Configuration Record.

Security Concerns

For proper maintenance of the switch, you should be alerted to all types of error messages. These include both hardware and software error messages.

Analysis

The Maintenance Port(s) are not outputting all of the recommended Error Messages. Error messages should include the hardware error monitor (ERR), the software error monitor (BUG) and the software audit (AUD) messages.

2.6. Night Service

Description

When activated, this feature allows incoming calls to the attendant to be routed to one of four Night Service DNs during specified periods of time. The Attendant places the system in Night Service by pressing a designated key on the console.

Security Concerns

A common method of communications abuse is to direct calls to unauthorized external numbers. For most applications, your Night Service numbers should be internal DNs such as a voice mail system or a night bell. External numbers should be examined to ensure that calls are being sent to approved numbers. They should also be tested to ensure they provide the recommended far end disconnect supervision of Fast Busy (120 IPM) when the far end goes on hook and the calling party remains off hook.

Analysis

1 of your Night Service DNs appear to be sending calls outside of the Communication Server. Please verify the following Night DNs to ensure that calls are not being sent to an unauthorized number:

Night DN 2 is 91201

3. Assessing and Measuring Abuse

An important part of a complete security regimen is to record and track the system access, software modifications, and traffic patterns of your Communication Server. An early warning sign of abuse is activity that does not conform to the typical patterns of your business. For example, calls being placed after-hours, or to unusual destinations could indicate improper use of the facilities. The topics in this section address several ways you can monitor your Communication Server activity. However, they are only the first part of assessing abuse. The data provided by these features must be checked regularly and compared against established norms to help control abuse.

3.1. History File

Description

The History File feature allows all system messages in the Communication Server to be stored in memory until a printout is requested, and is available either on-site with a terminal, or with a device from a remote location. The size of a History File is defined on a system basis.

Security Concerns

You should review this file to monitor any unauthorized administration access into the system, particularly during the night hours. For maximum benefit, the file should be able to record 20,000 words of Maintenance, Service Change, and Software Error messages.

Analysis

You have a History File defined, but you should increase its size from 10,000 words to a minimum of 20,000 words. Too small a History File may not be able to store enough information for adequate assessment.

Your History File is collecting the recommended messages.

3.2. Audit Trail

Description

Activity messages in the Communication Server are stored in memory with the Audit Trail feature. It provides detailed access information such as dates, log-in and log-out times, passwords, user IDs and the overlays that were accessed. As with the History File, this information is available to administrators, either on-site or remotely, and can be printed out.

Security Concerns

Knowing when administrative changes are made to the Communication Server, and by whom, can be valuable information when you suspect abuse. Together with the Log-In Name option and the Limited Access Passwords, this information can trace back modifications to a single individual.

Analysis

You do not have an Audit Trail for monitoring password usage. You should enable the Audit Trail feature, and set its size to 1,500 words.

3.3. Traffic Settings

Description

A traffic port can be defined in the Communication Server to collect pertinent traffic data about calling patterns and suspicious activity. The traffic data can be stored in a collection device, or with Release 19 and higher, in a traffic log, and downloaded to a maintenance port at a later date.

Security Concerns

Several traffic reports are helpful in identifying areas of toll fraud and abuse. These include Customer traffic reports TFC001, TFC002 and TFC104, System traffic reports TFS401, TFS411, TFS402, and TFS412, and Network traffic reports TFN001 and TFN002. You should be collecting these reports, especially during off-hours, to a properly configured device. In addition, it is recommended to use the All Trunks Busy threshold feature to help alert you to unusually high trunking usage during off-hours. Refer to the manufacturer's documentation to understand the format of these reports, and how to use the data they contain.

Analysis

You are not outputting any traffic data on TTY devices. You should define a Traffic Log File in your Configuration Record, or have one TTY device outputting Traffic Information.

You currently have Customer Traffic data scheduled for the following period, although it is not being output to any device:

Starting: March 30
Ending: April 6
Hours: 0 - 23
On the following days: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

You should verify this schedule covers your vulnerable time periods, including off-business hours.

You are not collecting the most important Customer Traffic data for monitoring abuse. You should collect at least TFC001 and TFC002 reports.

Your All Trunks Busy Threshold is currently set to 0.0%. You should set the All Trunks Busy Threshold to an appropriate value (based on your current trunking capacity) to monitor unusual activity during your reporting schedule above, and perform threshold tests if you suspect unauthorized activity.

You are not collecting the most important Network Traffic data for monitoring abuse. You should collect at least TFN001 and TFN002 reports.

💡 Did You Know?

After you complete your Security review you might want to consider running an InfoPlus Traffic Study. The altering of calling privileges may change traffic patterns and usage that would be reflected in the study, possibly leading to additional savings or improved service.

3.4. Call Detail Recording

Description

Call Detail Recording, or CDR, is a feature that captures key information for every call made in the system. This information includes such details as the time and duration of the call, the called/calling parties involved and access codes used to place the call.

Security Concerns

Calls placed during off-hours, or to unusual locations, can indicate improper use of the Communication Server facilities. CDR should be used to monitor your calling patterns and establish norms against which you can compare future activity. However, since the CDR records can include sensitive data, it is important to control their output. If a hard copy of the CDR is produced, it should be disposed of properly.

Analysis

You do not have Call Detail Recording enabled, although you do have the software package required for it. You may want to consider enabling this feature to monitor activity.

4. Stations

Many of the calling capabilities that have significant impact on long-distance charges are defined at the set level. Each station can be assigned a unique set of features to allow or deny various types of access to the public network. In this section, we analyze each of the stations defined in your Communication Server, and look for potential holes in your security setup. To make these checks easier to understand, we've grouped them by similar functionality. To avoid long lists of information, we only provide information on stations that fail one or more of our tests.

💡Did You Know?

While this section of the Security Audit will address the security aspects of stations, an InfoPlus SourceBook may be ordered to gain a more complete understanding of the configuration of your system. The SourceBook will tell you how every button of every instrument is programmed, and provide, for the first time, a reference guide to the programming of your entire system.

4.1. Basic Access Restrictions

Description

This topic addresses the two features that define the basic access restrictions for stations: Class of Service and Trunk Group Access Restriction. The Class of Service of a station defines the overall access this station has to the public network (for example, can only place outgoing non-toll calls). Trunk Group Access Restriction, or TGAR, controls which stations have access to which routes.

Security Concerns

The Unrestricted Class of Service provides no toll restriction on a station; a potentially expensive security hole. In reality, this Class of Service isn't needed when using BARS/NARS and should be avoided. You should classify your routes into Route Lists of varying capability and expense, and restrict stations to only the Route Lists they need. A TGAR of 0 provides no trunk access restrictions on the station, and permits the station to bypass the programming in BARS/NARS least cost routing and directly access outbound trunk routes.

Analysis

The following table displays all stations in your switch with an Unrestricted Class of Service (UNR column) and/or an unrestricted Trunk Group Access Restriction (TGAR column). An unrestricted TGAR is any TGAR that does not appear in the TARG list of any route. CLS CTD and TGAR 1 with a TARG 1 assignment for the Route Data Block are recommended.

DN	Name	TN	Type	UNR	TGAR
7262	Barbara Grant	011 0 00 10	3904	✓	
7265	Bernard Burns	009 0 00 14	500	✓	
7654	Donald Harris	014 0 00 04	3904	✓	
7771	DES: 6149	006 0 00 04	3904	✓	
7790	Gladys Carlson	006 0 00 15	3904	✓	
7798	Glenn Mcdonald	006 0 00 11	3904	✓	
7919	Janet Sims	019 0 00 11	500	✓	
7933	Jesus Porter	009 0 00 13	500	✓	

4.2. Station Features

Description

This topic addresses five powerful features of stations:

- Flexible Trunk to Trunk Connection controls the connections between trunks for transfers and conference calls.
- ACD Supervisory Set Observation allows ACD Supervisor sets to observe other Supervisor sets.
- Maintenance telephones allow the user to send commands to the Communication Server, instead of using the system terminal.
- Station Specific Authorization Codes restricts which Authorization Codes can be used at a particular station.
- Station Control Password is a station-specific password used to control the Electronic Lock and Remote Call Forward features.

Security Concerns

The use of most of these features is a business/personnel decision. For example, Unrestricted Flexible Trunk to Trunk Connections may allow unsupervised conference calls in which a user can conference in two long-distance parties, and then drop out of the conversation leaving them conferenced. This is not a recommended setting due to its abuse potential. The ability of ACD supervisors to observe other supervisors is a feature you may wish to verify is required for stations that have it enabled. Maintenance telephones should only be defined for technicians' use, and should be located in properly secured areas. If the Station Specific Authorization Code feature is enabled, we'll present which Authorization Codes are permitted at the station. They should be verified for appropriate use. Finally, if a Station Control Password is used, it should be sufficiently difficult to guess to prevent unauthorized use and the same password should not be used on many stations.

Analysis

Your Station Control Password Length is 0. This disables the Electronic Lock, User Selectable Call Redirection, and Remote Call Forward features discussed in Chapter 7.

Flexible Trunk to Trunk Options are either disabled or not installed, so stations with Unrestricted Flexible Trunk to Trunk Connections are not reported.

The following table lists all stations that meet one or more of the following conditions:

- Has ACD Observe Supervisor allowed (AOS column)
- Is defined as a Maintenance Telephone (MTA column)
- Uses Station Specific Authorization Codes (we list the codes allowed) (AUTR column)

DN	Name	TN	Type	AOS	MTA	AUTR
7654	Donald Harris	014 0 00 04	3904		✓	
7771	DES: 6149	006 0 00 04	3904		✓	
7790	Gladys Carlson	006 0 00 15	3904		✓	
7798	Glenn Mcdonald	006 0 00 11	3904		✓	

Controlling Hunting and Forwarding   ABC Company

4.3. Controlling Hunting and Forwarding

Description

The hunting and forwarding capabilities of stations can provide significant toll abuse potential. In this topic, we address three features that can be employed to control their use. First, Call Forward External allows or denies stations from forwarding calls to an external number. Next, User Selectable Call Redirection allows users at the telephone to modify the DNs of several hunting and forwarding features. Finally, the length of the Call Forward All Calls number can be set to restrict how many digits can be entered for this number.

Security Concerns

Allowing the forwarding of calls externally is a common source of toll abuse, and should be restricted whenever possible. Also see the External References topic in this section for checks of individual hunting and forwarding numbers. Enabling users to change their redirection numbers is potentially dangerous. While other security features should be in place to prevent these DNs from being set to inappropriate numbers, it may be a security risk to allow their modification at all. If a station requires forwarding to a particular external number, it is recommended that an adequate station control password be used to secure the feature. Finally, allowing a Call Forward All Calls number of more than 7 digits allows calls to be forwarded to toll-incurring numbers, which should be avoided in most cases.

Analysis

Your Station Control Password length is set to 0, so User Selectable Call Redirection is disabled. Please note, however, that if you change the Station Control Password length, User Selectable Call Redirection will be enabled for those stations with USRA listed below. The following table lists all stations that meet one or more of the following criteria:

- Has Call Forward External allowed (CFXA Column)
- Has User Selectable Redirection allowed (USRA column)
- Has a Call Forward All Calls number length of more than 7 digits (CFW Length > 7 column)

DN	Name	TN	Type	CFXA	USRA	CFW Length > 7
2999	DES: 6074B	015 0 00 12	3904	✓		
7116	DES: 6049	018 0 00 04	3904	✓		
7118	Angela Hart	016 0 00 04	3904	✓		
7120	Anita Lucas	007 0 00 09	3904	✓		
7120	Anita Lucas	061 0 00 01	I2050			✓ (16)
7123	Ann Kelley	013 0 00 02	3904	✓		
7128	Anna Andrews	006 0 00 13	3904	✓		
7160	Anne Lynch	007 0 00 06	3904	✓		
7161	Annie Moreno	007 0 00 05	3904	✓		
7161	Annie Moreno	008 0 00 02	3904	✓		
7162	DES: 6042	011 0 00 02	3904	✓		
7163	Anthony Rodriguez	012 0 00 02	3904	✓		
7165	Antonio Hayes	014 0 00 02	3904	✓		
7205	DES: 6141	017 0 00 08	3904	✓		
7211	DES: 6140	011 0 00 09	3904	✓		
7226	DES: 7139	007 0 00 14	3904	✓		

40

DN	Name	TN	Type	CFXA	USRA	CFW Length > 7
7262	Barbara Grant	011 0 00 10	3904	✓		
7263	Barry Ramos	012 0 00 10	3904	✓		
7264	Benjamin Ward	013 0 00 10	3904	✓		
7266	Betty Gardner	015 0 00 10	3904	✓		
7267	Beverly Fernandez	016 0 00 10	3904	✓		
7284	Billy Brooks	015 0 00 02	3904	✓		
7285	Bobby Jenkins	007 0 00 07	3904	✓		
7289	Bradley Tucker	008 0 00 07	3904	✓		
7290	DES: 6064	007 0 00 02	3904	✓		
7291	Brandon Peterson	014 0 00 01	3904	✓		
7340	Brenda Bradley	015 0 00 09	3904	✓		
7341	Brian Robinson	016 0 00 09	3904	✓		
7342	Bruce Torres	017 0 00 09	3904	✓		
7343	Bryan Ford	018 0 00 09	3904	✓		
7344	Carl Parker	006 0 00 10	3904	✓		
7345	Carlos Henderson	008 0 00 11	3904	✓		
7346	Carmen Byrd	008 0 00 10	3904	✓		
7393	DES: 6073	018 0 00 11	3904	✓		
7394	Carrie Shelton	012 0 00 11	3904	✓		
7395	Catherine Austin	014 0 00 11	3904	✓		
7396	Chad Gomez	015 0 00 11	3904	✓		
7397	Charles Wilson	013 0 00 11	3904	✓		
7398	Charlotte Barrett	011 0 00 11	3904	✓		
7399	Cheryl Chapman	016 0 00 11	3904	✓		
7451	Christina Alvarez	017 0 00 02	3904	✓		
7452	Christine Elliott	018 0 00 02	3904	✓		
7601	Cindy Hopkins	013 0 00 09	3904	✓		
7602	Clara Watts	014 0 00 09	3904	✓		
7603	Clarence Foster	014 0 00 08	3904	✓		
7604	Clifford Black	015 0 00 08	3904	✓		
7607	Craig Washington	018 0 00 08	3904	✓		
7610	Cynthia Snyder	008 0 00 09	3904	✓		
7612	Daniel Thomas	008 0 00 01	3904	✓		
7614	Danny Myers	016 0 00 07	3904	✓		
7615	DES: 6119	017 0 00 01	3904	✓		
7616	David Davis	012 0 00 12	3904	✓		
7617	DES: 6091	006 0 00 08	3904	✓		
7619	DES: 6092	007 0 00 12	3904	✓		
7620	Dawn Pearson	008 0 00 08	3904	✓		
7621	Debbie Holt	011 0 00 08	3904	✓		
7622	Deborah Olson	012 0 00 08	3904	✓		
7623	Debra Carpenter	012 0 00 13	3904	✓		
7651	Diana Mendoza	006 0 00 14	3904	✓		

