Lucent Technologies
Bell Labs Innovations

Lucent Gateway Platform
Feature Packages Description Guide

Part Number 255-400-012R5.1.0.1
Issue 2, June 2007
Software Version 5.1.0.1

Notice

Every effort has been made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Mandatory customer information

Safety

Always observe the Safety Instructions when operating the system.

Trademarks

All trademarks and service marks specified herein are owned by their respective companies.

Ordering information

The order number of this document is 255-400-012R5.1.0.1.

Support

Technical support

Please contact your Lucent Technologies Local Customer Support Team (LCS) for technical questions about the information in this document.

Information product support

To comment on this information product online, go to ***http://www.lucent-info.com/comments*** or email your comments to ***comments@lucent.co***m.

Introduction

This document contains the following sections:

Scope

The *Feature Packages Guide* (255-400-012) is part of the overall switch documentation set.

The *Feature Packages* provides an overview of the key Feature Packages that are supported by the Lucent Gateway Platform.

Note: For detailed descriptions and illustrations of the switching system hardware, refer to the *Lucent Gateway Platform Planning and Engineering Guide.*

This introduction describes the *Feature Packages Guide* and how it relates to other manuals within the system documentation set. It also describes the switching system documentation set. Specifically, these topics are described in this introduction:

- Scope and Audience
- Reason for Reissue
- Manual Organization
- Using the CD-ROM
- Switch Documentation

Audience

This manual is intended for personnel who would like to know more about the functions and features supported by the switch software. It may be helpful initially to the customer trying to determine whether or not the switch suits their needs, or after the sale and installation process, to the person responsible for provisioning the switch. Regardless of the person using this manual, these personnel must have a thorough knowledge of telecommunications.

Reason for Reissue

This manual was introduced for system software version 5.1.0.

Manual Organization

The manual contains detailed descriptions of key Feature Packages features supported by the switching system software, as well as the following information:

- The Introduction contains a description of the system manuals and manual organization, and general information about the system documentation.
- The Gateway MSC section describes the Gateway MSC Feature Package.
- The Enahnced Routing section describes the advanced routing features that are available on the Compact Switch and Network Controller and explains how to provision the Feature Package.
- The AIN section describes the call processing subsystem architecture flexibility to support both internal (on-board) and external features using the AIN message and parameter set.
- The 9-1-1 Service section describes the Enhanced 9-1-1 Service capabilities that are supported.
- The SIP section describes the Session Initiation Protocol and its relationship to VoIP.
- The Packetized VoIP section describes the IP call types supported by various protocols, as well as CODEC negotiation information.

Using the System Documentation CD-ROM

Like many documentation sets today, the switch documentation set is provided a CD-ROM sent to you, the customer, with the switch. When inserted into a drive, the CD-ROM will automatically open to the Main Menu page. As directed by the *Read Me First* page included in your packed materials, you can select any manual listed from the Main Menu page on the CD-ROM. Once you have selected a manual, you can move to different areas of a manual using the bookmarks on the left side of the page. Clicking on the + sign in front of a topic will expand it; clicking on the – sign will minimize it. Table of Contents information in blue font will also move you to that identified topic. Clicking on the cover page or the title of the third page (Manual Contents) will return you to the Main Menu page.

System Documentation

One set of system documentation on CD-ROM (255-400-007) is sent to you with each switch you purchase. Each set consists of, at a minimum, these core manuals and release notes:

System Documentation Set

Product	Part Number	Product Description
Lucent Gateway Platform Operations Manual	255-400-000	Contains the platform provisioning procedures.
Lucent Gateway Platform Maintenance and Troubleshooting Guide	255-400-001	Contains the procedures for adding and upgrading modules, and maintaining and troubleshooting switch alarms.
Lucent Gateway Platform TL1 Commands Reference Guide	255-400-002	Description of all the TL1 commands needed to provision the platform, functional entities and services.
Lucent Gateway Platform Planning and Engineering Guide	255-400-003	Contains the information necessary for designing an installation site including: hardware specifications; cabling schematics; and cabling, floor plan, environmental and power requirements.
Lucent Gateway Platform Product Overview Guide	255-400-004	Contains descriptions of the base switching platform, functional entities (Network Controller, Signaling Gateway; Network Gateway, Compact Switch) and supported provisioning methods.
Lucent Gateway Platform System Release Notes	255-400-006	Contains new features and feature enhancements, new and modified TL1 commands, hardware and software limitations and other important release-specific information not available elsewhere.
Lucent Gateway Platform Feature Packages Guide	255-400-012	Contains detailed feature package descriptions.
Lucent Gateway Platform Billing and Traffic Collection (BTC) Guide	255-400-403	Contains installation, upgrade, and applications procedures.

Product	Part Number	Product Description
Lucent Gateway Platform BTC Release Notes	255-400-404	Contains software features and release-specific information that is not available elsewhere.
Lucent Gateway Platform System Documentation CD-ROM	255-400-007	Contains all of the manuals and the release notes listed above in Adobe Acrobat PDF format.

Printed versions of these documents can be ordered individually, using the part numbers listed.

PlexView Documentation

Other manuals and release notes, which are available upon purchase of additional software include:

PlexView Documentation Set

Product Documentation	Part Number	Product Description
Lucent Gateway Platform Element Management System (EMS) User Guide	255-400-400	EMS provisioning reference guide.
Lucent Gateway Platform Element Management System (EMS) Installation Guide	255-400-401	Installing the EMS software on a Sun workstation.
Lucent Gateway Platform EMS Software Release Notes	255-400-402	Contains software features and release-specific information that is not available elsewhere.
Lucent Gateway Platform Billing Traffic Collection (BTC) Guide	255-400-403	Contains installation, upgrade, and applications procedures.
Lucent Gateway Platform BTC Release Notes	255-400-404	Contains software features and release-specific information that is not available elsewhere.

Product Documentation	Part Number	Product Description
Lucent Gateway Platform EMS/BTC Documentation CD-ROM	255-400-406	Contains: • EMS User Guide 255-400-400 • EMS Installation Guide 255-400-401 • EMS Software Release Notes 255-400-402 • BTC Guide 255-400-403 • BTC Release Notes 255-400-404
Lucent Gateway Platform Advanced Reporting System (ARS) User's Guide	255-400-200	ARS provisioning reference guide.
Lucent Gateway Platform Advanced Reporting System (ARS) Installation Guide	255-400-201	Installation and upgrade information for the ARS software.
Lucent Gateway Platform Advanced Reporting System (ARS) with Advanced Traffic Collector (ATC) Installation Guide	255-400-202	Provides installation and upgrade information for the ATC and ARS in sequential order.
Lucent Gateway Platform ARS Software Release Notes	255-400-203	ARS software features and release-specific information that is not available elsewhere
Lucent Gateway Platform ARS Documentation CD-ROM	255-400-204	Contains: • ARS User Guide 255-400-200 • ARS Installation Guide 255-400-201 • ARS with ATC Installation Guide 255-400-202 • ARS Software Release Notes 255-400-203

Notes:

Gateway MSC Software Feature Package

This document contains the following sections:

Executive Summary

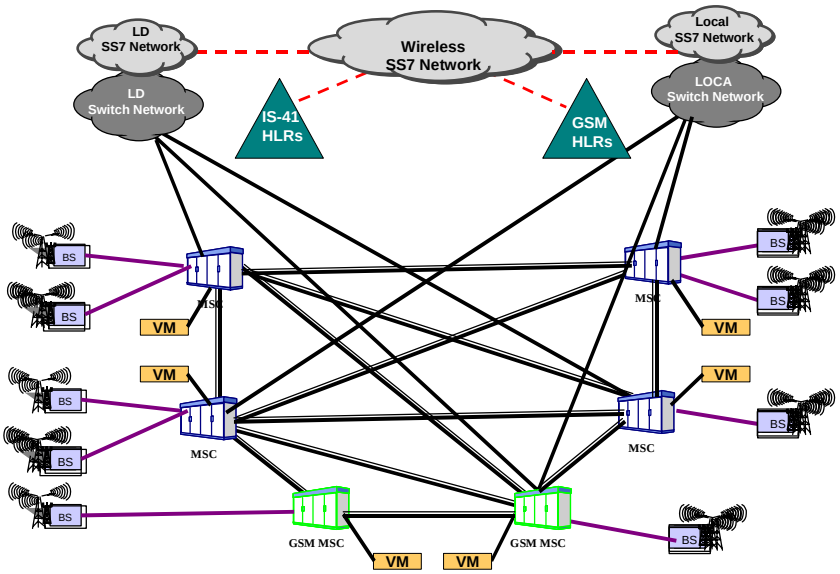
The Wireless market is growing at a rapid rate. More mobile users are connecting, each generating increasing Minutes of Use (MoU). However, as traffic rises, the CAPEX required to build out the Wireless infrastructure is increasingly disproportionate to the associated revenue increases. Wireless carriers are also in the

process of migrating to new technologies. Some are replacing TDMA systems with GSM systems and all carriers are considering the migration to third-generation (3G) networks, and associated voice over packet technologies. Additionally, Wireless carriers are mandated to provide support for Wireless Number Portability (WNP). While this can represent opportunity for Wireless carriers, allowing them to compete for other carriers' customers (potentially including wireline carriers), it also represents a significant cost in upgrades. Lucent Technologies Gateway MSC Feature Package has been designed to cost-effectively and flexibly addresses all these challenges.

Feature Package Description

Today's Wireless networks have been built using highly meshed TDM facilities. Routing between Mobile Switching Centers (MSCs) is highly inefficient. As traffic rises, CAPEX increases required to build out the Wireless infrastructure is increasingly disproportionate to increases in revenues.

Figure 1. Today’s Wireless Network



Unlike traditional wireless networks, where calls can traverse two or more legacy MSCs, the Gateway MSC Feature Package routes calls directly to the end destination, resulting in improved routing efficiency for roaming calls (which accounts for over 50% of calls), forwarded calls, and voicemail services which frees up tens of thousands of legacy MSC ports, reducing inter-MSC and PSTN

interconnection facilities, resulting in significantly lower OPEX and CAPEX increases that now match subscriber MoU increases.

The Gateway MSC Feature Package also flexibly address a number of technological and deployment challenges since it supports GSM as well as ANSI-41 on the same software load and provides further flexibility by enabling both TDM and packet based solutions that can be deployed in either an integrated switching (Figure 2) or distributed switching architecture (Figure 3).

Figure 2. Gateway MSC (Integrated Architecture)

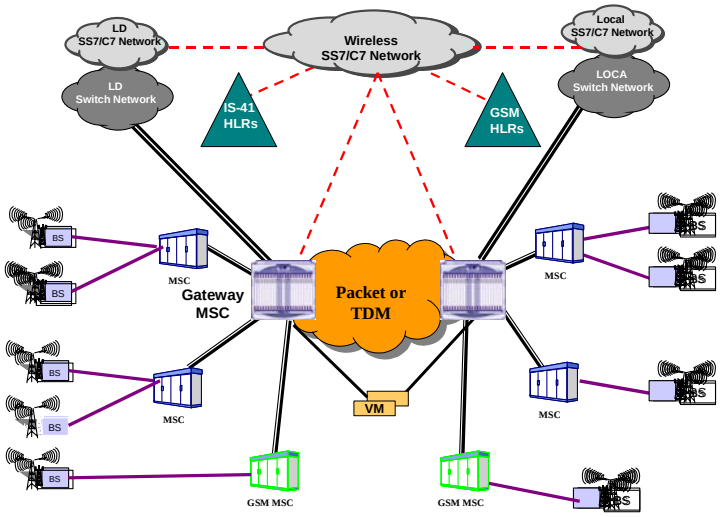
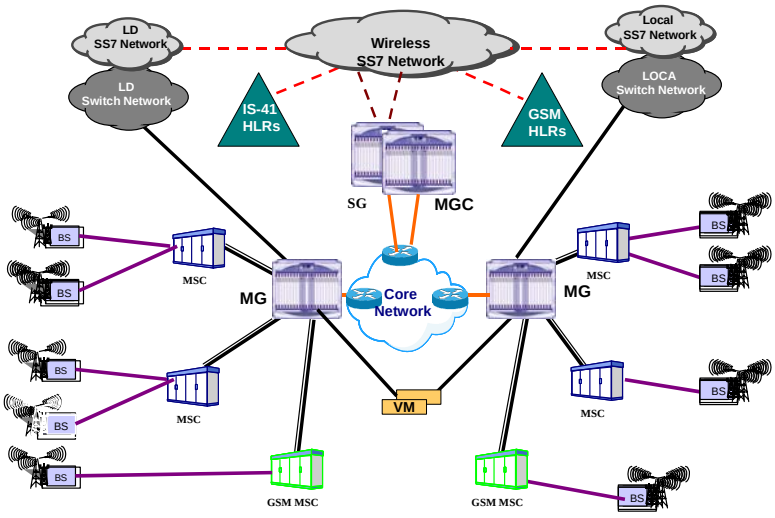


Figure 3. Gateway MSC (Distributed Architecture with Packet Core)



Features

The following sections detail the features in the Gateway MSC Feature Package.

SS7/C7 Signaling

Default ANSI/ITU SS7 Routing

Enables the routing of TCAP messages and responses to other SSP(s) in the absence of having explicitly configured SS7 routes for them. This capability benefits applications like Automatic Call Back and GMSC Optimal Routing. Default Routing is supported for SCCP messages only. Default Routing for ISUP messages is not supported.

This feature is enabled using either the `ROUTE-SS7` TL1 command or the EMS `Add SS7 Route` Screen by setting the point code value to "`DEF_ANSI`" or "`DEF_ITU`". Refer to the *TL1 Reference Guide* or the Provisioning the SS7 Node Chapter in the *EMS User Guide* for detailed information.

