InfoPlus

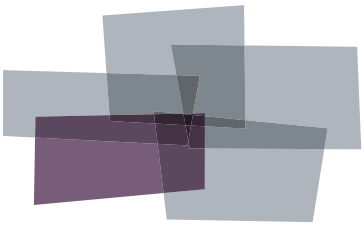
Security Audit

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

Produced For

Avaya Communication Manager Demo

Customer Number: **12345**
Reflecting information from: **1/8/2018**



Inventory
Configuration
Performance
Security
Backup

DISCLAIMER

Bristol Capital, Inc. and its authorized distributors provide assistance to Avaya customers in reducing the risk of loss due to toll fraud and unauthorized Communication Server access. Bristol Capital does not guarantee security nor warrant that any solution or product will stop toll fraud abuse or prevent unauthorized access. Bristol Capital does not assume liability for any losses due to breaches of security in a customer's system subsequent to any audit services provided by Bristol Capital and/or its authorized distributors.

The information contained in this document is based upon data retrieved remotely from a Communication Server. Some of the information presented may be derived, in whole or in part, from this data. Inconsistent and/or incorrect programming of the Communication Server may cause these derivations to be inaccurate. For the sake of consistency in these reports, there may be cases in which a best-effort attempt is made to derive particular information based upon related data. As the reporting facilities of the Communication Server's hardware and software improve, the enhanced data will lead to more accurate InfoPlus reports. Technical errors encountered during the remote transfer of data may cause spurious results in the report. Bristol Capital, Inc. does not guarantee the accuracy of the information presented, although reasonable attempts have been and will continue to be made to ensure InfoPlus reports are as accurate as possible.

This report and the information contained herein is to be used only for the purposes intended. Any disclosure of the information contained herein to parties other than the subscriber of this service, or the organization whose information is represented, is strictly prohibited.

InfoPlus® is a registered trademark of Bristol Capital, Inc. Montvale, NJ
Copyright © 2005-2018 Bristol Capital, Inc. All Rights Reserved.

All InfoPlus reports for the Avaya product line have been:

Communications Management with InfoPlus

Inventory
Configuration
Performance
Security
Backup

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.

Security – The increasing importance of communications security is met through the InfoPlus Communication Server Security Audit. Over 50 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 assembled 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 telecommunications 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 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 an ARS Access code, AAR Access Code or Trunk Group Access Code.

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.

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

Your Communication Server is not currently behind a VPN or a secure modem device. It is recommended you configure VPN access, or install a secure modem to protect your Communication Server.

1.2. NETCON Class Of Restriction (COR)

Description

NETCON data modules are used for administration of the Communication Server. Access to NETCON ports can be configured through the use of COR-to-COR restrictions.

Security Concerns

If NETCON ports are not properly restricted, it may be possible for an unauthorized individual to gain administrative access to your Communication Server by transferring to these ports and bypassing any external security devices (e.g., ASG Guard II/RPSD). To ensure proper restrictions, it is necessary to review the COR-to-COR restrictions of your Voice Mail COR especially. NETCON ports should be in their own unique COR.

Analysis

All NETCON ports are using a single COR, as recommended.

The following Classes of Restriction are in use by your NETCON ports:

COR: 1

This COR is not unique to NETCON ports.

The following CORs are not restricted from calling COR 1: 0-95

The following NETCON ports are assigned to COR 1:

Extension	Name	Port	Location
5000	NETCON PT	02B0100	

1.3. Login Names and Passwords

Description

The data in your Communication Server, from the basic platform configuration to the Telephony data (Translations) is protected through a login and password system. The Login Name that a person uses can be assigned to a Profile, which determines what he or she can view, modify, or create. Even without administrative access to SAT or the Web interface, a Login Name can have access to administer, create, or delete other Login Names.

Security Concerns

Since they are the key to the main gate of the Communication Server, the Login Names and passwords should both be difficult to guess, and protected as sensitive data. Locally defined Login Names should be at least 7 characters long, use 90-day or less password aging, and require ASG Authentication. All passwords should be changed frequently, be at least 7 characters long, and have a combination of letters and numbers at minimum. No Login Name should be granted more privilege than is needed to do their work, which might make the use of a Custom Profile appropriate. Communication Manager Administrators are assigned to the Super Users group, which by default allows them full access to the Communication Server's Web Administration interface. If that is not desired, the Web Access Mask associated with that Login Name should be examined to ensure proper security.

Analysis

Note: Only locally-defined Login Names are analyzed below. This Communication Server appears to be configured to use an external LDAP or Active Directory server. LDAP based servers can define Login Names and their profile assignments that are beyond the control of the local Communication Server. Please review these Login Names to ensure the highest security.

Access Security Gateway (ASG) is enabled in the Customer Options of this Communication Server.

You have 3 locally-defined Login Names in your system. The following list explains the capabilities of each of these Login Names. Unacceptable Login Names are noted as such and should be changed. The use of ASG is also noted for each Login Name. Passwords and Password aging cannot be analyzed, but a policy should be in place to ensure that they are not too simple and they are cycled regularly.

Login Name: harvey354

Profile: None (No SAT Access)

This Login Name is not a Communication Manager administrator.

This Login Name appears to be acceptably complex.

Login Name: maya

Profile: 3 - prof3 (Services, craft equivalent)

This Login Name is not a Communication Manager administrator.

This Login Name is unacceptable for the following reason(s):

- Login Name is less than 7 characters long.
- Login Name does not contain both alpha and numeric characters.

Login Name: tradmin

Profile: 18 - prof18 (Customer Super-User)

This Login Name is a Communication Manager Administrator. Please review this Profile's Web Access Mask to ensure that this is an appropriate level of access.

This Login Name is unacceptable for the following reason(s):

- Login Name does not contain both alpha and numeric characters.

1.4. Login Privileges (Profiles)

Description

The Profile that a Login Name is assigned to is what determines the level of access it has to Telephony data. In order for a Login Name to administer the Communication Server data through the use of SAT or the Web interface, it must be assigned to exactly one Profile. It is important to only allow the level of access needed to each profile. For example, those profiles used solely for administering stations should not have access to trunk administration or maintenance commands. Restrictions may also be put in place so that a technician who is only allowed to administer specific areas of the Communication Server cannot alter programming of other sensitive data (such as Vectors). Profiles 0 through 19 are pre-defined by Avaya for specific purposes, while Profiles 20 through 69 are customizable.

Security Concerns

Login Names should only be granted enough privilege to perform the tasks they are responsible for, and no more. Consequently, the Profile that a Login Name is assigned to is extremely important. Custom Profiles are useful in creating very specific rights according to your business needs, but can also be configured to give nearly as much access as a high-level Profile. The following Profile data should be checked against the Logins section to ensure that everyone has an appropriate level of access.

Analysis

Built-In Profiles

Avaya provides twenty built-in Profiles with predefined access capabilities and roles. The following chart summarizes these built-in Profiles and what they can do. Additionally, where applicable, the Login Name that the Profile is most similar to from earlier releases will be noted. (e.g. craft, inads) For complete details on built-in Profiles, please consult Avaya documentation.

Profile #	Name/Role	Users With Profile	Notes
0	Services Super-User	init	Completely Unrestricted. Equivalent to the "init" Login Name in previous releases.
1	Services Manager	inads	Equivalent to the "inads" Login Name in previous releases.
2	Business Partner	dadmin	This profile requires licensing to activate. It is equivalent to the "dadmin" Login Name in previous releases.
3	Services	craft, maya	Equivalent to the "craft" Login Name in previous releases.
4-15	Reserved		Reserved by Avaya, these profiles should not be used.
16	Call Center Manager		Used by the MIS application to administer CMS/CCR logins. Equivalent to the "mis" Login Name in previous releases.
17	SNMP	acpsnmp	Used by SNMP Monitoring Agents, should not be assigned to users.
18	Customer Super User	tradmin	Used for local Administrators, has default Administrative privilege and full Web Access.

Profile #	Name/Role	Users With Profile	Notes
19	Customer Non-Super User		This profile has no SAT permissions at all, but it does have limited access to the Communication Manager Administative Web site.

Custom Profiles

Custom Profiles are useful for creating sets of permissions which fit your business needs in a specific way. For example, allowing one user to access certain command objects as an administrator while entirely restricting access to other objects. Each Custom Profile that is detected in your Communication Server is listed below, along with each SAT Command category that it has any access to. "All", "Some", or "None" will be displayed for both Administrative and Maintenance permissions depending on whether that Profile has access to the Command objects represented by the category. For a list of all the command objects represented by each category in your Communication Server, please refer to the appendix "Command Objects In Profile Categories".

While Administrative privileges need to be the most carefully restricted as they have access to commands like "add" and "change", there are certain Maintenance commands that can cause disruption to your Communication Server if used improperly. Therefore it is recommended that Custom Profiles be reviewed regularly to ensure the highest level of security. Further, the Profile's Web Access Mask in the Web Maintenance interface should be seperately reviewed as Web permissions are entirely seperate from SAT.

We were not granted permission to access this data. Please review the Login Names defined in your system for proper levels of security.

1.5. Invalid Logins - Lockout & Notification

Description

The Communication Server has the ability to alert you when invalid login attempts are made. The threshold for the number of invalid login attempts (Login Threshold) within a certain time period (Time Interval) can be defined. Furthermore, each Login Name can be administered to be "locked out" upon causing a Security Violation Notification.

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 Security Violation Notification (SVN) feature makes this process unattractive by limiting the "guesses" that can be made in a given time period, as well as alerting on-site personnel to the hacking activity detected. Avaya recommends administering a notification threshold of 5 invalid login attempts in a 3 minute time interval. When using SVN, it is important to make sure the Referral Destination is being monitored regularly by appropriate personnel.

Analysis

Your Communication Server is currently using Invalid Login Security Violation Notification, as recommended.

Invalid Login SVN Originating Extension: 6582
Invalid Login SVN Referral Destination: 6589
Invalid Login SVN Threshold: 5
Invalid Login SVN Time Interval: 3 Minutes

Your threshold for Invalid Login Attempts meets Avaya's maximum recommendation of 5 attempts.

Your lockout Time Interval meets Avaya's minimum recommendation of 3 minutes.

1.6. Logoff Screen Notification

Description

There are two features that Avaya has deemed a security risk if left enabled - Facility Test Call and Remote Access. The logoff screen notification allows each user to be alerted if these features are enabled. Furthermore, an acknowledgment can be required in order to successfully logoff from the Communication Server. Facility Test Call allows stations to access trunks directly, bypassing certain restrictions. Remote Access allows incoming calls to receive "secondary dial-tone" and make outgoing calls. Both of these features are covered more in-depth in later sections of this document.

Security Concerns

Alerting technicians to the administration of Facility Test Call and Remote Access can greatly increase the security and lower the potential for abuse in your Communication Server. This notification can be used as a reminder that the features are to be removed when not in use, and can also alert the technician in the event that the features were enabled by an unauthorized individual.

Analysis

The following table displays the logoff screen notifications for your customer-level Login Names:

Login Name	Facility Test Call Notification	Remote Access Notification
tradmin	Y	Y

1.7. TTI Security Code Analysis

Description

Terminal Translation Initialization (TTI) is mainly used for relocating stations from one port in the Communication Server to another. An administrator or user may use a code to change the programming of a station.

Security Concerns

If your TTI security code is too simple or less than 4 digits, then a hacker may guess it and exploit the TTI feature. It is always recommended to change the TTI security code from the default to prevent this exploit.

Analysis

Terminal Translation Initialization (TTI) is enabled in both the Customer Options and System Features of your Communication Server. The feature is active, for additional security it is recommended that it be disabled if not required.

Your TTI Security code appears to be acceptably complex.

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 and recommend steps you can take to increase the overall security of your Communication Server.

Did You Know?

While this section of the Security Audit will address certain high-level features of your system, an InfoPlus SourceBook may be ordered to gain a more complete understanding of the configuration of your system. The SourceBook answers many of the questions you may have about your system's configuration.

2.1. Software Version

Description

Avaya assigns a software version/release number for all enhancements that have been made since the introduction of the Definity G3 Communication Server platform.

Security Concerns

As with any software, problems and bugs found in older versions are fixed in later releases. In addition, features for improving the security of the Communication Server are often added over time. For these reasons, it is recommended to keep your software version current. Also, older software releases are no longer fully supported by Avaya, which can present problems when requiring assistance.

Analysis

Your current software version is Communication Manager 5.0 (Load 825.4), which was released on 01/08/2008.

The latest version of Communication Manager Software is not installed on this system.

It is recommended that you upgrade your software to Communication Manager 7.0, which was released on 08/24/2015.

**Note that Communication Manager 7.x is equivalent to Release 17 software.

2.2. I/O Devices

Description

Input/Output Devices are required for communication with the Avaya Communication Server. These devices can be either on-site (local) or at a remote location. The standard devices for communication include a TTY/VDT terminal and the INADS modem. Later releases of software also support communication with the Communication Server via Ethernet. A printer may also be connected directly to the Communication Server to keep hard-copies of system error messages, logs, and scheduled commands.

Security Concerns

The proper configuration of your Input/Output devices can help control access to the Communication Server and its programming. Using a printer to record system messages and logs is also recommended as a way to monitor suspicious remote activity.

Analysis

Customer Access to INADS port

Customer Access to the INADs port is enabled in system maintenance.

The INADs port is used for remote administration and maintenance. Extensive security measures can be taken to ensure that this port is only accessed by authorized personnel. (See External Security section 1.1) By disabling access to the INADs port, you significantly decrease the chance of unauthorized access to the Communication Server. However, you will also relinquish the ability to use this port for remote administration and maintenance.

Printer Configuration

Your Communication Server is currently not configured to use a printer. Please configure a printer and ensure that it is working properly in order to effectively monitor your Communication Server.