DN	Name	TN	Type	CFXA	USRA	CFW Length > 7
7652	Diane Lawson	017 0 00 11	3904	✓		
7653	Don Mason	015 0 00 04	3904	✓		
7654	Donald Harris	014 0 00 04	3904	✓		
7682	Donna Pierce	013 0 00 00	3904	✓		
7683	Doris Carr	014 0 00 16	3904			✓ (16)
7683	Doris Carr	014 0 00 00	3904	✓		
7684	Dorothy Dunn	015 0 00 00	3904	✓		
7685	Douglas Phillips	012 0 00 01	3904	✓		
7686	Earl Griffin	017 0 00 00	3904	✓		
7687	Eddie Morales	018 0 00 00	3904	✓		
7689	Edith Wade	006 0 00 01	3904	✓		
7691	Edna Jensen	017 0 00 07	3904	✓		
7694	Elaine Jimenez	011 0 00 01	3904	✓		
7695	DES: 6117	016 0 00 01	3904	✓		
7696	Eleanor Pena	015 0 00 01	3904	✓		
7697	Elizabeth Knight	008 0 00 12	3904	✓		
7698	Ellen Graves	013 0 00 01	3904	✓		
7708	DES: 6116	006 0 00 09	3904	✓		
7738	DES: 6104	008 0 00 03	3904	✓		
7739	Emma Gregory	011 0 00 03	3904	✓		
7740	Eric Hill	012 0 00 03	3904	✓		
7741	Ernest Long	013 0 00 03	3904	✓		
7742	DES: 6016	014 0 00 03	3904	✓		
7743	Esther Castro	015 0 00 03	3904	✓		
7744	Ethel Barnett	016 0 00 03	3904	✓		
7745	Eugene Ross	017 0 00 03	3904	✓		
7746	Eva Chambers	018 0 00 03	3904	✓		
7747	Evelyn Castillo	008 0 00 14	3904	✓		
7748	Florence Douglas	007 0 00 08	3904	✓		
7771	DES: 6149	006 0 00 04	3904	✓		
7773	DES: 6148	008 0 00 00	3904	✓		
7774	Francis Stevens	011 0 00 00	3904	✓		
7775	Francisco Holmes	012 0 00 00	3904	✓		
7786	Frederick Hicks	018 0 00 01	3904	✓		
7788	George Martin	016 0 00 00	3904	✓		
7807	Gloria Vasquez	008 0 00 04	3904	✓		
7808	Grace May	011 0 00 04	3904	✓		
7809	DES: 6144	012 0 00 04	3904	✓		
7811	Gregory Baker	008 0 00 05	3904	✓		
7901	Harold Turner	011 0 00 05	3904	✓		
7903	Hazel Craig	012 0 00 05	3904	✓		
7904	Heather Ryan	013 0 00 05	3904	✓		
7905	Helen Stephens	014 0 00 05	3904	✓		

DN	Name	TN	Type	CFXA	USRA	CFW Length > 7
7906	Henry Campbell	015 0 00 05	3904	✓		
7907	DES: 6006	016 0 00 05	3904	✓		
7908	Herbert Hunter	017 0 00 05	3904	✓		
7910	DES: 03021	006 0 00 03	3904	✓		
7911	Howard Barnes	006 0 00 06	3904	✓		
7912	Irene Little	007 0 00 10	3904	✓		
7913	Jack Morris	008 0 00 06	3904	✓		
7914	Jacob Murray	011 0 00 06	3904	✓		
7915	Jacqueline Dean	013 0 00 08	3904	✓		
7916	James Smith	012 0 00 06	3904	✓		
7917	Jamie Hale	013 0 00 06	3904	✓		
7918	Jane Burton	014 0 00 06	3904	✓		
7920	DES: 6132	016 0 00 06	3904	✓		
7921	Janice Meyer	017 0 00 06	3904	✓		
7922	Jason Lee	014 0 00 07	3904	✓		
7923	Jean Wheeler	006 0 00 07	3904	✓		
7924	Jeff Ortiz	007 0 00 11	3904	✓		
7925	Jeffery Cruz	007 0 00 03	3904	✓		
7926	Jeffrey King	011 0 00 07	3904	✓		
7927	Jennifer Ferguson	012 0 00 07	3904	✓		
7928	Jeremy Price	013 0 00 07	3904	✓		
7929	DES: 6014	018 0 00 06	3904	✓		
7930	Jerry Nelson	015 0 00 07	3904	✓		
7931	Jesse Flores	008 0 00 13	3904	✓		
7932	Jessica Carroll	007 0 00 13	3904	✓		
7934	Jimmy Diaz	015 0 00 06	3904	✓		
7935	Joan Richards	006 0 00 02	3904	✓		

4.4. External References

Description

Several redirection numbers on a station can be defined to go to numbers external to the Communication Server. Usually this incurs long-distance charges, and should be monitored for inappropriate use. In this topic we examine these redirection numbers, and highlight those that appear to route a call outside the Communication Server. We look at Hunt DNs, Call Forward DNs, Hotline DNs, Call Forward No Answer DNs, External Hunt DNs and Flexible Call Forward DNs.

Security Concerns

External redirection numbers should be checked for appropriateness. Certain uses are common, such as an external Voice Mail system. Abuses occur when individuals forward their phone for personal use.

Analysis

The following table list stations whose various redirection DNs appear to be external. The DNs in question are listed under each category:

- Hunting DNs (Hunt column)
- Forward Don't Answer (FDN column)
- Call Forwarding DNs (CFW column)
- External Hunting DNs (EHT column)
- External Forwarding DNs (EFD column)
- Hotline DNs (Hot column)

The DNs may also be Alternate DNs for the type listed (AEFD, AEHT, AHNT, etc.).

If the DN and TN columns are highlighted in the following table, it indicates that the station has User Selectable Call Redirection Allowed (USRA). This feature allows the users of the station to modify the dialing sequences for the Hunt, FDN, EFD, and EHT features. For these stations, it is especially important to check the external references are valid destinations and the user is not abusing the USRA feature.

DN	TN	Hunt	FDN	CFW	EHT	EFD	Hot
7285	007 0 00 07		63902				
7620	008 0 00 08		91900				

5. Trunking

Together with your stations, your trunking configuration defines the calling abilities of your users. It is important to manage your trunks, and organize them by expense and/or business needs. Certain settings on trunks and trunk routes should be avoided to help you maintain a secure switch. In this section, we're going to analyze your trunk routes, trunks, and other trunking configuration issues.

Did You Know?

While this section of the Security Audit will address the security aspects of Trunks, an InfoPlus SourceBook may be ordered to gain a more complete understanding of the configuration of your system. For example, the Routes Section of the SourceBook will clearly present exactly which routes are used in the placing of outgoing calls and the order in which they are used. The SourceBook answers all of the questions you may have about your system's configuration.

5.1. Routes and Trunks

Description

Your trunks should be organized functionally into Trunk Routes, or just Routes for short. By definition, all of the trunks in a route are of the same type and function. In the Communication Server, each route has its own configuration. Like most of the Communication Server programming, there are certain settings at the route level that could leave them vulnerable to abuse. We'll investigate those settings in this topic. In addition, each trunk of the route has a configuration that will also be analyzed.

Security Concerns

There are many potential pitfalls to avoid when defining routes and trunks. Something as simple as allowing outgoing calls on a route that is supposed to be incoming only could be a security problem. Other problems include a short or simple Trunk Route Access Code, an incorrectly configured Trunk Access Restriction Group, failure to collect Call Detail Recording data for the route, or having the route incorrectly modify numbers dialed through it.

The Trunks themselves can pose their own security issues. We'll be checking for unrestricted access privileges, auto-terminating trunks, and trunks that have external Night Service, Auto-Terminating, or Private Line directory numbers.

Analysis

Route Number: 0

Route Type: DID
Route Description: LONGD1

Trunk Route Access Code: 2290 This code should be at least 7 digits long.

This Route allows both Incoming and Outgoing calls.

TARG assignment: Empty

There is no Trunk Access Restriction Group (TARG) for this Route. You should modify the TARG to restrict stations, trunks, authorization codes, etc., which do not require direct access to this route.

Call Detail Recording data is not being collected for this Route. You may want to consider enabling CDR for this route as part of your Call Detail Recording strategy.

This Route is using Incoming DID Digit Conversion to modify the dialed digits of received calls. Your daytime Incoming Digit Conversion configuration appears to be valid. Your nighttime Incoming Digit Conversion configuration appears to be valid.

It could not be determined whether you are using joint disconnect control.

You have 23 Trunk(s) defined in this Route. The following table lists the Trunks in this Route. We note trunks that have the following conditions:

- A Network Class of Service greater than 0
- A potentially external Night DN

Member	TN	ID	NCOS	NITE
1	001 01		0	

Member	TN	ID	NCOS	NITE
2	001 02		0	
3	001 03		0	
4	001 04		0	
5	001 05		0	
6	001 06		0	
7	001 07		0	
8	001 08		0	
9	001 09		0	
10	001 10		0	
11	001 11		0	
12	001 12		0	
13	001 13		0	
14	001 14		0	
15	001 15		0	
16	001 16		0	
17	001 17		0	
18	001 18		0	
19	001 19		0	
20	001 20		0	
21	001 21		0	
22	001 22		0	
23	001 23		0	

Route Number: 1

Route Type: DID
Route Description: LONGD2

Trunk Route Access Code: 2991 This code should be at least 7 digits long.

This Route allows both Incoming and Outgoing calls.

TARG assignment: Empty

There is no Trunk Access Restriction Group (TARG) for this Route. You should modify the TARG to restrict stations, trunks, authorization codes, etc., which do not require direct access to this route.

Call Detail Recording data is not being collected for this Route. You may want to consider enabling CDR for this route as part of your Call Detail Recording strategy.

This Route is using Incoming DID Digit Conversion to modify the dialed digits of received calls. Your daytime Incoming Digit Conversion configuration appears to be valid. Your nighttime Incoming Digit Conversion configuration appears to be valid.

It could not be determined whether you are using joint disconnect control.

You have 23 Trunk(s) defined in this Route. The following table lists the Trunks in this Route. We note trunks that have the following conditions:

- A Network Class of Service greater than 0

- A potentially external Night DN

Member	TN	ID	NCOS	NITE
1	002 01	101	0	
2	002 02	101	0	
3	002 03	101	0	
4	002 04	101	0	
5	002 05	101	0	
6	002 06	101	0	
7	002 07	101	0	
8	002 08	101	0	
9	002 09	101	0	
10	002 10	101	0	
11	002 11	101	0	
12	002 12	101	0	
13	002 13	101	0	
14	002 14	101	0	
15	002 15	101	0	
16	002 16	101	0	
17	002 17	101	0	
18	002 18	101	0	
19	002 19	101	0	
20	002 20	101	0	
21	002 21	101	0	
22	002 22	101	0	
23	002 23	101	0	

Route Number: 2

Route Type: TIE
Route Description: LONGD3

Trunk Route Access Code: 2992 This code should be at least 7 digits long.

This Route allows both Incoming and Outgoing calls.

TARG assignment: Empty

There is no Trunk Access Restriction Group (TARG) for this Route. You should modify the TARG to restrict stations, trunks, authorization codes, etc., which do not require direct access to this route.

Call Detail Recording data is not being collected for this Route. You may want to consider enabling CDR for this route as part of your Call Detail Recording strategy.

It could not be determined whether you are using joint disconnect control.

You have 23 Trunk(s) defined in this Route. The following table lists the Trunks in this Route. We note trunks that have the following conditions:

- An Unrestricted Class of Service
- An unrestricted Trunk Group Access Restriction
- A Network Class of Service greater than 0

- A potentially external Night DN

Member	TN	ID	UNR	TGAR	NCOS	NITE
1	003 01		✓	0	0	
2	003 02		✓	0	0	
3	003 03		✓	0	0	
4	003 04		✓	0	0	
5	003 05		✓	0	0	
6	003 06		✓	0	0	
7	003 07		✓	0	0	
8	003 08		✓	0	0	
9	003 09		✓	0	0	
10	003 10		✓	0	0	
11	003 11		✓	0	0	
12	003 12		✓	0	0	
13	003 13		✓	0	0	
14	003 14		✓	0	0	
15	003 15		✓	0	0	
16	003 16		✓	0	0	
17	003 17		✓	0	0	
18	003 18		✓	0	0	
19	003 19		✓	0	0	
20	003 20		✓	0	0	
21	003 21		✓	0	0	
22	003 22		✓	0	0	
23	003 23		✓	0	0	

Route Number: 3

Route Type: DID
Route Description: BACKUP

Trunk Route Access Code: 2993 This code should be at least 7 digits long.

This Route allows both Incoming and Outgoing calls.

TARG assignment: 1

Call Detail Recording data is not being collected for this Route. You may want to consider enabling CDR for this route as part of your Call Detail Recording strategy.

You have 8 Trunk(s) defined in this Route. The following table lists the Trunks in this Route. We note trunks that have the following conditions:

- A Network Class of Service greater than 0
- A potentially external Night DN

Member	TN	ID	NCOS	NITE
1	005 0 00 00		0	
2	005 0 00 01		0	

Member	TN	ID	NCOS	NITE
3	005 0 00 02		0	
4	005 0 00 03		0	
5	005 0 00 04		0	
6	005 0 00 05		0	
7	005 0 00 06		0	
8	005 0 00 07		0	

Route Number: 4

Route Type: COT
Route Description: COTBACKUP

Trunk Route Access Code: 2994 This code should be at least 7 digits long.

This Route allows both Incoming and Outgoing calls.

TARG assignment: Empty

There is no Trunk Access Restriction Group (TARG) for this Route. You should modify the TARG to restrict stations, trunks, authorization codes, etc., which do not require direct access to this route.

Call Detail Recording data is not being collected for this Route. You may want to consider enabling CDR for this route as part of your Call Detail Recording strategy.

You have 8 Trunk(s) defined in this Route. The following table lists the Trunks in this Route. We note trunks that have the following conditions:

- A Network Class of Service greater than 0
- A potentially external Night DN

Member	TN	ID	NCOS	NITE
1	020 0 00 00		0	
2	020 0 00 01		0	
3	020 0 00 02		0	
4	020 0 00 03		0	
5	020 0 00 04		0	
6	020 0 00 05		0	
7	020 0 00 06		0	
8	020 0 00 07		0	

Route Number: 6

Route Type: COT
Route Description: TEST

Trunk Route Access Code: 2996 This code should be at least 7 digits long.