ANSI-41D

This feature provides the operation as a Gateway MSC, using the messages defined in the ANSI-41D standard, as it applies to Gateway MSC operation. The following messages are supported:

- Sending of Location Request Invoke
- Receipt of Location Request Return Result
- Mandatory parameters
  - Electronic Serial Number
  - Mobile Identification Number
  - MSCID
- Optional parameters
  - AccessDeniedReason
  - Digits (Carrier)
  - Digits (Destination)
  - DMH_AccountCodeDigits
  - DMH_AlternateBillingDigits
  - DMH_BillingDigits
  - DMH_RedirectionIndicator
  - DMH_ServiceID
  - RoutingDigits TerminationList
  - MobileDirectoryNumber
  - RedirectingNumberDigits
  - Note: One of the following optional parameters must be received: Digits (Destination) or AccessDeniedReason
- Sending of Transfer to Number Request Invoke
- Receipt of Transfer to Number Request Return Result
- Mandatory parameters
  - Digits (Destination)
- Optional parameters
  - AccessDeniedReason
  - Digits (Carrier)
  - DMH_AccountCodeDigits
  - DMH_AlternateBillingDigits
  - DMH_BillingDigits
  - DMH_RedirectionIndicator
  - DMH_ServiceID
  - MobileDirectoryNumber
  - TerminationList
  - RedirectingNumberDigits
- Receipt of Redirection Request Invoke
- Sending of Redirection Request Return Result

To enable this feature you need to provision the Service Logic Host Route (SLHR) to the HLR using the `SLHR-SCP` TL1

command or the EMS SLHR SCP Screen. Key SLHR GMSC parameters include:

- ROUTETYPE message (GTT, PC-SSN)
- SVCREQSSN (up to five switch-based requesting SSNs)
- SVCPROVSSN (single SSN on the HLR)
- TCAPUSER (IS41)
- TCAPVARIANT (ANSI1992)
- SCCPVARIANT (ITU1992)

GSM MAP

This feature set provides the operation as a Gateway MSC, using the messages defined in the GSM MAP Phase 2 standard, as it applies to Gateway MSC operation. The following messages are supported:

- Sending of Send Routing Information (Basic and Forwarding interrogation types) message.
- Receipt of Send Routing Information Ack message.
- Receipt of Resume Call Handling message.
- Receipt of Resume Call Handling Ack message.

To enable this feature you need to provision a Service Logic Host Route to the HLR using the SLHR-SCP TL1 command or the EMS SLHR SCP Screen. Key SLHR GMSC parameters include:

- ROUTETYPE(GTT, direct)
- SVCREQSSN(up to five switch-based requesting SSNs)
- SVCPROVSSN(single SSN on the HLR)
- TCAPUSER(MAP)
- TCAPVARIANT(ETSI1992, ITU1992)
- SCCPVARIANT(ITU1992)

Enable/Disable EXM

Allows the enabling/disabling of the Exit Message (EXM) when the GMSC's OwnClass is Access Tandem and the FarEndClass is End Office. This feature would typically be optionally used against the trunk groups that connect the GMSC to the wireless carrier's MSCs, which typically don't support the EXM message. This feature is enabled by setting the setting the class of service to "WTDM" using either the Tl1 ENT/ED-TRKGRP command or the EMS Provisioning the Routing Parameters Tab in the Add Trunk Group Routing Parameters Screen.

Optimal Call Redirection / Routing

Efficiently re-routes calls in scenarios where the mobile terminated call, originally routed to the Serving MSC by the GMSC, needs to be redirected back to the GMSC for re-routing to a forwarded-to number (in cases of CFNA, Call Collision, etc.). Call redirection is automatically enabled upon receipt of an ANSI Redirection Request from the Serving MSC. In GSM, the optimal routing flag must be enabled, using the TL1 `GMSC-GSMSYS` command or the `EMS Modify Gateway MSC GSM System` Screen, in addition to receiving a Resume Call Handling Request from the Serving MSC.

Call Processing

Mobile Digit Screening

This feature allows the service provider to create and delete up to 1024 based mobile digit screening table entries for all the subtending MSC(s) to which the GMSC can route calls. The screening is performed using the longest prefix match comparison method. Table entries of size 3, 6, 7, 8, 9 and 10 are supported. Supported mobile digit screening types (triggers):

- MOBILE TERMINATION: incoming calls matching the entry will be subject to ANSI-41 interrogation. If the ANSI HLR returns an unknown subscriber, then the GSM HLR will be queried (default).
- MOBILE TERMINATION ANSI: incoming calls matching the entry will be subject to ANSI-41 interrogation only.
- MOBILE TERMINATION GSM: incoming calls matching the entry will be subject to GSM interrogation only.

This feature is enabled using either the TL1 `AINTRIGGER` command or EMS `Add AIN Trigger Screen`.

Mobile Digit Screening Escape Lists

Service providers can also create and delete digit screening escape lists that contain up to 50 entries of the form (NAP-NXX-XXXX) or (NPA-NXX-XXXX to NPA-NXX-XXXX range). Any call whose Called Party Number (CdPN) exactly matches an entry in this escape list is not subject to mobile digit screening. This feature is enabled using either the TL1 `LIST-TRIGESC` command pr the EMS `Add Trigger Escape List` Screen.

Router Support for Over-Decadic Digits

This feature allows the GMSC to analyze over-decadic digits (A, B, C, D, E) in the Called Party Number and related ANSI 41/GSM HLR fields. Over-decadic digits are useful as prefixes that denote special routing instructions (an AB-XX prefix denotes a specific voicemail system).

Customizable Announcements

Service provider-specific announcement playback, along with system default playback, is supported for the following cases:

- An HLR returns a TCAP error of “User Busy”.
- An HLR returns a TCAP error of “No Response”.
- An HLR sends a response of “Unknown Subscriber” (ANSI-41 or GSM screening).
- Both HLRs send a response of “Unknown Subscriber” (DUAL screening).
- A RedirectionRequest or ResumeCallHandling fails due to a session mismatch (the GMSC cannot locate the session that the Serving MSC indicates needs redirecting)

Service provider-specific announcements are configured using the TL1 `PRFL-FAILCND`, `TREATMENT` commands or the EMS `Add Failure Condition Screen` and the EMS `Common Routing Elements>Treatments` section. The TL1 `AUDIO-ANNC` and `AUDIO-MSG` commands are used to specify new service provider-specific audio announcement and pre-recorded audio messages that are stored on-board the switch, if required.

Wireless Intelligent Network Bypass Mode

When enabled, the GMSC indicates to the HLR, either using ANSI-41 Locreq Invoke Request/Response messages and WIN triggers that Wireless Number Portability is supported. If the HLR responds with triggers for the call, the GMSC tandems the call to the subtending MSC using the original Called Party Number (CdPN) or Location Routing Number (LRN), as appropriate.

Wireless Number Portability

Call Termination - If the HLR responds with triggers for the call, a number portability query (see note below) will be sent to the NPDB. If an LRN is returned, the GMSC checks the returned LRN against the provisioned LRN table. If there is a match in the table, indicating that the call is destined toward an adjacent MSC, the

LRN is used to locate the correct HLR and the CdPN found in the Ported Gap is sent in the HLR query.

Mobile Origination - If the NP query is to be performed, the GMSC sends an NPREQ query to the NPDB. If the NPDB returns a valid LRN, the GMSC analyzes the LRN against the LRN table. If a match is found in the table, call processing continues with HLR call processing, using the LRN to locate the correct HLR. If a match is not found in the LRN table, the call is routed using the LRN as the CdPN, with the original CdPN in the GAP field.

In the course of number portability processing for a mobile terminated call, if the subscriber is "ported in", and the subscriber is also a CALEA target, no mobile service processing occurs (no HLR query is sent to the HLR that is associated with the LRN) and the call is treated as a tandem call, using the LRN as the CdPN and the subscriber DN in the GAP field.

This feature is enabled using the TL1 `GMSC-ANSISYS` and `GMSC-GSMSYS` commands or the EMS `Modify Gateway MSC GSM System` and EMS `Modify Gateway MSC ANSI System` Screens. Key parameters are WIN/CAMEL phase and the optional bypass string that is applied as a prefix to the CdPN if the GMSC logic is bypassed and the call is transited through the GMSC without performing an HLR query.

Note: Wireless ANSI-41 WNP and AIN LNP have been implemented as mutually exclusive services based on the assumption that a common NPDB is used for Wireline and Wireless numbers and the ANSI-41 WNP and AIN LNP queries are accessing the same NPDB. Therefore, once one Number Portability service is activated, the other cannot be activated. For example, if Number Portability is configured to perform ANSI-41 NPREQ queries to the NPDB, then the GMSC platform cannot be configured to perform AIN queries to the NPDB.

CALEA/Lawful Intercept Bypass

Introduction

The feature works with in conjunction with the Lawfully Authorized Electronic Surveillance (LAES) for CALEA feature on the Executive Cellular Processor (ECP), as well as 5ESS® DCS controlled features.

CALEA (Communication Assistance for Law Enforcement Act) is a law that requires a telecommunications vendor to meet certain standards for surveillance functions.

Availability

The CALEA Bypass feature is available in Gateway Platform Release 5.1.0.1, and later releases.

Feature Description

This feature ensures that calls that are subject to LEA surveillance are routed based on Called Number, resulting in the call being forwarded to the Home MSC where existing Serving MSC-based lawful intercept mechanisms can be activated. Provisioning commands ensure that access is restricted to CALEA user privilege and that the Directory Numbers that are under surveillance are suppressed from the system log files. The Lawful Intercept table can either be provisioned using the `Service Provider Administration (SPA)` component in the Lucent Technologies Delivery Unit (LTDU) or via the `GMSC-LAESDN` TL-1 command. **Note:** Due to security considerations, the Lawful Intercept table is not provisionable using the PlexView EMS.

How It Works

When a target is to be put under surveillance, the service provider uses the SPA (Service Provider Administration) component of the LTDU (Lucent Technologies Delivery Unit) to add a target's MDN (MSISDN) to the CALEA Bypass database on the Gateway MSC. Once a target has been added, any incoming call that is received for a CALEA target is tandemed to the associated Bypass-to MSC, where it is put under surveillance using the existing CALEA call origination and call termination infrastructure (hardware, call processing and provisioning software) that is already in place on the Bypass-to MSC. An optional service provider specified prefix is applied to the MDN (MSISDN) to indicate to the Bypass-To MSC that the call was tandemed and that a location request has not been sent to the HLR.

CALAEA Bypass Database

The CALAEA Bypass database on the GMSC can hold up to 1024 active targets. Each row of the database supports insert, update, and delete operations. All existing GP database overload controls, query mechanisms, and security measures apply to the CALEA Bypass database. The CALEA Bypass database contains the Subscriber/Target's mobile identification number (MIN/IMSI [International Mobile Station Identity]). A secure Ethernet link is used between the LTDU and the GMSC to provision the CALEA Bypass database.

LAES Database

A LAES database is provided on each MSC with enough capacity to hold up to 500 separate surveillance target data records. Each displayed RC/V field of the database supports insert, update, and delete operations. All existing ECPC database overload controls, query mechanisms, and security measures apply to the LAES database.

The LAES database may contain information to identify both home and roaming subscribers as targets. This database is accessible by RC/V and text RC/V from the ECP and the OMP. The database includes the following information:

- Subscriber/Target's mobile identification number (MIN/IMSI [International Mobile Station Identity])
- Indication of whether the court order requires any of the following:
  - Call data
  - Call content
  - Location
- Trunk group(s) and member number(s) for special-routing trunks and/or bridge trunks

LAESTK Database

A LAESTK database is provided on each MSC with enough capacity to hold up to 5000 separate currently active (in-progress) call content surveillance circuit records. Each displayed RC/V field of the database supports review and delete operations only. All existing ECPC database overload controls, query mechanisms, and security measures apply to the LAESTK database.

The LAESTK database contains information to identify all currently active call content circuits for both home and roaming target subscribers. This database is accessible by RC/V and text RC/V from the ECP and the OMP. The database includes (among others) the following information:

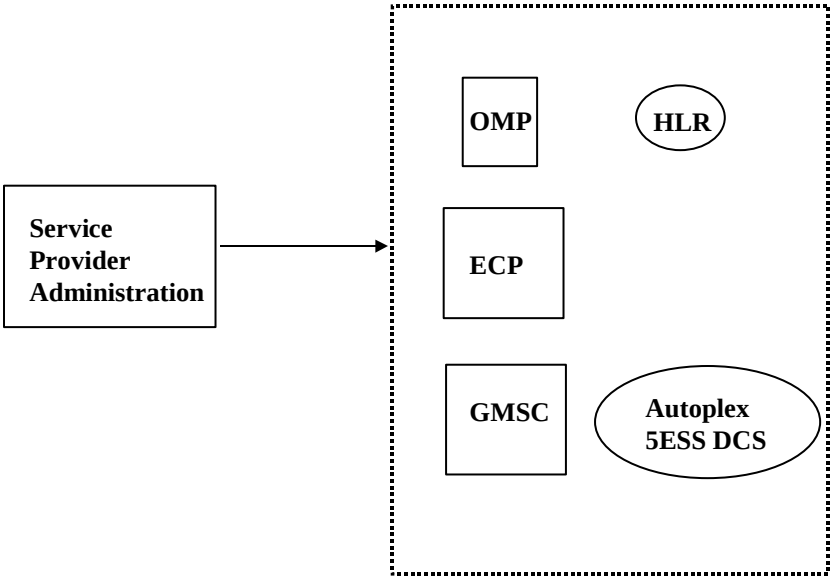
- Active CDN
- Active DCS
- Active Trunk Group
- Active Trunk Group Member

NOTE:

The LAESTK database is intended primarily as a maintenance administrative tool.

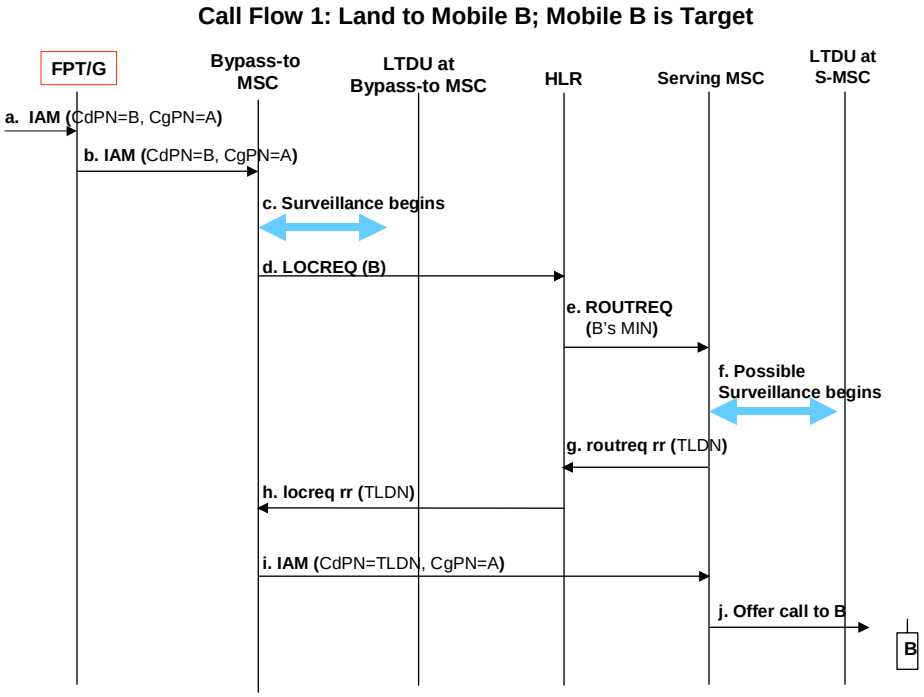
The information contained in this database is entirely maintained by call processing, and any unauthorized record deletions from this database can have adverse effects.