2.3. Alarm Monitoring Configuration

Description

Avaya Communication Servers have the ability to record and alert you to warnings, errors and alarms, both minor and major, via the Operations Support System (OSS) or Simple Network Management Protocol (SNMP). Alarm origination via OSS sends alarms out over the existing TDM infrastructure, while SNMP uses the IP network. Alarms are sent to alarm-monitoring destinations, or end-points where they should be monitored regularly. For OSS, this could be a telephone, modem, or Voice Mail-related device. For SNMP, alarms (as SNMP 'traps') would be sent to a computer or server for processing.

Security Concerns

It is important to review the alarm monitoring configuration regularly. A Communication Server hacker may disable alarm monitoring to prevent detection of malicious activities. Alarm monitoring features such as Restart Notification and Cleared Alarm Notifications are important because they prevent an attacker from being able to restart your Communication Server or clear alarms generated while hacking the system without being detected. If a Customer-Provided Alarm Device (CPAD) is being used, make sure that the Customer-Provided Equipment (CPE) Alarm Activation Level is appropriate. If it is set to 'none', CPE alarms are only generated on the CPAD when a cabinet or the switch enters the Emergency Transfer state.

Making sure Alarm Origination is active and a functioning alarm end-point is configured facilitates fast responses to potentially service-affecting issues. Without a proper alarm monitoring configuration, you can experience service outages that are longer than necessary. Be sure to test the alarm-monitoring device regularly to ensure that it is functioning properly. The presence of any Major or Minor alarms active at the time of data collection will be indicated. If there are active alarms, make sure that the person responsible is aware of them, and that they are resolved promptly.

Analysis

You have OSS Alarm Origination activated and at least one OSS endpoint number/extension configured. This is a recommended configuration. Please verify that all configured OSS endpoints are functioning properly.

CPE Alarm Activation Level: Minor
OSS Telephone Number: 18001234567
Alarm Origination to OSS Numbers: first-only
Cleared Alarm Notification: Yes
Restart Notification: No

Restart Notification is not activated. Please enable Restart Notification to ensure a higher level of security.

2.4. Night Service Configuration

Description

Night Service allows incoming calls to be redirected to alternate endpoints when activated. Night Service is activated and deactivated by the use of a feature button on a console or station. Consoles, Trunk Groups, Hunt Groups, Tenants, and Listed Directory Numbers (LDN) can all have a Night Service redirection defined.

Security Concerns

A common method of communications abuse is to redirect calls to unauthorized external numbers. For most applications, your Night Service numbers should be internal extensions such as a Voice Mail system or a night bell. External numbers should be examined to ensure that calls are being sent to approved destinations. 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

The following is a list of all Night Service destinations found in your Communication Server. Those that appear to be external are flagged for your review.

Type	Night Service Destination	Location
Tenant 1	8181	N/A
Trunk Group 1	6549	2
Trunk Group 1	6588	2

The following devices have the ability to activate and deactivate Night Service:

Extension	Equipment Type	Name	Night Service Type	Location
6552	Station	Ernest Long	System	2

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 the activity on your Communication Server. 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 Log Configuration

Description

The Communication Server has the ability to store a log of system access and command execution, as well as other system-related messages. The history log is easily printed out or viewed on either a local or remote terminal. There are options to enable or disable certain history messages in later releases of software.

Security Concerns

You should review the Communication Server's history to monitor any unauthorized administrative access to the system, particularly during night hours. For maximum benefit, the history log should record all possible messages.

Analysis

Some history data is not being collected. It is recommended that all history log options be turned on.

Record CTA/PSA/TTI Transactions in history log?: Yes
Record submission failures in history log?: Yes
Record PMS/AD Transactions in history log?: No
Record IP Registrations in history log?: No

3.2. ASG - History Analysis

Description

Newer releases of Communication Server software allow for ASG one-time challenge/response authentication to be used for individual Login Names. With this feature enabled, the Communication Server keeps a log of customer-level ASG logins.

Security Concerns

When a user logs in using ASG, a record of the login attempt is kept in the ASG history. Logins that fail to authenticate will show up as being rejected. Rejections can be the result of an invalid response to a challenge, an invalid password, or an expired Login Name. A high number of rejections is often an indication of unauthorized attempts to access your system's administration interface.

Analysis

The following Login Names appear in your ASG History log. We note how many total entries appear for each Login Name, and if rejections were logged we highlight which kinds and how many.

adam

Login Name has 2 entries in the ASG History Log.

This Login Name was rejected for the following reasons:

Bad Password: 1 Rejection(s)

charlie

Login Name has 2 entries in the ASG History Log.

This Login Name was rejected for the following reasons:

Blocked Login: 1 Rejection(s)
Invalid Login Name: 1 Rejection(s)

donna46

Login Name has 7 entries in the ASG History Log.

This Login Name was rejected for the following reasons:

Bad Challenge Response: 6 Rejection(s)

3.3. Traffic Measurements

Description

The Communication Server allows you to track traffic measurements on Trunk Groups, thus enabling you to identify unexplained escalations in call volume, especially outside of normal operating hours.

Security Concerns

Avaya recommends you regularly review traffic measurements of various types, including unusually high peg counts, excessive numbers of long and short holding times, high usage of Route Patterns used for 0 + and 011 + calls, out-of-range busy hours of Trunk Groups, and the switch occupancy profile as compared to a typical 24-hour period.

Traffic Measurements

Your Communication Server is not currently measuring the following Trunk Groups hourly: 1 and 2. It is recommended that you enable hourly measurements for all Trunk Groups.

Your Communication Server is not currently measuring Route Patterns which are used for 0+ calls. The following Route Patterns should have hourly measuring enabled: 3 and 5

Your Communication Server is not currently measuring Route Patterns which are used for 011+ calls. The following Route Patterns should have hourly measuring enabled: 3 and 5

Did You Know?

While this section of the Security Audit covers the security aspects of Traffic Measurement, an InfoPlus Traffic Study may be ordered to gain a more complete understanding of your organization's Communication Server traffic. The Traffic Study answers many of the questions you may have about your system's capacity to handle your needs.

3.4. Scheduled Reports

Description

The Communication Server has the ability to schedule certain reports to be printed at specified intervals. This can be particularly useful when looking for abnormal activity related to system access and off-hours usage.

Security Concerns

By monitoring reports such as Processor Occupancy, Trunk Group Traffic and even sending the history log to the system printer, you can monitor your Communication Server usage. By keeping and comparing printouts of this information, it should be easier to spot abnormal fluctuations in usage.

Analysis

Scheduled Commands

Command	Days of Week	Time
list history	Tue	08:00

It is recommended that you schedule the commands "list measurements occupancy", and "list measurements trunk-group" to monitor your Communication Server's usage.

The command "list history" is scheduled, as recommended.

3.5. Call Detail Recording (CDR)

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 the Authorization Code 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 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

CDR is currently configured to use CDR1 as the primary endpoint. Please verify that this is the correct destination and that collection is functioning properly.

You are currently suppressing CDR for ineffective call attempts. This is not the recommended setting and should be changed in the CDR System Parameters.

Trunk Group 2 is not generating CDR data and should be changed to enable this feature.

Did You Know?

InfoPlus CDR is a web-based Call Detail Recording service that removes the burden of system operation and management while delivering a selection of completed weekly or monthly reports to your desktop. The same web portal that delivered this report can satisfy many of your communications management needs.

4. Stations

Many of the calling capabilities that have significant impact on long-distance charges are defined with the Class of Restriction and Class of Service of your stations. Access to certain features depends upon both the station's configuration and its COR and COS assignments. In these cases, it's best to review all members in the COR/COS since the stations' configuration may change at any time, perhaps inadvertently. In this section we analyze several of these features and capabilities, and look for potential holes in your security setup.

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 answers many of the questions you may have about your system's configuration.

4.1. Basic Access Restrictions

Description

This topic addresses two Class of Restriction settings that define the basic access restrictions for stations: Calling Party Restriction and Facility Restriction Level. Calling Party Restriction defines the overall access the station has to the public network (for example, can only place outgoing non-toll calls). The Facility Restriction Level is a further check that allows the station to only access facilities with an identical or lower FRL.

Security Concerns

Stations with a Calling Party Restriction of "none" or "tac-toll" are the least restricted and normally have access to the public network. Facility Restriction Levels range from 0, the most restrictive, to 7, the least restrictive. Stations with an FRL of 7 generally have more trunking facilities available to them, and should be reviewed to ensure the high FRL is necessary.

Analysis

Listed below are all CORs in your Communication Server with a Calling Party Restriction of "none" or "tac-toll" and/or which are assigned an FRL of 7. For each of these CORs, we list the stations belonging to it so a decision can easily be made whether the enhanced permissions are appropriate for the group.

COR: 0

Calling Party Restriction: none
Facility Restriction Level: 0

The following stations are assigned to COR 0:

Extension	Name	Equipment Type	Location
No stations are assigned to this COR.			

COR: 1

Calling Party Restriction: none
Facility Restriction Level: 1

The following stations are assigned to COR 1:

Extension	Name	Equipment Type	Location
6550	Dennis Carter	6408D+	
6558	Heather Ryan	2500	

COR: 2

Calling Party Restriction: none
Facility Restriction Level: 2

The following stations are assigned to COR 2:

Extension	Name	Equipment Type	Location
No stations are assigned to this COR.			

COR: 3

Calling Party Restriction: none
Facility Restriction Level: 3

The following stations are assigned to COR 3:

Extension	Name	Equipment Type	Location
No stations are assigned to this COR.			

COR: 5

Calling Party Restriction: none
Facility Restriction Level: 5

The following stations are assigned to COR 5:

Extension	Name	Equipment Type	Location
2420	Aaron Bennett	6424D+	
6544	Adam Gray	6408D+	2
6545	Barbara Grant	6416D+	1
6546	Benjamin Ward	6408D+	1
6547	Carlos Henderson	6408D+	1
6548	Carol Berry	6408D+	2
6549	Danielle Newman	6408D+	1
6551	Edna Jensen	6416D+	2
6552	Ernest Long	6416D+	2
6553	Florence Douglas	6408D+	1
6556	George Martin	6408D+	2
6580	Janet Sims	6424D+	1
6581	Jerry Nelson	6416D+	1
6582	Kathryn Reid	6416D+	2
6583	Kyle Simpson	6416D+	1
6584	Lillian Bowman	6416D+	2
6585	Luis Graham	6416D+	2
6586	Marjorie Horton	6416D+	2
6588	Nicholas Cox	6416D+	2
6589	Pauline Sutton	6416D+	1
6590	Ralph Cooper	6416D+	1
6591	Ricky Kennedy	6416D+	2
6592	Samuel Bailey	6416D+	1
6593	Sharon Arnold	POLY	1
6596	Victoria Herrera	6408D+	2
6597	Wanda Gilbert	6408D+	

COR: 14

Calling Party Restriction: none
Facility Restriction Level: 5

The following stations are assigned to COR 14:

Extension	Name	Equipment Type	Location
6554	Frederick Hicks	6408D+	2
6557	Gloria Vasquez	2500	1
6559	First Floor Fax	FAX	1
6587	Miguel Daniels	6416D+	1
6594	Teresa Schmidt	6408D+	1
6595	VDN	6408D+	

COR: 76

Calling Party Restriction: none
Facility Restriction Level: 0

The following stations are assigned to COR 76:

Extension	Name	Equipment Type	Location
No stations are assigned to this COR.			

COR: 77

Calling Party Restriction: none
Facility Restriction Level: 0

The following stations are assigned to COR 77:

Extension	Name	Equipment Type	Location
5004	VOICE MAIL PORT 1	VMAIL	1
5005	VOICE MAIL PORT 2	VMAIL	1
5006	VOICE MAIL PORT 3	VMAIL	1
5007	VOICE MAIL PORT 4	VMAIL	1

COR: 80

Calling Party Restriction: none
Facility Restriction Level: 3

The following stations are assigned to COR 80:

Extension	Name	Equipment Type	Location
No stations are assigned to this COR.			

COR: 95

Calling Party Restriction: none
Facility Restriction Level: 0

The following stations are assigned to COR 95:

Extension	Name	Equipment Type	Location
No stations are assigned to this COR.			

4.2. Restricted Call List (RCL)

Description

The Restricted Call List is a table of dialed numbers that are denied access. Once a COR is programmed to use the RCL, access to the numbers on the RCL will be blocked through AAR/ARS regardless of the COR's Facility Restriction Level (FRL).

Security Concerns

To help reduce toll-abuse, high-toll area codes and exchanges as well as popular paid-for service numbers can be placed on the Restricted Call List. CORs with the same FRL can have different calling capabilities based upon whether or not they use the Restricted Call List, thus providing a finer degree of control.

Analysis

Area Codes known for high toll-abuse which you may wish to add to your Restricted Call List include: 268, 473, 649, 664, 758, 767, 784, 809, 868, and 876. These are Caribbean destinations in which your organization may not conduct business regularly. In addition, you may want to deny 1010-XXX 'Equal Access' numbers, 1-900 paid services, and 1-800 carrier specific services (e.g., 1-800-CALL-ATT).