This Route allows both Incoming and Outgoing calls.

TARG assignment: Empty

There is no Trunk Access Restriction Group (TARG) for this Route. You should modify the TARG to restrict stations, trunks, authorization codes, etc., which do not require direct access to this route.

<u>This is an auto-terminating Route.</u> Please see the 'Trunks' portion of this analysis to see the number(s) to which the route terminates, and verify them.

<u>Call Detail Recording data is not being collected for this Route.</u> You may want to consider enabling CDR for this route as part of your Call Detail Recording strategy.

<u>There are no trunks defined for this Route.</u> This Route should be removed.

5.2. Matching TGAR and TARG

Description

Trunk Group Access Restrictions are used to allow or deny direct access to a route. Each telephone, DISA directory number, TIE trunk, and Authorization Code gets assigned a TGAR value. All trunk routes are assigned a Trunk Access Restriction Group, or TARG. When calls are attempted by directly accessing the trunk route, the TARG of the route is compared to the TGAR of the station, TIE trunk, etc. If they match, the call is blocked.

Security Concerns

The TGAR/TARG configuration is a powerful way to control direct route access, if set up correctly. Each assigned TGAR should be blocked for outgoing toll routes, or it may be able to bypass the restrictions of the BAR/NARS design. Similarly, each TARG entry should block some station, TIE trunk, Authorization Code, or DISA directory number.

Analysis

All of your non-zero TGAR assignments are blocked by one or more Routes. You may have stations, trunks, etc. with a TGAR assignment of 0. These are highlighted in their appropriate topics in the report.

All of your TARG assignments are blocking one or more station, TIE trunk, DISA directory number, or Authorization Code. You may have Routes with no TARG assignment; these are reported in Section 5.1.

Permitting direct trunk access can enable users to bypass the restrictions of BARS/NARS programming; this may allow the ability to make toll calls they were unable to access through BARS/NARS.

Did You Know?

Apart from Security issues addressed in the Security Audit, many people ask, "Who has the ability to call where?" The Calling Privileges section of the InfoPlus SourceBook answers these and other similar questions about the configuration of your Communication Server.

6. Controlling Calling Privileges

The configuration of your stations and trunks define basic access restrictions within the Communication Server. However, there are many other ways to modify these restrictions with various features and services. This section presents these features and addresses the configuration of each one individually. Some features further limit the capabilities of a station or trunk, while others circumvent restrictions already in place. Their intelligent use allows you to design a telecommunications solution that provides only the necessary functionality without opening the doors to unauthorized use.

6.1. System Speed Call

Description

The Speed Call feature (also known as "abbreviated dialing") allows users to place internal or external calls by dialing a 1-, 2-, or 3-digit code. System Speed Call extends these capabilities by allowing a user to bypass their assigned class of service and trunk group access restrictions when dialing a list entry number. You can program up to 1,000 numbers in System Speed Call, each containing as many as 31 digits.

Security Concerns

Because System Speed Call can override the Class of Service and Trunk Group Access Restriction of stations, it is important to verify the numbers stored in the list(s) are approved destinations. It is also important to control the individuals who can modify these lists, known as a System Speed Call Controller.

Analysis

You have 1 System Speed Call List(s) defined. Following is each of your System Speed Call Lists, and the entries currently programmed. These entries should be verified as approved destinations.

Speed Call List: 0

Maximum Number of Digits for Entries: 31
List Size: 100

List Entries

Entry #	Destination
4	65551234
5	65551234
7	65551234
8	912015551234
11	65551234
14	912015551234
17	912015551234
18	65551234
20	912015551234
21	912015551234
22	912015551234
24	912015551234
25	912015551234
26	912015551234
28	912015551234
29	912015551234
31	912015551234
33	912015551234
35	912015551234
37	912015551234

Entry #	Destination
40	912015551234
44	912015551234
49	912015551234
51	65551234
56	7600
58	912015551234
59	912015551234
62	912015551234
65	912015551234
67	912015551234
71	912015551234
72	67222000
73	912015551234
74	912015551234
76	912015551234
77	912015551234
78	65551234
82	912015551234
83	912015551234
99	2929

The following is a list of Controllers for this System Speed Call List:

DN	Name	TN	Type
N/A	N/A	007 0 00 00	2250
7654	Donald Harris	014 0 00 04	3904

6.2. Network Speed Call

Description

Network Speed Call provides access to the System Speed Call feature via your private network and, using the Direct Inward System Access (DISA) feature, through the public network. As in the case of System Speed Call, a network caller can also bypass access restrictions when dialing a list entry number from the Network Speed Call List.

Security Concerns

Since Network Speed Call Lists are System Speed Call Lists that can be accessed from the Network, the same concerns apply as did with System Speed Call Lists. Review the System Speed Call Lists designated as Network Speed Call lists to ensure the entries are appropriate destinations for access from the Network. Additionally, review the section of this security audit on DISA to be certain the public network access to the Network Speed Call list is protected.

Analysis

You do not have any Network Speed Call Lists defined.

6.3. Code Restriction

Description

Stations and TIE trunks having a Toll Denied Class of Service are permitted limited access to the toll exchange network with this feature. A code restriction block is built for each trunk route that will permit access to specific area and exchange codes by checking the first 3 digits dialed after the trunk route access code. This feature applies when the route is directly accessed and does not apply to calls made using BARS/NARS access codes.

Security Concerns

Since Code Restriction can override the intended limitations of Toll Denied, Conditionally Toll Denied, and Conditionally Unrestricted stations and TIE trunks, it is important to ensure this feature is programmed correctly. It can be used to allow access to certain area codes and exchanges, or ALL area codes and exchanges. Typically, if it were intended to provide access to all area and exchange codes, the station or TIE trunk would not be toll-denied.

Analysis

You have no Code Restriction Blocks defined.

6.4. New Flexible Code Restriction

Description

Providing an even greater level of flexibility than Code Restriction, New Flexible Code Restriction controls the access of Toll Denied telephones and TIE trunks to outgoing trunk routes, as well as the digits dialed on them. For a particular Route, each FRL can be assigned a New Flexible Code Restriction tree that defines the dialable digits when accessed by a station with that FRL. The definition of dialable digits is more flexible than with Code Restriction since the entries can be of varying lengths. This feature applies when routes are directly accessed and does not apply to BARS/NARS calls.

Security Concerns

Like Code Restriction, New Flexible Code Restriction can override the intended limitations of Toll Denied, Conditionally Toll Denied, and Conditionally Unrestricted stations, trunks, DISA DNs and Authorization Codes. Therefore, it is important to ensure this feature is programmed correctly. It can be used to allow access to specified sequences of dialed digits, or ALL sequences of dialed digits. When activated, New Flexible Code Restriction overrides Code Restriction when placing calls.

Analysis

You do not have any New Flexible Code Restriction Trees defined.

6.5. Scheduled Access Restrictions

Description

With this feature, you can program access restrictions (TGAR, COS and NCOS), by groups, for different hours and days. Although customers use this feature mostly for off-hours and/or off-days, there is the flexibility of programming up to 1000 groups, with up to eight different periods for a particular group.

Security Concerns

Since this feature modifies Class of Service and Trunk Group Access Restrictions, it can have a significant impact on calling privileges. It is recommended that no scheduled period have the unrestricted configurations we've been checking for, namely Unrestricted Class of Service and Trunk Group Access Restriction 0.

Analysis

You have no SAR groups defined.

6.6. Controlled Class of Service and Enhanced Controlled Class of Service

Description

With Controlled Class of Service, stations users that are designated as "controllers" can, through the use of a multi-button set or a background terminal, temporarily change a telephone's class of service. Enhanced Controlled Class of Service extends the controller function of CCOS to attendant consoles and Meridian 3000 sets equipped with a controller key. Additionally, it makes available to users two additional customer-defined levels of CCOS restrictions. Station users can also activate and deactivate the Controlled Class of Service mode with the Electronic Lock feature, if appropriate Flexible Feature Codes and Station Control Passwords are defined. When 'locked', stations are also assigned the Controlled Network Class of Service. Users can activate Electronic Lock to prevent unauthorized access when they're away from their station.

Security Concerns

The Controlled Class of Services can actually be set to any restriction level, including Unrestricted (UNR), which is the default. This could actually increase the capabilities of 'controlled' stations. For normal usage, these Controlled Classes of Service should be restrictive (Semi-Restricted or Fully Restricted). In addition, the Controlled NCOS, which is used by the Electronic Lock feature, should be restrictive.

Analysis

Your Controlled Classes of Service are
Controlled Class of Service: UNR
Enhanced Controlled Class of Service, Level 1: UNR
Enhanced Controlled Class of Service, Level 2: UNR

The Controlled Classes of Service in red are not sufficiently restrictive, and should be changed to CTD, FR1, FR2, FRE, SRE, or TLD.

The Controlled Network Class of Service, which is used during Electronic Lock feature activation, is:
0

This low Controlled Network Class of Service meets recommendations.

6.7. Basic and Network Authorization Codes

Description

Authorization codes (or authcodes as they are commonly referred to), allow a user to temporarily override the access restrictions assigned to sets, DISA directory numbers or TIE trunks. Authorization codes are also used as a means to bill calls to specific accounts or employees. You can assign 4,096 basic or 20,000 network authorization codes per customer, with up to 14 digits in length for each code.

Security Concerns

Authorization codes should be sufficiently long to prevent unauthorized personnel from guessing them. In addition, you should not use an individual's social security number, Employee ID, phone number, etc. as their Authorization Code. A list of codes should be managed and updated when employees leave or change positions. Although authcodes are used to override a station's restrictions, they should not be too powerful, assigning privileges you would otherwise avoid.

Analysis

You do not have the Authorization Code feature enabled, though you do have the software for the feature installed.

6.8. Forced Charge Account

Description

The Forced Charge Account feature permits toll-denied users to temporarily override Class of Service restrictions. When activated, this feature allows a user to place long distance calls from a restricted telephone by entering an account code number. The Communication Server then validates only the number of digits dialed, not the actual digits themselves.

Security Concerns

It is recommended that the Authorization Code feature, which can essentially perform the same function, be used instead of Forced Charge Account. Authorization Codes verify the actual digits dialed, increasing security.

Analysis

Forced Charge Account is inactive.

7. Controlling Feature Access

The Communication Server has many calling features, which if not properly controlled could allow unauthorized users to commit toll fraud. Many of these features can be activated or deactivated at any station, or even through voice mail ports. The most powerful features have additional security in the form of a Station Control Password; however you can increase security by disabling those features all together.

7.1. Flexible Feature Codes

Description

Flexible Feature codes (FFCs) are user-defined numbers of up to four digits that can be used instead of the existing Special Prefix (SPRE) codes defined in the Communication Server. With this feature, you can define different dialing codes to activate, de-activate and modify defined features. Option 150, the DN Expansion package, increases the maximum length of defined feature codes from four to seven.

Security Concerns

Flexible Feature Codes for features with security implications should not be accessible through voice mail. If applicable, see the Permission/Restriction Lists topic in the Meridian Mail section. Furthermore, it is recommended that no FFC be defined for Remote Call Forward Activate, Deactivate, and Verify unless the feature is protected by a station control password, and the feature usage is tracked on Call Detail Recording.

Analysis

The most critical Flexible Feature Codes are either empty, or are non-numeric and do not need to be blocked in voice mail.

7.2. End of Dialing Indication

Description

The End of Dialing Indicator is by default a '#'. It can be modified to be a string of digits, '#', and/or '*' that let the Communication Server know dialing is complete when using Flexible Feature Codes. If you use '#' in your dialing plan, you may have to modify the default value of the End of Dialing Indicator for Flexible Feature Codes.

Security Concerns

If using a non-standard End of Dialing Indicator, you must verify that this string is blocked in the voice mail, and in Meridian Mail Restriction/Permission lists, if applicable.

Analysis

You are using the default End of Dialing Indicator, #, which is recommended.

7.3. Station Control Password

Description

The Station Control Password (SCPW) is used with many features including the Electronic Lock, User Selectable Call Redirection and Remote Call Forward features. In order to initiate or disable these features, the Station Control Password for the particular station must be entered.

Reference the topic on Controlled Class of Service for more information about the Electronic Lock feature.

Security Concerns

Specifying a Station Control Password Length of 0 disables the Electronic Lock, User Selectable Call Redirection, and Remote Call Forward features. Using the same station control password on any or all sets with these features defeats the security of the SCPW.

Analysis

Your Station Control Password Length is 0. This disables the Electronic Lock, User Selectable Call Redirection, and Remote Call Forward features.

7.4. Special Prefix Code

Description

The Special Prefix Code (SPRE) is a one to four-digit number programmed in the Communication Server to activate and/or modify a feature. (It is particularly useful for single line sets users to allow them to access features without programming a specific feature access key on sets with that capability.)

Security Concerns

The Special Prefix Code should be 4 digits long to prevent unauthorized feature access. It should be blocked in the Restriction/Permission tables of the voice mail system, if applicable.

Analysis

Your Special Prefix Code is 1. Verify that this code is blocked in the Permission/Restriction lists of Meridian Mail (see the Meridian Mail section), or restrict voice mail systems from thru-dialing the SPRE code.

8. Controlling Call Forward All Calls

The Call Forward All Calls feature requires special attention because of its toll-abuse potential. Without the proper guidelines in place, users could forward their phone to a remote destination, a trunk-access code, or a BARS/NARS access code, and use the forwarding capabilities for personal use. This section presents topics that allow you to limit the liability associated with this feature.

8.1. Remote Call Forward

Description

Remote Call Forward (RCFW) allows users to define call forward destinations from both inside and outside the Communication Server. This feature is assigned on a station-by-station basis, and should be password protected to prevent abuse.

Security Concerns

With this feature, users could forward their calls to an unauthorized number for personal use. Since changes can be made remotely, unauthorized personnel could also 'take control' of a station for their own use, leaving the company to pick up the bill. External access is provided via Direct Inward System Access (DISA). (also see the chapter on DISA)

Analysis

You do not have Remote Call Forward enabled. This increases the security of your switch.

8.2. Call Forward All Calls Control

Description

This option allows you to decide whether the calling restrictions (Class of Service) that are in place during a forwarded call are based on the restrictions of the originating party or the forwarding party. This choice affects all forwarded calls for both stations and trunks.

Security Concerns

Using the Forwarding Party's Class of Service to determine access to services and features could circumvent restrictions placed on the originating party. The originating party's Class of Service is recommended to control access.

Analysis

You have Call Forward All Calls Control specified for the Originating Party, which is recommended.