The figure below shows how the CALEA Bypass and LAES feature work within the Flexent/AUTOPLEX Mobile Switching Center environment.



CALEA in AUTOPLEX MSC Environment

* These are logical functionalities. They could represent one or various distributed physical platforms.

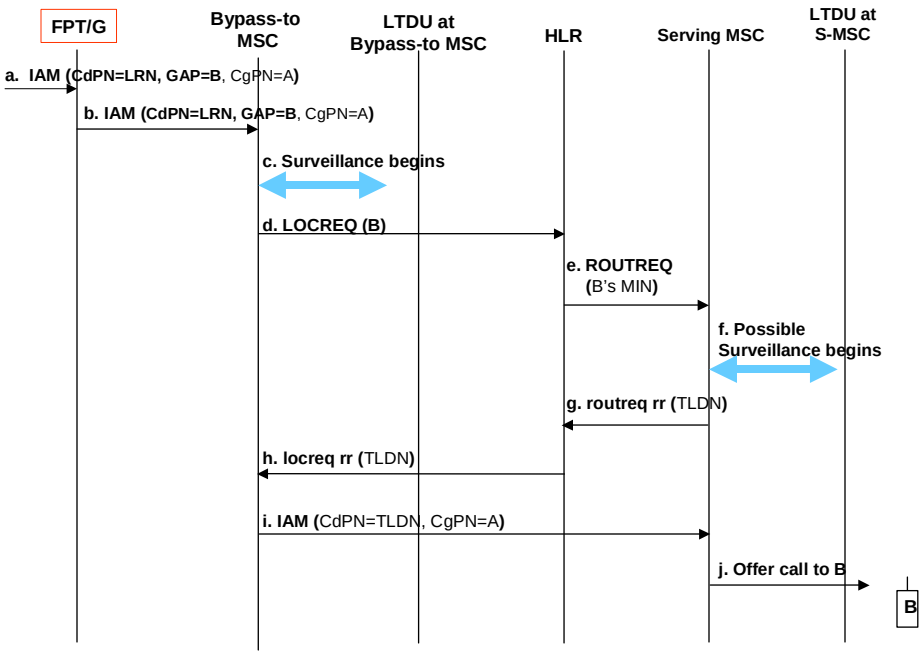


Call Flow 1 Notes

This call flow shows the CALEA Bypass feature in operation. In this case, the Called Number Party that is received at the GMSC matches a subscriber number in the CALEA Bypass database. The GMSC routes the call without an HLR query, which results in the call being routed to the subscriber's Home MSC, where CALEA mechanisms are activated.

- IAM arrives at FPT/G with CdPN=B and CgPN=A. FPT/G recognizes that B is a CALEA target.
- FPT/G tandems the call out to the Bypass-to MSC, with the same IAM parameters (CdPN=B, CgPN=A).
- Bypass-to MSC receives in-call for B, and recognizes that B is a CALEA target, and begins surveillance on this call. (CALEA surveillance details are not shown here but are represented by the blue arrow.)
- Bypass-to MSC sends LOCREQ for B to the HLR, based on the dn2e translations present in the MSC for the MDN.
- (Ordinary call delivery) HLR sends ROUTREQ to serving MSC.
- S-MSC may also have CALEA surveillance set up on this mobile, and if so, surveillance begins.
- (Ordinary call delivery) S-MSC returns TLDN back to HLR
- (Ordinary call delivery) HLR returns TLDN back to Bypass-to MSC in the locreq rr.
- (Ordinary call delivery) Bypass-to MSC does call delivery to B, sending out IAM to TLDN.
- (Ordinary call delivery) Call is offered to B.

Call Flow 2: Land to Mobile B; Mobile B is Target who Ported In with WNP



Call Flow 2 Notes:

In the course of number portability processing for a mobile terminated call, if the subscriber is "ported in" from another service provider with WNP, and the subscriber is also a CALEA target, no mobile service processing occurs (no HLR query is sent to the HLR that is associated with the LRN) and the call is treated as a tandem call, using the LRN as the CdPN and the subscriber DN in the GAP field.

- This call flow is similar to the previous call flow.
- At the Bypass-to MSC, the translations must include home LRN translations for this LRN, so that the MSC can correctly process this call and send a LOCREQ to the HLR.

Provisioning Commands

The CALEA Bypass feature provides TL1 as mechanisms for the service provider to provision the Gateway MSC (GMSC) to provide the wiretap. However, the service provider is expected to use the GUI provided with the LTDU's SPA functionality to provision these court orders; the (text) TL1 command capability is intended only for the internal use only by the SPA to effect the appropriate switch provisioning. Note that due to security considerations, the Lawful Intercept table is not provisionable

using the PlexView Element Management System that is used to manage the Gateway Platform.

Provisioning commands ensure that the Directory Numbers that are under surveillance are suppressed from the system log files. (e.g. 508-804-8100 is replaced with ***-***-**** in the system log files). Additionally, access is restricted to CALEA user privilege, in the case of TL1 command execution.

The following LTDU ASN.1 messages are supported by the GMSC.

Add Targets

This message is sent to the DSS to add a surveillance target or targets. Up to 2048 targets may be added with one message.

Add Targets Response

This message is the expected response from the DSS to the Add Targets message. It should contain the same number of records as the corresponding Add Targets message. For each record there will be a sequence or record entry number and a reason code that indicates the success/reason for failure of the database insert.

Delete Targets

This message is sent to the DSS when a surveillance target or targets must be deleted from the target database. Up to 2048 targets may be deleted with one message.

Delete Targets Response

This message is the response from the DSS to the Delete Targets message. It should contain the same number of records as the corresponding Delete Targets message. For each record there will be a sequence or record entry number and a reason code that indicates the success/reason for failure of the delete.

Modify Targets

This message is sent to the DSS to modify a surveillance target or targets. Up to 2048 targets may be modified with one message.

Modify Targets Response

This message is the expected response from the DSS to the Modify Targets message. It should contain the same number of records as the corresponding Modify Targets message. For each record there will be a sequence or record entry number and a reason code that indicates the success/reason for failure

of the action.

Reset
This message is sent to the DSS to delete all existing targets from its surveillance list. The LTDU may then send one or more Add Targets messages if the DSS's surveillance list is to be repopulated. (Note that it is possible to add the maximum number of records in the target database (2048) with one Add Targets message.)

Reset Response
This is the response to the Reset message. It contains a reason code value.

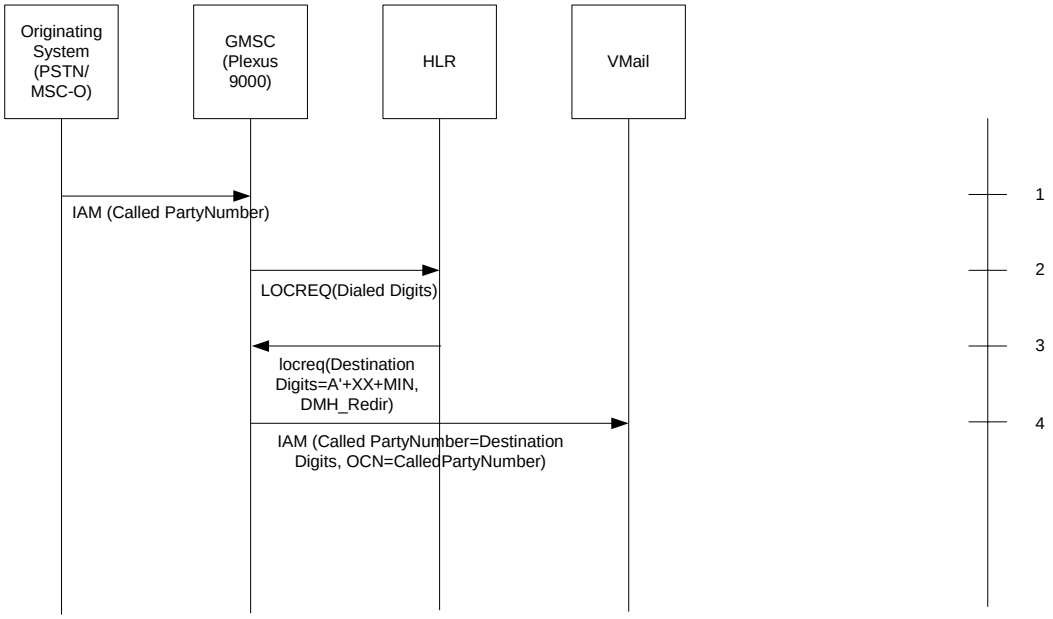
Retrieve Targets
This message is sent to the DSS. It is a request to send surveillance target records to the Administration Function so the targets can be validated. Up to 2048 target records may be queried with one message.

Voice Mail Forwarding

Enables routing by either the HLR-returned voice mail deposit number or forward-to-number prefix digits (digits or overdecadic A-E) as well as selective digit stripping of the forward-to-number prefix. This voice mail prefix is enabled using the TL1 `GMSC-ANSISYS` and `GMSC-GSMSYS` commands or the EMS `Modify Gateway MSC GSM System` and EMS `Modify Gateway MSC ANSI System` Screens.

Call to Mobile Subscriber, Call Forward to Voice Mail

In this scenario, the HLR returns the Destination Digits set to MIN prefixed by A'+XX (where XX is a two digit voicemail system identifier) in order to differentiate call delivery to a voice mail system from call delivery to a PSTN number. Note that while the call flow shown is for a TDMA subscriber, an analogous call flow can also occur for a GSM subscriber.



1. If the originating switch is ISUP capable, IAM with called party number set to the MIN/MDN of the mobile subscriber will make its way to the GMSC due to pre-configured routes in that switch and any other tandem switches along the way.
2. On receiving the call origination request (via IAM if ISUP is used) with called party number that passes wireless screening, GMSC issues a Location Request to the HLR. This message is sent and routed to the HLR using Global Title Translation. Global Title Indicator type 2 (0010) is used. A translation type value of 3 for "MIN to HLR" translation is used if the Called Party Number is treated as the MIN and a configurable translation type (there is no standard value for MDN translation type, hence carriers may use different translation types) for "MDN to HLR" translation is used if the Called Party Number is treated as the MDN. The global title address information field contains the MIN/MDN. The attributes sent are as follows:

Parameter Name	**Source**
BillingId	Made up of multiple components 1. Market Id (Provisioned Data) 2. SwitchNumber (Provisioned Data) 3. Unique call identifier (Internally generated while insuring uniqueness) 4. Segment Counter (Set to 255)

Parameter Name	Source
Digits (Dialed)	Called Party Number from incoming IAM for ISUP protocol or equivalent for other protocols.
MSCID (Originating)	Made up of multiple components 1. Market Id (Provisioned Data) 2. SwitchNumber (Provisioned Data)
SystemMyTypeCode	Hard-coded to a value currently unassigned to any vendor (e.g., 50)
CallingPartyNumber1	Calling Party Number from IAM for ISUP protocol, if available or network provided calling party number information for other protocols.
CallingPartyNumber 2	Generic Address (type 2 or 3) from IAM for ISUP protocol, if available or user provided calling party number information for other protocols.
CallingPartySubaddress	Not Sent if incoming protocol is ISUP. Obtained from Calling Party Subaddress from Setup Message for ISDN protocol or equivalent if available for other protocols.
MSCIdentificationNumber (Originating)	Not Sent
PC_SSN (Originating)	Sent based on Provisioned Data
RedirectingNumberDigits	Redirecting Number from IAM for ISUP protocol, if available or equivalent for other protocols. For Mobile to Mobile forwarded calls, set to the Called Party Number from the original IAM for ISUP or equivalent call setup message for other protocols.
RedirectingSubaddress	Not Sent if incoming protocol is ISUP. Obtained from Redirecting Party Subaddress (??) from Setup Message for ISDN protocol or equivalent if available for other protocols.
TerminationAccessType	Set to Mobile to Mobile Directory Number Access or Land to Mobile Directory Number Access depending upon the ingress trunkgroup.
TransactionCapability	Hard coded to indicate support for following transaction capability- Busy Detection

Parameter Name	Source
	TerminationList parameter (MultipleTerminations=1)

3. On receiving the request, if the HLR finds call forwarding active (because of unconditional forwarding or Busy condition), it sends the forwarding digits back to the GMSC either directly in the Destination digits parameter of the Location Request RR or Destination digits sub-parameter of the Termination List, if both the HLR and GMSC are capable of supporting Termination Lists. HLR also provides the reason for redirection (e.g., CFU, CFD, CFB etc) in the DMH_RedirectionIndicator, expect in this case except in this case the HLR has added the prefix A'+XX (where XX is a two-digit voicemail system identifier) to the MIN, which indicates that the call is to be routed to the Octel voicemail system for deposit. Expected attributes are as follows:

Parameter Name	Usage
Electronic Serial Number	Uniquely identifies calls for call redirection scenarios. Ignored if received.
MobileIdentificationNumber	Uniquely identifies calls for call redirection scenarios. Ignored if received.
MSCID (Serving)	Identifies the Serving MSC. Ignored if received.
AccessDeniedReason	Not present in this scenario
AnnouncementList	Ignored if received.
CallingPartyNumberString1	Ignored if received.
CallingPartyNumberString2	Ignored if received.
Digits (Carrier)	Specifies the preferred inter-exchange carrier, if any for calls being routed to PSTN. It will also be included in the TNS parameter of the outgoing IAM.
Digits (Destination)	Will be used as the Called Party Number in the outgoing IAM, if routing digits are not present. This parameter will take precedence over TerminationList parameter.
Digits (Routing Number)	Not present in this scenario
DMH_AccountCodeDigits	Ignored if received.
DMH_AlternateBillingDigits	Ignored if received.