The Restricted Call List contains the following entries:

Dialed Sequence	Digit Length
1900	11
1900555	11

The following Classes of Restriction which are assigned to stations are not using the Restricted Call List:

COR: 1

The following stations are assigned to COR 1

Extension	Name	Equipment Type	Location
6550	Dennis Carter	6408D+	
6558	Heather Ryan	2500	

COR: 5

The following stations are assigned to COR 5

Extension	Name	Equipment Type	Location
2420	Aaron Bennett	6424D+	
6544	Adam Gray	6408D+	2
6545	Barbara Grant	6416D+	1
6546	Benjamin Ward	6408D+	1
6547	Carlos Henderson	6408D+	1
6548	Carol Berry	6408D+	2
6549	Danielle Newman	6408D+	1

Extension	Name	Equipment Type	Location
6551	Edna Jensen	6416D+	2
6552	Ernest Long	6416D+	2
6553	Florence Douglas	6408D+	1
6556	George Martin	6408D+	2
6580	Janet Sims	6424D+	1
6581	Jerry Nelson	6416D+	1
6582	Kathryn Reid	6416D+	2
6583	Kyle Simpson	6416D+	1
6584	Lillian Bowman	6416D+	2
6585	Luis Graham	6416D+	2
6586	Marjorie Horton	6416D+	2
6588	Nicholas Cox	6416D+	2
6589	Pauline Sutton	6416D+	1
6590	Ralph Cooper	6416D+	1
6591	Ricky Kennedy	6416D+	2
6592	Samuel Bailey	6416D+	1
6593	Sharon Arnold	POLY	1
6596	Victoria Herrera	6408D+	2
6597	Wanda Gilbert	6408D+	

COR: 14

The following stations are assigned to COR 14

Extension	Name	Equipment Type	Location
6554	Frederick Hicks	6408D+	2
6557	Gloria Vasquez	2500	1
6559	First Floor Fax	FAX	1
6587	Miguel Daniels	6416D+	1
6594	Teresa Schmidt	6408D+	1
6595	VDN	6408D+	

COR: 77

The following stations are assigned to COR 77

Extension	Name	Equipment Type	Location
5004	VOICE MAIL PORT 1	VMAIL	1
5005	VOICE MAIL PORT 2	VMAIL	1
5006	VOICE MAIL PORT 3	VMAIL	1
5007	VOICE MAIL PORT 4	VMAIL	1

4.3. Service Observe Feature

Description

The Service Observe feature allows certain users the ability to monitor calls placed within the Communication Server. Users with access to the Service Observe feature may monitor calls placed to extensions, Vector Directory Numbers and Agent Login IDs.

Security Concerns

If toll-abuse is suspected, the Service Observe feature can be used to monitor suspicious calls. Observers may use "listen" or "listen and talk" mode when monitoring calls. Optionally, a warning tone may be generated and heard by all listeners when a call is being monitored. It is recommended that you check with your local, state and federal laws to determine if the warning tone option must be enabled. Due to the nature of this feature and its potential for abuse, it is recommended to carefully and regularly review the users who have access to it. If the feature is not needed by your organization, it is recommended the two Feature Access Codes associated with it are left blank.

Analysis

Below is a list of the settings in your Communication Server related to Service Observing. It is recommended that the Service Observing related Feature Access Codes be left blank unless required by your business. Check with your local, state, and federal authorities to determine the legalities surrounding the Service Observe tone options.

Service Observing Warning Tone Enabled: Y
Service Observing Conference Tone Enabled: N
Service Observing Allowed with Exclusion: Blank
Service Observing Listen Only Access Code: Blank
Service Observing Listen and Talk Access Code: Blank

The following is a list of stations which have a Service Observe button assigned:

Extension	Name	Type	Location
6550	Dennis Carter	6408D+	

The following Classes of Restriction can be service observers: 1. Any station in these CORs can Observe with either a button assignment or a Feature Access Code.

COR: 1

Stations in this Class of Restriction can observe the following Classes of Restriction: 0-95.

The following is a list of stations assigned to COR 1:

Extension	Name	Equipment Type	Location
6550	Dennis Carter	6408D+	
6558	Heather Ryan	2500	

4.4. Station Features

Description

This topic addresses three powerful features of stations - Trunk-to-Trunk Transfer, Console Permissions, and Data Privacy. Trunk-to-Trunk Transfer allows an incoming call to be automatically redirected to an outbound trunk. Console Permissions allow a station to change the Facility Restriction Level (FRL) of other stations, thus altering their calling permissions. Data Privacy prevents analog data calls from being interrupted by attendant intrusion or features such as call waiting.

Security Concerns

The use of most of these features is a business and personnel decision. For example, Trunk-to-Trunk Transfer 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 the recommended setting due to its abuse potential. It is also recommended to disable Trunk-to-Trunk Transfer Override, which can bypass COR-to-COR restrictions during a transfer, if it is not required. Console Permissions should only be given to sets which require the ability to change FRL levels and should not be located in publicly-accessible areas. Finally, it is recommended the Data Privacy feature only be enabled on modems, fax machines, credit card authorization devices, and other data terminals which require it.

Analysis

All Trunk-to-Trunk transfers are disallowed in your feature-related system-parameters. This is the recommended configuration.

Listed below are all COSs in your Communication Server with Console Permissions, Data Privacy, or Trunk-to-Trunk Transfer Override enabled. For each of these COSs, we list the stations belonging to it so a decision can easily be made whether the enhanced permissions are appropriate for the group.

COS: 1

Console Permissions are disabled for this COS, as recommended.

Data Privacy is enabled for this COS.

Trunk-to-Trunk Transfer Override is enabled for this COS.

The following stations are assigned to COS 1:

Extension	Name	Equipment Type	Location
2420	Aaron Bennett	6424D+	
5004	VOICE MAIL PORT 1	VMAIL	1
5005	VOICE MAIL PORT 2	VMAIL	1
5006	VOICE MAIL PORT 3	VMAIL	1
5007	VOICE MAIL PORT 4	VMAIL	1
6544	Adam Gray	6408D+	2
6545	Barbara Grant	6416D+	1
6546	Benjamin Ward	6408D+	1
6547	Carlos Henderson	6408D+	1

Extension	Name	Equipment Type	Location
6548	Carol Berry	6408D+	2
6549	Danielle Newman	6408D+	1
6550	Dennis Carter	6408D+	
6551	Edna Jensen	6416D+	2
6552	Ernest Long	6416D+	2
6553	Florence Douglas	6408D+	1
6554	Frederick Hicks	6408D+	2
6556	George Martin	6408D+	2
6557	Gloria Vasquez	2500	1
6558	Heather Ryan	2500	
6580	Janet Sims	6424D+	1
6581	Jerry Nelson	6416D+	1
6582	Kathryn Reid	6416D+	2
6583	Kyle Simpson	6416D+	1
6584	Lillian Bowman	6416D+	2
6585	Luis Graham	6416D+	2
6586	Marjorie Horton	6416D+	2
6587	Miguel Daniels	6416D+	1
6588	Nicholas Cox	6416D+	2
6589	Pauline Sutton	6416D+	1
6590	Ralph Cooper	6416D+	1
6591	Ricky Kennedy	6416D+	2
6592	Samuel Bailey	6416D+	1
6593	Sharon Arnold	POLY	1
6594	Teresa Schmidt	6408D+	1
6595	VDN	6408D+	
6596	Victoria Herrera	6408D+	2
6597	Wanda Gilbert	6408D+	

COS: 2

Console Permissions are disabled for this COS, as recommended.

Data Privacy is disabled for this COS, as recommended.

Trunk-to-Trunk Transfer Override is enabled for this COS.

The following stations are assigned to COS 2:

Extension	Name	Equipment Type	Location
No stations are assigned to this COS.			

COS: 5

Console Permissions are disabled for this COS, as recommended.

Data Privacy is enabled for this COS.

Trunk-to-Trunk Transfer Override is disabled for this COS, as recommended.

The following stations are assigned to COS 5:

Extension	Name	Equipment Type	Location
No stations are assigned to this COS.			

COS: 14

Console Permissions are enabled for this COS.

Data Privacy is disabled for this COS, as recommended.

Trunk-to-Trunk Transfer Override is disabled for this COS, as recommended.

The following stations are assigned to COS 14:

Extension	Name	Equipment Type	Location
No stations are assigned to this COS.			

4.5. Call Forward Capabilities

Description

In the Avaya Communication Server, the Classes of Service control access to various Call Forwarding Features. These features include Call Forward (Busy/DA, All), Extended Call Forward (Busy/DA, All) and Call Forward Off-Net.

Security Concerns

While there are valid reasons to forward a phone, it is recommended that you review which stations have call forwarding capabilities. While it is commonly acceptable to allow normal Call Forwarding capabilities, only telecommuters should have access to the Extended Call Forward feature. Due to its abuse potential, Call Forward Off-Net should always be restricted unless there is a valid need to implement it in your Communication Server.

Analysis

Listed below are all COSs in your Communication Server with Call Forward All Calls, Call Forward Busy/DA, Extended Call Forward Busy/DA, or Extended Call Forward All Calls enabled. COSs with Restrict Call Forward Off-Net disabled will also be displayed. For each of these COSs, we list the stations belonging to it so a decision can easily be made whether the enhanced permissions are appropriate for the group.

Class of Service: 1

Call Forward All Calls: Enabled
Call Forward Busy/DA: Disabled
Extended Call Forward Busy/DA: Disabled
Extended Call Forward All Calls: Disabled
Restrict Call Forward Off-Net: Enabled

The following stations are assigned to COS 1:

Extension	Name	Equipment Type	Location
2420	Aaron Bennett	6424D+	
5004	VOICE MAIL PORT 1	VMAIL	1
5005	VOICE MAIL PORT 2	VMAIL	1
5006	VOICE MAIL PORT 3	VMAIL	1
5007	VOICE MAIL PORT 4	VMAIL	1
6544	Adam Gray	6408D+	2
6545	Barbara Grant	6416D+	1
6546	Benjamin Ward	6408D+	1
6547	Carlos Henderson	6408D+	1
6548	Carol Berry	6408D+	2
6549	Danielle Newman	6408D+	1
6550	Dennis Carter	6408D+	
6551	Edna Jensen	6416D+	2
6552	Ernest Long	6416D+	2
6553	Florence Douglas	6408D+	1
6554	Frederick Hicks	6408D+	2

Extension	Name	Equipment Type	Location
6556	George Martin	6408D+	2
6557	Gloria Vasquez	2500	1
6558	Heather Ryan	2500	
6580	Janet Sims	6424D+	1
6581	Jerry Nelson	6416D+	1
6582	Kathryn Reid	6416D+	2
6583	Kyle Simpson	6416D+	1
6584	Lillian Bowman	6416D+	2
6585	Luis Graham	6416D+	2
6586	Marjorie Horton	6416D+	2
6587	Miguel Daniels	6416D+	1
6588	Nicholas Cox	6416D+	2
6589	Pauline Sutton	6416D+	1
6590	Ralph Cooper	6416D+	1
6591	Ricky Kennedy	6416D+	2
6592	Samuel Bailey	6416D+	1
6593	Sharon Arnold	POLY	1
6594	Teresa Schmidt	6408D+	1
6595	VDN	6408D+	
6596	Victoria Herrera	6408D+	2
6597	Wanda Gilbert	6408D+	

Class of Service: 4

Call Forward All Calls: Enabled
Call Forward Busy/DA: Enabled
Extended Call Forward Busy/DA: Enabled
Extended Call Forward All Calls: Enabled
Restrict Call Forward Off-Net: Disabled

The following stations are assigned to COS 4:

Extension	Name	Equipment Type	Location
No stations are assigned to this COS.			

Class of Service: 7

Call Forward All Calls: Enabled
Call Forward Busy/DA: Disabled
Extended Call Forward Busy/DA: Disabled
Extended Call Forward All Calls: Disabled
Restrict Call Forward Off-Net: Enabled

The following stations are assigned to COS 7:

Extension	Name	Equipment Type	Location
No stations are assigned to this COS.			

4.6. 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 all of a station's coverage points, as well as any currently forwarded destination.

Security Concerns

External redirection numbers should be checked to ensure they have an appropriate business need. Certain uses are common, such as an external Voice Mail system. Abuses occur when individuals forward their phone for personal use.

Analysis

The following tables lists stations whose various redirection destinations appear to be external. The destinations in question are listed under each category:

- Coverage Points
- Call Forward Destination

The following extensions use a Coverage Path containing one or more Remote Coverage Points. For each entry, we show the actual number dialed along with the Remote Coverage Point.

Extension	Location	Cov. Path #	Coverage Point	Destination	Remote Coverage Point
6557	1	2	1	19007654321	7
			2	912125551212	25

The following extensions have a Call Forwarding destination assigned that appears to be external:

Extension	Location	Name	Forwarded Destination
6552	2	Ernest Long	919005551234

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 Groups should be avoided to help you maintain a secure switch. In this section, we're going to analyze your Trunk Groups, 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 Trunk Groups section of the SourceBook will clearly present exactly which Trunk Groups are used in the placing of outgoing calls and the order in which they are used. The SourceBook answers many of the questions you may have about your system's configuration.

5.1. Trunk Groups and Members

Description

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

Security Concerns

There are many potential pitfalls to avoid when defining Trunk Groups. Something as simple as allowing outgoing calls on a Trunk Group that is supposed to be incoming only could be a security problem. Another common issue is enabling 'dial access' to a Trunk Group, and then defining a short or simple Trunk Access Code. It is recommended that all Trunk Access Codes be 4 digits long and non-trivial. If possible, 'dial access' to the Trunk Group should be disabled and all calls routed through ARS for increased security. Assigning a Trunk Group an FRL of 7 when a lower value would suffice is another sign of a poor security implementation. If an incoming destination is defined for a Trunk Group, it is recommended the number be verified, especially if it's an external destination. Other problems include failing to collect Call Detail Recording data for all Trunk Groups and incorrectly configured Classes of Restriction (COR). It is recommended that the CORs assigned to Trunk Groups are not used for other resources (e.g., stations) so that a robust COR-to-COR restriction plan can be defined. Finally, it is recommended that Automatic Circuit Assurance (ACA) is enabled for your Trunk Groups to help warn you about extremely short or long holding times which may be an indication of unauthorized activity.

The trunks themselves can pose their own security issues. We'll be checking specifically for trunks that have Night Service extensions programmed, as this represents a substantial risk to your Communication Server's security. All Night Service destinations should be verified, especially if the number is external to the Communication Server.

Analysis

Below is a list of all of the Trunk Groups in your Communication Server. Any items which do not agree with the Security Concerns are highlighted for review.

Trunk Group: 1

The following security-related items are part of the configuration for Trunk Group 1:

Trunk Group Name: ISDN
Trunk Group Type: isdn
Location(s) of Members: 2
Trunk Group Direction: two-way
Incoming Destination:
Trunk Access Code (TAC): 123
Dial Access: Enabled
Class of Restriction (COR): 95
Facility Restriction Level (FRL): 0
Call Detail Recording: Enabled
Night Service Extension: 6549
Automatic Circuit Assurance: Disabled

COR 95 appears to be unique to Trunk Groups, as recommended.