8.3. Call Forward to Trunk Access Code

Description

With this feature, you have the capability of restricting users from forwarding calls to a trunk route access code programmed in the Communication Server. Forwarding calls to a route access code would allow the caller to dial additional digits, placing a call through the Communication Server at the company's expense and bypassing the programming restrictions built into the BARS/NARS design.

Security Concerns

Allowing forwarding to a Trunk Route Access Code has significant toll-abuse potential. A user could Call Forward their DID station to a Trunk Route Access Code, and then place long-distance calls from home by dialing their office number and receiving dial tone. The user would only pay for a local call to the office, while the company foots the long-distance charges.

Analysis

You have Call Forward to Trunk Access Codes allowed. It is recommended you disable this feature to increase security.

9. Remote User System Access

This section addresses Direct Inward System Access (DISA) and Mobile Service Access (MSA). Both of these features allow users to have remote access to your private network. They require special consideration due to potential toll-abuse originating from the public network. Due to the sensitivity of these features they are delivered in separate software packages that can be completely disabled.

9.1. DISA

Description

Direct Inward System Access, the DISA feature, permits selected users to directly access the Communication Server from the public network by dialing a special Directory Number. The DISA user dials the number from any location outside the network, and once the call has been answered, the features and calling capabilities of the Communication Server are as accessible as if the caller were on site. To protect against unauthorized use of this feature, special security codes of up to eight digits can be assigned to each DISA-DN.

In addition to the security code assigned to the DISA-DN, it is recommended that each DISA user be assigned an authorization code to track usage and billing using Call Detail Recording. Refer to the section on Authorization Codes.

Security Concerns

DISA, even when properly configured, can open the Communication Server to toll-abuse from the public network. If it is not required, removing this feature from the Communication Server software provides the greatest security. It is most cost-effective to remove the DISA feature when performing a software upgrade. If DISA is required, it should be heavily protected through the use of Authorization Codes, Security Codes, Network Speed Call Lists, and tight Access Restrictions. In addition, DISA dial-in numbers should not be published, and their distribution should be limited to employees who require the feature.

Analysis

You do not have the DISA software package installed on your Communication Server. This provides the greatest security level when considering this feature.

9.2. Mobile Service Access

Description

Mobile Service Access, (MSA), allows access to the Communication Server from mobile devices, such as cell phones. Mobile users can access the Communication Server from private and public networks by calling an MSA DN. If they are an authorized mobile user they will be granted access to the calling features and dialing plan of the private network. All calls made by the mobile user will appear to originate from within the private network. As such this feature offers great flexibility to mobile users. It also presents serious security risks that need to be addressed.

Access to the Communication Server through an MSA DN can be restricted through the use of security codes, authorization codes and collect call signal blocking.

Security Concerns

When considering your configuration as described below, keep the following in mind. If improperly configured, MSA can open your system up to toll-abuse from the public network. In addition, calls through the MSDN appear to originate from within the private network. If access is compromised, malicious calls could masquerade as being officially endorsed by your organization. Because of MSA's significant power it is recommended that both security and authorization codes be required. Security codes and authorization codes should be least 6 digits for adequate security. MSA DNs should be non-published numbers.

Analysis

You do not have the Mobile Extensions software package installed on your Communication Server. This provides the greatest level of security when considering this feature.

10. Automatic Call Distribution

This section addresses security issues that arise during the programming of Automatic Call Distribution queues. The main concerns are where calls are sent during off-hours or heavy traffic periods. Also included is a topic on the Meridian Integrated Personal Call Director card, which uses ACD facilities to implement a 'follow-me' application.

💡Did You Know?

Once again, the InfoPlus SourceBook could be used to completely identify which and how many Agents belong to each ACD Group, providing a higher level, managerial perspective of important ACD group configurations.

10.1. ACD

Description

Automatic Call Distribution (ACD) is used to equally distribute a large number of incoming calls to a group of assigned stations. The grouping is referred to as an ACD Group, and its members are made up of "agents". The calls are generally answered on a first-in, first-out basis, and distributed among the available stations, so that the agent position that remains inactive the longest is provided with the call.

Security Concerns

Each ACD DN can be configured with a Night Call Forward DN (where calls are sent during Night treatment) and an Interflow DN (where calls can be directed during heavy traffic). Both the Night Call Forward DN and the Interflow Directory Number should be checked to ensure they are not unauthorized external numbers.

Analysis

The following table summarizes the Night Call Forward and Interflow Directory Numbers for your ACD DNs. Numbers that appear to be external to the Communication Server are highlighted in red. They should be verified to ensure calls are being routed to valid locations. Note that ACD Groups with no agents are always in Night Mode.

ACD DN	Always in Night Mode	Night Call Forward	Interflow
2888	✓	5555555	
2929	✓	5555555	
2930	✓	5555555	
7119	✓	912014760600	
7164	✓	2929	
7169	✓	912014760600	
7260	✓	912014760600	
7261	✓	912014760600	
7349	✓	912014760600	
7390	✓	912014760600	
7391	✓	912014760600	
7392	✓	912014760600	
7606	✓	2929	
7618	✓	912014760600	
7680	✓	912014760600	
7681	✓	912014760600	
7749	✓	912014760600	
7780	✓	912014760600	
7791	✓	912014760600	
7792	✓	912014760600	
7799	✓	912014760600	
7813		0	
7817	✓	912014760600	
7818	✓	912014760600	

ACD DN	Always in Night Mode	Night Call Forward	Interflow
7819	✓	912014760600	
7939		5555555	5555555

10.2. MIPCD Agents

Description

The Meridian Integrated Personal Call Director (MIPCD) card allows users to define a series of 'follow-me' numbers that will be called either sequentially or in parallel to locate the user when they're away from their phone. Users can modify their personal schedules and destination numbers using a Web-based browser or telephone/voice prompt interface.

Security Concerns

When the MIPCD card places outgoing calls, it uses the facilities of virtual ACD agents to actually place the calls through the Communication Server. While an administrator can define "Call Screening Dial Restrictions" in the MIPCD's database to restrict the outcalling numbers, the basic access restrictions of the virtual ACD agents have the final word on whether a particular call is allowed or not. In addition to maintaining the Call Screening Restrictions, one should limit the dialing capabilities of the agents as well to prevent unauthorized calls.

Analysis

You have no ACD agents defined as the manufacturer requires for an MIPCD card. If you do indeed have an active MIPCD card, verify that the discrepancies between the agents' key assignments and the manufacturer's recommendations are intentional.

11. Call Routing

In addition to the restrictions placed at the station or trunk level, it's important to control how both incoming and outgoing calls are routed through the Communication Server network. We'll be analyzing the various features of the Electronic Switched Network package and Basic Automatic Route Selection and Network Automatic Route Selection (BARS/NARS) features, looking for unusual routing configurations. Incorrect routing could prevent certain calls from being placed or received at all, or could send calls over unnecessarily expensive trunking facilities. The routing configuration is also used to supplement the definition of individual calling restrictions, defining who can call where and at what times.

Did You Know?

While this Section of the Security Audit will present security concerns regarding the routing of calls, an InfoPlus Traffic Study would help determine the proper number and types of trunks to have based upon specific call volumes and patterns. InfoPlus Traffic Studies typically result in lower communications expense by optimizing and eliminating unnecessary resources.

11.1. Route List Indices

Description

For each network call translated at a Communication Server Node, BARS or NARS selects a route from a list of out-going alternate routes to complete the call. A list of alternate routes to a particular destination is called a route list, and each route specified in the list is termed an entry. Typically, the first entries (routes) in a route list should be the least expensive routes to a destination, and the remaining routes in the list are more expensive.

Security Concerns

Route List entries can be associated with a Digit Manipulation table, which should be examined for any inappropriate digits being inserted. Also, each entry may have a Time of Day Schedule assigned that restricts when calls may be placed on that route.

Analysis

All of your Route List entries reference Routes with trunk assignments.

The following Route List entries reference Digit Manipulation Tables which insert suspicious digit sequences:

Route List	Entry	Digit Manipulation Table	Digits Inserted
10	0	1	9
10	1	1	9
18	1	9	12015551234
18	2	9	12015551234

All of your Route List entries have at least one Time of Day Schedule in effect.

11.2. Routing Control

Description

Routing Control allows you to automatically alter the network access capabilities of users during a specified time frame each day, and/or on weekends. It can also be activated manually by an attendant. This feature is used to restrict people from accessing unattended telephones after hours to place unauthorized calls.

Security Concerns

You want to ensure the Routing Control schedule is properly configured for off-hours to protect stations against unauthorized use. Ensure the altered Network Class of Service is more restrictive during off-hours.

Analysis

Routing Control is not enabled. It is recommended that you consider enabling this feature to restrict network access during off-business hours.

11.3. Pretranslation Lists

Description

Pretranslation Lists allow you to create a flexible numbering plan by analyzing the first digit of a dialed sequence and modifying the dialed number by blocking the call, deleting the first digit, replacing the first digit with a specified string of digits, or passing the number unchanged. Each telephone, trunk, or console gets assigned one of 255 possible Pretranslation Lists that determines this behavior.

Security Concerns

While the proper setup of Pretranslation Lists can be quite complicated, such as in hospitality environments, the main security concern is that list entries do not provide direct access to trunks or BARS/NARS access codes.

Analysis

You do not have the Pretranslation option enabled, although you do have the software package for this feature installed.

11.4. Digit Manipulation

Description

Digit Manipulation enables the Communication Server to modify dialed digits to conform to the specific dialing requirements of individual trunks by deleting up to 15 leading digits, and inserting up to 24 leading digits. A total of 255 Digit Manipulation tables can be specified.

Security Concerns

The digits inserted by Digit Manipulation tables should be checked to ensure that no external numbers are being inserted in the dialing sequence.

Analysis

You have 10 Digit Manipulation table(s) defined, which are summarized in the following chart. We've highlighted tables inserting suspicious digit sequences.

Table Number	Digits Deleted	Digits Inserted
1	0	9
2	0	1
3	0	0
6	4	6
9	8	12015551234
10	0	1
11	1	
13	3	
66	4	6
68	7	4321

11.5. Incoming DID Digit Conversion

Description

Incoming DID Digit Conversion (IDC) allows the digits received from a DID call to be converted into an internal DN of up to eight digits. This feature can be used standalone, or in an ISDN environment. The conversion takes place at the network node where the call arrives prior to the digits being processed.

Security Concerns

It is important to ensure the result of any Incoming DID Digit Conversion is an authorized destination. Results that return dial tone to the caller, such as Trunk Route Access Codes, or BARS/NARS access codes, should be avoided. Similarly, any translation to an external number should be verified.

Analysis

You have 1 Incoming DID Digit Conversion tree(s) defined.

None of your IDC trees are empty, which is the recommended configuration.

All of the entries in the IDC trees appear to be internal DNs, which is the recommended configuration.

All of your IDC trees are in use by at least one Route, which is the recommended configuration.

11.6. Incoming Trunk Group Exclusion

Description

The Incoming Trunk Group Exclusion (ITGE) feature applies standard call blocking to calls from a specific incoming trunk group tandeming out to a specific Numbering Plan Area (NPA), Exchange (NXX), Special Number (SPN) or Location (LOC) code at the ESN node. With this feature in place, users cannot use another Communication Server in the network to circumvent dialing restrictions at their home location.

Security Concerns

This feature should be employed to prevent remote Communication Server users from routing calls over TIE lines to another Communication Server in the network to circumvent the calling restrictions at their home Communication Server.

Analysis

You have no Incoming Trunk Group Exclusion indices defined.

11.7. Free Calling Area Screening

Description

Free Call Area Screening (FCAS) provides full 6-digit screening to determine the route choice for completion of off-net calls. You can allow calls to NXX codes within the "free calling area" and restrict those NXX codes that would incur long distance charges.

Security Concerns

If you are using Free Call Area Screening for its intended purpose, it's important to verify the entries in each FCAS table specify the "free calling area" around a particular on-net location. If there are billable, non-local exchanges (NXXs) included in the FCAS table, they should be removed.

Analysis

You have no Free Calling Area Screening tables defined.

11.8. Network Translation

Description

The BARS/NARS Network Translation tables determine which Route List is used to route calls to particular locations. Each area code or local exchange is assigned a Route List that defines the Routes available for calls to that particular destination. Using the Supplemental Digit Restriction and Recognition (SDRR) feature, you can restrict certain dialing sequences for each area code or local exchange, and also have the Communication Server recognize public switched network calls placed to on-network destinations to avoid unnecessary expense. Special Numbers (SPN) and Location Codes (LOC) can also be assigned a Flexible Length that defines the minimum number of digits that can be dialed to complete a call or at least generate a CDR record.

Security Concerns

The entries that appear in your BARS/NARS translation tables determine which numbers can be dialed through BARS/NARS. Omitting unauthorized entries, such as calls to 1-900 pay services, area codes known for their high toll abuse (i.e. 809), and international area codes, is a critical part of your BARS/NARS configuration. Other translation table entries that should be monitored include the 976 exchange, international access codes, 'Equal Access' codes, and 1-800 carrier specific services. Entries for international (011) and operator assisted (0) calls should specify an appropriate Flexible Length to prevent users from truncating CDR records by pausing during the dialing sequence.

Another potential area for abuse is Digit Manipulation tables that are used to modify the dialed sequence. A Digit Manipulation table could be defined to turn an unused area code or exchange into the sequence for an unauthorized destination. Therefore, it is important to analyze both the entries in the translation tables themselves, and also what digits are outpulsed to the network.

Analysis

We analyze your BARS/NARS translation tables to uncover dialing sequences that can incur above-average expense. If a Digit Manipulation table (DMI) is used to modify the dialed sequence, the result of the manipulation is checked rather than the entry itself. Since Route Lists may have more than one entry, a particular network translation entry (NPA, NXX, SPN, etc.) may appear more than once in the table if manipulated into more than one sequence.