Parameter Name	Usage
DMH_BillingDigits	Ignored if received.
DMH_RedirectionIndicator	Should indicate call forward (CFU, CFB, CFO, or CFD)
GroupInformation	Ignored if received.
MobileDirectoryNumber	Uniquely identifies calls for call redirection scenarios.
NoAnswerTime	Should not be present
OneTimeFeatureIndicator	Ignored if received.
PC_SSN (Serving MSC/VLR)	Ignored if received.
RedirectingNumberDigits	Identify the number, which is being redirected. For the first redirection, it is going to be the number of the mobile subscriber itself. Subsequent redirections will result in the next mobile subscriber number being placed in this field. Gateway MSC will set the RedirectingNumber in the outgoing IAM with this information.
RedirectingNumberString	Carries the identification of the redirecting party. Gateway MSC will set the GenericName parameter with this information.
RedirectingSubaddress	Carries subaddress identification of the redirecting party. Not used in the ISUP cases
RoutingDigits	Specifies special routing information, normally is where the TLDN is returned .
TerminationTriggers	Ignore if received
TerminationList (TL)	Used to provide originating MSC with routing information for one or more terminations. A separate list of parameters is reported based on whether the termination is local, inter-msc or PSTN. Gateway MSC expects to receive a list targeted towards inter-MSC or PSTN termination, since, it can never be a serving MSC for a certain mobile subscriber. There is duplication between some parameters present within this list and the parameters discussed above. Typically only one of them would be provided, but, if both are provided, the

Parameter Name	Usage
	parameters outside the TerminationList in general would have precedence.
TL-MSC	Ignored of received, should be sent to Serving MSC only.
TL-InterSystem-DestinationDigits	Ignore if received
TL-InterSystem-MSCID	Ignore if received
TL-InterSystem-AccessDeniedReason	Ignore if received
TL-InterSystem-BillingID	Ignore if received
TL-InterSystem-CarrierDigits	Ignore if received
TL-InterSystem-ESN	Ignore if received
TL-InterSystem-LegInformation	Ignore if received
TL-InterSystem-MDN	Ignore if received
TL-InterSystem-MIN	Ignore if received
TL-InterSystem-MSCIdentificationNumber	Ignore if received
TL-InterSystem-RoutingDigits	Ignore if received
TL-InterSystem-TerminationTriggers	Ignore if received
TL-PSTN-DestinationDigits	Will be used as the Called Party Number in the outgoing IAM, if routing digits are not present. The Destination Digits outside the TerminationList will take precedence if present.
TL-PSTN-CarrierDigits	Specifies the preferred inter-exchange carrier, if any for calls being routed to PSTN. It will also be included in the TNS parameter of the outgoing IAM.
TL-PSTN-ESN	Uniquely identifies calls for call redirection scenarios.
TL-PSTN-LegInformation	Ignored if received.
TL-PSTN-MIN	Uniquely identifies calls for call redirection scenarios.
TL-PSTN-RoutingDigits	Specifies special routing information. Gateway MSC gives this precedence over DestinationDigits present in the TerminationList. Not normally present in this scenario.
TL-PSTN-	Ignore if received

Parameter Name	Usage
TerminationTriggers	

4. Since the returned digits are not TLDN, the GMSC initiates digits screening from start. In this call scenario, it is assumed that the digits indicate voice mail system because they are prefixed by A'+XX. As a result GMSC routes the call to the associated TDMA MSC hosting the voice mail system. The original called party number is set to the called party number to convey to the voice mail system that it is being accessed for voice mail deposit and not retrieval.

Interface Support

The switch may be configured with a variety of physical interfaces; this allows the I/O configuration to be matched to the service density requirements and existing switch infrastructure. The chassis provides space for 17 IOMs allowing for a high degree of plug-in scalability and flexibility. All of the IOMs are hot swappable.

The interfaces fit into two categories, which are PSTN line termination and network access. The Octal DS3 IOM is capable of being provisioned as DS3 or STS-1 on a per port basis. The number of interfaces supported per IOM and number of IOMs per shelf in these categories are given in Table A. The maximum number of IOMs assumes that the IOMs are operating in protected mode.

Table A. Supported Input/Output Interfaces

Type	Interface	Ports per IOM	Max IOMs	Protect Mode
TDM	DS-1	28	16	1:16
	E1	28	16	1:16
	DS-3/STS-1	3 or 8	15	1:7 and 1:8
	Channelized OC-3, STM-1	4	4	1:1
VoIP Network Access	1000BaseT 1000BaseSX 1000BaseLX	4	1	1:1

Protocols

Wireless Protocols:

ANSI 41-D, GSM MAP Phase 2+, WNP, WIN, CAMEL

IP Protocols:

MEGACO/H.248, SIP, SIP-T, SigTran

SS7 Protocols:

ISUP, TCAP, AIN 0.2, LNP, GR-317, GR-394

ISUP Parameter Mapping

The ISUP protocol and parameter mapping is limited to those messages and parameters that need to be modified as a result of Gateway MSC operation. All other ISUP parameters are passed transparently.

IAM (Call Delivery to Serving MSC)

Parameter Name	Source
Called Party Number	ANSI-41: Number received in Routing Digits or Destination Digits parameter of Location Request Return Result from the HLR. GSM: Number received in MSRN or Forwarded-To Number parameter of Send Routing Information Ack from the HLR.
Forward Call Indicator	ANSI-41 & GSM: The M-bit is set to 1 to indicate that number translation has been done and the serving / home MSC does not need to do any subsequent NP lookups.

IAM (Call Forwarding Scenario)

Parameter Name	Source
Called Party Number	ANSI-41: Number received in Routing Digits or Destination Digits parameter of Location Request Return Results from the HLR. GSM: Number received in Forwarded-To Number parameter of Send Routing Information Ack from the HLR.

Parameter Name	Source
Original Called Number	ANSI-41 & GSM: Set to forwarding party number (mobile subscriber's number) only if it is not already set (meaning a first attempt at call forwarding).
Charge Number	ANSI-41 & GSM: Set to forwarding party's number (the same number as is indicated in the Redirecting Number field)
Redirecting Number	ANSI-41 & GSM: The called party number in the first IAM received by the Gateway MSC, which triggered the HLR lookup. Set to forwarding party number, in our case, the mobile subscriber who is forwarding the call
Redirection Information	ANSI-41 & GSM: Counter is updated and redirecting reason is indicated

Performance/Capacity

The GMSC has been designed to support a sustained call arrival rate of 90 cps with Billing enabled, running in an integrated (non-distributed) switching architecture, with the following call model (all SS7 ISUP):

- 50% Tandem Calls (mobile originated)
- 2.5% Call Forward Unconditional (ANSI)
- 2.5% Call Forward Unconditional (GSM)
- 5% ANSI Redirect to Voice Mail
- 5% GSM RCH to Voice Mail
- 15% ANSI-41 Mobile Terminated Call – single ANSI41 HLR query
- 5% GSM Mobile Terminated Call - ANSI & GSM HLR "Double Dip"
- 15% GSM Mobile Terminated Call – single GSM HLR query (due to cache match, with cache @ 1M entries)

OSS Interfaces

Multiple interfaces are supported to ensure seamless integration of switch components into a variety of customers' back-office environments. A TL1 interface is provided to allow quick integration with Lucent legacy OSSs as well as those provided by

Telcordia Technologies. An XML interface allows integration with more modern OSSs. An SNMP interface provides additional capability for forwarding and filtering of fault messages to network management systems like HP OpenView. The PlexView EMS provides two northbound interfaces, TL-1 Gateway and SOAP XML API, that provide a centralized access point for integrating with existing OSSs to create flow-through and error-free provisioning processes.

Wireless Billing

Two different types of billing mechanisms are supported (AIN, WIRELESS) for recording calls that require HLR dips. The AIN method will model this service as an AIN service and utilize generic AIN AMA billing.

The WIRELESS method will utilize AMA extensions for cellular calls which mirror the AMA records that are generated by Lucent's Flexent^{R}/AUTOPLEX^{R} Wireless Networks Executive Cellular Processor (ECP). These records support the following structure codes:

- SC x2118 - Tandem Call With Carrier Interconnect (CI) Information
- SC x2119 - Tandem Call Without Carrier Interconnect (CI) Information
- SC x2329 - Cellular Originated Call Without Carrier Interconnect (CI) Information
- SC x2330 - Cellular Originated Call With Carrier Interconnect (CI) Information

A CDR search tool is available to enable a technician to pinpoint the cause when customers report service problems, such as a poor connection or dropped calls. The tool examines CDRs that are in the Automatic Message Accounting Data Network System (AMADNS) format. The desired mobile directory number and the time interval must be specified. AMA record information based on structure code and call type is displayed on the PC where the CDR search tool is executed. If no data is available for a particular field, the field will remain blank. Refer to the *Billing and Traffic Collection Guide* for detailed information..

Element Management

The PlexView EMS fits into the TMN architecture at the Element Management Layer and provides an integrated solution for managing Fault, Configuration, Accounting, Performance, and Security functions for the Softswitch Services and the switching

system hardware platform. A single EMS is used to operate, administer, manage and provision all softswitch products regardless of applications and physical network element configurations.

Performance Monitoring

In addition to standard system performance monitoring, these additional GSMC call statistics are maintained.

- Number of mobile terminating (MT) calls handled
- Number of MT calls successfully handled
- Number of MT calls failed as subscriber is unknown at HLR
- Number of calls subjected to dual dips
- Number of calls subjected to TLDN routing
- Number of calls subjected to MSRN routing
- Number of calls forwarded by ANSI HLR
- Number of calls forwarded by GSM HLR
- Number of calls subjected to successful GSM cache lookup
- Number of ANSI calls redirected by S-MSC
- Number of GSM calls redirected by VMSC
- Number of ANSI calls transferred as a result of Termination Trigger hit (post Locreq routing)

The GMSC performance monitoring can be initialized via the TL1 `INIT-REG-GMSC` command or the EMS `Init Register GMSC` screen. Current performance monitoring values can be retrieved using the TL1 `RTRV-PM-GMSC` command or the EMS `Initializing and Retrieving Performance Monitoring for GMSC` Screen.

Notes:

Enhanced Routing

This document contains the following sections:

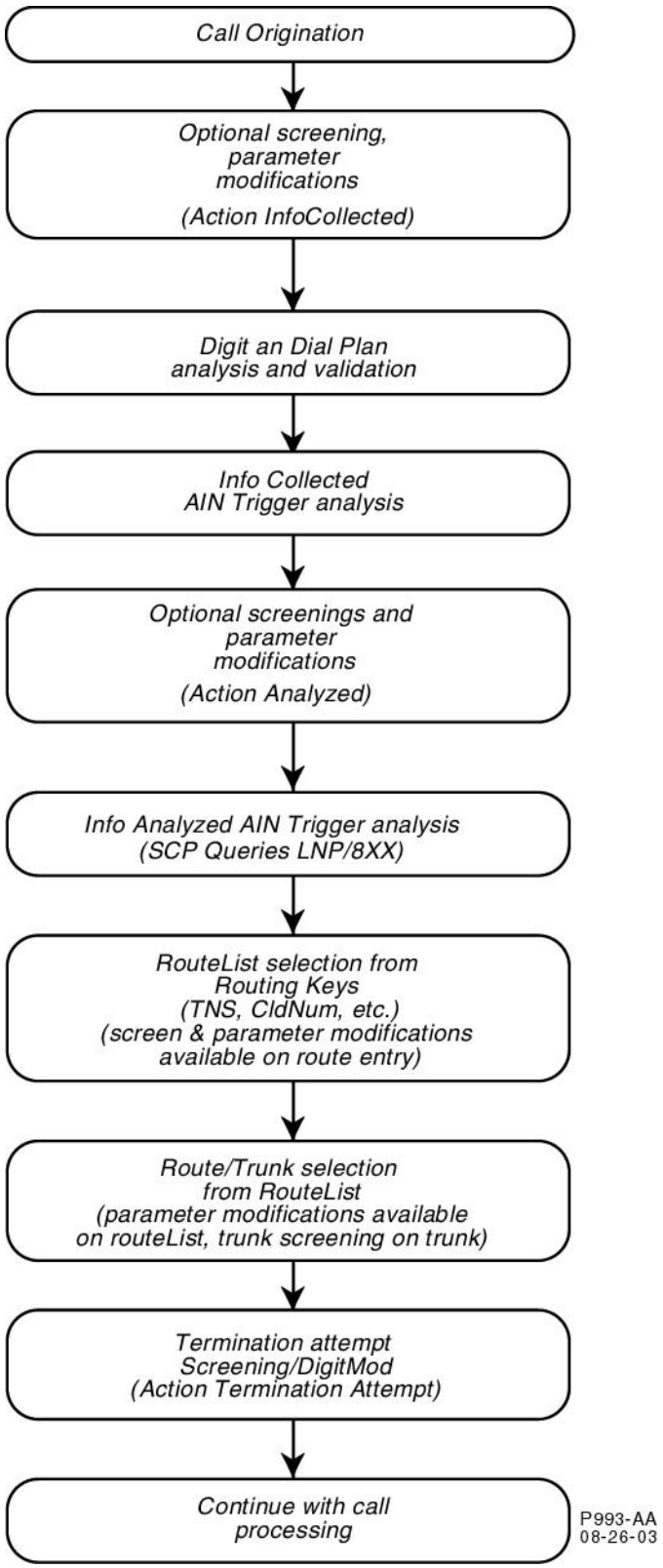
Scope

Routing is the process of matching any incoming call to the switch with a specific egress path to a destination switch. The incoming call parameters, combined with the translation plan, usually drive this process, but in certain circumstances, other parameters may supplement or completely override the number. Such modifying factors include digit manipulation/stripping, screening, and application of treatment when processing the call.

Calls enter and leave the switch on trunks, which are consolidated into trunk groups, which in turn are grouped into routes associated with a translation plan. A route is a path to a destination, not just the next switch, and is defined as a prioritized list of trunk groups and/or interfaces (ISDN, SS7, CAS, SIP, BICC) identified by a route name. On the incoming side, the trunk group on which a call is received is associated with a translation plan that determines how the call is handled -- that is, whether the called number or other parameters will determine the routing. On the egress side, a route is a path to a final destination (the called number). In some cases, there will be several ways to reach the final destination, represented by different next-hop switches directly connected to the switch by trunk groups. Thus, all the trunk groups in a route do not necessarily terminate on the same switch. While each trunk group must be terminated on one far end switch, a route may have trunk groups terminating on several different switches, all representing possible paths to reaching the called number. This provides diversity in reaching the final destination in the event of adjacent switch congestion or trunk failure.