The following Station CORs are not restricted from calling this Trunk Group's COR: 14. You should disable calling directly from station CORs to Trunk Group CORs to prevent users from bypassing ARS.

You have 23 trunk members programmed in this Trunk Group. The following table lists all members in this Trunk Group. We note trunks that have Night Service Extensions defined, highlighting those that appear to be external destinations.

Member Number	Name	Port	Night
1		02A1001	6588
2		02A1002	
3		02A1003	
4		02A1004	
5		02A1005	
6		02A1006	
7		02A1007	
8		02A1008	
9		02A1009	
10		02A1010	
11		02A1011	6588
12		02A1012	
13		02A1013	
14		02A1014	
15		02A1015	
16		02A1016	
17		02A1017	
18		02A1018	
19		02A1019	
20		02A1020	
21		02A1021	
22		02A1022	
23		02A1023	

Trunk Group: 2

The following security-related items are part of the configuration for Trunk Group 2:

Trunk Group Name: POTS TRUNKS
Trunk Group Type: co
Location(s) of Members: 1
Trunk Group Direction: two-way
Incoming Destination: 2420
Trunk Access Code (TAC): 456
Dial Access: Enabled
Class of Restriction (COR): 94
Facility Restriction Level (FRL): 0
Call Detail Recording: Disabled
Automatic Circuit Assurance: Disabled

COR 94 appears to be unique to Trunk Groups, as recommended.

The following Station CORs are not restricted from calling this Trunk Group's COR: 14 and 77. You should disable calling directly from station CORs to Trunk Group CORs to prevent users from bypassing ARS.

You have 5 trunk members programmed in this Trunk Group. The following table lists all members in this Trunk Group. We note trunks that have Night Service Extensions defined, highlighting those that appear to be external destinations.

Member Number	Name	Port	Night
1	2125554321	01A0401	
2	2125555432	01A0402	
3	2125556543	01A0403	
4	2125557654	01A0404	
5	2125558765	01A0405	

5.2. Direct Trunk Access

Description

Users can be given the ability to bypass the ARS least-cost routing feature and dial Trunk Access Codes directly. If the COR-to-COR restriction table does not restrict a station's COR from accessing a particular Trunk Group's COR, and the Trunk Group has the 'dial access' feature enabled, then direct access of the Trunk Group is possible from the station. This disables all of the security features built into the ARS design. Once a Trunk Group is accessed directly, the Calling Party Restrictions of the station's COR will be used to determine whether a particular call is allowed.

Security Concerns

When combined with a Calling Party Restriction of "none", "tac-toll" or "all-toll", directly accessing a Trunk Group gives users the full capabilities of the public network. This includes the ability to place any toll call including international numbers. With a Calling Party Restriction of "outward" the user is restricted to directly accessing only TIE Trunk Groups, but still has the ability to dial any string of digits including international, high-toll and long distance destinations.

Analysis

The following CORs have direct access to one or more Trunk Groups, and their configuration should be reviewed to ensure proper security:

COR: 14

Calling Party Restriction: none

Stations in this COR have direct access to the following Trunk Groups:

Group Number	Group Name	COR
1	ISDN	95
2	POTS TRUNKS	94

The following stations are assigned to COR 14:

Extension	Name	Equipment Type	Location
6554	Frederick Hicks	6408D+	2
6557	Gloria Vasquez	2500	1
6559	First Floor Fax	FAX	1
6587	Miguel Daniels	6416D+	1
6594	Teresa Schmidt	6408D+	1
6595	VDN	6408D+	

COR: 77

Calling Party Restriction: none

Stations in this COR have direct access to the following Trunk Groups:

Group Number	Group Name	COR
2	POTS TRUNKS	94

The following stations are assigned to COR 77:

Extension	Name	Equipment Type	Location
5004	VOICE MAIL PORT 1	VMAIL	1
5005	VOICE MAIL PORT 2	VMAIL	1
5006	VOICE MAIL PORT 3	VMAIL	1
5007	VOICE MAIL PORT 4	VMAIL	1

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 Abbreviated Dialing List

Description

The System Abbreviated Dialing List (also referred to as "Speed Call") allows users to place internal or external calls to predefined numbers by dialing a 2-digit code. The System Abbreviated Dialing List can store up to 100 entries with up to 24 digits each.

Security Concerns

Because a privileged System Abbreviated Dialing List can override the Class of Restriction (COR) of stations, it is important to verify the numbers stored in the list are approved destinations.

Analysis

Your System Abbreviated Dialing List is not currently configured as Privileged, meaning the station's COR will be checked when accessing numbers stored in this list. This is the recommended configuration.

The following is your System Abbreviated Dialing List, and the entries currently programmed. These entries should be verified as approved destinations. Numbers identified as external to the Communication Server are shown in red and underlined.

Dial Code	Digits Dialed
05	6553
33	19001234567
55	18005551212

6.2. Group Abbreviated Dialing Lists

Description

The Group Abbreviated Dialing Lists (also referred to as "Speed Call" lists) allow users to place internal or external calls to predefined numbers by dialing a 2-digit code. The Communication Server is capable of having up to 100 different lists programmed. Each Group Abbreviated Dialing List can store up to 100 entries with up to 24 digits each.

Security Concerns

Because privileged Group Abbreviated Dialing Lists can override the Class of Restriction (COR) of stations, it is important to verify the numbers stored in the list are approved destinations. It is also important to control the individuals who can modify these lists.

Analysis

You have 2 Group Abbreviated Dialing Lists defined. Following is each of your Group Abbreviated Dialing Lists, and the entries currently programmed. These entries should be verified as approved destinations.

Group Abbreviated Dialing List: 1

This Group Abbreviated Dialing List is not currently configured as Privileged, meaning the station's COR will be checked when accessing numbers stored in this list. This is the recommended configuration.

List Programmer Extension: None
List Size: 10

Dial Code	Digits Dialed
No entries are programmed in this list.	

Group Abbreviated Dialing List: 2

This Group Abbreviated Dialing List is currently configured as Privileged, meaning the station's COR will not be checked when accessing numbers stored in this list.

List Programmer Extension: None
List Size: 5

Dial Code	Digits Dialed
11	919009876543
13	6557
14	912015551212

6.3. Authorization Codes

Description

Stations and trunks originating calls can use Authorization Codes to alter their Facility Restriction Level (FRL). Each Authorization Code is mapped to a COR and the caller assumes that COR's FRL when entered.

Security Concerns

Security Violation Notification (SVN) for Authorization Codes should be enabled when Authorization Codes are in use. It is recommended to use an SVN threshold of 10 or fewer invalid attempts in 3 or more minutes, and to ensure the Referral Destination is being monitored regularly by appropriate personnel. Authorization Codes that contain less than 7 digits or are simple to guess are not recommended since they don't provide adequate security for the enhanced privileges they provide. Those codes assigned to CORs with high FRLs and low Calling Party Restrictions can also present a possible security problem if not managed carefully.

Analysis

Authorization Codes are enabled in the Customer Options of your Communication Server, but disabled in System Features. The Authorization Code feature is disabled, but SVN for Authorization Codes is enabled as recommended.

Authorization Codes SVN Originating Extension: 6582
Authorization Codes SVN Referral Destination: 6589
Authorization Codes SVN Threshold: 20
Authorization Codes SVN Time Interval: 2 Minutes

The following table lists all Authorization Codes in the Communication Server. The highlighted codes have failed one or more of the following checks:

- Contains a run of four or more consecutive digits
- Contains a run of four or more identical digits
- Is fewer than 7 characters long
- Code is assigned to a COR with an FRL of 6 or greater
- Code is assigned to a COR with a Calling Party Restriction of "none"

Authorization Code	COR	FRL	CPR = "none"
1234567	1	1	✓
3332222	72	0	
6271935	72	0	

6.4. Account Codes

Description

The Communication Server can be configured to use CDR Account Codes for calls placed on the Toll List. The system administrator can configure the number of digits (1 to 15) that must be dialed within a certain time, and if the proper number of digits are not dialed, the call will not complete. The specific digits dialed are not verified in any way, only the number of digits must be correct. This feature is often used to associate an identifier (e.g., an account number) with calls for billing purposes.

Security Concerns

Requiring Account Codes for toll calls can offer a modest level of security against unauthorized users, and provide an additional means of tracking Communication Server usage. These codes will show up in CDR records and can assist you in recognizing toll-abuse.

Analysis

Your CDR configuration is currently configured to force entry of Account Codes, however no CORs are configured to use this feature. Configuring your CORs to force entry of Account Codes gives you an additional means of tracking Communication Server usage.

7. Controlling Feature Access

Avaya Communication Servers have 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. Access to several of these features can be controlled by settings within the Class of Service, while others may be disabled altogether.

7.1. Feature Access Codes

Description

Feature Access Codes (FAC) are user-defined numbers of up to four digits which can be used to enable or disable Communication Server features. When a code is not defined, the associated feature is generally inaccessible.

Security Concerns

Feature Access Codes for features with security implications should not be accessible through Voice Mail. Ensure that the digits of these Feature Access Codes are blocked in the Voice Mail system, or translated to an extension, attendant, announcement or disconnect - never to the Feature Access Code itself. It is recommended that you leave the Feature Access Code empty for any features that are not required by your organization, as a measure to prevent inappropriate use.

Analysis

AAR/ARS/ISDN Feature Access Codes

Ensure that the following digits are blocked or intercepted from your Voice Mail system:

Feature Name	Feature Access Code
AAR	444
ARS - Access Code 1	9
ARS - Access Code 2	Blank
ISDN Access Code	Blank

Critical Feature Access Codes

The following Feature Access Codes have security implications and should be blocked in your Voice Mail system. If it is not necessary to have them enabled, their Feature Access Code should be left blank.

Feature Name	Feature Access Code
Abbreviated Dialing - List 1	#1
Abbreviated Dialing - List 2	Blank
Abbreviated Dialing - List 3	*5
Call Forward Activation - Busy/DA	Blank
Call Forward Activation - All	#9
Change Coverage	Blank
Data Origination	Blank
Data Privacy	Blank
Facility Test Call†	552
Personal Station Access Associate	Blank
Personal Station Access Dissociate	Blank
Station Security Code Change	#12

†The Facility Test Call code should only be enabled when in use. After testing is complete, Avaya recommends removing the access code from the Communication Server in order to increase security.

7.2. Station Security Codes

Description

Station Security Codes (SSC) are used with several features, including Station Lock, Personal Station Access (PSA) and User Administration of Redirected Calls. In order to use these features, the Station Security Code for the particular station must be entered.

Security Concerns

Short or simple Station Security Codes may not provide adequate security. It is recommended the minimum length of Station Security Codes be set to at least 4. Any station that does not require the use of the features protected by a Station Security Code should not have one defined. You can prevent users from changing the Station Security Code by removing the Feature Access Code for 'Station Security Code Change Access Code'. Security Violation Notifications for Station Security Codes should be enabled when available in later Avaya software. It is recommended to use an SVN threshold of 10 or fewer invalid attempts in 3 or more minutes, and to ensure the Referral Destination is being monitored regularly by appropriate personnel.

Analysis

Station Security Codes Security Violation Notification: Disabled

The minimum station security code length as defined in the Communication Server's security-related system parameters is 2 digits. It is recommended that you increase the minimum length to at least 4 digits.

There are 1 stations in your Communication Server with a Station Security Code currently defined. The Station Security Code Change option is enabled in your Feature Access Codes, allowing a user to alter their existing code at any time.

The following stations in your Communication Server have Station Security Codes assigned:

Extension	Name	Equipment Type	Location
6544	Adam Gray	6408D+	2

7.3. Modems and Faxes

Description

Avaya recommends reviewing the capabilities of ports configured for fax machines and modems, to ensure that they are not using features which may be exploited.

Security Concerns

Certain types of fax machines, modems and answering machines respond to specific tones presented to them, sometimes allowing dial tone to be returned to the caller. Upon receiving dial tone from the Communication Server, the caller is free to dial any number allowed by the COR of the fax machine or modem. In order to ensure that these ports are protected from this sort of exploitation, Avaya recommends disabling the Switch Hook Flash and Distinctive Audible Alert features in the station programming.

Analysis

Below is a list of all stations identified as possible security risks. These stations all have "FAX", "FX", or "MOD" in their name, or the station type is aliased to "modem" or "fax", and meet one of the following additional criteria:

- Distinctive Audible Alert is enabled
- Switch Hook Flash is enabled

Please note that it is possible for some modems or faxes in your Communication Server to be missed by this test, or for stations which are neither a modem nor a fax machine to be detected. While the following list can act as a guideline, it is recommended that you review your stations in depth.

Extension	Name	COR	Switch Hook Flash	Distinctive Audible Alert	Location
No modems or faxes matching above criteria were detected.					

8. Remote Access

This section addresses Remote Access, a very powerful feature that if not properly controlled could open your Communication Server to abuse by external callers. This feature requires special consideration. Although the feature is part of the standard Communication Server configuration, it can and should be disabled system wide upon initial installation if not required for your business.

8.1. Remote Access Feature (DISA)

Description

The Remote Access feature, sometimes referred to as Direct Inward System Access or DISA, allows a user to dial an extension in the Communication Server and receive secondary dial-tone. Depending on the configuration, the user may then dial internal or external numbers as if they were using a station in the Communication Server. This feature is often used by businesses where employees are traveling regularly and need to place business-related calls from outside the office.

Security Concerns

Remote Access, 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. If Remote Access is required, it should be heavily protected through the use of Authorization Codes, Barrier Codes and tight access restrictions. It is recommended that Security Violation Notifications for Remote Access be enabled if this feature is in use, and that the SVN system disable the Remote Access feature upon the thresholds being reached. You should define an SVN threshold of 10 or fewer invalid attempts in 3 or more minutes, and ensure the Referral Destination is being monitored regularly by appropriate personnel. In addition, Remote Access dial-in numbers should not be published, and their distribution should be limited to employees who require the feature.

Analysis

Remote Access is enabled in your Communication Server. Please review the following information with great care to ensure that your Remote Access programming is as secure as it can be.