It is recommended that you remove the following entries from your Network Translation tables, or verify that the NCOS is high enough to properly restrict their use:

Access Code	Table	Entry	Using DMI	Becomes	Reason
AC1	NPA	1204	-	1204	International (Canada)
AC1	NPA	1242	-	1242	International (Bahamas)
AC1	NPA	1246	-	1246	International (Barbados)
AC1	NPA	1250	-	1250	International (Canada)
AC1	NPA	1264	-	1264	International (Anguilla)
AC1	NPA	1268	-	1268	High Toll Fraud Potential
AC1	NPA	1284	-	1284	International (British Virgin Is.)
AC1	NPA	1289	-	1289	International (Canada)
AC1	NPA	1306	-	1306	International (Canada)
AC1	NPA	1345	-	1345	International (Cayman Is.)
AC1	NPA	1403	-	1403	International (Canada)
AC1	NPA	1416	-	1416	International (Canada)

Access Code	Table	Entry	Using DMI	Becomes	Reason
AC1	NPA	1418	-	1418	International (Canada)
AC1	NPA	1441	-	1441	International (Bermuda)
AC1	NPA	1450	-	1450	International (Canada)
AC1	NPA	1473	-	1473	High Toll Fraud Potential
AC1	NPA	1506	-	1506	International (Canada)
AC1	NPA	1514	-	1514	International (Canada)
AC1	NPA	1519	-	1519	International (Canada)
AC1	NPA	1604	-	1604	International (Canada)
AC1	NPA	1613	-	1613	International (Canada)
AC1	NPA	1647	-	1647	International (Canada)
AC1	NPA	1649	-	1649	High Toll Fraud Potential
AC1	NPA	1664	-	1664	High Toll Fraud Potential
AC1	NPA	1705	-	1705	International (Canada)
AC1	NPA	1709	-	1709	International (Canada)
AC1	NPA	1758	-	1758	High Toll Fraud Potential
AC1	NPA	1767	-	1767	High Toll Fraud Potential
AC1	NPA	1778	-	1778	International (Canada)
AC1	NPA	1780	-	1780	International (Canada)
AC1	NPA	1784	-	1784	High Toll Fraud Potential
AC1	NPA	1807	-	1807	International (Canada)
AC1	NPA	1809	-	1809	High Toll Fraud Potential
AC1	NPA	1819	-	1819	International (Canada)
AC1	NPA	1867	-	1867	International (Canada)
AC1	NPA	1868	-	1868	High Toll Fraud Potential
AC1	NPA	1869	-	1869	International (St. Kitts & Nevis)
AC1	NPA	1876	-	1876	High Toll Fraud Potential
AC1	NPA	1902	-	1902	International (Canada)
AC1	NPA	1905	-	1905	International (Canada)
AC1	NXX	211	-	211	Possible Toll Service
AC1	NXX	311	-	311	Possible Toll Service
AC1	NXX	411	-	411	Information
AC1	NXX	511	-	511	Possible Toll Service
AC1	NXX	611	-	611	Repair
AC1	NXX	711	-	711	Possible Toll Service
AC1	NXX	811	-	811	Possible Toll Service
AC1	SPN	00	-	00	Long Distance Operator
AC1	SPN	01	-	01	International
AC1	SPN	011	-	011	International
AC1	SPN	02	-	02	Operator
AC1	SPN	03	-	03	Operator
AC1	SPN	04	-	04	Operator
AC1	SPN	05	-	05	Operator
AC1	SPN	06	-	06	Operator
AC1	SPN	07	-	07	Operator

Access Code	Table	Entry	Using DMI	Becomes	Reason
AC1	SPN	08	-	08	Operator
AC2	NPA	1242	-	1242	International (Bahamas)
AC2	NPA	1246	-	1246	International (Barbados)
AC2	NPA	1250	-	1250	International (Canada)
AC2	NPA	1264	-	1264	International (Anguilla)
AC2	NPA	1268	-	1268	High Toll Fraud Potential
AC2	NPA	1284	-	1284	International (British Virgin Is.)
AC2	NPA	1345	-	1345	International (Cayman Is.)
AC2	NPA	1441	-	1441	International (Bermuda)
AC2	NPA	1450	-	1450	International (Canada)
AC2	NPA	1473	-	1473	High Toll Fraud Potential
AC2	NPA	1600	-	1600	International (Canada)
AC2	NPA	1649	-	1649	High Toll Fraud Potential
AC2	NPA	1664	-	1664	High Toll Fraud Potential
AC2	NPA	1758	-	1758	High Toll Fraud Potential
AC2	NPA	1767	-	1767	High Toll Fraud Potential
AC2	NPA	1784	-	1784	High Toll Fraud Potential
AC2	NPA	1867	-	1867	International (Canada)
AC2	NPA	1868	-	1868	High Toll Fraud Potential
AC2	NPA	1869	-	1869	International (St. Kitts & Nevis)
AC2	NPA	1876	-	1876	High Toll Fraud Potential

Using Supplemental Digit Restriction and Recognition, specific dialing sequences within an area code or exchange can be denied. It is recommended to use this feature to deny calls to high-toll exchanges like 976 in all area codes. Some area codes have exchanges other than 976 that are reserved for toll-service calls and are included in the following analysis.

The following Network Translation table entries allow calls to be placed to high toll exchanges:

Access Code	Table	Entry	Using DMI	Becomes	Recommendation
AC1	NPA	1202	-	1202	Deny 915
AC1	NPA	1204	-	1204	Deny 940
AC1	NPA	1205	-	1205	Deny 924
AC1	NPA	1206	-	1206	Deny 960
AC1	NPA	1207	-	1207	Deny 940
AC1	NPA	1208	-	1208	Deny 960
AC1	NPA	1212	-	1212	Deny 540, 550, 970
AC1	NPA	1214	-	1214	Deny 703
AC1	NPA	1215	-	1215	Deny 556, 846, 936
AC1	NPA	1216	-	1216	Deny 931
AC1	NPA	1301	-	1301	Deny 915
AC1	NPA	1303	-	1303	Deny 960
AC1	NPA	1307	-	1307	Deny 960
AC1	NPA	1308	-	1308	Deny 960
AC1	NPA	1315	-	1315	Deny 540, 550, 970
AC1	NPA	1401	-	1401	Deny 940

Access Code	Table	Entry	Using DMI	Becomes	Recommendation
AC1	NPA	1402	-	1402	Deny 960
AC1	NPA	1410	-	1410	Deny 915
AC1	NPA	1412	-	1412	Deny 556
AC1	NPA	1413	-	1413	Deny 550, 940
AC1	NPA	1504	-	1504	Deny 636
AC1	NPA	1505	-	1505	Deny 960
AC1	NPA	1507	-	1507	Deny 960
AC1	NPA	1508	-	1508	Deny 940
AC1	NPA	1512	-	1512	Deny 766
AC1	NPA	1513	-	1513	Deny 499
AC1	NPA	1516	-	1516	Deny 540, 550, 970
AC1	NPA	1518	-	1518	Deny 540, 550, 970
AC1	NPA	1602	-	1602	Deny 676, 960
AC1	NPA	1603	-	1603	Deny 940
AC1	NPA	1605	-	1605	Deny 960
AC1	NPA	1607	-	1607	Deny 540, 550, 970
AC1	NPA	1610	-	1610	Deny 846, 936
AC1	NPA	1617	-	1617	Deny 550, 940
AC1	NPA	1703	-	1703	Deny 844
AC1	NPA	1713	-	1713	Deny 766
AC1	NPA	1716	-	1716	Deny 540, 550, 970
AC1	NPA	1718	-	1718	Deny 540, 550, 970
AC1	NPA	1719	-	1719	Deny 898
AC1	NPA	1801	-	1801	Deny 960
AC1	NPA	1809	-	1809	Deny 817, 892
AC1	NPA	1817	-	1817	Deny 892
AC1	NPA	1914	-	1914	Deny 540, 550, 970
AC1	NPA	1917	-	1917	Deny 540, 550, 970
AC1	NXX	976	-	976	Remove this entry
AC2	NPA	1212	-	1212	Deny 540, 550, 970, 976
AC2	NPA	1242	-	1242	Deny 976
AC2	NPA	1246	-	1246	Deny 976
AC2	NPA	1250	-	1250	Deny 976
AC2	NPA	1264	-	1264	Deny 976
AC2	NPA	1268	-	1268	Deny 976
AC2	NPA	1284	-	1284	Deny 976
AC2	NPA	1340	-	1340	Deny 976
AC2	NPA	1345	-	1345	Deny 976
AC2	NPA	1347	-	1347	Deny 976
AC2	NPA	1441	-	1441	Deny 976
AC2	NPA	1450	-	1450	Deny 976
AC2	NPA	1456	-	1456	Deny 976
AC2	NPA	1473	-	1473	Deny 976
AC2	NPA	1516	-	1516	Deny 540, 550, 970, 976

Access Code	Table	Entry	Using DMI	Becomes	Recommendation
AC2	NPA	1600	-	1600	Deny 976
AC2	NPA	1631	-	1631	Deny 976
AC2	NPA	1646	-	1646	Deny 976
AC2	NPA	1649	-	1649	Deny 976
AC2	NPA	1664	-	1664	Deny 976
AC2	NPA	1670	-	1670	Deny 976
AC2	NPA	1671	-	1671	Deny 976
AC2	NPA	1718	-	1718	Deny 540, 550, 970, 976
AC2	NPA	1758	-	1758	Deny 976
AC2	NPA	1765	-	1765	Deny 976
AC2	NPA	1767	-	1767	Deny 976
AC2	NPA	1784	-	1784	Deny 976
AC2	NPA	1787	-	1787	Deny 976
AC2	NPA	1843	-	1843	Deny 976
AC2	NPA	1845	-	1845	Deny 976
AC2	NPA	1867	-	1867	Deny 976
AC2	NPA	1868	-	1868	Deny 976
AC2	NPA	1869	-	1869	Deny 976
AC2	NPA	1876	-	1876	Deny 976
AC2	NPA	1887	-	1887	Deny 976
AC2	NPA	1914	-	1914	Deny 540, 550, 970, 976
AC2	NPA	1917	-	1917	Deny 540, 550, 970, 976

You may wish to deny 1-800-CALL-ATT from your 1800 entry.

You may wish to deny 1-800-COLLECT from your 1800 entry.

The following SPN or LOC entries have a Flexible Length of 0: SPN 00, SPN 01, SPN 011, SPN 02, SPN 03, SPN 04, SPN 05, SPN 06, SPN 07, SPN 08. The Flexible Length of these entries should be increased to the expected length of numbers dialed with the SPN/LOC.

It is recommended to increase the Flexible Length of your SPN 011 entry to 10 digits or more.

It is recommended to increase the Flexible Length of your SPN 01 entry to 10 digits or more.

11.9. Trunk Group Access Restrictions in BARS/NARS

Description

The BARS/NARS design can be configured to either use or ignore Trunk Group Access Restrictions (TGARs) when deciding whether a call is allowed to be placed. If the TGAR is ignored, the BARS/NARS software assesses the Class of Service and the FRL to determine which facilities are eligible to the place the call.

Security Concerns

When BARS/NARS is configured to use Trunk Group Access Restrictions, direct access is no longer blocked due to an incomplete TGAR/TARG matrix. It is therefore recommended to program the BARS/NARS software to ignore the TGAR when determining call eligibility.

Analysis

The BARS/NARS software does not examine Trunk Group Access Restrictions when determining which facilities are eligible for a particular call. This is the recommended configuration.

11.10. Network Class of Service

Description

Network Class of Service (NCOS) is an integral part of the BARS and NARS features at a Communication Server Node, and of the Network Signaling feature at a Communication Server ESN Main. NCOS provides the means to control which trunk routes are eligible for call completion, whether queuing is offered to the call originator, whether the call originator receives a warning tone when an expensive trunk is selected, and whether the user is allowed to access the Network Speed Call feature.

Security Concerns

Each NCOS is assigned one of 8 Facility Restriction Levels that determines which Route List entries are available for stations with that NCOS. Therefore, NCOS assignments should be used to control access to expensive or limited resources.

Analysis

Your Network Class of Service assignments do not meet traditional recommendations. The following is recommended: For NCOS 0 through 7, the FRL should match the NCOS number. For NCOS 8 and greater, the FRL may vary, but the feature permission (queuing, etc.) should be different than NCOS 0 through 7. This assigns exactly one NCOS for each of the available Facility Restriction Levels.

The following NCOS assignments outside of the recommended range assign a non-zero FRL. Verify these are valid assignments and are not being used inappropriately.

NCOS	FRL Assigned
69	4

None of your Network Class of Service groups have access to Network Speed Call, because you do not have any Network Speed Call Lists defined.

The following Network Classes of Service are defined but never used: 69.

11.11. Network Attendant Service

Description

Network Attendant Service allows Attendant services to be distributed throughout a network. Any node in the network may have its attendant services located at any other node in the network, part-time or full-time. When attendant service is needed, and is not available at the local node, the call is forwarded to a remote node where an attendant is available.

Security Concerns

For increased security, it is recommended the Network Attendant Service feature is monitored closely using traffic studies and CDR to keep records on long distance charges and activity that may result with the feature use.

Analysis

You have Network Attendant Service Routing disabled, as recommended.

<u>You have Network Attendant Service Attendant Control enabled.</u> You should disable this feature if it is not being used.

11.12. Coordinated Dialing Plan

Description

Coordinated Dialing Plan (CDP) allows a customer to share a three to seven digit dialing plan with multiple Communication Server locations. A station at one Communication Server can call a station at another Communication Server within the CDP group by dialing a unique 3 to 7 digit number without any access codes.

Security Concerns

Local Steering Codes should not employ any Digit Manipulation Table which inserts BARS/NARS access codes or trunk route access codes at the remote locations. Distant Steering Codes and Trunk Steering Codes should not reference Route Lists that use such Digit Manipulation Tables, empty Routes, empty FCAS tables, or empty Time of Day schedules. An incorrectly configured Distant or Trunk Steering Code could use routes that are public facilities (COT, WAT, FX, etc.) instead of the intended private network facilities (TIE routes, ISA routes, etc.). This could allow calls that are intended for on-net locations to be routed to the public network.

Analysis

You do not have any Local Steering Codes defined.

You do not have any Distant Steering Codes or Trunk Steering Codes defined.

12. International Calling and Direct Trunk Access

To help control the potential for internal abuse, it is necessary to have a clear picture of which resources (users, trunks, DISA DNs, etc.) have various capabilities. While this document is not intended to be a management tool, identifying resources with extremely powerful or potentially expensive capabilities could be seen as part of your security program. This chapter incorporates information from several of the features discussed elsewhere in the document to give you a clear understanding of which users, trunks, etc. have two potentially expensive and often abused features - the ability to call internationally, and the ability to bypass the BARS/NARS configuration and access routes directly.

12.1. International Calling

Description

If programmed correctly, the BARS/NARS system can handle directly dialed international numbers (those beginning with 011) just like any other long-distance number. A user's or trunk's Network Class of Service indirectly determines whether international dialing is allowed through BARS/NARS.

Security Concerns

The high expense of international calls is the primary reason to restrict this capability to only those users that require it. If your organization does not have a need to regularly call internationally, you should consider requiring an authorization code to gain the ability. As this topic only addresses BARS/NARS dialing, you should also reference the Direct Trunk Access topic below to investigate the ability to dial internationally without using BARS/NARS.

Analysis

The lowest FRL required to access the route lists associated with your international network translation entry, 011, is zero. This allows all of your Stations, Trunks, System Speed Call Lists, DISA DNs, Authorization Code Classes, and SAR Periods to make general international calls.