Figure 1 provides a sample of the information analyzed on an incoming call when being routed through the switch. The actual flow of the call and tables containing provisioning information is shown in Figure 2.

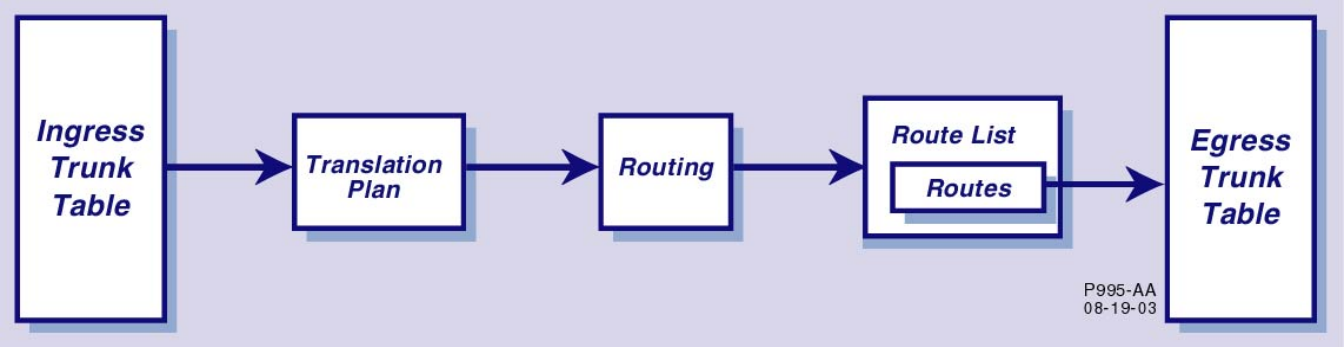
Figure 1. Routing a Call



Routing Flow

When a call comes into the switch, it follows the flow shown in Figure 2. Every ingress trunk group has a unique translation plan assigned to it. The translation plan can be specific to a particular trunk group or be reused as needed by many trunk groups.

Figure 2. Basic Routing Flow



The translation at a minimum defines the routing for the call and may also describe other actions that may be performed on the call, such as screening, digit manipulation, or application of a treatment rather than processing the call. The translation plan specifies up to three routing keys (such as TNS parameter or Called Number, for example) that may be used to route the call in order of priority. If the first key is not matched, then the second will be used, and then the third. In no key is matched, the translation plan specifies the treatment to be applied.

A successful match passes the call to the routing tables as shown in Figure 2. Here each possible key match is paired with a route destination, which will usually be a route list. For example, if the key were TNS, the routing tables would list every TNS supported and pair each with a route list or other destination. These other destinations could be other translation plans or treatments. The routing also allows a cost or weight to be specified for the call when selecting possible trunk groups from the route list.

The route list contains routes and their associated properties, including hunting algorithms, overflow treatment and re-routing instructions if no route is available. The route list is used to select routes from the route table. Percent allocation of calls among routes is also specified here.

The illustration shown in Figure 2 provides a high-level example of the basic flow of a call as it is routed through the switch. This illustration represents the flow of a call that has no special treatments or actions applied to it but, rather, is sent directly to the route list.

From the illustration, you can see that the Ingress Trunk Group Table points to the Translation Plan Table.

Each step in the process is depicted and represented by these Translation Tables:

- Ingress Trunk Table
- Trunk Group Table
- Translation Plan Table
- Routing Table
- Route List Table
- Routes Table
- Egress Trunk Table

The Translation Plan Table is shown in Table I and is represented in the switch by a database table containing various routing information.

Translation Plan

The Translation Plan Table lists up to three entries, or keys, on which to base the call for routing. The Translation Plan key can be any one of the following:

- Called Party Number (CDPN) – nature of address + digits
- Calling Party Number (CGPN) – nature of address + digits
- Charge Number (CHRGN) – nature of address + digits
- Generic Digits – (GENDGTS) – type + digits
- Generic Address – (GAP) – type + digits
- Calling Party Category (CPC) - value
- Originating Line Information (OLI) - value
- Bearer/Trunk Group (BGN) – type + number
- Transit Network Service (TNS) – CIC + CktCode/1NX/0ZZ + prot
- Carrier Identification Parameter (CIP) - CIC
- Carrier Selection Information (CSI) – (presubdial, notpresub)
- LATA – value
- Jurisdiction (JIP) - value
- Call Type (InterLATA, IntraLATA, International)
- Subscriber

When a call comes in on a trunk group, the Translation Plan does a search of the switch database based on the three keys entered into the Translation Plan. The search is conducted using the keys, in the order in which they are listed in the database. For instance, suppose that the three keys consist of the following:

- Route1-TNS
- Route1-CDPN
- Route2-CDPN

The switch first performs a search on Route1-TNS. If no match can be found for that key, then the switch proceeds to the next key and begins a search based on that criteria (Route1-CDPN, in this case). The switch searches the database until a match can be found for the key.

Note: In the various tables, you provision a parameter of NOTPRESENT in case no match can be found. When provisioning NOTPRESENT, you specify an alternate number to which the call can be placed in case a match cannot be found.

Once a match is found, the call is placed through routing, with possible treatments or actions applied, and sent to a Route List and then a Route, where it is then sent out through the Egress Trunk Group Table. This is all based on parameters previously provisioned for that particular Translation Plan.

An alternate Translation Plan key can also be entered. The alternate Translation Plan key overrides the original Translation Plan key and goes into effect as soon as it is entered into the Translation Plan Table.

Translation of the incoming call information ultimately results in the selection of a route to use to transport the call.

The route selected is also associated with the Translation Table via a Route key stored in the Translation Table. The Translation information, then, is used by the Routing Table to determine routing instructions. The Routing Table, using its Route Destination and analyzing the various parameters, knows what actions to perform on the route, or to send the call to a route list.

Often, an action, such as digit modification, will be performed on the incoming call. These actions are also used for screening Class 4 subscribers, performing digit modification for TNS, or applying a treatment, such as a cause code or announcement. Up to six actions can be applied to one call. For more information on various actions, refer to section Translation Plan Actions.

Refer to Table I for a list of Translation Plan parameters.

Routing

Along with Translation keys, the Routing key must be provisioned. The Routing key is used in addition to the Translation key to determine the NPA-NXX number. This information is taken from the Routing Table and is used as the second key when routing the call. From the Routing Table, routing instructions for different key and value matches can be found. The Routing key can consist of one of these four Route Destinations:

- Route List
- Next Routing Partition/Key
- New Translation Plan
- Treatment

This means that the call is either passed on to a Route List, sent back to a Translation Plan, or sent to the next Route Destination. The destination is determined by the Route Partition portion of the Route Destination key. The Route Partition is the set or characters prior to the first hyphen in the Route Destination key. For example:

RTLIST-SBC3 – RTLIST is the Route Destination.

Minimum and maximum costs of trunk groups are also determined by information entered into the Routing Table. Cost information for trunk groups enables you to include only trunks within a certain range, such as low-cost trunks, for example.

Note: Minimum and maximum cost criteria can also be entered into the Subscriber Table.

Refer to Table L for a description of Route Table parameters.

Route Partitioning

With the router, call processing supports partition-based routing. Routing partitions are assignable on the authorization code, ANI, CIC, trunk group, gateway or network level. If a match is not found in a particular partition, a default routing partition will apply.

Call processing also supports the redirection of a call from one routing partition to another. Instead of a route, the routing entry in the partition points to another partition. During a redirection from one partition to another, call processing allows manipulation of the dialed digits either partially or entirely prior to entering the new partition.

Route List

The Route List Table, as defined in Table K, lists the common properties associated with a list of routes. The hunting algorithm, or allocation method, for the route is provided in this table. Using a specified hunting algorithm against an ingress trunk group, the switch routing process selects an available egress trunk group and trunk from the database table to carry the call. Refer to Table K for a description of Route List parameters.

Overflow treatment of calls is also available through this table, enabling you to reroute calls or have two routes inside of one route list in case of overflow.

Routes

Once the Route List is identified, the call is sent to a specific route, as provisioned in the Route Table. The Route Table contains an ordered list of routes which support ISUP, SIP, CAS and BICC trunks, and ISDN lines. A route can also be sent to another Route List, as in the case of overflow, when calls need to be re-routed.

Refer to section 3.4 for a description of the parameters in the Route Table.

Trunk Groups

Calls enter and exit the via trunk groups. Incoming calls assume values set up in the Ingress Trunk table, and outgoing calls exit the switch based on routing criteria and information stored in the Egress Trunk table. Specifically, the Ingress Trunk table points to a Translation Plan, which passes the call through the switch with previously established values associated with the intended Translation Plan. Refer to Table H for an explanation of the Ingress Trunk Table.

The Egress Trunk table contains fields that help determine the outgoing reroute. Specifically, the information entered into the Digit Screen field identifies the outgoing trunk group screening table name. The cost of the trunk group also helps determine on what trunk the call will exit the switch, as well as the bearer cap, which identifies bearer capabilities for the trunk group. The information in the ActionTermAttmpt field identifies the action to take after the trunk group has been chosen on an outgoing interface for the call. Refer to Table T for an explanation of the Egress Trunk Table.

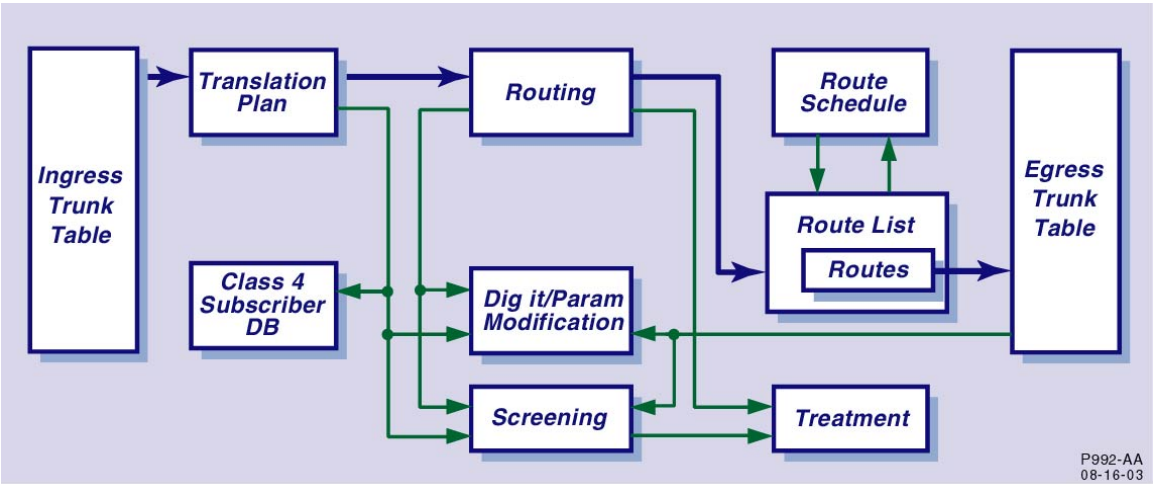
Translation Plan Actions

The Translation Plan assigns criteria to various calls, depending on the type of call. For instance, from the Translation Plan Table, these tables can be referenced:

- Class 4 Subscriber Table
- Screening Table
- Digit Modification Table
- Treatment Table

Refer to Figure 3 for a sample route flow which includes Class 4 subscriber parameters, screening, digit modification and special treatment.

Figure 3. Translation Plan Applying Class 4 Subscriber, Screening, Treatment and Digit/Param Modification Values



Class 4 Subscriber

Class 4 subscribers, which rely on aggregate ANI-based services and controls, are identified by the dialed number and call type or carrier. If the Translation Plan is to reference the Class 4 Subscriber Table, as shown in Figure 3, it is specified to do so in the Action Info Analyzed field of the Translation Plan Table.

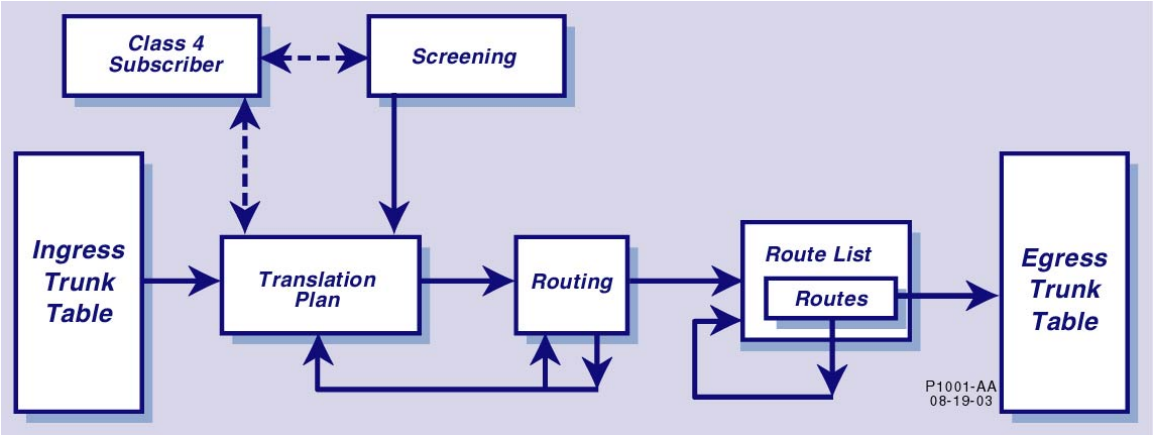
Information assigned to Class 4 subscribers is listed in Table M.

Other information specified in the Class 4 Subscriber Table includes:

- Authorization code and/or account code verifications
- Minimum/maximum trunk group cost
- Billing number
- Screening

Refer to Figure 4 for a sample of the call flow for routes referencing Class 4 subscriber parameters.

Figure 4. Class 4 Subscriber Screening



Call Screening

The Screening Table is also referenced by the Translation Plan Table. If the Translation Plan is to reference screening, as shown in Figure 5, it is specified to do so in the Info Collected or Info Analyzed fields of the Translation Plan Table.