Remote Access Security Violation Notification: Disabled
Remote Access Extension: 6585
Authorization Codes: Not Required

Remote Access Disable After a Violation is not defined in your Communication Server. It is recommended that this feature be enabled to guard against intrusion attempts, or that you permanently disable Remote Access if the feature is not needed.

It is recommended that your remote access extension length be changed to at least 6 digits.

It is recommended that you require Authorization Codes for Remote Access.

8.2. Barrier Codes

Description

For additional security, Remote Access should be assigned Barrier Codes that must be entered before the user gains access to secondary dial-tone. These codes can be 4 to 7 digits in length and are assigned to a specific COR, Tenant and COS. They can also be assigned a maximum number of calls and an expiration date to limit their use.

Security Concerns

Barrier Codes that are easy to guess should not be used. They should all be at least 6 digits in length, although 7 is always preferred. If the Barrier Code length is left blank, then no Barrier Codes are required for secondary dial-tone, significantly lowering the security of the Remote Access feature. The Class of Restriction and Class of Service assigned to each Barrier Code should be fairly restrictive to ensure that remote users are only able to dial necessary numbers. If applicable, a low number of maximum calls should be specified, as well as an expiration date less than 1 month from the date the Barrier Code was created.

Analysis

Your Barrier Code length is set to 5. It is recommended that this length be increased to at least 6 digits.

Below is a list of every Barrier Code in your Communication Server and its associated programming. Potential security risks have been highlighted in red and underlined. Remote Access programming should be reviewed on a regular basis and should be permanently disabled if not necessary to your business.

NOTE: *If Remote Access is permanently disabled, only Avaya can re-enable this feature.*

The following table lists all Barrier Codes that are defined:

Barrier Code	COR	COS	Expiration Date	No. of Calls	Calls Used
12345	1	1	07/22/2008	9	0
47298	1	1		50	0
88888	1	1		9	0

9. 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 Avaya's Alternate Route Selection (ARS) feature, 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.

9.1. Route Patterns

Description

For each network call translated in an Avaya Communication Server, ARS or AAR selects a Trunk Group from a list of possible outgoing Trunk Groups to complete the call. The list of possible Trunk Groups to a particular destination is called a Route Pattern, and each Trunk Group specified in the pattern is given a preference. Typically, the first preference in a Route Pattern should be the least expensive Trunk Group to a destination, and the remaining Trunk Groups in the list are more expensive.

Security Concerns

Each Route Pattern preference may both delete and insert digits. These digits should be carefully examined for any strange redirection of calls. Assigning an entry in a Route Pattern an FRL of 0 should be limited, as this permits all other resources to access it.

Analysis

This table lists all Route Pattern preferences which insert digits when selected. These Route Pattern preferences should be carefully reviewed to ensure that the inserted digits don't cause calls to be be redirected inappropriately.

Route Pattern preferences which insert digits:

Route Pattern	Preference	No. Deleted Digits	Digits Inserted
20	1	3	1212332
20	2	3	1212332
21	1	3	1845123
22	1	3	1201476
22	2	3	1201476
23	1	7	90
23	2	3	1310205

The following table presents a list of all Route Patterns and preferences, as well as their associated FRL values. Low FRLs should be reviewed and increased if necessary.

Route Pattern	Preference	FRL
1	1	1
1	2	1
2	1	2
2	2	2
3	1	5
3	2	5
5	1	6
5	2	6
6	1	1
6	2	1
7	1	3
9	1	0

Route Pattern	Preference	FRL
9	2	0
20	1	2
20	2	2
21	1	2
21	2	2
22	1	2
22	2	2
23	1	2
23	2	2
24	1	2
24	2	2

9.2. Alternate FRL

Description

The Avaya Communication Server can allow stations and trunks to use an alternate (and usually less-restrictive) FRL when necessary to modify their calling permissions. This feature is activated and deactivated by the console.

Security Concerns

If an Alternate FRL is assigned incorrectly, certain stations and trunks may not be as restricted as they would appear if you analyzed only the FRL of their associated CORs. Vice versa, an Alternate FRL that is too restrictive may hinder a station or trunk from being able to place calls as needed.

Analysis

The following presents a list of your FRLs (0-7) and their associated Alternate FRL. If the Alternate FRL allows greater access, it will be highlighted for review.

FRL	Alternate FRL
0	0
1	1
2	7
3	2
4	7
5	5
6	6
7	7

9.3. Time of Day Routing

Time of Day Routing

Time of Day Routing can be used to alter a station's calling abilities based on both the time of day and day of the week. This feature is normally used to restrict long distance access after business hours.

Security Concerns

Since Time of Day Routing changes which Route Patterns are used when dialing through AAR/ARS, it is important to ensure that access to long distance and international destinations is properly restricted. Any off-hours configuration granting long distance or international access should be reviewed.

Analysis

Time of Day Routing Plan: 1

The extensions using Time of Day 1 use the following CORs: 0-13, 15-75, 78, 79 and 81-95.

30 stations are assigned to this plan.

Time Period	PGN	CORs with Long Distance Access	CORs with International Access
Monday - Sunday, 00:00 - 05:59	2	None	None
Monday - Sunday, 06:00 - 22:59	1	5	5
Monday - Sunday, 23:00 - 23:59	2	None	None

Time of Day Routing Plan: 2

The extensions using Time of Day 2 use the following CORs: 80.

0 stations are assigned to this plan.

Time Period	PGN	CORs with Long Distance Access	CORs with International Access
Monday - Sunday, 00:00 - 23:59	1	None	None

Time of Day Routing Plan: 3

NOTE: *Plan uses a 'Default Configuration'.*

The extensions using Time of Day 3 use the following CORs: 14, 76 and 77.

11 stations are assigned to this plan.

Time Period	PGN	CORs with Long Distance Access	CORs with International Access
Monday - Sunday, 00:00 - 23:59	3	14	14

Time of Day Routing Plan: 4

NOTE: *Plan uses a 'Default Configuration'.*

Time of Day 4 is not in use by any COR.

0 stations are assigned to this plan.

Time Period	PGN	CORs with Long Distance Access	CORs with International Access
Monday - Sunday, 00:00 - 23:59	4	None	None

Time of Day Routing Plan: 5

NOTE: *Plan uses a 'Default Configuration'.*

Time of Day 5 is not in use by any COR.

0 stations are assigned to this plan.

Time Period	PGN	CORs with Long Distance Access	CORs with International Access
Monday - Sunday, 00:00 - 23:59	5	None	None

Time of Day Routing Plan: 6

NOTE: *Plan uses a 'Default Configuration'.*

Time of Day 6 is not in use by any COR.

0 stations are assigned to this plan.

Time Period	PGN	CORs with Long Distance Access	CORs with International Access
Monday - Sunday, 00:00 - 23:59	6	None	None

Time of Day Routing Plan: 7

NOTE: *Plan uses a 'Default Configuration'.*

Time of Day 7 is not in use by any COR.

0 stations are assigned to this plan.

Time Period	PGN	CORs with Long Distance Access	CORs with International Access
Monday - Sunday, 00:00 - 23:59	7	None	None

Time of Day Routing Plan: 8

NOTE: *Plan uses a 'Default Configuration'.*

Time of Day 8 is not in use by any COR.

0 stations are assigned to this plan.

Time Period	PGN	CORs with Long Distance Access	CORs with International Access
Monday - Sunday, 00:00 - 23:59	8	None	None

9.4. Digit Manipulation

Description

AAR, ARS as well as each Route Pattern in the Communication Server can optionally define a number of digits to delete from a dialed sequence, and/or a digit sequence to insert. Digits are deleted from the beginning of the sequence that was dialed, and the new digits may be added in their place potentially changing the call's destination after it has passed through AAR/ARS. This can be used to route specific calls to a different location than they would normally go, such as routing a call over a TIE line to another office where the call would be local. Digit Manipulation can also be used to add outpulsed digits that may be required by the central office for certain call types.

Security Concerns

Digit Manipulation is a feature that can easily be exploited to make calls that would otherwise be denied by a properly configured AAR/ARS table. Since digits are deleted and inserted from the beginning of the sequence that is dialed, it would be an easy matter for someone to create a Route Pattern that replaces whatever area code was dialed with, for example, a 1-900 number. This Route Pattern could be assigned to an otherwise unused, innocuous looking AAR/ARS entry and allow fraudulent calls to be placed.

Another, more difficult to detect approach to fraud would be the creation of a Digit Manipulation entry which results in an extremely short dialed sequence. Once the call routes using this entry, few or no digits will be outpulsed to the Trunk, which may then wait for more digits. The caller can then enter more digits from their keypad, potentially allowing them to make calls that bypass AAR/ARS rules for both entries and sequence length.

Analysis

The following tables list all of the AAR/ARS entries in your Communication Server for which the high-level AAR/ARS digit manipulations are applied. For each entry, we list the number of digits that are deleted, the digits which are inserted and an example of what the entry would become after manipulation. All manipulated sequences should be checked for accuracy to ensure calls are being routed as expected. We highlight those entries which can result in fewer than three outpulsed digits, as these entries can be exploited by users dialing extra digits after the AAR/ARS analysis.

AAR Table Manipulations

Entry	# Deleted Digits	Inserted Digits	Becomes	Min Length	Next Type	Analysis	Applies in Location
No digit conversions were detected in your AAR Digit Conversion table.							

ARS Table Manipulations

Entry	# Deleted Digits	Inserted Digits	Becomes	Min Length	Next Type	Analysis	Applies in Location
No digit conversions were detected in your ARS Digit Conversion table.							

The following tables list all the AAR/ARS entries in your Communication Server which ultimately point to Route Patterns that perform digit manipulation. For each entry, we list the number of digits that are deleted, the digits which are inserted, an example of what the entry would become after manipulation, and the fewest number of digits that can result from the entry. All manipulated sequences should be checked for accuracy to ensure calls are being routed

as expected. We highlight those entries which can result in fewer than three outpulsed digits, as these entries can be exploited by users dialing extra digits after the AAR/ARS analysis.

AAR Route Pattern Manipulations

Entry	Route Pattern	Pref	# Deleted Digits	Inserted Digits	Becomes	Min Length	Analysis
710	21	1	3	1845123	1845123	11	
710	21	2	7	-		0	Empty sequence
711	22	1	3	1201476	1201476	11	
711	22	2	3	1201476	1201476	11	
712	23	1	7	90	90	2	Fewer than 3 digits
712	23	2	3	1310205	1310205	11	
717	20	1	3	1212332	1212332	11	
717	20	2	3	1212332	1212332	11	

ARS Route Pattern Manipulations

Entry	Route Pattern	Pref	# Deleted Digits	Inserted Digits	Becomes	Min Length	Analysis
No digit manipulations were detected in any Route Patterns used by your ARS tables.							

Unused Route Patterns

The following Route Patterns do not appear to be in use by your AAR/ARS system. Those which define digit manipulations are highlighted. It is recommended that you review these Route Patterns and consider deleting any that will not be used.

Route Pattern	Pref	FRL	# Deleted Digits	Inserted Digits
7	1	3		

9.5. High Toll Calling

Description

The AAR/ARS tables determine which Route Pattern is used to route calls to particular locations. Each area code or local exchange is assigned a Route Pattern or Partition Group that defines the Trunk Groups available for calls to that particular destination. Each entry within the AAR/ARS tables has a maximum and minimum number of digits expected.

Security Concerns

It is critical to make sure calls such as 1-900 pay services, area codes known for their high toll abuse (i.e. 809), and international area codes be properly restricted in your AAR/ARS 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 minimum and maximum expected length to prevent users from truncating CDR records by pausing during the dialing sequence. It is possible to inadvertently allow calls to numbers you intend to restrict through the inclusion of higher-priority entries, especially involving the use of the wildcard character 'x', so every rule that is added to the AAR/ARS tables should be inspected for possible side-effects.

Even with appropriate and sufficient AAR/ARS tables, toll fraud can still be achieved through misconfiguration of the Digit Manipulation feature of the Route Patterns. Please refer to the Digit Manipulation section for details on this feature.