12.2. Direct Trunk Access

Description

Users can be given the ability to bypass the BARS/NARS least-cost routing feature and dial route access codes directly. This disables all of the security features built into the BARS design, such as Supplemental Digit Restriction and Recognition and Flexible Length. Once a route is accessed directly, the Class of Service associated with the station, trunk, DISA DN, etc. will still be utilized to determine whether a particular call is allowed.

Security Concerns

When combined with a Unrestricted Class of Service, directly accessing a trunk route gives users the full capabilities of the public network. This includes the ability to place any toll call including international numbers. Without an Unrestricted Class of Service, facilities are still limited to non-toll calls (those not beginning with 0 or 1).

Analysis

The following Communication Server resources have direct access to one or more outgoing Routes by dialing the Route's access code, and can place toll calls (1+ or 0+ dialing) because of their Unrestricted Class of Service. It is recommended to limit direct route access to only those facilities whose needs cannot be handled by a properly designated BARS/NARS system.

Stations

DN	Name	TN	TGAR	Has Direct Access to Outgoing Routes
7262	Barbara Grant	011 0 00 10	1	0, 1, 2, 4, 6
7265	Bernard Burns	009 0 00 14	1	0, 1, 2, 4, 6
7654	Donald Harris	014 0 00 04	1	0, 1, 2, 4, 6
7771	DES: 6149	006 0 00 04	1	0, 1, 2, 4, 6
7790	Gladys Carlson	006 0 00 15	1	0, 1, 2, 4, 6
7798	Glenn Mcdonald	006 0 00 11	1	0, 1, 2, 4, 6
7919	Janet Sims	019 0 00 11	1	0, 1, 2, 4, 6
7933	Jesus Porter	009 0 00 13	1	0, 1, 2, 4, 6

Other Resources

Description of Resource	TGAR	Has Direct Access to Outgoing Routes
Trunk 003 01 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 02 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 03 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 04 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 05 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 06 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 07 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 08 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 09 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 10 (TIE)	0	0, 1, 2, 3, 4, 6

Description of Resource	TGAR	Has Direct Access to Outgoing Routes
Trunk 003 11 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 12 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 13 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 14 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 15 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 16 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 17 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 18 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 19 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 20 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 21 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 22 (TIE)	0	0, 1, 2, 3, 4, 6
Trunk 003 23 (TIE)	0	0, 1, 2, 3, 4, 6

13. Multi-Tenant Service

This section addresses topics involved with configuring Multi-Tenant service, which allows a Communication Server Customer to further divide their resources among a number of 'tenants.' Many of the decisions that need to be made regarding Multi-Tenant service are more business-oriented than security-oriented. The capabilities of each tenant should be reviewed, and changes made as appropriate.

13.1. Multi-Tenants

Description

Multi-Tenant services (TENS) offers you the flexibility of dividing the services and resources of the Communication Server into smaller subgroups called tenants. While all tenants share the same numbering plan and certain features of the Communication Server, access to other tenants, attendant consoles and trunk routes can be configured so that tenants can selectively share, or have exclusive use of facilities.

Security Concerns

Tenants can share or have private access to various Communication Server resources. Therefore, verify that all Tenants defined can be accounted for, and any unused tenants are removed from the Communication Server programming.

Analysis

You do not have any tenants defined, <u>although you do have the Multi-Tenant software installed.</u>

Meridian Mail

1. System Configuration

Our analysis of the Meridian Mail begins with two topics that define the overall security of the system - which release of Meridian Mail you are using, and access to the administrative terminal. Throughout the various releases of Meridian Mail, many features have been added that specifically address security. As a general rule, the more recent your release, the more tools are at your disposal to control and track Meridian Mail access. However, with every release of Meridian Mail, the front door to the entire system is your administrative terminal, where all changes to the database are made. Having a current release of Meridian Mail with a protected terminal is the first step in designing an effective security strategy.

1.1. Meridian Mail Release

Description

Your Meridian Mail Release is the version of Meridian Mail that you currently have installed. The current version is Release 13.

Security Concerns

Meridian Mail features vary from one release to another. The more current releases provide more security options, and allow greater control over access restrictions. In addition, some older releases are no longer supported by the manufacturer.

Analysis

You are currently running Meridian Mail Release 13.12.1.

This is not the latest Release of Meridian Mail. You may want to upgrade to the latest Release for additional features and security options.

As of October 2009, all Meridian Mail platforms have been classified as End of Services Support by Avaya. Replacement hardware and/or technical support will not be provided by the manufacturer.

1.2. Administration Terminal

Description

Meridian Mail requires an administration terminal where changes to the Meridian Mail database are entered by technicians. In addition, up to three additional terminals can be configured with the Multiple Administration Terminal option.

Security Concerns

Like the Communication Server, Meridian Mail requires a password be entered before the software can be accessed. This password, which by default is 'ADMINPWD,' should be treated like the Level 1 and 2 passwords of the Communication Server. It should be difficult to guess, and only distributed to personnel who need to make changes in the Meridian Mail. In addition, if Multiple Administration Terminals, or MATs, are installed, their passwords should all be unique.

An equally important security concern relating to the administration terminal is physical access to the terminal itself. Terminals should be located in a secure environment with access restricted to only those employees or technicians that require it.

Analysis

Your main administrative terminal's password is:

This password is unacceptable for the following reasons:

- shorter than 8 characters
- does not contain both alpha and numeric characters

You have defined the minimum length for administrative passwords to be 5 characters. It is recommended the minimum length of administrative passwords be 8 characters.

You do not have the Multiple Administrative Terminal feature installed.

2. Mailbox Passwords

User mailboxes are typically the first things that come to mind when thinking about a voice mail system. The ability to listen to messages, forward them, and delete them constitutes a significant capability that must be protected from un- authorized access. This is accomplished by defining a password for every user mailbox. The complexity of these passwords is a vital part of the messaging security program, and the Meridian Mail has several features that help prevent passwords from being compromised. This section discusses those features.

2.1. Password Settings

Description

Each Mailbox in the Meridian Mail system is protected by a password that the user enters to listen to new messages, change greetings, etc. This password can also be changed by the user once they are logged in to their mailbox. The administrator can define guidelines that determine how often these passwords need to be changed, and what they can be changed to.

Security Concerns

For increased security, users should be forced to change their passwords at least every 60 days, and not accept as the new password any of the previous 5 passwords used. The minimum length of mailbox passwords should be at least 6 characters.

Analysis

The minimum length of mailbox passwords is set to 4. It is recommended you increase this to 6 characters or more for better security.

You do not have the Forced Password change feature enabled. It is recommended that users are required to change passwords at least every 60 days, giving them a warning message 10 days before their password expires. Users should be required to change their password 5 times before a password can be repeated.

You are requiring a password change during the first log-in for new mailboxes, as recommended.

Passwords are suppressed on station displays during Log-In. This is the recommended configuration.

2.2. Invalid Log-In Attempts

Description

The administrator can define an invalid log-in threshold which disables mailboxes when too many incorrect passwords are entered. In addition, a log-in 'session' can be terminated when a defined threshold of invalid passwords is entered. The number of invalid attempts per session is independent of the invalid attempts per mailbox.

Security Concerns

To prevent unauthorized personnel from guessing mailbox passwords, you should limit the number of invalid passwords that can be entered before the mailbox is disabled to 3 or less, and the number of invalid passwords that can be entered before the session is terminated to 3 or less. These settings make the task of cracking passwords difficult and time consuming for a hacker.

Analysis

Mailboxes are disabled after an incorrect password is entered 9 times. <u>It is recommended you decrease this threshold to 3 or less.</u>

Log-In sessions are terminated after an incorrect password is entered 3 times. This meets or exceeds recommendations.

2.3. Old Passwords

Description

Meridian Mail keeps track of the last date each mailbox's password was changed.

Security Concerns

Even when change is not forced by Meridian Mail settings, users should still change their passwords at least every 60 days. This reduces the risk that any passwords have been compromised.

Analysis

There are 20 users that haven't changed their passwords in the past 60 days. These users are listed below. You should encourage all users to change their passwords, or use the Forced Password Change feature.

Mailbox Number	First Name	Last Name	Days since Changed
2911	AARON	BENNETT	4417
2912	Adam	Gray	4630
2913	Alan	Butler	4622
2929	Albert	Rogers	6154
2933	Alexander	Reyes	4598
2934	Alfred	Webb	5249
2935	Alice	Fields	4447
2936	Allen	Ellis	4493
2938	Amanda	Weaver	4297
2993	Amber	Rodriquez	4493
2994	Amy	Lane	4297
3932	Andrea	Jacobs	5270
7117	Andrew	Green	4669
7118	Angela	Hart	4858
7120	Anita	Lucas	4258
7123	Ann	Kelley	4497
7128	Anna	Andrews	5228
7160	Anne	Lynch	5228
7161	Annie	Moreno	5229
7163	Anthony	Rodriguez	5229

3. Mailboxes to Investigate

There are several aspects of a mailbox configuration that may suggest it is being used inappropriately, or should no longer exist. Looking for signs of unauthorized use should be a continuous process to help fend-off wide spread abuse. In addition, keeping the mailbox database clean of unused or unknown mailboxes gives hackers fewer places to hide without their actions being detected. A well-managed mailbox database can save technician time, system resources, and expense from unauthorized persons.

3.1. Disabled Mailboxes

Description

Mailboxes are disabled manually by a technician, or automatically by the Meridian Mail when the defined invalid log-in attempt threshold is reached. When a mailbox is disabled, the Meridian Mail will still receive and store messages for the mailbox, but the user cannot log-in to retrieve the messages.

Security Concerns

The existence of disabled mailboxes can be a sign that an unauthorized individual is trying to gain access to the mail system. Mailboxes which were manually disabled should be removed from the Meridian Mail if they are no longer being used.

Analysis

There are 2 disabled mailboxes in your Meridian Mail. For each mailbox listed, you should determine whether the mailbox is in use and should be re-enabled, or is no longer in use and should be deleted. If there are many disabled mailboxes, it could indicate attempted access by an unauthorized individual.

Mailbox Number	First Name	Last Name
3932	Andrea	Jacobs
7128	Anna	Andrews

3.2. Unused Mailboxes

Description

The Meridian Mail keeps track of the last date each mailbox was logged into.

Security Concerns

Mailboxes that haven't been accessed in 30 days may be inactive. You should remove them from the Meridian Mail if they are not being used.

Analysis

There are 20 mailboxes that haven't been accessed for 30 days or more. For each mailbox listed, you should determine whether the mailbox is still in use, or is no longer is use and should be deleted.

Mailbox Number	First Name	Last Name	Days since last access
2911	AARON	BENNETT	4417
2912	Adam	Gray	Never Accessed
2913	Alan	Butler	4248
2929	Albert	Rogers	4249
2933	Alexander	Reyes	4255
2934	Alfred	Webb	4248
2935	Alice	Fields	4252
2936	Allen	Ellis	4249
2938	Amanda	Weaver	4248
2993	Amber	Rodriquez	4252
2994	Amy	Lane	4248
3932	Andrea	Jacobs	4248
7117	Andrew	Green	4256
7118	Angela	Hart	4249
7120	Anita	Lucas	4258
7123	Ann	Kelley	4293
7128	Anna	Andrews	4248
7160	Anne	Lynch	4248
7161	Annie	Moreno	4251
7163	Anthony	Rodriguez	4249

3.3. Invalid Login Attempts

Description

The Meridian Mail keeps track of how many invalid log-in attempts have been made for each mailbox since the last mailbox password change.

Security Concerns

Mailboxes with many invalid log-in attempts may indicate an unauthorized individual has been trying to gain access to them. It could also indicate the password has been changed by someone other than the user, and the user is unable to log-in with their old password. Passwords for these mailboxes should be lengthened and changed every 60 days.

Analysis

There are 2 mailboxes that have had 9 or more invalid log-in attempts. Users of these mailboxes should be contacted to see if they are generating the invalid attempts, or if the attempts are from an outside party. Either way, the password should be changed and the mailboxes should be monitored for suspicious activity.

Mailbox Number	First Name	Last Name	# of Invalid Log-in Attempts
3932	Andrea	Jacobs	14
7128	Anna	Andrews	12

3.4. External Revert DNs

Description

Mailbox users can specify a custom revert DN. Callers are transferred to this number when '0' is dialed during or after leaving a message.

Security Concerns

Without the proper Restriction/Permission lists in place, custom Revert DNs can be defined as access codes or external numbers. This may allow unauthorized calls to be routed back through the Communication Server from the Meridian Mail.

Analysis

<u>There are 2 mailboxes whose Custom Revert DN appears to be external to the Communication Server.</u> If not required, these DNs should be changed, and you should prevent future external revert DNs by selecting a Restriction/Permission list that restricts external numbers.

Mailbox Number	First Name	Last Name	Revert DN
2935	Alice	Fields	912015551234
2993	Amber	Rodriquez	912015551234

4. Restriction/Permission Lists

One of the most expensive security risks involving the Meridian Mail is the ability for callers, users, and the Meridian Mail itself to dial additional digits to access other resources, both in the Meridian Mail and in the Communication Server. Features such as User Extension Dialing, Custom Revert DNs, and Remote Notification all involve the ability to dial extra digits to perform requested actions. The Restriction/Permission Lists are a powerful system for controlling all of these dialing sequences.

4.1. List Definitions

Description

Restriction/Permission Lists allow you to define dialing sequences that are either denied or permitted when using various features of the Meridian Mail. In later releases of Meridian Mail, up to 80 named tables, each with up to 30 twenty-digit entries, may be entered. *If a particular dialing sequence is not listed as either permitted or restricted in a Restriction/Permission table, it is permitted.* Typically, these tables are given names that indicate the type of access they provide, such as "On Switch", "Local", etc. Other features in Meridian Mail may use custom Restriction/Permission Lists, which are analyzed in the topics discussing those features.

Security Concerns

You should carefully monitor Restriction/Permission Lists that allow external calls through BARS/NARS or Trunk Route Access Codes, or access to Communication Server features through SPRE or Flexible Feature codes.

Analysis

You have 80 Permission/Restriction Lists defined in the Meridian Mail. Below are the definitions of each non-default Restriction/Permission List in the Meridian Mail, with a table of dialing sequences that are permitted in each list that may have security implications. *Lists which have not changed from their default settings restrict all dialing sequences, and their entries are not displayed. They are listed together under the heading 'Fully Restricted Lists' after the non-default RPLs.*

List Number: 1

List Name: On switch

Restriction Entries

0	1	2	3	4
5	6	7	8	9

Permission Entries: None

All security-related dialing sequences are fully restricted in this Restriction/Permission List.

List Number: 2

List Name: Local

Restriction Entries

0	1	2	3	4
5	6	7	8	9

Permission Entries: None

All security-related dialing sequences are fully restricted in this Restriction/Permission List.