Calls can be screened on the following information:

- Called Party Number (CDPN) – nature of address + digits
- Calling Party Number (CGPN) – nature of address + digits
- Charge Number (CHRGN) – nature of address + digits
- Generic Digits (GENDGTS) – type + digits
- Generic Address (GAP) – type + digits
- Calling Party Category (CPC) – value

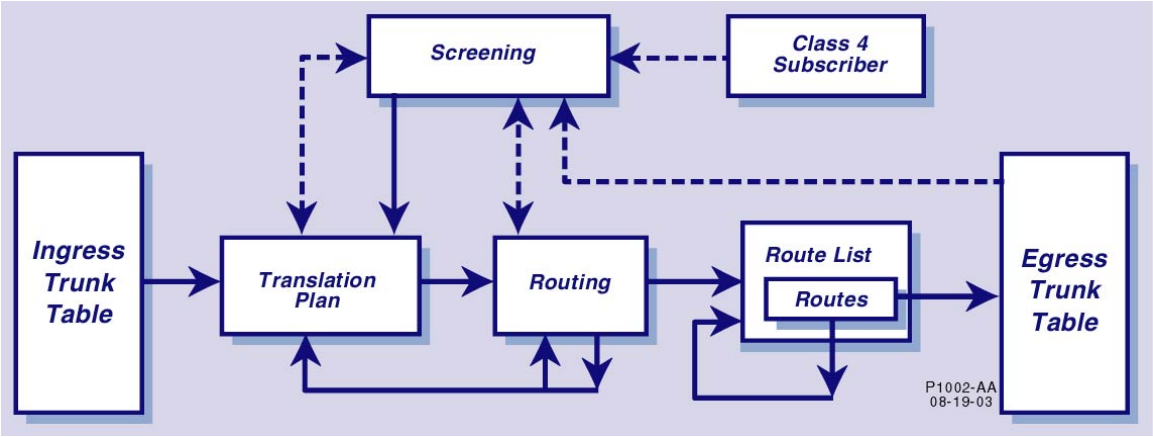
- Originating Line Information (OLI) – value
- Bearer/Trunk Group (BGN) – type + number
- Transit Network Service (TNS) – CIC+CktCode/1NX/0ZZ + port
- Carrier Identification Parameter (CIP) – CIC
- Carrier Selection Information (CSI) – presubdial, notpresub
- LATA – value
- Jurisdiction (JIP) – value
- Call Type (InterLATA, IntraLATA, International)
- SubStatus – IS, OOS, NOTINDB

Screening calls enables the router to perform a number of actions against a call if it meets certain criteria. Specifically, the router can perform these actions on a call:

- Pass/Fail
- Assign Treatment
- Screen for Authorization/Account Codes
- Mark as fraud call
- Assign new Translation Plan
- Send to Next Screen Table

Screening can also be referenced from the Routing Table and the Terminating Trunk Group. Screening keys are listed in Table N.

Figure 5. Screening



Digit Modification

Switch routing provides the ability to generically modify (strip/insert), replace or delete digits from the following:

- Called Party Number
- Calling Party Number
- Charge Number

- GAP
- Generic Digits
- CPC
- OLI
- JIP
- Call Type
- CIP
- LATA
- TNS

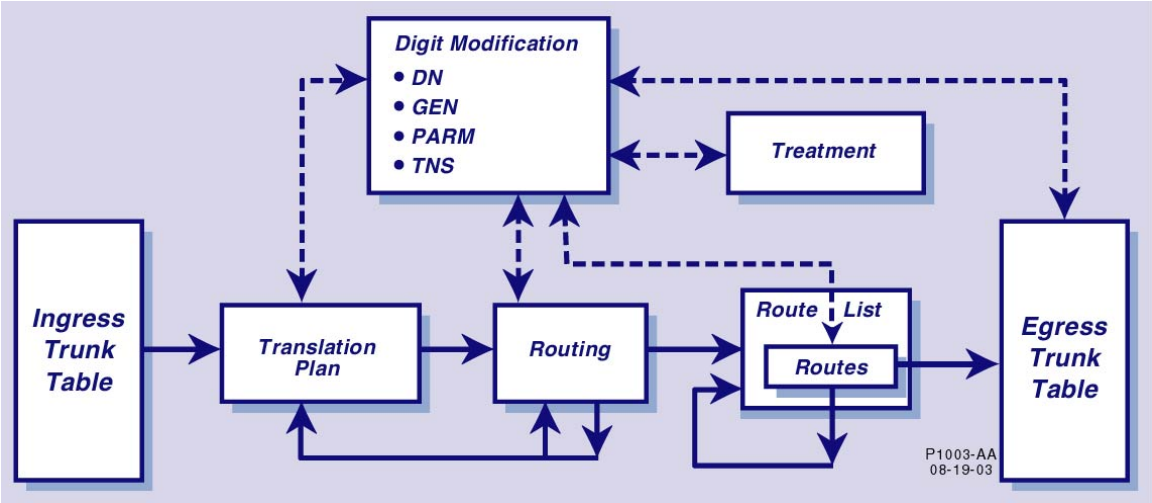
You can strip digits from the beginning, middle or end of a number. The switch is capable of prefixing or stripping digits to/from the called party number after selecting the route list and before sending the outgoing message. Stripped digits can be stored for later re-use.

Digit modification can be done on the following criteria, grouped into four separate tables:

- Dialed number
- Generic parameters
- TNS parameters
- Other parameters

Refer to Figure 6 for an illustrated example of call flow using digit modification.

Figure 6. Digit Modification Parameters



The Digit Modification, Dialed Number Table (Table O) provides the ability to generically modify (strip/insert), replace, or delete digits from the Calling Party Number, Called Party Number or Charge Number.

The Digit Modification, Generic Parameters Table (Table P) provides the ability to generically modify (strip/insert), replace, or delete digits from the GAP and Generic Digits.

The Digit Modification, Parameters Table (Table Q) provides the ability to generically modify (strip/insert), replace or delete digits from the following:

- CPC
- OLI
- JIP
- Call Type
- CIP
- LATA

The Digit Modification, TNS Table (Table R) provides the ability to generically modify (strip/insert), replace or delete digits from the TNS.

Treatment of Calls

A treatment, on the other hand, is used to route calls to another source for call handling. For instance, if you want to send a call to an announcement, you assign the call, from the Route List, to a tones/announcement box.

If there are no special treatments or actions to be performed against the call, the call is sent directly to a route list. It is then that the hunting algorithm is applied to the call.

The treatment of a call determines what happens to the call if it is to be handled other than by sending it to a route list. For instance, if a call is to be routed as an announcement, then the play tone/announcement treatment is applied. If a call is set up with a fail condition, then it will not be routed.

These are the treatments that can be applied to incoming calls:

- Play tone/announcement
- Failure condition
- Re-route (with digit modification, if required)
- Next treatment

Play Tone/Announcement

Play tone/announcement sends the call to a tones/announcement box where an announcement can be played. After the tone or announcement is played, the call can be released or sent to another treatment-specified parameter.

The announcement ID is stored in the Treatment Table and is entered using the RTRV-AUDIO-ANNC TL1 command. If the announcement requires variable arguments, such as time (TME_12, for instance), or phone number (DIG_NDN, for example), then you must provide the source of the variable field in the "annc args" of the treatment. For example, to create an announcement ID of 3000, provision that ID to play a time announcement and provide a treatment that references the announcement and specifies the time to be played as the current time, you would use the following TL1 command:

ENT-AUDIO-ANNC::3000:::name=dateandtime,desc=DATETIMEAUDIOFILE,msglist=TME_T12;

ENT-TREATMENT::TREATTOD:::TREATYPE=annc,anncid=3000,anncarg=TIME-CURRTIME;

As another example, you could create an announcement ID of 3001 which plays "<CalledNumber> is busy" and use the announcement in a treatment. As an example, you could use the following TL1 commands to use the announcement in a treatment.

ENT-AUDIO-ANNC::3001:::name=busymsg,desc=NUMISBUSY,msglist=DIG_NDN-28;

ENT-TREATMENT::TREATTOD:::TREATYPE-annc,anncid=3001,anncarg=CDPN;

Failure Condition

The release cause of a failed call is defined by a Failure Condition and Translation Plan, which enables you to enter overriding failure condition parameters. Specifically, the Failure Condition Table contains the fail type, treatment, release cause, release location and release standard for each route key configured in the Translation Plan Table. The Translation Plan Table also contains a Failure Condition Plan Profile which identifies the release failure profile which overrides the default failure condition profile for a Translation Plan.

Re-route

Re-routing of calls occurs during overflow. When overflow occurs, calls are re-routed to another Route List where they are cycled through the route process again.

Next Treatment

'Next Treatment' applies only to announcements (treatType=ANNC) and enables you to provision call processing to continue after an announcement ends. To provision for this, you assign CONTINUE to the nextTreat parameter. CONTINUE is only valid for screening.

Matching a Translation Plan to a Route Name

Ingress trunks are matched to a Translation Plan via the Ingress Trunk Table. In this table, a trunk group is assigned to a specific Translation Plan. The plan, then, corresponds to a Route Label and Key.

In the simplified view of the Translation Table, the Plan ID is associated with at least one Route Label and Key; however, you can enter up to three Route Label/Key combinations. The router searches on the first Route Label/Key entered, and continues searching until a match is found. If a match is not found for the first key, then the router moves on to the second key. If a match is not found for the second key, the router searches on the third key. The other fields in the Translation Plan Table are used with key fields in the Routing Table to determine the destination of the call. Table A illustrates a sample of the Translation Plan Table.

Table A. Sample Information Taken from the Translation Plan Table

Plan ID	Route Label/Key	Translation Modifiers
Basic	SBC-TNS & BOSTON-CDPN & ASIA-GENDGTS	●●●●●●

The Route Label/Key then, is matched with the Routing table, defined in Table B. This table contains a list of label keys/values, route destinations and corresponding actions. This simplified view highlights the two primary parameters involved: the Label and the route destination to which it points. In the switch, every label key must be paired with a Route Destination in order to route calls.

Table B. Linking the Routing Table to the Route List Table

Label Key and Values	Route Destination	Route Modifiers
SBC-TNS-0211-DEFAULT	RTLIST-SBC	
BOSTON-CDPN-INTNATNUM-91	RTLIST-BOSTON	
ASIA-GENDGTS-DEFAULT	TRANS-ASIA	●●●●●●

In the Table B example, the label key is used as the route key, and every route destination to which the switch can route calls is entered in the table and associated with a label key.

The rest of the columns shown in Table B consist of a large number of parameters labeled Route Modifiers. These Route Modifiers define how the route will be used for that specific Route Destination only. Keep in mind that all information stored in the

Route lists associated with a route label are identified in the Route Destination field of the Routing Table. Details for each route list identified in the Route Table are stored in the Route List Table. In Table B above, you can see that SBC-TNS-0211-DEFAULT is associated with RTLIST-SBC. In Table C, below, you can see that RTLIST-SBC is assigned an allocation method of circular and that overflow treatment does not apply. For BOSTON-CDPN-INTNATNUM-91, the associated route list is RTLIST-BOSTON, the allocation method is Distribution and overflow treatment does apply. This means that Overflow Treatment is used if the call set up on this route fails because no bearers are available.

Table C. Linking the Translation Plan Table to the Routing Table

Route List Name	Allocation Method	Overflow Treatment
RTLIST-SBC	Circular	
RTLIST-BOSTON	Distribution	Y

A route list is then associated with a route, where the bearer group type and group number are assigned to the route. This information, combined with information stored in the Egress Trunk Table, help determine where the call is finally to be routed. Refer to Table D to see the Route Table fields.

Table D. Linking the Routing Table to the Route List Table

Route List Name and Index	Bearer Group Type	Group Number	Route List ID	Digit Modify ID	Weight
RTLIST-SBC-1	TGN	203			
RTLIST-BOSTON-20	ISDNIF	1400			

Time of Day Routing

Route Lists can be provisioned to point to Time of Day routing parameters. When TIMEOFDAY is selected as the allocation method on the Route List Table, the router accesses the Route Schedule Table, as shown in Table E.

In the switch, using a Profile Name enables scheduling of different routes for an incoming call based on time of day for each day of the week and for specific dates. Table E, for example, illustrates various profile names and the route lists with which they are associated.

Table E. Time of Day Route Schedule Table

Route List Name	Profile Name	Route List
RL_TOD	TODP_Holidays	RL_WCA
RL_TOD	TODP_Weekdays	RL_WCA
TL_TOD	TODP_Weeknights	RL_VZ
RL_TOD	TODP_Weekends	RL_VZ
RL_TOD	TODP_Default	RL_VZ

Table F shows each profile and the date, day and time each profile is to be applied to the calls associated with the matching Route List.

Profiles may be created either by time of day/day of week or for specific days of the year, allowing different routing treatment for days such as holidays.

Table F. Time of Day Schedule Profile Table

Profile Name	Date/Day/Time
TODP_Holidays	12/25,10/31,1/1
TODP_Weekdays	MTWRF-6am-6pm
TODP_Weeknights	MTWRF-6pm-6am
TODP_Weekends	SS-all hours
TODP_Default	Add days, all hours

Matching a Route List Name to a Bearer Group

A selected route, in turn, points to a Route List Table that lists all route lists and the allocation (hunting algorithm) used to route each call. Each route list consists of routes that exist in the Route Table. The Route List Name and Index in the Route List correspond with the Route List ID, which determines which route list the call will use. The Bearer Group Type and Bearer Group Number are also key fields in the Route Table which help to determine over what interface or protocol (CAS, ISUP, GR-303, for instance) the call will be routed.

If a bearer group and group number are not used to route the call, then the call is assigned to a route list ID. Specifications within the route list are what is used to route the call.

The Route Table contains an ordered list of trunk groups, lines and other routes.

Table G. Route Table

Route List Name and Index	Bearer Group Type	Group Number	Route List ID
Route1-1	TGN	203	
Route1-10	ISDNIF	14000	
Route1-20			Route2

Routing Tables

The following tables display the various parameters and information needed to successfully route a call through the switch. These tables are described in this section:

- Ingress Trunk Table
- Translation Plan Table
- Routing Table
- Route List Table
- Route Table
- Class 4 Subscriber Table
- Screening Table
- Digit Modification, Dialed Numbers Table
- Digit Modification, Generic Table
- Digit Modification, Parameters Table
- Digit Modification, TNS Table
- Treatment Table
- Egress Table

Ingress Trunk Table

Incoming calls assume values set up in the Ingress Trunk Table, in order to be routed through the switch. The Ingress Table (Table H) associates a trunk group with a translation plan.