Analysis

Foreign Area Codes

Pattern: 1-236-xxx-xxxx (Canada)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
123	11	11	ARS	p2	1	2	Any
123	11	11	ARS	p2	2	6	Any
123	11	11	ARS	p2	3	2	Any

Pattern: 1-246-xxx-xxxx (Barbados)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1246	11	11	ARS	p3	1	5	Any
1246	11	11	ARS	p3	2	6	Any
1246	11	11	ARS	p3	3	5	Any

Pattern: 1-249-xxx-xxxx (Canada)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
124	11	11	ARS	p2	1	2	Any
124	11	11	ARS	p2	2	6	Any
124	11	11	ARS	p2	3	2	Any

Pattern: 1-264-xxx-xxxx (Anguilla)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1264	11	11	ARS	p3	1	5	Any
1264	11	11	ARS	p3	2	6	Any
1264	11	11	ARS	p3	3	5	Any

Pattern: 1-268-xxx-xxxx (Antigua & Barbuda)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1268	11	11	ARS	p3	1	5	Any
1268	11	11	ARS	p3	2	6	Any
1268	11	11	ARS	p3	3	5	Any

Pattern: 1-343-xxx-xxxx (Canada)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
134	11	11	ARS	p2	1	2	Any
134	11	11	ARS	p2	2	6	Any
134	11	11	ARS	p2	3	2	Any

Pattern: 1-345-xxx-xxxx (Cayman Is.)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1345	11	11	ARS	p3	1	5	Any
1345	11	11	ARS	p3	2	6	Any
1345	11	11	ARS	p3	3	5	Any

Pattern: 1-365-xxx-xxxx (Canada)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
136	11	11	ARS	p2	1	2	Any
136	11	11	ARS	p2	2	6	Any
136	11	11	ARS	p2	3	2	Any

Pattern: 1-431-xxx-xxxx (Canada)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
143	11	11	ARS	p2	1	2	Any
143	11	11	ARS	p2	2	6	Any
143	11	11	ARS	p2	3	2	Any

Pattern: 1-437-xxx-xxxx (Canada)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
143	11	11	ARS	p2	1	2	Any
143	11	11	ARS	p2	2	6	Any
143	11	11	ARS	p2	3	2	Any

Pattern: 1-473-xxx-xxxx (Grenada)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1473	11	11	ARS	p3	1	5	Any
1473	11	11	ARS	p3	2	6	Any
1473	11	11	ARS	p3	3	5	Any

Pattern: 1-579-xxx-xxxx (Canada)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
157	11	11	ARS	p2	1	2	Any
157	11	11	ARS	p2	2	6	Any
157	11	11	ARS	p2	3	2	Any

Pattern: 1-581-xxx-xxxx (Canada)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
158	11	11	ARS	p2	1	2	Any
158	11	11	ARS	p2	2	6	Any
158	11	11	ARS	p2	3	2	Any

Pattern: 1-587-xxx-xxxx (Canada)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
158	11	11	ARS	p2	1	2	Any
158	11	11	ARS	p2	2	6	Any
158	11	11	ARS	p2	3	2	Any

Pattern: 1-639-xxx-xxxx (Canada)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
163	11	11	ARS	p2	1	2	Any
163	11	11	ARS	p2	2	6	Any
163	11	11	ARS	p2	3	2	Any

Pattern: 1-649-xxx-xxxx (Turks & Caicos Is.)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1649	11	11	ARS	p3	1	5	Any
1649	11	11	ARS	p3	2	6	Any
1649	11	11	ARS	p3	3	5	Any

Pattern: 1-664-xxx-xxxx (Montserrat)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1664	11	11	ARS	p3	1	5	Any
1664	11	11	ARS	p3	2	6	Any
1664	11	11	ARS	p3	3	5	Any

Pattern: 1-721-xxx-xxxx (St. Martin)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
172	11	11	ARS	p2	1	2	Any
172	11	11	ARS	p2	2	6	Any
172	11	11	ARS	p2	3	2	Any

Pattern: 1-758-xxx-xxxx (St. Lucia)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1758	11	11	ARS	p3	1	5	Any
1758	11	11	ARS	p3	2	6	Any
1758	11	11	ARS	p3	3	5	Any

Pattern: 1-767-xxx-xxxx (Dominica)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1767	11	11	ARS	p3	1	5	Any
1767	11	11	ARS	p3	2	6	Any
1767	11	11	ARS	p3	3	5	Any

Pattern: 1-778-xxx-xxxx (Canada)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1778	11	11	ARS	p3	1	5	Any
1778	11	11	ARS	p3	2	6	Any
1778	11	11	ARS	p3	3	5	Any

Pattern: 1-784-xxx-xxxx (St. Vincent & The Grenadines)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1784	11	11	ARS	p3	1	5	Any
1784	11	11	ARS	p3	2	6	Any
1784	11	11	ARS	p3	3	5	Any

Pattern: 1-849-xxx-xxxx (Dominican Republic)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
184	11	11	ARS	p2	1	2	Any
184	11	11	ARS	p2	2	6	Any
184	11	11	ARS	p2	3	2	Any

Pattern: 1-868-xxx-xxxx (Trinidad & Tobago)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1868	11	11	ARS	p3	1	5	Any
1868	11	11	ARS	p3	2	6	Any
1868	11	11	ARS	p3	3	5	Any

Pattern: 1-869-xxx-xxxx (St. Kitts & Nevis)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1869	11	11	ARS	p3	1	5	Any
1869	11	11	ARS	p3	2	6	Any
1869	11	11	ARS	p3	3	5	Any

Pattern: 1-873-xxx-xxxx (Canada)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
187	11	11	ARS	p2	1	2	Any
187	11	11	ARS	p2	2	6	Any
187	11	11	ARS	p2	3	2	Any

Pattern: 1-876-xxx-xxxx (Jamaica)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1876	11	11	ARS	p3	1	5	Any
1876	11	11	ARS	p3	2	6	Any
1876	11	11	ARS	p3	3	5	Any

High Toll/Fraud Area Codes and Exchanges

Pattern: xxx-976-xxxx (High Toll Exchange)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
011	10	23	ARS	p3	1	5	Any
011	10	23	ARS	p3	2	6	Any
011	10	23	ARS	p3	3	5	Any
714	10	10	ARS	2		2	Any

Pattern: 1-205-924-xxxx (976 Lookalike)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
120	11	11	ARS	p2	1	2	Any
120	11	11	ARS	p2	2	6	Any
120	11	11	ARS	p2	3	2	Any

Pattern: 1-212-550-xxxx (976 Lookalike)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
121	11	11	ARS	p2	1	2	Any
121	11	11	ARS	p2	2	6	Any
121	11	11	ARS	p2	3	2	Any

Pattern: 1-212-970-xxxx (976 Lookalike)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
121	11	11	ARS	p2	1	2	Any
121	11	11	ARS	p2	2	6	Any
121	11	11	ARS	p2	3	2	Any

Pattern: 1-315-540-xxxx (976 Lookalike)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
131	11	11	ARS	p2	1	2	Any
131	11	11	ARS	p2	2	6	Any
131	11	11	ARS	p2	3	2	Any

Pattern: 1-505-960-xxxx (976 Lookalike)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
150	11	11	ARS	p2	1	2	Any
150	11	11	ARS	p2	2	6	Any
150	11	11	ARS	p2	3	2	Any

Pattern: 1-518-970-xxxx (976 Lookalike)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
151	11	11	ARS	p2	1	2	Any
151	11	11	ARS	p2	2	6	Any
151	11	11	ARS	p2	3	2	Any

Pattern: 1-603-940-xxxx (976 Lookalike)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
160	11	11	ARS	p2	1	2	Any
160	11	11	ARS	p2	2	6	Any
160	11	11	ARS	p2	3	2	Any

Pattern: 1-610-936-xxxx (976 Lookalike)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
161	11	11	ARS	p2	1	2	Any
161	11	11	ARS	p2	2	6	Any
161	11	11	ARS	p2	3	2	Any

Pattern: 1-268-xxx-xxxx (High Fraud Area Code)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1268	11	11	ARS	p3	1	5	Any
1268	11	11	ARS	p3	2	6	Any
1268	11	11	ARS	p3	3	5	Any

Pattern: 1-473-xxx-xxxx (High Fraud Area Code)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1473	11	11	ARS	p3	1	5	Any
1473	11	11	ARS	p3	2	6	Any
1473	11	11	ARS	p3	3	5	Any

Pattern: 1-649-xxx-xxxx (High Fraud Area Code)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1649	11	11	ARS	p3	1	5	Any
1649	11	11	ARS	p3	2	6	Any
1649	11	11	ARS	p3	3	5	Any

Pattern: 1-664-xxx-xxxx (High Fraud Area Code)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1664	11	11	ARS	p3	1	5	Any
1664	11	11	ARS	p3	2	6	Any
1664	11	11	ARS	p3	3	5	Any

Pattern: 1-758-xxx-xxxx (High Fraud Area Code)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1758	11	11	ARS	p3	1	5	Any
1758	11	11	ARS	p3	2	6	Any
1758	11	11	ARS	p3	3	5	Any

Pattern: 1-767-xxx-xxxx (High Fraud Area Code)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1767	11	11	ARS	p3	1	5	Any
1767	11	11	ARS	p3	2	6	Any
1767	11	11	ARS	p3	3	5	Any

Pattern: 1-784-xxx-xxxx (High Fraud Area Code)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1784	11	11	ARS	p3	1	5	Any
1784	11	11	ARS	p3	2	6	Any
1784	11	11	ARS	p3	3	5	Any

Pattern: 1-849-xxx-xxxx (High Fraud Area Code)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
184	11	11	ARS	p2	1	2	Any
184	11	11	ARS	p2	2	6	Any
184	11	11	ARS	p2	3	2	Any

Pattern: 1-868-xxx-xxxx (High Fraud Area Code)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1868	11	11	ARS	p3	1	5	Any
1868	11	11	ARS	p3	2	6	Any
1868	11	11	ARS	p3	3	5	Any

Pattern: 1-876-xxx-xxxx (High Fraud Area Code)

Dial String	Min Digits	Max Digits	Table	Route Pattern	Partition Group Number	Route Pattern FRL	Applies in Location
1876	11	11	ARS	p3	1	5	Any
1876	11	11	ARS	p3	2	6	Any
1876	11	11	ARS	p3	3	5	Any

9.6. International Calling

Description

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

Security Concerns

The high expense of international calls is the primary reason to restrict this capability to only those users who require it. If your organization does not have a need to regularly call internationally, you should consider requiring an Authorization Code to place these calls. It is also recommended that the Route Patterns allowing international calls require an FRL greater than 0 on all entries to appropriately limit the resources that can use them. As this topic only addresses ARS dialing, you should also reference the Direct Trunk Access topic to investigate the ability to dial internationally without using ARS.

Analysis

The lowest FRL required to access the Route Pattern(s) associated with your international network translation entry, 011, is 5. This programming should be reviewed to ensure that only stations and trunks with a requirement to dial internationally are allowed to do so.

The following stations appear to be able to access international route patterns based on FRL, and should be reviewed for appropriateness:

Extension	Name	Equipment Type	COR	FRL	Location
2420	Aaron Bennett	6424D+	5	5	
6544	Adam Gray	6408D+	5	5	2
6545	Barbara Grant	6416D+	5	5	1
6546	Benjamin Ward	6408D+	5	5	1
6547	Carlos Henderson	6408D+	5	5	1
6548	Carol Berry	6408D+	5	5	2
6549	Danielle Newman	6408D+	5	5	1
6551	Edna Jensen	6416D+	5	5	2
6552	Ernest Long	6416D+	5	5	2
6553	Florence Douglas	6408D+	5	5	1
6554	Frederick Hicks	6408D+	14	5	2
6556	George Martin	6408D+	5	5	2
6557	Gloria Vasquez	2500	14	5	1
6559	First Floor Fax	FAX	14	5	1
6580	Janet Sims	6424D+	5	5	1
6581	Jerry Nelson	6416D+	5	5	1
6582	Kathryn Reid	6416D+	5	5	2
6583	Kyle Simpson	6416D+	5	5	1
6584	Lillian Bowman	6416D+	5	5	2
6585	Luis Graham	6416D+	5	5	2

Extension	Name	Equipment Type	COR	FRL	Location
6586	Marjorie Horton	6416D+	5	5	2
6587	Miguel Daniels	6416D+	14	5	1
6588	Nicholas Cox	6416D+	5	5	2
6589	Pauline Sutton	6416D+	5	5	1
6590	Ralph Cooper	6416D+	5	5	1
6591	Ricky Kennedy	6416D+	5	5	2
6592	Samuel Bailey	6416D+	5	5	1
6593	Sharon Arnold	POLY	5	5	1
6594	Teresa Schmidt	6408D+	14	5	1
6595	VDN	6408D+	14	5	
6596	Victoria Herrera	6408D+	5	5	2
6597	Wanda Gilbert	6408D+	5	5	

The following Trunk Groups appear to be able to access international route patterns based on FRL, and should be reviewed for appropriateness:

Trunk Group Number	Name	COR	FRL	Location
No Trunk Groups can access FRL 5.				

10. Voice Mail Ports

The power and flexibility of modern Voice Mail applications make them a common target of hackers attempting to gain unauthorized access to a Communication Server. Because of this, the Communication Server interface to the Voice Mail system demands special scrutiny. The following sections analyze the configuration of this system's Voice Mail ports to limit their vulnerability.

10.1. Voice Mail Ports Class of Restriction (COR)

Description

Avaya recommends that all Voice Mail ports be configured with specific settings to increase the security of the application. By assigning specific COR settings, the ports can be restricted from calling out altogether, or be limited by your AAR/ARS configuration.

Security Concerns

If the outcalling feature of the Voice Mail is not needed, Avaya recommends configuring the COR with a Calling Party Restriction (CPR) of "outward". If outcalling is necessary, then it is recommended that you review your AAR/ARS configuration to ensure that is it limited as much as possible. Voice Mail ports with a high FRL are less restricted by AAR/ARS, so Avaya recommends an FRL assignment of 0. By restricting the COR of the Voice Mail ports from the COR of the Trunk Groups in your system (using COR-to-COR permissions), you can prevent the Voice Mail from calling a Trunk Access Code and providing external dialtone. For ease of administration and increased security, the Voice Mail ports should be assigned their own unique COR.

Analysis

All Voice Mail extension ports share the same COR, as recommended.

The following are the CORs that appear to contain Voice Mail ports:

COR: 77

This COR is unique to Voice Mail ports, as recommended.

The FRL of this COR is set to 0, as recommended.

The Calling Party Restriction (CPR) of this COR is set to "none".

COR 77 is not restricted from accessing the following Trunk Group CORs: 94. It is recommended that you restrict Voice Mail from directly accessing Trunk Groups and instead use ARS for outgoing call routing.

The following CORs are not restricted from accessing COR 77: 2-4, 6-13 and 15-95.

The following Voice Mail station ports are assigned to COR 77:

Extension	Name	Port	Location
5004	VOICE MAIL PORT 1	01A0701	1
5005	VOICE MAIL PORT 2	01A0702	1
5006	VOICE MAIL PORT 3	01A0703	1
5007	VOICE MAIL PORT 4	01A0704	1

The following Voice Mail trunk ports are assigned to COR 77:

Trunk Group Num	Member Num	Port	Name	Location
No Voice Mail trunk ports were detected.				

10.2. Voice Mail Ports Class of Service (COS)

Description

Avaya recommends that all Voice Mail ports be configured with specific settings to increase the security of the application. By assigning specific COS settings, the ports can be restricted from having certain high-risk features enabled.

Security Concerns

Avaya recommends that the Voice Mail ports be in their own unique Class of Service (COS). Call Forwarding for all Voice Mail ports should be disabled. Call Forwarding Off-Net should be restricted. Console Permissions, Data Privacy, and Trunk-to-Trunk Transfer Override should all be denied. By restricting these features, your Voice Mail ports are less likely to be used for toll fraud/abuse.

Analysis

All Voice Mail ports share the same COS, as recommended.