List Number: 3

List Name: Long distance 1

Restriction Entries

0	1	2	3	4
5	6	7	8	9

Permission Entries: None

All security-related dialing sequences are fully restricted in this Restriction/Permission List.

List Number: 4

List Name: Long distance 2

Restriction Entries

0	1	2	3	4
5	6	7	8	9

Permission Entries: None

All security-related dialing sequences are fully restricted in this Restriction/Permission List.

Fully Restricted Lists

Restriction/Permission Lists 5-80 have not been changed from their default values. The default values totally restrict any Thru-Dialing sequences.

5. Classes of Service

To help organize the many parameters that define mailbox access to the various features of Meridian Mail, Class of Service was developed. This allows you to form groups of privileges for the various users in your organization, and make sure all of their mailboxes are configured consistently. In addition, a Personal Class of Service can be assigned to mailboxes with individual needs. This section addresses the Classes of Service that are defined, and highlights the special needs of mailboxes with a Personal Class of Service.

5.1. Definitions

Description

For each mailbox in Meridian Mail, a group of settings referred to as a Class of Service is assigned. Each Class of Service is given a name, and defines such parameters as maximum available voice storage, administrator capability, automatic logon capability, and which Restriction/Permission Lists are used for various features. You should define a Class of Service for each business-defined user level in your organization and assign appropriate parameters to the class.

Security Concerns

When defining a Class of Service, there are several parameters that have security implications. Enabling administration capability allows users to record system greetings, and personal verifications for other users. Enabling Automatic Logon allows users to log on to Meridian Mail without entering a mailbox number or password. Assigning an appropriate Voice Storage Limit prevents users from over-consuming limited system resources. Lastly, Restriction/Permission Lists are used to restrict features like External Call Sender, Extension Dialing, Custom Revert DN, and Outcalling. Verify that appropriate parameters are assigned for each Class of Service. Reference the Restriction/Permission section to determine the potential security risks in each of the Restriction/Permission Lists used.

To help determine which Restriction/Permission list is appropriate, below is a brief description of the features impacted by Class of Service settings:

Call Sender: Allows a user to immediately call back someone who has left a message by pressing 9 after listening to the message.
Extension Dialing: Allows users to transfer to another extension number or valid telephone number once they log in to Meridian Mail.
Revert DN: Once Meridian Mail answers, callers may dial zero (0) anytime during the personal greeting or during the record cycle, and transfer to a predefined extension. This extension is the Revert DN.
Remote Notification: Remote Notification allows a user to be notified at a remote telephone or pager when a new message arrives in his or her mailbox. Users can define their own remote notification schedules and target DNs from their telephone sets.
Delivery to Non-User: Allows a Meridian Mail user to compose and send a voice message to someone who is not a Meridian Mail user.
AMIS Networking: Allows users to send voice messages to other voice mail systems in a networked environment.

Analysis

You have 8 Classes of Service defined in your Meridian Mail. Below are two tables describing the most security-relevant settings for each Class of Service.

The first table presents information about Administration capability, Voice Storage Limits, and Automatic Logon. It is recommended to restrict Administration capability to only a separate 'Admin' class of service, to limit Voice Storage to less than 20 minutes, and to disable Automatic Logon.

Name	Administration Capability	Voice Storage Limit	Automatic Logon
EXECUTIVE		60	
MANAGER		10	
STAFF		10	
HUMAN RESOURCES		10	
30 min storage 5 min msg		30	

Name	Administration Capability	Voice Storage Limit	Automatic Logon
MED SVC OUTSIDE		3	✓
NOMSG		1	
REMOTE		60	

The second table presents which Restriction/Permission List is used for various features in each Class of Service. Restriction/Permission Lists which were found to permit some security-related dialing sequences are noted in red. Verify the appropriateness of each setting.

Name	Restriction/Permission List Used					
	Call Sender	Extension Dialing	Revert DN	Remote Notification	Delivery to Non-User	AMIS
EXECUTIVE	On switch	On switch	On switch	N/A	N/A	N/A
MANAGER	On switch	On switch	On switch	N/A	N/A	N/A
STAFF	On switch	On switch	On switch	N/A	N/A	N/A
HUMAN RE-SOURCES	On switch	On switch	On switch	N/A	On switch	N/A
30 min storage 5 min msg	Local	Local	Local	Local	N/A	N/A
MED SVC OUT-SIDE	On switch	On switch	On switch	N/A	N/A	N/A
NOMSG	Local	Local	Local	N/A	N/A	N/A
REMOTE	Local	Local	Local	Local	N/A	N/A

5.2. Personal Class of Service

Description

Any mailbox can be assigned a Personal Class of Service instead of one of the defined Classes of Service as discussed in the previous topic. When a mailbox is assigned a Personal Class of Service, you specify the same parameters as a Defined Class of Service, but these parameters only pertain to that one mailbox. You typically use a Personal Class of Service for mailboxes with special needs that are not required for any of your defined Classes of Service.

Security Concerns

A Personal Class of Service assignment can give a mailbox unrestricted thru-dial or revert DN capabilities. Typically, there should be very few mailboxes that require a Personal Class of Service. Any Personal Class of Service assignments should be reviewed, and the details of the assignment should be verified for appropriate use.

Analysis

You have 1 mailbox that is assigned a Personal Class of Service. Below is a list of these mailboxes. If there are a large number of them, you should re-examine your defined Classes of Service to see if you can perhaps define a new class or classes that will accommodate the needs of these users. Mailboxes that are assigned Administration Capabilities, Automatic Logon, or that have unrestricted Restriction/Permission lists are noted with a check in the appropriate column.

Mailbox Number	First Name	Last Name	Admin Capability	Voice Storage Limit	Auto Logon	Unrestricted RPL
7117	Andrew	Green		3		

6. Messaging Features

Many of the Messaging Features in the Meridian Mail, such as Operator Revert, Remote Notification, and Delivery to Non-User, are controlled in the definitions of the Classes of Service. However, there are a few features that are defined elsewhere in the Meridian Mail. These include Secure Messaging, which prevents external access to mailbox log-ins, and Call Answering/Expressing Messaging Thru-Dial.

6.1. Secured Messaging

Description

This is a system wide feature that prevents users from being able to log on to their mailbox from off-site phones. It can only be installed by contacting your sales representative, and once enabled, it cannot be disabled.

Security Concerns

This feature is used in extremely security-conscious environments, and provides significant protection from unauthorized access to mailboxes. However, it is not appropriate for many organizations in which users need to remotely check their messages.

Analysis

You do not have Secured Messaging enabled, allowing users to remotely log on to their mailboxes.

6.2. Call Answering/Express Messaging Thru-dial

Description

This feature allows callers to transfer themselves to another number during call answering and express messaging sessions. They activate this feature by dialing 0 followed immediately by a phone number.

Security Concerns

This feature could allow callers to place unauthorized external calls through the Communication Server that would be billed back to the system. You must apply an appropriate Restriction/Permission list to this feature to prevent unauthorized use by callers.

Analysis

The Restriction/Permission list enabled for Call Answering/Express Messaging Thru-dial is "*On switch*".

It is recommended that the assigned RPL allow only internal extensions to be dialed. The RPL used does not permit any security-related dialing sequences, as recommended.

7. Voice Services

In addition to the messaging capabilities, Meridian Mail has extensive voice services that allow administrators to design sophisticated automated attendant systems. However, there are several features of these voice services which, if not configured correctly, could leave the Meridian Mail open to abuse. One of these is the 'Call' feature of voice menus, which places a call through the Communication Server when a caller selects a particular key. Also of concern are the Thru-Dialer definitions. Thru-Dialer definitions are associated with a specific Restriction/Permission list. The list assigned should restrict callers to only those necessary on-site extensions.

7.1. Voice Menus

Description

Voice Menus allow you to create a sophisticated automated attendant system, presenting callers with a list of menu choices they can select with a touch-tone phone. The result of each selection could be any of several actions, including connecting the call to a specified internal or external number, allowing the caller to record a message, or to play an announcement.

Security Concerns

One security concern associated with Voice Menus is the Revert DN associated with the voice menu. Users are routed to the Revert DN when they dial '0' while listening to the voice menu. The Revert DN can route callers to any valid number including BARS/NARS access codes and Route Access Codes. Revert DNs which appear to route calls outside the switch should be checked to verify they are authorized numbers. Another area of concern is the update and access passwords designed to protect the Voice Menu from unauthorized access. If assigned, these passwords should be complex and not easily guessed. Finally, one of the features of Voice Menus is their ability to call other numbers based on user responses. The 'Call' command (CL) is programmed with a specific number that is automatically dialed when the caller selects that menu option. Improperly programmed Call Commands could allow unauthorized calls from the Communication Server resulting in toll charges, or could permit unauthorized access to toll facilities.

Analysis

The following Voice Menus have one or more of the following conditions and should be checked:

- A Revert DN that appears to be external
- An update password that is unacceptable
- An access password that is unacceptable

Please review the following list to verify the Revert DNs, and check their appropriateness. Change any passwords that are highlighted in red to make them more complex.

Menu ID	Title	Revert DN	Update Password	Access Password
0	DAY GREETING		0000	
0100	Extended Warranty		0000	
0303	Warranty		0000	
0322	Pre-sales Service		0000	
0325	New Orders		0000	
0326	Comments		0000	
0340	Customer Service		0000	
0350	Appointments		0000	
0354	Cancellations		0000	
0360	Holiday		0000	
0361	Claims		0000	
0362	Meeting		0000	
0364	Current Balance		0000	
0365	No one available		0000	

Menu ID	Title	Revert DN	Update Password	Access Password
0366	Emergency		0000	
0370	Payments		123456	
0371	Credit Card		0000	
0372	Directions		0000	

The following Voice Menu options employ the Call command to place a call to what appears to be an external DN. Please review the following list to verify the digits dialed, and check their appropriateness. In the following table's 'Key' column, the 'Initial No Response' action is indicated by 'INR', and the Delayed Response action is indicated by 'DR'.

Menu ID	Title	Key	Number Dialed	Comments
0370	Payments	1	6750	
0370	Payments	2	6751	
0370	Payments	INR	6751	
0370	Payments	DR	6751	
0372	Directions	1	6752	
0372	Directions	2	6753	
0372	Directions	INR	6753	
0372	Directions	DR	6753	

7.2. Thru-Dialers

Description

Thru-Dialers are used primarily for Dial by Name and Dial by Extension applications. If they are configured incorrectly, or use an RPL that permits access to toll facilities, hackers can tandem through the Communication Server and into the Public Switched Telephone Network.

Security Concerns

Each Voice Menu Thru-Dialer is associated with a Restriction/Permission list that defines which digits can be entered during the Thru-Dialer's use. Using the proper Restriction/Permission list for your Thru-Dialers is vital to preventing unauthorized access. Thru-Dialers can also be associated with a Custom Restriction/Permission list. These custom Restriction/Permission lists should block the same codes that the defined lists do (BARS/NARS access codes, Trunk Route access codes, SPRE codes, and Flexible Feature codes).

Analysis

Following is a table of the Thru-Dialers you have defined, and the Restriction/Permission list they use. If the Restriction/Permission List used was previously found to allow some security-related dialing sequences, it is noted in red. If a Thru-Dialer is using a Custom Restriction/Permission list, it is noted as 'Custom,' and an analysis of the list is provided after the table.

Thru-Dial ID	Title	Restriction/Permission List
120	2XXX	Custom
130	Dial By Extension	Custom
131	Transfer to Support	Custom
134	Marketing	Custom
140	4XXX	Custom
170	MARY P.	Custom
180	Dial By name	Custom

Below is an analysis of each Custom Restriction/Permission list defined for your Thru-Dialers:

Thru-Dial ID: 120

Thru-Dial Title: 2XXX

Restriction Entries

0	1	3	4	5
6	7	8	9	

Permission Entries: None

Codes that are not fully restricted in this Custom Restriction/Permission List:

Type	Code	Unrestricted	Partially Restricted
Route Access Code	2290	✓	
Route Access Code	2991	✓	
Route Access Code	2992	✓	

Type	Code	Unrestricted	Partially Restricted
Route Access Code	2993	✔	
Route Access Code	2994	✔	
Route Access Code	2996	✔	

Thru-Dial ID: 130

Thru-Dial Title: Dial By Extension

Restriction Entries

0	4	5	6	7
8	9	1		

Permission Entries: None

Codes that are not fully restricted in this Custom Restriction/Permission List:

Type	Code	Unrestricted	Partially Restricted
Route Access Code	2290	✔	
Route Access Code	2991	✔	
Route Access Code	2992	✔	
Route Access Code	2993	✔	
Route Access Code	2994	✔	
Route Access Code	2996	✔	

Thru-Dial ID: 131

Thru-Dial Title: Transfer to Support

Restriction Entries

0	1	2	4	5
6	7	8	9	

Permission Entries: None

All security-related dialing sequences are fully restricted in this Custom Restriction/Permission List.

Thru-Dial ID: 134

Thru-Dial Title: Marketing

Restriction Entries

0	1	2	4	5
7	8	9		

Permission Entries: None

Codes that are not fully restricted in this Custom Restriction/Permission List:

Type	Code	Unrestricted	Partially Restricted
BARS/NARS Access Code	6	✔	

Thru-Dial ID: 140

Thru-Dial Title: 4XXX

Restriction Entries

0	1	2	3	5
6	7	8	9	

Permission Entries

4				

All security-related dialing sequences are fully restricted in this Custom Restriction/Permission List.

Thru-Dial ID: 170

Thru-Dial Title: MARY P.

Restriction Entries

0	1	2	3	4
5	6	8	9	

Permission Entries: None

All security-related dialing sequences are fully restricted in this Custom Restriction/Permission List.

Thru-Dial ID: 180

Thru-Dial Title: Dial By name

Restriction Entries

0	1	4	5	6
7	8	9		

Permission Entries: None

Codes that are not fully restricted in this Custom Restriction/Permission List:

Type	Code	Unrestricted	Partially Restricted
Route Access Code	2290	✓	
Route Access Code	2991	✓	
Route Access Code	2992	✓	
Route Access Code	2993	✓	
Route Access Code	2994	✓	
Route Access Code	2996	✓	

8. Fax Services

Your Meridian Mail is not equipped with Fax On Demand capability, whose features are normally analyzed in this chapter. All security concerns relating to the sending and administration of faxed documents are irrelevant in your current configuration. For more information about the Fax On Demand capabilities of Meridian Mail, refer to the manufacturer's literature.

9. Additional Features and Services

The Meridian Mail system has expanded its feature content with each release, and can now support advanced interactions with PC based services and other voice mail systems. Often these new features have security risks that must be addressed to broaden the capabilities of the Meridian Mail without opening the system to abuse. This section addresses the security implications of these additional features.