Table H. Ingress Trunk Table

Field	Default Value	Description
trkGrpNum	Default Value:	The number of the incoming trunk group to be associated with a Translation Plan.
plan		The Translation Plan name.
dgtScrn	Default Value: NULL	Identifies the outgoing trunk group screening table name, previously defined with ENT-DIGIT-SCREEN and which contains a list of restricted trunk groups. This parameter prevents incoming/outgoing trunk combinations
routeCost	Default Value: 0	Identifies the cost of the trunk group. The value 101 indicates that the trunk group is not available for routing.
bearerCap	Default Values: SPEECH&UNRESDIGITAL& VIDEO&DIGITALWITH TONES (for BICC/ISUP/SIP)	Identifies the bearer capabilities for the trunk group, with ampersands (&) to separate multiple bearer capabilities.
ActionTermAttmpt	Default Value: NULL	Identifies the action to take after the trunk group has been chosen as an outgoing interface for the call.
UseSwitchID	Default Value: N	Identifies whether to enable DMS switch identification routing/transport.

Translation Plan Table

Table I shows the complete set of parameters that can be entered as modifiers in the Translation Plan Table. These parameters modify the behavior of the route with which they are associated. Digit manipulation and screening is also available at this level. This allows digits to be added or deleted to the DN when this particular Trunk Group is accessed by this Route.

Table I. Translation Plan Table

TRANSLATION PLAN		
Field	**Default Value**	**Description**
plan	Default Value:	The dial or numbering plan to be applied before the call is set up.
actnInfoCol	Default Value: NULL	Action Information Collected is done before number analysis/dial plan analysis and defines the various manipulations that need to be performed on this partition. The string format is specified as a separate section, named Action String.
actnInfoAnlz	Default Value: NULL	Action Information Analyzed is performed prior to AIN trigger analysis and defines the various manipulations that need to be

		performed on this partition. The string format is specified as a separate section named Action String.
RtLbl & rtKey	Default Value:	This defines the Routing Table label, that is, the Routing key used for routing. This key combination must exist in the ROUTE-DIGITS Table.
rlsFailCndPrfl	Default Value: NULL	Any exceptions defined in the Fail Condition Profile Table will override the default exception behaviors. This must be previously defined using the PRFL-FAILCND command.
altPlan	Default Value: NULL	Alternate Translation Plan. If this is not NULL, the parameters in this plan are ignored, and the parameters in the identified plan are used instead. This can be used for emergency procedures.

Routing Table

Table J represents the Routing Table. This table defines parameters necessary to route the call to its destination. The Row ID contains a partition that reflects the Translation Plan to be applied.

Table J. Routing Table

ROUTING		
Field	**Default Value**	**Description**
rowId	Default Value:	Consists of the Translation Plan ID, type of call, type of number.
rtDest		Route Destination must be defined as a Translation Plan, Treatment ID, or Route Partition and key to use.
actn	Default Value: NULL	The various actions to be performed on values that match this route.
minCost	Default Value: 0	The minimum cost of the outgoing trunk group.
maxCost		The maximum cost of the outgoing trunk group.
reRoute		Indicates whether calls getting to this route are rerouted on call setup failure on a downstream switch. Options are: Y, N

Route List Table

The keys in the Route List Table (Table K) identify the hunting algorithm to be applied to the call, as well as whether or not to support call overflow.

Table K. Route List Table

ROUTE LIST		
Field	**Default Value**	**Description**
rtListName	Default Value:	The Route List Name is the name of the route list associated with a specific hunting algorithm. All numbers entered into this route list are treated in the same manner.
alloc		The Allocation Method indicates the hunting algorithm to be used when searching for a route. Options are: • Ascending • Descending • Circular • % Distribution • Least Cost • TimeofDay • Random
ovrFlowTreat	Default Value: NULL	An entry in this field determines whether or not overflow treatment applies to calls included in this route list. Overflow Treatment should be used if the call set up on this route fails because no bearers are available.

Route Table

The keys in the Route Table (Table J) identify the Bearer Group Interface Type and Number.

Table L. Route Table

ROUTE		
Field	**Default Value**	**Description**
RtList & index	Default Value:	The Route List name and Index identify the name of the route list to which this route belongs or to which this route entry points.
bgnType		The Bearer Group Interface Type. The Bearer Group must be provisioned before the interface type. The trunk group number covers

		ISUP, BICC, CAS and SIP trunks. Options are: CASIF GR303 ISDNIF MGCP TGN
bgnNum	Default Value:	The Bearer Group Number covers ISUP, BICC, CAS and SIP trunks. Options are: CASIF range: 1-2147483647 GR303 range: 1-32767 ISDNIF range: 1-32767 MGCP range: 1-10000 TGN range: 1-9999
rtList	Default Value: NULL	The Route List entry points to another route that needs to be used. It cannot be used when the Bearer Group Number is used.
DgtModKey		The optional Digit Modification key is used to change parameters that reach this route.
weight	Default Value: 10	This field indicates the relative weight of this route, if the hunting method for the route list is set to DISTRIBUTION.

Class 4 Subscriber Table

The keys in the Class 4 Subscriber Table (Table M) identify the number of an incoming subscriber call, and the carrier for which the subscriber assignment parameters apply.

Table M. Class 4 Subscriber Table

CLASS 4 SUBSCRIBER		
Field	**Default Value**	**Description**
SubscriberId & callType	Default Value:	The Subscriber ID is the NPA-NXX-XXXX of the subscriber. The call type reflects the call type for which the subscriber assignment parameters apply. Options are: InterLATA IntraLATA International
carrier	Default Value:	This field indicates the carrier for which the subscriber assignment parameters apply.

subStatus		This field indicates the status fo the subscriber. Options are: ACTIVE INACTIVE

Screening Table

The Screening Table (Table N) lists the parameters for screening for authorization, blocking and identification of fraud calls.

Table N. Screening Table

SCREENING		
Field	**Default Value**	**Description**
resultType	Default Value: FAIL	The Result specified what, of the following actions, has to be done. Options are: PASS – call has passed screening FAIL – call will be disconnected TREATMENT – specified treatment will be performed AUTHCODE – call must be authorized – can only be used if called from InfoAnalyze SCREEN – more screening needs to be done TRANSPLAN – change translation plans during a screening step. Only valid if the screening is called as an InfoCollected action.
fraudTrapPrfl	Default Value: NULL	This field represents the fraud trap profile to use if this is a fraud situation.
treatment	Default Value: NULL	This field cannot be NULL if the result type is TREATMENT. It should not be specified otherwise.
dgtScrnKey	Default Value: NULL	This field indicates the next screening operation to be performed. This field cannot be NULL if the result type is SCREEN. It should not be specified otherwise.
authPrompt	Default Value: ANNC	This field specifies the type of prompt for the user to enter the authorization code. This can be either a tone or an announcement

		message. Options are: 350 400 ANNC
authMode	Default Value: NONE	This field indicates the mode of authcode operation, which can be: - One pinCode per one authCode - Many pins per one - Only authCodes - Only pinCodes - Account code length >0 - Account code length >0 and authCodes cannot be NONE if result type is AUTHCODE Options are: ONEPIN ONLYAUTH NONE ONLYPIN ONLYACNT ACNTAUTH
AcntCodeLen	Default Value: 0	The length of the account code. 0 implies this option is disabled. The entry in this field cannot be 0 if authMode is ONLY ACNT or ACNT AUTH.
AuthList	Default Value: NULL	An authorization list is created previously with ENT-LIST-AUTHCODE. The entry in this field cannot be NULL if authMode is ONEPIN, ONLYAUTH, ONLYPIN or ACNTAUTH.
Transplant	Default Value: NULL	If specified, this is the translation plan that is to be used on a screening match. The entry in this field cannot be NULL if resultType is TRANSPLAN. It should not be specified otherwise.

Digit Modification Tables

The Digit Modification Tables consist of these tables:

- Dialed Numbers
- Generic
- Parameters
- TNS

Digit Modification, Dialed Numbers Table

The Dialed Numbers Table (Table O) identifies the Nature of Address Indicator, modification type, strip digits and insert digits.

Table O. Digit Modification, Dialed Number Table

DIALED NUMBER		
Field	**Default Value**	**Description**
dnLbl	Default Value:	The digit modification label.
nai	Default Value: DEFAULT	The nature of address indicator, different for the three types.
minDgts	Default Value: 0	The minimum length of the incoming addressing digits (CDPN, CGPN, CHRGN) for this rule to be matched.
modType	Default Value: NOACTION	The type of manipulation to perform on the primary key. This value validates the rest of the parameters present. Options are: STRIPONLY – removes the number of digits specified by STRIPDGTS parameter STRIPINSERTDGTS – removes the number of digits and inserts new digits STRIPINSERTSRC – removes the number of digits and inserts from the specified source INSERTDGTS – inserts specified digits INSERTSRC – inserts digits from the specified source REPLACEDGTS – replaces digits with those specified in the INSERTDGTS parameter REPLACENAI – used in cases where the digits are not changed, just the NAI. DELETE – removes the parameter NOACTION – no action taken.
altModType	Default Value: NOACTION	The type of manipulation to perform on the alternate parameter. Options are: REPLACE DELETE NOACTION
maxDgts	Default Value: 31	Maximum length to match this rule.
stripDirn	Default Value:	Specifies where to start from before

	LEFT	moving StripPos number of digits over. LEFT starts at the leftmost digit and works inwards to the right. RIGHT starts at the right most digits and works inwards to the left.
stripPos	Default Value: 0	Specifies the digit position in the string where stripping will begin (for example, 1 means starting at the first digit). This entry cannot be 0 when using STRIP mode.
stripDgts	Default Value: 0	The number of digits to strip. This entry is ignored if only inserting. This entry cannot be 0 when using STRIP mode.
stripDest	Default Value: NULL	Identifies a register or parameter to store the stripped digits. REG1-3 are scratchpad registers for holding digits during a translation. These registers are only valid during one call translation, that is, they cannot be passed from one call to another.
insertDirn	Default Value: LEFT	Identifies whether to insert on the left side or the right side of the specified position.
insertPos	Default Value: 0	Specifies the digit position in the string where inserting will begin (for example, 1 means starting at the first digit). This entry cannot be 0 when using INSERT mode.
insertDgts	Default Value: NULL	Specifies digits to insert. This entry cannot be NULL when using INSERT mode.
insertSrc	Default Value: NULL	Identifies another parameter/call-related value to prefix. Options are: OLI CPC REG1 REG2 REG3
newNai	Default Value: NULL	Specifies the new NAI for this number. NULL leaves the NAI unchanged.

altParamValue	Default Value: NULL	A key and value. This is a way of changing non-key parameters on a match on the key field. This entry cannot be NULL if altModType is REPLACE.
nextDgtMod	Default Value: NULL	The digit modification table label to call next on a match for this row. This entry cannot be NULL when both modType and altModType are NOACTION.

Digit Modification, Generic Table

The Generic Table (Table P) identifies the parameters used for identifying calls with generic digits or generic address parameters.

Table P. Digit Modification, Generic Table

GENERIC		
Field	**Default Value**	**Description**
dmLbl	Default Value:	The digit modification table label.
genType		The key to use for matching. Options are: GAP GENDGTS
nmbrType		The key to use for matching. Options are: 0-31 for GAP 0-255 for GENDGTS
digits	Default Value: DEFAULT	The leading digits of the number to match. Depending on the type, it could be hexadecimal, ASCII or BCD.
modType	Default Value: NOACTION	The type of manipulation to perform on the primary key. This value validates the rest of the parameters present. STRIPONLY – removes the number of digits specified by STRIPDGTS parameter STRIPINSERTDGTS – removes the number of digits and inserts new digits STRIPINSERTSRC – removes the number of digits, inserts digits from the specified source INSERTDGTS – inserts specified digits INSERTSRC – inserts digits from

		the specified source REPLACEDGTS – replaces digits with those specified in the INSERTDGTS parameter DELETE – removes the parameter NOACTION – no action is taken
altModType	Default Value: NOACTION	The type of manipulation to perform on the Alternate parameter. Options are: REPLACE – replaces the parameter digits specified in AltParam DELETE – removes the parameter specified in AltParam NOACTION – no action is taken
stripDirn	Default Value: LEFT	Specifies where to start from before moving StripPos number of digits over. LEFT starts at the leftmost digit and works inwards to the right. RIGHT starts at the rightmost digits and works inwards to the left.
stripPos	Default Value: 0	Specifies the digit position in the string where stripping will begin (for example, “1” means starting at the first digit). The entry cannot be 0 when using STRIP mode.
stripDgts	Default Value: 0	The number of digits to strip. This entry is ignored if only inserting. The entry cannot be 0 when using STRIP mode.
stripDest	Default Value: NULL	Identifies a register or parameter to store the stripped digits. REG1-3 are scratchpad registers for holding digits during a translation. These registers are only valid during one call translation; that is, they cannot be passed from one call to another.
insertDirn	Default Value: LEFT	Identifies whether to insert on the left side or the right side of the specified position.
insertPos	Default Value: 0	Specifies the digit position in the string where inserting will begin (for example, “1” means starting at the first digit). The entry cannot be 0 when using INSERT mode.
insertDgts	Default Value: NULL	Digits to insert. The entry cannot be NULL when using INSERT mode.
insertSrc	Default Value: NULL	Identifies another parameter/call-related value to prefix. Options are: NULL OLI CPC REG1

		REG2 REG3
altParamValue	Default Value: NULL	A key and value. This is a way of changing non-key parameters on a match on the key field. The entry cannot be NULL if altModType is REPLACE.
newValue	Default Value:	Specifies the new value the parameter key should take. If the newValue is equal to NONE, the key is removed. The length is 2 for CPC/OLI, 4 for CIP/PCIC. For TNS if it is 4, only the carrier value is changed; if it is 7, the carrier and OZZ/CktCode values are changed. Other lengths are invalid.
nextDgtMod	Default Value: NULL	The digit modification table label to call next on a match for this row. This entry cannot be NULL when both modType and altModType are NOACTION.

Digit Modification, Parameters Table

The Parameters Table (Table Q) lists the parameters used for identifying calls with various call parameters.