The following are the COSs that appear to contain Voice Mail ports:

COS: 1

This COS is not unique to Voice Mail ports.

Call Forward-All Calls is enabled for this COS.

Call Forwarding Busy/DA is disabled for this COS, as recommended.

Restrict Call Forward-Off Net is enabled for this COS, as recommended.

Console Permissions are disabled for this COS, as recommended.

Data Privacy is enabled for this COS.

Trunk-to-Trunk Transfer is enabled for this COS.

The following Voice Mail ports are assigned to COS 1:

Extension	Name	Port	Location
5004	VOICE MAIL PORT 1	01A0701	1
5005	VOICE MAIL PORT 2	01A0702	1
5006	VOICE MAIL PORT 3	01A0703	1
5007	VOICE MAIL PORT 4	01A0704	1

10.3. Voice Mail Port Configuration

Description

Avaya recommends that all Voice Mail ports be configured with "Switchhook Flash" enabled and "Distinctive Audible Alert" disabled.

Security Concerns

Unauthorized individuals have been known to exploit the misconfiguration of Voice Mail ports to return secondary dialtone, allowing them to make calls from your Communication Server.

It is especially important to disable Distinctive Audible Alert on any adjunct port (fax machines, Voice Mail, Voice Recognition ports) as these are the most common areas of attack and are not physically monitored by a person.

Analysis

The following stations have been identified as incorrectly configured Voice Mail station ports:

Extension	Name	Type	Switchhook Flash	Distinctive Audible Alert	Location
5005	VOICE MAIL PORT 2	VMAIL	N	Y	1
5006	VOICE MAIL PORT 3	VMAIL	Y	Y	1
5007	VOICE MAIL PORT 4	VMAIL	N	N	1

11. Voice Recognition Units

Like Voice Mail, Voice Recognition applications can be exploited to gain elevated capabilities, and require special attention. The following sections analyze the configuration of this system's Voice Recognition ports to limit their vulnerability.

11.1. Voice Recognition Ports Class of Restriction (COR)

Description

Avaya recommends that all Voice Recognition ports be configured with specific settings to increase the security of the application. By assigning specific COR settings, the ports can be restricted from calling out altogether, or be limited by your AAR/ARS configuration.

Security Concerns

If off-net calling for Voice Recognition ports is not needed, Avaya recommends configuring the COR with a Calling Party Restriction (CPR) of "outward". If off-net calling is necessary, then it is recommended that you review your AAR/ARS configuration to ensure that it is limited as much as possible. Voice Recognition ports with a high FRL are less restricted by AAR/ARS, so Avaya recommends an FRL assignment of 0. By restricting the COR of the Voice Recognition ports from the COR of the Trunk Groups in your system (using COR-to-COR permissions), you can prevent the Voice Recognition ports from calling a Trunk Access Code and providing external dialtone. For ease of administration and increased security, the Voice Recognition ports should be assigned their own unique COR.

Analysis

No Voice Recognition ports were detected.

11.2. Voice Recognition Ports Class Of Service (COS)

Description

Avaya recommends that all Voice Recognition ports be configured with specific settings to increase the security of the application. By assigning specific COS settings, the ports can be restricted from having certain high-risk features enabled.

Security Concerns

Avaya recommends that the Voice Recognition ports be in their own unique Class of Service (COS). Call Forwarding for all Voice Recognition ports should be disabled. Call Forwarding Off-Net should be restricted. Console Permissions, Data Privacy, and Trunk-to-Trunk Transfer Override should all be denied. By restricting these features, your Voice Recognition ports are less likely to be used for toll fraud/abuse.

Analysis

No Voice Recognition station ports were detected.

11.3. Voice Recognition Port Configuration

Description

Avaya recommends that all Voice Recognition ports be configured with "Switchhook Flash" enabled and "Distinctive Audible Alert" disabled.

Security Concerns

Unauthorized individuals have been known to exploit the misconfiguration of Voice Recognition ports to return secondary dialtone, allowing them to make calls from your Communication Server.

It is especially important to disable Distinctive Audible Alert on any adjunct port (fax machines, Voice Mail, Voice Recognition ports) as these are the most common areas of attack and are not physically monitored by a person.

Analysis

No Voice Recognition station ports were detected.

12. Vectors and Vector Directory Numbers

The following section analyzes various aspects of this system's Vectors and Vector Directory Numbers.

12.1. Vectors

Description

Vectors are a collection of steps used to handle the routing of calls. These steps can be used to collect digits from the caller and route the call to another destination.

Security Concerns

If not configured properly, a Vector could allow an unauthorized user to enter digits that establish an off-premise call. All Vectors with steps to collect digits and route calls should be reviewed to ensure that they are restricted as much as possible. Any Vector that includes a route-to step to an off-premise number should be checked to ensure the legitimacy of that number.

Analysis

The following Vectors in your Communication Server have been identified as having "collect" steps. These Vectors should be reviewed to determine how the collected digits are being used. Steps which have been programmed but are currently 'commented-out' are not currently active, and are shown with a checkmark in the 'Disabled' column.

Vector Number	Vector Name	Step Number	Disabled
1	MAIN MENU	7	
1	MAIN MENU	12	
2	SALES	3	
10	THANK YOU	3	

The following Vectors in your Communication Server have been identified as having "route-to" steps. Any steps which appear to route to an external destination are highlighted for review. Steps which have been programmed but are currently 'commented-out' are not currently active, and are shown with a checkmark in the 'Disabled' column.

Vector Number	Vector Name	Step Number	Route-To Destination	Disabled
1	MAIN MENU	8	6546	
1	MAIN MENU	9	6546	
1	MAIN MENU	10	6546	
1	MAIN MENU	13	6546	
1	MAIN MENU	14	Collected Digits	
2	SALES	4	6546	
2	SALES	5	Collected Digits	
2	SALES	11	919005551212	
2	SALES	13	6546	
2	SALES	15	6546	
2	SALES	17	6546	
2	SALES	19	6546	
2	SALES	21	6546	
10	THANK YOU	4	6546	
10	THANK YOU	5	Collected Digits	

12.2. Vector Directory Numbers Class Of Restriction (COR)

Description

Vector Directory Numbers (VDN) are "soft extensions" in the Communication Server that direct a call to a Vector. If the call is re-routed by the Vector, the call carries the Facility Restriction Level (FRL) and Calling Party Restrictions (CPR) of the VDN.

Security Concerns

You should assign the lowest possible FRL and most restrictive CPR (preferably "outward") to the COR used by VDNs. Facility Test Call should also be denied in the COR programming, as unauthorized users can possibly exploit the feature to generate calls without the restrictions or AAR/ARS. Avaya recommends that any CORs assigned to your VDNs are not used by other facilities (e.g., stations).

Analysis

All VDNs share the same COR, as recommended.

The following CORs are in use by VDNs in your Communication Server:

COR: 8

This COR is unique to VDNs, as recommended.

The FRL of this COR is set to 0, as recommended.

The Calling Party Restriction (CPR) of this COR is set to "outward".

COR 8 is not restricted from accessing the following Trunk Group CORs: 95. It is recommended that you restrict VDNs from directly accessing Trunk Groups and instead use ARS for outgoing call routing.

The following CORs are not restricted from accessing COR 8: 0-95.

Facility Test Call is disabled for this COR, as recommended.

The following Vector Directory Numbers are assigned to COR 8. Any vector with a "collect" or "route-to" step is highlighted and should be reviewed. See the "Vectors" section for details.

VDN	Name	Vector Number
6595	VDN	1

Command Objects in Profile Categories

The following table lists all of the Profile object categories in your Communication Server, along with the Objects associated with them. This Appendix can be used in concert with the "Login Privileges (Profiles)" Section in order to better understand those Objects that a Custom Profile might have access to.

Command Objects in Profile Categories Listing

Category Name	Command Object Name
Adjuncts	
	adjunct-names
	aesvcs cti-link
	aesvcs interface
	aesvcs link
	aesvcs-server
	comm-intf proc-chan
	communication-interface links
	intra-switch-cdr
	mis
	processor-ip-interface
Call Center	
	agent
	agent-loginID
	announcement
	bcms agent
	bcms skill/split
	bcms summary agent
	bcms summary skill/split
	bcms summary trunk
	bcms summary vdn
	bcms system
	bcms trunk
	bcms vdn
	bcms-vustats loginIDs
	best-service-routing
	crm-features
	meet-me-vdn
	mg-key
	page-link
	service-hours-table
	skill-status
	unstaffed-agents
	variables
	vdn
	vector

Category Name	Command Object Name
	vrt
	vustats-display-format
Features	
	abbreviated-dialing 7103-buttons
	abbreviated-dialing enhanced
	abbreviated-dialing group
	abbreviated-dialing personal
	abbreviated-dialing system
	administered-connection
	alternate-frl
	audio-group
	carrier-frequencies
	conference
	directory
	extended-pickup-group
	group-page
	groups-of-extension
	hunt-group
	intercom-group
	list node-names
	mct-group-extensions
	mct-history
	members hunt-group
	members trunk-group
	mmi
	monitored-station
	music-sources
	night-service attendant-group
	night-service hunt-group
	night-service trunk-group
	node-names audix
	node-names ip
	paging code-calling-ids
	paging loudspeaker
	pickup-group
	tenant
	term-ext-group
	tti-ip-stations
	tti/psa
Hardware	
	atm board (status)
	atm pnc
	atm pnc-pairs
	atm ports

Category Name	Command Object Name
	atm trunk-board
	atm wsp
	board
	boot-image
	bri-port
	bri-trunk-board
	cabinet
	carrier
	cau
	circuit-packs
	data-module
	ds1
	ds1-facility
	ds1-loop
	eda-external-device-alrm
	firmware download
	firmware radio-controller
	firmware station-download
	firmware wfb
	firmware-counters
	hardware-group
	integrated-annc-boards
	ip-interface
	ipserver-interface
	led
	media-gateway
	media-processor all
	media-processor board
	pkt
	pnc & pnc-standby
	port
	port-location
	port-network
	radio-controller
	session
	status media-gateways
	tdm
	tone-clock
	val
	val-ip
	virtual-mac-address
Hospitality	
	do-not-disturb group
	do-not-disturb station

Category Name	Command Object Name
	journal-link wakeup-log
	journal-printer pms-log
	journal-printer wakeup-log
	pms-down
	pms-link
	wakeup incomplete
	wakeup requests
	wakeup station
IP	
	ethernet-options
	failed-ip-network-region
	ip-address
	ip-board
	ip-codec-set
	ip-hoteling
	ip-network-map
	ip-network-region
	ip-network-region monitor
	ip-network-region qos
	ip-parameters
	ip-reg-tti
	ip-registration
	ip-route
	ip-services
	registered-ip-stations
Maintenance	
	amw all
	amw asai
	amw audix
	amw pms
	analog-testcall board
	analog-testcall port
	analog-testcall trunk
	arp
	bulletin-board
	cdr-link primary
	cdr-link secondary
	clan-all
	clan-ip
	clan-port
	clan-usage
	configuration all
	configuration atm
	configuration board

Category Name	Command Object Name
	configuration carrier
	configuration circuit-pack
	configuration control
	configuration ds1
	configuration license
	configuration media-gateway
	configuration port-network
	configuration power-supply
	configuration radio-controller
	configuration software-versions
	configuration stations
	configuration trunks
	configuration wt-stations
	cti-link
	customer-alarm
	environment
	errors
	esm
	events
	fiber-link
	file
	filesystem
	filexfer
	health
	initcauses
	integ-annc-brd-loc
	internal-dat bept_rec & bri-port
	internal-data atd-port
	internal-data bconf-tab
	internal-data bhist-tab
	internal-data callr
	internal-data conf-tab
	internal-data ext-map
	internal-data hunt-group
	internal-data isg-callr
	internal-data isg-cnfr
	internal-data loginID
	internal-data mmi-tab
	internal-data off-pbx-telephone
	internal-data s-tab
	internal-data sta-port
	internal-data susr_rec
	internal-data trk-port
	internal-data uid-map

Category Name	Command Object Name
	internal-data vc-tab
	internal-data wireless-terminal
	license
	link
	maintenance
	marked-ports
	mo-all
	modem-pool
	mst
	np-registration
	packet-interface
	periodic-scheduled
	ping node-name
	power-shutdown
	radio-sync all
	radio-sync port-network
	report-scheduler
	shell
	socket-usage
	sp-link
	survivable-processor
	suspend-alm-orig
	sys-link
	system
	system conn
	system scr
	system view1
	system view2
	test-schedule
	testcalls detail
	testcalls summary
	tone-generation
	trace advocate agent
	trace advocate skill
	trace attendant
	trace data-module
	trace ewt high
	trace ewt low
	trace ewt medium
	trace ewt top
	trace media-gateway
	trace media-gateway identifier
	trace media-gateway ip-address
	trace page-links

Category Name	Command Object Name
	trace previous
	trace ras forced_urqs
	trace ras ip-address
	trace ras ip-stations
	trace station
	trace tac
	trace vdn
	trace vector
Measurements and Performance	
	alarms
	capacity
	meas call-rate service-link
	meas ds1-facilit esf-error-event
	meas ds1-facilit loopback/span-t
	meas expansion-services-mod hour
	meas expansion-services-mod sum
	meas ip dsp-resource detail
	meas ip dsp-resource hourly
	meas ip dsp-resource summary
	meas load-balance incoming
	meas load-balance intercom
	meas load-balance outgoing
	meas multimedia-interface hourly
	meas multimedia-interface sum
	meas occupancy busiest-intervals
	meas security-violations summary
	meas tone-receiver detail
	meas tone-receiver summary
	meas voice-conditioners hourly
	meas voice-conditioners summary
	meas wideband-trunk-group hourly
	meas wideband-trunk-group sum
	meas-selection coverage
	meas-selection principal
	meas-selection route-pattern
	meas-selection trunk-group
	meas-selection wideband-trunk-gr
	measurements aca
	measurements announce integ-all
	measurements announcements all
	measurements announcements board
	measurements atm board
	measurements atm latency-histogr