9.1. Personal Mailbox Administration

Description

This feature allows mailbox users to administer their own mailbox settings via a web interface over the internet. They can modify personal distribution lists, passwords, languages, greetings, and other parameters.

Security Concerns

It is recommended you manage the access to this powerful feature. It is not recommended for all users to have access to the web-based administration. Limiting access reduces the risk of compromise by unauthorized personnel.

Analysis

This Meridian Mail is not equipped with the Personal Mailbox Administration feature.

10. Monitoring Access

An important part of managing the security of Meridian Mail is monitoring suspicious activity. The system has several features that aid in this task. Meridian Mail is able to collect data about usage, known as 'Operational Measurements', that can be viewed and compared to established norms to help detect unusual activity. When unusual activity is suspected, employ the Meridian Mail to help you monitor the situation with the Hacker Monitor feature. This suite of services can be used to notify administrators when particular mailboxes or Thru-Dial services are accessed. With Meridian Mail keeping close track of the usage of your mail system, administration resources are alerted when potential problems arise.

10.1. Operational Measurements

Description

The Meridian Mail system allows you to collect information detailing how and when the system is used, including system traffic, user usage, and outcalling and fax audit trails. This data can then be viewed by administrators to detect unauthorized or inappropriate use.

Security Concerns

Since use of these measurements can detect unauthorized access to the system, it is recommended to enable these features, and review the data periodically. Traffic information should be collected during off-business hours, when abuse occurs most often.

Analysis

A separate analysis for each type of measurement is performed below:

Meridian Mail System Traffic

You are currently collecting Traffic Data on the Meridian Mail.

Data is being collected from 1:00 AM to 1:00 AM.

Verify this period covers your off-business hours.

Traffic Data is being stored for 8 days.

This configuration meets or exceeds recommendations.

User Usage/Session Trace Data

You are currently collecting User Usage/Session Trace Data on the Meridian Mail.

User Data is being stored for 31 days.

This configuration meets or exceeds recommendations.

Fax and Outcalling Audit Trails

Audit Trail Collection data is not available.

10.2. Hacker Monitor

Description

The Hacker Monitor feature allows you to monitor mailbox logins and use of Thru-Dial services. You can monitor selected mailboxes for logins during a specified "monitoring period", and either all or selected Thru-Dial services from all sources or specific Calling Line IDs. These features help you check for activity that could indicate the presence of a hacker.

Security Concerns

The features of Hacker Monitor should be employed to alert the system administrator of potential unauthorized activity. How these features should be used is a business decision that will depend upon your corporation's methods and areas of operation.

Analysis

Your Monitoring Period is currently defined as
Start Time: 11:00 PM
End Time: 5:00 AM

You should verify this period covers your off-business hours, and should be defined to cover holiday periods as well.

There are no mailboxes being monitored during the monitoring period.

None of your Thru-Dialers are being monitored during the monitoring period.

You are not monitoring any Calling Line IDs for mailbox log-in or Thru-Dial access.

11. Virtual ACD Agents for Meridian Mail

Security of the Communication Server and Meridian Mail would not be complete without addressing the interface between the two. Of primary concern are the Meridian Mail agents defined in the Communication Server that carry the various voice and messaging services between the Meridian Mail, local Communication Server users and the public network. In addition to the many settings in the Meridian Mail database that help control calling privileges, the traditional Communication Server security features should also be employed for an additional layer of protection. This section analyzes the programming on the Communication Server side that can help avoid abuse of the Meridian Mail system.

11.1. Access Restrictions

Description

Meridian Mail requires several 'virtual ACD agents' to be defined in the Communication Server for communication, acting as an interface between the Communication Server and the Voice Mail system. There are no physical sets associated with these ports. Their role is to provide access to voice mail and voice mail services; these stations have fairly limited needs, and should be configured appropriately.

Security Concerns

The configuration of these virtual stations defines the access that various Meridian Mail features, like External Call Sender, Message Delivery to Non-Users, Remote Notification, and Custom Operator Revert, have to the Communication Server. It is recommended that Voice Mail ports have a Conditionally Toll Denied (CTD) Class of Service, a Trunk Group Access Restriction of 1, and a Network Class of Service of 2 or lower.

Analysis

You have 4 Voice Mail ports defined in your system. The following table describes these stations, and highlights settings which do not meet the recommendations:

DN	Name	TN	COS	TGAR	NCOS	FRL
2901	DES: VMAIL	010 0 00 04	CTD	1	0	0
2902	DES: VMAIL	010 0 00 05	CTD	1	0	0
2903	DES: VMAIL	010 0 00 12	CTD	1	0	0
2904	DES: VMAIL	010 0 00 13	CTD	1	0	0

Viewing your Security Audit on the Web

Introduction

Every InfoPlus Security Audit that is run will be automatically archived and uploaded to our web site for secure online viewing. Access to this information is via a password protected login which provides a list of all InfoPlus reports archived for the account, and the dates they were run. We will store every Security Audit for at least three years, allowing you to compare current information with previous audits. Also, this technology allows any number of your people, across town or across the country, to view the data simultaneously and discuss its implications.

Suggested Software

The Security Audits will be stored in PDF format, also known as Adobe Acrobat® format. You will need the Adobe Reader® application (version 5.0 or later) and any web browser to view the PDF files. Adobe Reader is free to download from Adobe's web site (www.adobe.com).

Instructions

Upon completion of this report, authorized users will receive a notification email with instructions on how to log in to their account. Depending on the level of access you're granted, you will be able to view and download reports for this system only, or use an enhanced interface for analyzing and downloading reports from multiple systems you manage. Once logged in, you will be presented with a list of all available InfoPlus reports for each system, along with the date each report was run. Select the report you wish to view, and it will either be presented directly in your browser window, downloaded to your computer, or displayed within a new Adobe Reader window. Use the navigation bar to flip through the report page by page, or use the bookmarks on the left to access a particular section.

Additional Security Precautions

There are several other areas of concern, in addition to the programming of your Communication Server and Meridian Mail, which must be addressed for a complete security audit. This appendix lists some additional, external sources of potential abuse or theft of telecommunications services which should be investigated.

Disconnect Supervision for External Calls

When calls are routed through your Communication Server to valid external destinations, such as a night call forward DN for ACD, it is recommended to verify the disconnect supervision at the far end. If a call is routed to the external destination, the disconnect supervision at the far end will be either a fast busy signal (120 IPM), or a burst of dial tone. A burst of dial tone can enable the caller to seize the trunk by dialing any digit. To prohibit this form of toll fraud, request the far end disconnect supervision be changed from dial tone to fast busy (120 IPM). This request should be made to the far end local service provider.

Dumpster Diving

Any printed or electronic copy of data from your Communication Server or Meridian Mail must be disposed of properly to prevent unauthorized individuals from using the data to perpetuate toll fraud or abuse. Documents that list passwords, authorization codes, DISA DNs, etc. are of particular importance, but any document exposing the programming of either the Communication Server or Meridian Mail can be a potential security risk. Shredding paper document or physically destroying any electronic media can help prevent this theft of information.

Employee Changes

Even if a snapshot of your telecommunications equipment programming shows no obvious signs of security problems, it is important to understand that this data operates in a dynamic environment and must be kept up to date. When employees leave the organization, it's vital to take a survey of their telecommunications resources and deactivate appropriate facilities. If they were assigned an authorization code, it should be removed from the switch and not reused. The station's control password, if assigned, should be removed or changed. Any voice mailboxes assigned to the user should be disabled or removed. Having a checklist for such situations may be helpful if they occur regularly.

IP Access

Modern Communication Servers have an additional means of communicating with the switch and performing administrative maintenance - through the Internet Protocol over your Local Area Network (LAN), and potentially the internet. If your switch has this ability, it is imperative that your network administrator restrict access to the Communication Server through the use of a hardware firewall. If this interface is not protected, it may allow any individual with internet access to attempt to log-in to the Communication Server. It is recommended to limit IP access to your local network, and only to authorized administrators on that network.

Glossary

Administration Terminal
A device by which one can enter commands into a Communication Server.

Attendant Administration Access Code
An additional password that allows an attendant to modify features assigned to telephones by using the Attendant Console as a system terminal.

Audit Trail
A text file kept by the Communication Server of all Log-In attempts and the Loads that were accessed.

Authorization Codes
Usually used as a billing mechanism, Authorization Codes can also temporarily override a station's access restriction so that a call can be completed while billing information is captured through CDR.

Basic Automatic Route Selection
Once programmed, the capability of the Communication Server to place outgoing calls over specific Trunk Routes through an analysis of the digits dialed.

Call Detail Recording
An ability of the Communication Server to capture and print the details of incoming and/or outgoing call attempts. Typically used for internal cost allocation purposes.

Call Forward All Calls Control
Determines whether the calling party's or the forwarding party's restrictions are used in the completion of a forwarded call.

Call Forwarding External
Allows a user to forward incoming calls to a number external to the switch.

Call Forwarding to a Trunk Access Code
This feature allows or denies the ability to forward calls to a Trunk Access Code.

Class of Service
A broad restriction class within the Communication Server that defines general calling capabilities. Actual calling capabilities of any station are further impacted by several additional parameters.

Code Restriction
A means by which calling to specific Area Codes may be allowed or denied.

Controlled Class of Service
A feature that allows 'Controllers' the ability to modify a station's Class of Service.

Coordinated Dialing Plan
Allows a customer to share a dialing plan among two or more Communication Server locations.

Digit Manipulation
The ability of the Communication Server to insert or delete leading digits of a dialed number.

Direct Inward System Access
Permits callers to directly access the Communication Server from the public network by dialing a special number. Once connected, the caller takes on all of the capabilities of an internal caller.

Failed Log-In Threshold
The number of incorrect passwords that may be entered at the Administration Terminal before the Communication Server disables access for a specified period of time.

FAX on Demand
Allows callers to request pre-defined faxes to be sent to them using a call-back delivery method.

Flexible Feature Codes
User defined codes that activate select station features.

Forced Charge Account
A weaker form of Authorization codes in that the actual code is not authenticated, just the number of digits.

Forwarding
A feature that directs the completion of an incoming call should the dialed number not answer.

Free Call Area Screening

A table in the Communication Server that allows tandem calls to reach only those Area Codes and Exchanges that will not incur toll charges.

History File

A text file kept by the Communication Server of all interactions with all administrative terminals.

Hunting

A feature that directs the completion of an incoming call should the dialed number be busy.

Incoming DID Digit Conversion

A feature that enables the Communication Server to convert incoming DID digits and redirect calls to an internal DN.

Incoming Trunk Group Exclusion

A feature that blocks calls from an incoming trunk group from accessing specific Area Codes, Exchanges or other facilities that would circumvent restrictions at their home location.

Level 1 Password

A valid Level 1 Password allows the modification of all Communication Server items except passwords, Authorization Codes and DISA settings.

Level 2 Password

A valid Level 2 Password allows the modification of all Communication Server items including passwords, Authorization Codes and DISA settings.

Limited Access Passwords

Level 1 passwords that are further restricted in their capabilities in that they may be denied access to specific Loads in the Communication Server.

Load(s)

Programs in the Communication Server designed to perform specific functions.

Lockout Time

The amount of time after which an access port is automatically re-enabled after being disabled due to unsuccessful attempts to gain entry to the system.

Log-In Name

Used in conjunction with Level 1 and Level 2 passwords, a valid Log-In Name and then a valid password can be required to gain access to the system.

Mailbox

An electronic storage repository for voice mail messages.

Multi Customer

A single Communication Server may be divided in software to act as any number of separate systems (up to 100 customers). Hardware is shared but the database is not.

Network Attendant Service

Allows Attendant services to be distributed throughout a network.

Network Automatic Route Selection

Extends the Basic Automatic Route Selection capability to operate over a multi-location corporate network.

Network Class of Service

A station's or trunk's NCOS determines eligible Trunk Routes for call completion.

Network Translation

Tables within the Communication Server that determine which Route List is to be used to route calls to a particular number.

New Flexible Code Restriction

An enhanced means by which calling to specific telephone numbers may be allowed or denied.

Night Service

A Communication Server feature that allows for the re-directing of in-ward calls to a console after normal business hours.

Personal Class of Service

A personal Class of Service has all of the parameters of Meridian Mail's system Classes of Service, but a Personal Class of Service applies to only one mailbox.

Redirection Numbers

Any number, either internal or external, that is referenced by a feature whose purpose is to redirect the termination of a call.

Remote Call Forwarding

Allows users to remotely change the destination of Call Forwarded calls.

Restriction/Permission Lists

Tables that define the dialing digits that are either allowed of denied when using the features of Meridian Mail.

Revert DN

Calls that are presented to a mailbox may be re-directed to another number through use of the revert DN feature.

Route Lists

Frequently, more than one Trunk Route can complete a call to a given telephone number. The Route List specifies the order in which Trunk Routes are to be sought.

Routing Control

A schedule which alters Route List assignments by time of day.

Scheduled Access Restriction

The ability to change the Access Restrictions of a group of stations and/or trunks on a scheduled basis.

Secure Data Password

An additional password that allows access to the database that controls Authorization Codes and the Direct Inward System Access features.

Secure Modem

A special type of modem that requires the entry of a password before allowing a caller to communicate with the Communication Server.

Secured Messaging

A system-wide feature that prevents users from being able to access their mailbox from an off-site telephone.

Security Banner

A textual security warning message displayed during any successful attempt to log into a system.

Set Relocation Security Code

A code required to activate the Set Relocation feature of a Communication Server.

Software Release

A naming convention defined by the manufacturer and used to keep track of software.

Special Prefix Code

A system defined code that is used to activate select station features.

Speed Call Lists

A form of abbreviated dialing whereby a number may be called by the dialing of a code instead of its complete number.

Station Control Password

A special password that is required to invoke or disable specific features on a station, such as Remote Call Forwarding.

Trunk

A communications path that connects a Communication Server to a central office, another Communication Server, or any number of special features such as a recorded announcement.

Trunk Access Restriction Group

A parameter that allows or denies a station or trunk access to a specific Trunk Route - assigned to the completion facility.

Trunk Group Access Restriction

A parameter that allows or denies a station or trunk access to a specific Trunk Route - assigned to the calling facility.

Trunk Route

A group of one or more trunks that have identical capabilities, to be used for identical purposes. A typical Communication Server would have several Trunk Routes.

Trunk Route Access Code

Every Trunk Route must be assigned a Trunk Route Access Code, although this number is usually not dialed by station users. Among other uses, this code is used in the testing of specific Trunk Routes.

TTY/VDT

One of the devices by which one may enter commands into a Communication Server. Literally meaning a teletype device or, more common, a Video Display Tube.

UNR

An unrestricted Class of Service

Voice Menu

A series of voice prompts to which a caller may respond by a dialing a series of numbers, # or *.