Category Name	Command Object Name
	measurements atm pnc-latency
	measurements atm setup-events
	measurements attendant group
	measurements attendant positions
	measurements blockage pn
	measurements blockage sn
	measurements call-rate data
	measurements call-rate multimedi
	measurements call-rate total
	measurements call-rate voice
	measurements call-summary
	measurements cbc-trunk-group
	measurements cell-traf cell-addr
	measurements cell-traf summary
	measurements clan ethernet
	measurements clan ppp
	measurements clan sockets detail
	measurements clan sockets hourly
	measurements clan sockets sumary
	measurements comm-link 33
	measurements comm-links 1-8
	measurements comm-links 17-24
	measurements comm-links 25-32
	measurements comm-links 9-16
	measurements coverage-path
	measurements ds1 esf-error-event
	measurements ds1 log
	measurements ds1 loopback/span-t
	measurements ds1 summary
	measurements ds1-facility log
	measurements ds1-facility sum
	measurements hunt-group
	measurements ip codec detail
	measurements ip codec hourly
	measurements ip codec summary
	measurements ip signaling-groups
	measurements lar-route-pattern
	measurements lightly-used-trunk
	measurements load-balance tandem
	measurements load-balance total
	measurements modem-pool
	measurements occupancy last-hour
	measurements occupancy summary
	measurements outage-trunk

Category Name	Command Object Name
	measurements principal
	measurements route-pattern
	measurements summary
	measurements trunk-group
	performance attendant
	performance hunt-group
	performance summary
	performance trunk-group
	traffic hunt-groups
	traffic trunk-groups
Remote Access	
	off-pbx-tel feature-name-ext
	off-pbx-tel mobile-feature-ext
	off-pbx-tel station-mapping
	off-pbx-telephone config-set
	remote-access
	status off-pbx-telephone station
	wfb
	wt-upgrade
	xmobile configuration-set
	xmobile mapping
Routing and Dial Plan	
	aar analysis
	aar digit-conversion
	aar route-chosen
	alphanumeric-dial-table
	ars analysis
	ars digit-conversion
	ars route-chosen
	ars toll
	calltype analysis
	calltype route-chosen
	cama-numbering
	dialplan analysis
	dialplan parameters
	digit-absorption
	emergency
	enp-number-plan
	listed-directory-numbers
	node-routing
	partition-route-table
	precedence-rout digit-conversion
	precedence-routing analysis
	precedence-routing route-chosen

Category Name	Command Object Name
	rhnpa
	route-pattern
	toll
	toll all
	toll restricted-call
	toll toll-list
	toll unrestricted-call
	uniform-dialplan
Security	
	authorization-code
	clear security-violations
	cor
	cos
	history
	logging-levels
	partitioned-group
	security-v station-security-code
	security-violations auth-code
	security-violations remote-acc
	ssh-keys
Servers	
	ess
	ess clusters
	ess port-networks
	lsp
	remote-office
	system-parameters ess
Stations	
	alias station
	attendant
	bridged-extensions
	button-labels
	button-location-aca
	button-restriction
	call-forwarding
	console-parameters
	coverage answer-group
	coverage path
	coverage remote
	coverage sender-group
	coverage time-of-day
	extension-station
	extension-type
	ip-stations

Category Name	Command Object Name
	multimedia endpoints
	multimedia h.320-stations
	multimedia ip-stations
	multimedia ip-unregistered
	personal-CO-line
	set-data
	site-data
	station
	svn-button-location
	terminal
	terminal-parameters
	tod-station lock
System Parameters	
	daylight-savings-rules
	display-mess auto-wakeup-dn-dst
	display-mess leave-word-calling
	display-mess malicious-call-trac
	display-mess misc-features
	display-mess property-management
	display-mess self-administration
	display-mess time-of-day-routing
	display-mess transfer-conference
	display-mess view-buttons
	display-messages ad-programming
	display-messages button-labels
	display-messages date-time
	display-messages posted-message
	display-messages softkey-labels
	display-messages vustats
	display-messges call-identifiers
	display-parameters
	exp-holiday-coverage-tbl
	feature-access-codes
	holiday-table
	ixc-codes
	location-parameters
	locations
	reason-code-names
	sit-treatment
	switch-node
	switch-node-clock
	system-param coverage-forwarding
	system-param customer-options
	system-param mg-recovery-rule

Category Name	Command Object Name
	system-param mode-code
	system-param multifrequency-sign
	system-parameters atm
	system-parameters cdr
	system-parameters crisis-alert
	system-parameters duplication
	system-parameters features
	system-parameters hospitality
	system-parameters ip-options
	system-parameters maintenance
	system-parameters mlpp
	system-parameters offer-options
	system-parameters sccan
	system-parameters security
	system-parameters special-apps
	system-params ipserver-interface
	tftp-server
	time
	time-of-day
Translations	
	translation
Trunking	
	(maintenance) synchronization
	aca-parameters
	access-endpoint
	call-screening
	calling-party-num-conv
	cpc-ii-conversion
	inc-call-handling-tr trunk-group
	isdn dcs-qsig-tsc-gateway
	isdn mwi-prefixes
	isdn network-facilities
	isdn private-numbering
	isdn public-unknown-numbering
	isdn qsig-dcs-tsc-gateway
	isdn tsc-gateway
	isdnpri-testcall
	multifrequency-signaling
	pri-endpoint
	private-numbering
	public-unknown-numbering
	signaling-group
	synchronization atm
	synchronization css

Category Name	Command Object Name
	synchronization port-network
	synchronization port-network ip
	tandem-calling-party-num
	telecommuting-access
	trunk
	trunk-group
	tsc-administered
	video-bridge
Usage	
	usage audio-group
	usage button-type crss-alert
	usage button-type hunt-ns
	usage button-type night-serv
	usage button-type trunk-ns
	usage comment
	usage cti-link
	usage digit-string
	usage extension
	usage forced-agent-logout
	usage holiday-table
	usage hunt-group
	usage integ-annc-board
	usage ip-address
	usage media-gateway
	usage node-name
	usage port-networks
	usage return
	usage server
	usage service-hours-table
	usage set
	usage trunk-group
	usage variables
	usage vdn-time-zone-offset
	usage vector
User Access	
	asg-key
	extended-user-profile
	login-ID
	password
	profile-base
	user-profile

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 Voice 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 Service number, 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 Voice 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, Remote Access numbers, etc. are of particular importance, but any document exposing the programming of either the Communication Server or Voice Mail can be a potential security risk. Shredding paper documents 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 Security Code, 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 login to the Communication Server. It is recommended to limit IP access to your local network, and only to authorized administrators on that network.

Glossary

Abbreviated Dialing
A feature providing station users access to system, group or personal lists allowing them to dial frequently called telephone numbers using a 1- to 3-digit code. System and Group lists may also be configured as 'privileged', thus overriding any restrictions placed on an extension.

Access Security Gateway (ASG)
A security system available to Avaya Communication Servers which use one-time challenge/response authentication and a hand-held ASG Key device to protect access to the administrative interface of the Communication Server.

Active (Coverage Paths)
A state where a user is on the phone and the instrument is capable of receiving another call on an additional call appearance button.

Audix
Avaya's Voice Mail platform for the Definity Call Servers.

Authorization Code
A code that a user may dial before placing a call to modify their Facility Restriction Level, usually to elevate their calling permissions. For example, you may require an Authorization Code before dialing international numbers to restrict their use.

Automatic Call Distribution (ACD)
A type of Hunt Group that presents incoming calls to multiple stations sequentially. These stations are called ACD Agents.

Automatic Circuit Assurance (ACA)
A feature which can monitor the holding times of trunk calls and notify personnel to unusually long or short call durations. This feature is often used to diagnose trunk malfunctions and highlight potential unauthorized use.

Automatic Route Selection (ARS)
A feature within the Communication Server which directs outbound calls to predefined Trunk Groups dependent upon the digits that were dialed.

Call Detail Recording (CDR)
A feature allowing the recording of information about selected calls, usually for cost allocation purposes.

Calling Party Restriction (CPR)
A setting within each Class of Restriction (COR) which allows or denies certain types of calls. For example, CORs with a CPR of "none" have no restriction, while CORs with a CPR of "outward" are not able to make any external calls.

Class of Restriction (COR)
Up to 96 (0 - 95) individual configurations of restrictions and permissions that control call origination and termination capabilities.

Class of Service (COS)
Assignments that determine certain calling options and features available to the telephone.

Control Circuit Packs
The circuit packs, or 'cards', not associated with stations or trunks, i.e. CPU, memory, software, and storage devices.

Coverage Answer Group
A group of up to 8 stations which act as an answer point for selected incoming calls. All phones in a Coverage Answer Group will ring simultaneously.

Coverage Path
A Coverage Path describes both the conditions under which incoming calls may be redirected and where they will be redirected.

Coverage Point
One of up to 6 answer points within a Coverage Path.

Direct Access
The ability of a station or trunk user to dial a Trunk Access Code (TAC) and receive dial-tone directly from a trunk, thus bypassing any restrictions of ARS.

Direct Inward System Access (DISA)
A general telecommunications-industry term for the Remote Access feature. See Remote Access.

DND/SAC
Do Not Disturb/Send All Calls - A feature allowing a user to temporarily deny their station the ability to receive incoming calls.

DS1
Refers to a digital signal trunking facility, e.g., T1.

Extension
A dialable number assigned to a station, data module, Hunt Group, Terminating Extension Group, Vector, etc.

External Number
When used in this audit, an 'external number' refers to a sequence of at least seven digits beginning with an AAR, ARS, or Trunk Group Access Code. These calls will potentially hit the public network and incur toll expenses.

Facility Restriction Level (FRL)
An FRL is assigned to each Class of Restriction (COR) and is used to allow or deny access to specific Trunk Groups. An FRL of 0 is the most restrictive, while 7 is the least restrictive and can commonly access more facilities.

Facility Test Call
A feature which allows a technician to place calls directly to specific trunks or phones for testing and problem diagnosis, bypassing the normal permission restrictions.

Feature Access Code
A one to four digit code dialed by a user to activate a particular feature. For example, an administrator could define '*12' be used to activate the Call Park feature.

Hunt Group
Allows a call to a busy extension to be redirected to an idle extension within the group.

INADS Port
Initialization and Administration System Port - A port on the Communication Server which provides remote administrative access to Communication Server programming.

Intercom Group
A grouping of stations that have the ability to call each other by using a 1- or 2-digit code.

LWC Reception
A setting within station programming which tells the Communication Server where Leave Word Calling information will be stored.

NETCON Port
A NETwork CONtrol data module which provides administrative access to the Avaya Communication Server.

Operations Support System (OSS)
An alarm monitoring and notification system in the Avaya Communication Server that can inform personnel of unusual system events.

PBX
Private Branch eXchange - A private telephone system which provides connectivity and switching functionality for an organization.

Personal Station Access (PSA)
A feature which allows a user to associate their telephone programming with another station of the same type. This allows the user to move their programming from one phone to another. Similar to the TTI feature used by technicians.

Pickup Group
A group of stations that are able to answer calls to any of the stations within the same group.

Port
The physical location of terminal equipment using the addressing scheme of Cabinet, Carrier, Slot, Port.

Port Address
An alphanumeric value corresponding to a specific card and port within the Communication Server. Every trunk, station and Voice Mail port has a specific and unique Port Address.

Port Circuit Packs
The circuit packs, or 'cards', associated with stations and trunks, e.g. Digital Line Cards, Analog Trunk Cards, DS1 Interfaces, and Audix Voice Mail.

Privileged
A setting within the programming of System and Group Abbreviated Dialing Lists which allows all programmed entries to be dialed, regardless of the originating station's COR.

Remote Access
A feature which allows off-site personnel to dial into the Communication Server and use the facilities of the Communication Server as if they were on-site. This feature is often used by traveling employees who need to make business calls from a distant location.

Restrict Call Forward Off Net
A setting within a Class of Service (COS) which when set to 'n' allows calls to be redirected off-premise (externally).

Restricted Call List (RCL)
A listing of dialed numbers that may not be accessed by CORs with the 'Restricted Call List?' set to 'y'.

Route Pattern
A list of Trunk Groups to be used when calling specific numbers (i.e. Area Codes).

SAT
Communication Manager System Administration Terminal. The primary interface by which one configures the telephony data in an Avaya Switch.

Security Violation Notification
A system for monitoring and reporting invalid attempts to access some resource of the Communication Server. For example, one can enable notifications for invalid Login Names, Barrier Codes, or Station Security Codes. A threshold of invalid attempts is defined for each type of notification, and the Communication Server can notify personnel when the threshold is exceeded.

Simple Network Management Protocol (SNMP)
A standards-based protocol for monitoring and managing devices on an IP network. Typical devices that support SNMP include routers, switches, servers, printers, etc. An SNMP 'trap' is an unsolicited message sent from a device to a monitoring application to report a significant event, such as an alarm or critical message.

Station Type
A field in the programming of each station designating a specific model of terminal equipment.

Terminal Translation Initialization (TTI)
A feature which allows a technician to move a user's telephone programming from one station to another. Similar to the Personal Station Access (PSA) feature.

Toll-Abuse
The action of making unauthorized calls through a Communication Server.

Toll List
A listing of dialed numbers to toll calling areas.

Trunk Access Code (TAC)
A dialable code assigned to each Trunk Group which provides direct access to the group, bypassing ARS.

Trunk
A voice and/or data channel between two telecommunications facilities. Trunks connect a Communication Server to the public telephone network or other private facilities.

Trunk Group
A collection of similar trunks performing an identical function. For example, all DID trunks for the main telephone number would be members of a single Trunk Group.

Unrestricted Call List (UCL)
One of ten individual listings of dialed numbers that may be accessed by otherwise restricted stations, even if the numbers are on the Toll List.

Vector
A set of treatments performed on incoming calls which can provide customized routing, announcements, and collection of data.

Vector Directory Number (VDN)
A 'soft-extension' which is not connected to any physical hardware, but rather provides access to a single Vector.

Voice Recognition Unit (VRU)
Hardware and software within the Communication Server which provides voice recognition and response capabilities.