Table Q. Digit Modification, Parameters Table

PARAMETERS		
Field	**Default Value**	**Description**
dmLbl	Default Value:	The digit modification table label.
modType	Default Value: NOACTION	The type of manipulation to perform. It validates the other non-null parameters. REPLACE: replaces the primary key. Cannot be used for CALLTYPE or BGN; that is, modType=NOACTION for these two keys. DELETE: removes the parameter NOACTION: skip this digit medication
altModType	Default Value: NOACTION	The type of manipulation to perform on the Alternate parameter. REPLACE: replaces the parameter digits specified in AltParam DELETE: removes the parameter specified in AltParam NOACTION: skip this digit modification

newValue	Default Value: NULL	The new value for this parameter. Cannot be specified for CALLTYPE or BGN; that is, you cannot change these two parameters. This entry cannot be NULL when modType is REPLACE.
altParamValue	Default Value: NULL	A key and value. This is a way of changing non-key parameter on a match on the key field. This entry cannot be NULL when altModType is REPLACE.
altValue		Specifies the new value the parameter key should take. Options are: TNS 0-9999255 CSI: PRESUBDIAL PRESUBNOTDIAL PRESUBUNKNOWN NOTPRESUB UNKNOWN
nextDgtMod		The digit modification table label to call next on a match for this row. This entry cannot be NULL when modType and altModType are both NOACTION.

Digit Modification, TNS Table

The TNS Table (Table R) identifies the parameters used for the transit network selection (TNS), which is the circuit code for ISUP calls, and the Carrier or 0ZZ codes for CAS Feature group D.

Table R. Digit Modification, TNS Table

TNS		
Field	**Default Value**	**Description**
dmLbl	Default Value:	The digit modification table label.
callTypeCode		The CAS 0ZZ,1NX code or ISUP Circuit Code. DEFAULT means CallType ignored.
prtcl		The incoming trunk group protocol.
modType	Default Value: NOACTION	The type of manipulation to perform. It validates the other non-null parameters. REPLACETNS: replaces both the Carrier ID and the Call Type Code REPLACECARRIER: replaces the Carrier ID REPLACECALLTYPE: replaces the Call Type Code DELETE: removes the parameter NOACTION: skip this digit

		modification
altModType	Default Value: NOACTION	REPLACE: replaces digits with those specified in the newTns parameter DELETE: removes the parameter NOACTION: skip this digit modification
newCarrier	Default Value: NULL	The new value of TNS on matching the TNS-0ZZ-prtcl. NULL implies no change. Can't be NULL for modTypes REPLACETNS and REPLACECARRIER
newCallTypeCode	Default Value: NULL	The new value of 0ZZ code or circuit code. Can't be NULL for modTypes REPLACETNS and REPLACECALLTYPE
altParamValue	Default Value: NULL	A key and value. This is a way of changing non-key parameter on a match on the key field. Can't be NULL if altModType is REPLACE
altValue		Specifies the new value the parameter key should take. Options are: CPC, OLI: 00-FF TNS: 0-9999255 CIP: 0-9999 CSI: PRESUBDIAL PRESUBNOTDIAL PRESUBUNKNOWN NOTPRESUB UNKNOWN
nextDgtMod	Default Value: NULL	Refer to section 1.1 for parameter details. The digit modification table label to call next on a match for this row. Can't be NULL when both modType and altModType are NOACTION

Treatment Table

The Treatment Table (Table S) contains the parameters that identify whether a call should receive tone/announcement treatment, failed condition, or some other treatment.

Table S. Treatment Table

TREATMENT		
Field	**Default Value**	**Description**
treatmentId	Default Value:	The identification of this treatment.
treatType		The type of treatment that is to be provided. ANNC: play an announcement REROUTE: Use the dgtModKey to reroute FAILCND: A condition to be generated.
anncId	Default Value: NULL	The ID of the announcement to be played. The announcement IDs must be in the range of the internal switch announcements (must be predefined by AUDIO-ANNC or ANNC-EXT). Only valid when treatType = ANNC.
failCnd	Default Value: NULL	The condition, previously defined in the condition table, triggered for this treatment. Use RTRV-FAILCND to determine the existing conditions. Usually used with routing to a treatment, which then uses a condition. This entry cannot be NULL if treatType is FAILCND.
dgtModKey	Default Value: NULL	The digit modification object that is used to change parameters for a reroute. Only valid when treatType = REROUTE.
nextTreat	Default Value: NULL	Only valid when treatType = ANNC. CONTINUE is a “special” treatment that lets call processing continue after the announcement ends. CONTINUE is only valid for screening.

Egress Trunk Group Table

The Egress Trunk Group Table (Table T) associates a trunk group with a route screen, bearer cap and cost.

Table T. Egress Table

EGRESS		
Field	**Default Value**	**Description**
trkGrpNum	Default Value:	The number of the outgoing trunk group.
dgtScrn	Default Value: NULL	Identifies the outgoing trunk group screening table name, previously defined with ENT-

		DIGIT-SCREEN and which contains a list of restricted trunk groups. This parameter prevents incoming/outgoing trunk combinations
routeCost	Default Value: 0	Identifies the cost of the trunk group. The value 101 indicates that the trunk group is not available for routing.
bearerCap	Default Values: SPEECH&UNRESDIGITAL& VIDEO&DIGITALWITH TONES (for BICC/ISUP/SIP)	Identifies the bearer capabilities for the trunk group, with ampersands (&) to separate multiple bearer capabilities.
ActionTermAttmpt	Default Value: NULL	Identifies the action to take after the trunk group has been chosen as an outgoing interface for the call.

Routing Scenarios

Re-routing of Incoming CGPNs

Scenario: The switch supports re-routing of specific incoming Calling Party Number (CGPNs) to alternate destinations, including treatment to customized announcements on a Carrier Identification Code (CIC) basis.

Conditions: Treatment1 sends a call to announcement 3000 and TreatFail1 fails the call if there is a vacant code. If the fail condition is applied, the call is released to PRIVNETRU-CCITT.

1. Establish routes for various trunk groups, assigning route lists to each. For example:

   ENT-ROUTE::RL18-1:::BGN=TGN-1029;
   ENT-ROUTE::RL19-1:::BGN=TGN-1030;
   ENT-ROUTE::RL20-1:::BGN=TGN-1020;

2. Create announcement 3000 using this command:

   ENT-AUDIO-
   ANNC::3000:::name=dateandtime,desc=DATETIMEAUDIOFILE,msglist=DAT_MD-TME_T12;

   OR

   ENT-ROUTE-DIGIT::RD49-TNS-0234:::RtDest=RTLIST-RL18;

3. Create a profile for the fail condition for VACANT_CODE using this command:

   ENT-PRFL-FAILCND::PCICFAIL1-VACANT_CODE-ISUP:::FailType=RELEASE,Release=2-
   PRIVNETRU-CCITT;\

4. Define TreatFail1 using this command and applying the conditions stated for this scenario:

   ENT-TREATMENT::TreatFail1:::TreatType=FAILCND,failcnd=VACANT_CODE;

5. Define Treatment1 using this command and applying the conditions stated for this scenario:

   ENT-TREATMENT::Treatment1:::TreatType=ANNC,AnncId=3000,ANNCARGS=DATE-
   CURRDATE&TIME-CURRTIME,NextTreat=TreatFail1;

6. Apply route digit destinations to a specific CGPN (5086808001) and to the default, and to the TNS of 0234 and the default. For example:

   ENT-ROUTE-DIGITS::RD48-CGPN-DEFAULT:::RtDest=RTLIST=RL11;
   ENT-ROUTE-DIGITS::RD48-CGPN-UNINATNUM-5086808001:::RtDest=RTKEY-RD49-TNS;
   ENT-ROUTE-DIGITS::RD49-TNS-DEFAULT:::RtDest=RTLIST=RL19;

ENT-ROUTE-DIGITS::RD49-TNS-0234:::RtDest=TREAT-Treatment1;

7. Create translation plan 47, establishing a release fail condition profile. For example:

   ENT-TRANS-PLAN::TP47:::rtKeyList=RD48-CGPN,RLSFAILCNDPRFL=RTFAILED;

8. Enter a trunk group and associate it with Translation Plan 47 using this command:

   ENT-TRKGRP::46:::ISUP:Name=TGN46,DPC=2-2-2,TGPROFILE=1,transplant=TP47;

9. Establish SS7 trunk 46 using this command:

   ENT-SS7-TRK::46-46&&-46:::IOMPORTDS0=IOM-3-T3-2-PORT-3-T0-22;

Time of Day Routing

Scenario: The switch supports Time of Day, Day of Week and Holiday routing filters that can be applied post routing.

1. Assign specific days and/or dates with specific times to each schedule. For example:

   ENT-PRFL-SCHED::SchWkEND:::SAT=0000-2400,SUN=0000-2400;
   ENT-PRFL-SCHED::SchHDAY:::DATE1=01-01,DATE2=07-04,DATE3=05-26,DATE4=09-01,DATE5=11-23,DATE6=11-24,DATE7=12-25,TIME=0000-2400;
   ENT-PRFL-SCHED::SchOPK1:::MON=0000-0700,TUE=0000-0700,WED=0000-0700,THU=0000-0700,FRI=0000-0700;
   ENT-PRFL-SCHED::SchPEAK::: MON=0000-2100,TUE=0000-2100,WED=0000-2100,THU=0000-2100,FRI=0000-2100;
   ENT-PRFL-SCHED::SchOPK2::: MON=2100-2400,TUE=2100-2400,WED=2100-2400,THU=2100-2400,FRI=2100-2400;

2. Designate route list RLSCHED1 as a Time of Day list using the following command:

   ENT-ROUTE-LIST::RLSCHED1:::ALLOC=TIMEOFDAY;

3. Assign different schedules already associated with RLSSCHED1 to various destination route lists. For example:

   ENT-ROUTE-SCHED::RLSCHED1-SchWkEND:::RTLIST=RTLIST17;
   ENT-ROUTE-SCHED::RLSCHED1-SchHDAY:::RTLIST=RTLIST18;
   ENT-ROUTE-SCHED::RLSCHED1-SchOPK1:::RTLIST=RTLIST19;
   ENT-ROUTE-SCHED::RLSCHED1-SchPEAK:::RTLIST=RTLIST20;
   ENT-ROUTE-SCHED::RLSCHED1-SchOPK2:::RTLSIT=RTLIST21;
   ENT-ROUTE-SCHED::RLSCHED1-SchDEFAULT:::RTLIST=RTLIST22;

4. Associate the route schedule RLSSCHED1 with a Called Party Number default. For example:

   ENT-ROUTE-DIGIT::RD36-CDPN-DEFAULT:::RtDest=RTLIST-RLSCHED1;

5. Associate a Translation Plan with a route destination for a Called Party Number. For example:

   ENT-TRANS-PLAN=TP37:::rtKeyList=RD36-CDPN;

6. Enter an ISUP trunk number of 36, assigning a DPC of 2-2-2, a trunk group profile of 1, and a Translation Plan of TP37. For example:

   ENT-TRKGRP::36:::ISUP:Name=TGN36,DPC=2-2-2, TGPROFILE=1,transplan=TP37;

Route Plans and Route Schedules

Scenario: The switch can support different routing plans depending on the Time, Date or holidays assigned to a route schedule.

1. Enter specific routing information for any Called Party, Calling Party, TNS, etc., associating it with a specific route list containing specific route schedules and times. For example:

   ENT-ROUTE-DIGITS::RD70-CGPN-UNINATNUM-5084808001:::rtdest=RTLIST-RL23;
   ENT-ROUTE-DIGITS::RD70-CGPN-UNINATNUM-DEFAULT:::rtdest=RTLIST-RL25;
   ENT-ROUTE-DIGITS::RD18-CDPN-NATNUM-908:::RTDest=RTLIST-RL11;
   ENT-ROUTE-DIGITS::RD18-CDPN-NATNUM-DEFAULT:::RTDest=RTLIST-RL12;
   ENT-ROUTE-DIGITS::RD19_1-TNS-111:::RTDest=RTLIST-RL13;
   ENT-ROUTE-DIGITS::RD19_1-TNS-DEFAULT:::RTDest=RTLIST-RL14;

2. Assign specific digit modification parameters to Called Party Number 408-8001. Other sample input which can be provided with this command is shown in the sample command:

   ENT-DIGITMOD-DN::REP908-CDPN-NATNUM-4088001:::Modtype=STRIPINSERTDGTS,strippos=1,stripdgts=3,InsertPos=1,insertDgts=908,maxdgts=31;

3. Assign a route list to each translation plan. For example:

   ENT-TRANS-PLAN::TP5013:::rtKeyList=RD19_1-TNS;
   ENT-TRANS-PLAN::TP5014:::actninfocol=DgtModKey-PRE908-CDPN,rtKeyList=RD18-CDPN;
   ENT-TRANS-PLAN::TP5015:::rtKeyList=RD70-CGPN;

   Note that a digit modification parameter has been set up so that digit modification is performed on all called party numbers having NPA 908, during the times associated with translation plan 5014.

4. Assign days, dates and times to schedule profiles already associated to translation plans. For example:

   ENT-PRFL-SCHED::SchPrfl1:::SAT=0000-2400,SUN=0000-2400;
   ENT-PRFL-SCHED::SchPrfl2:::DATE1=01-01,DATE2=07-04,DATE3=05-26,DATE4=09-01,DATE5=11-23,DATE6=11-24,DATE7=12-25,TIME=0000-2400;
   ENT-PRFL-SCHED::SchPrfl3:::MON=0000-0700,TUE=0000-0700,WED=0000-0700,THU=0000-0700,FRI=0000-0700;
   ENT-PRFL-SCHED::SchPrfl4:::MON=0700-2100,TUE=0700-2100,WED=0700-2100,THU=0700-2100,FRI=0700-2100;
   ENT-PRFL-SCHED::SchPrfl5:::MON=2100-2400,TUE=2100-2400,WED=2100-2400,THU=2100-2400,FRI=2100-2400;

5. Assign Translation Plan and Schedule Profile to a Translation Plan combining the two. For example:

   ENT-TRANS-SCHED::TSC1-SCHPRFL5:::Transplan=TP5014;
   ENT-TRANS-SCHED::TSC1-SCHPRFL4:::Transplan=TP5015;
   ENT-TRANS-SCHED::TSC1-SCHPRFL3:::Transplan=TP5014;
   ENT-TRANS-SCHED::TSC1-SCHPRFL2:::Transplan=TP5013;
   ENT-TRANS-SCHED::TSC1-SCHPRFL1:::Transplan=TP5013;
   ENT-TRANS-SCHED::TSC1-DEFAULT:::Transplan=TP5013;

6. Associate ISUP trunk group 5013 with DPC 2-2-2, trunk group profile 1, and Translation Plan TSC1. For example:

   ENT-TRKGRP::5013:::ISUP:Name=TGN5013,DPC=2-2-2,TGPROFILE=1,transplan=TSC1;

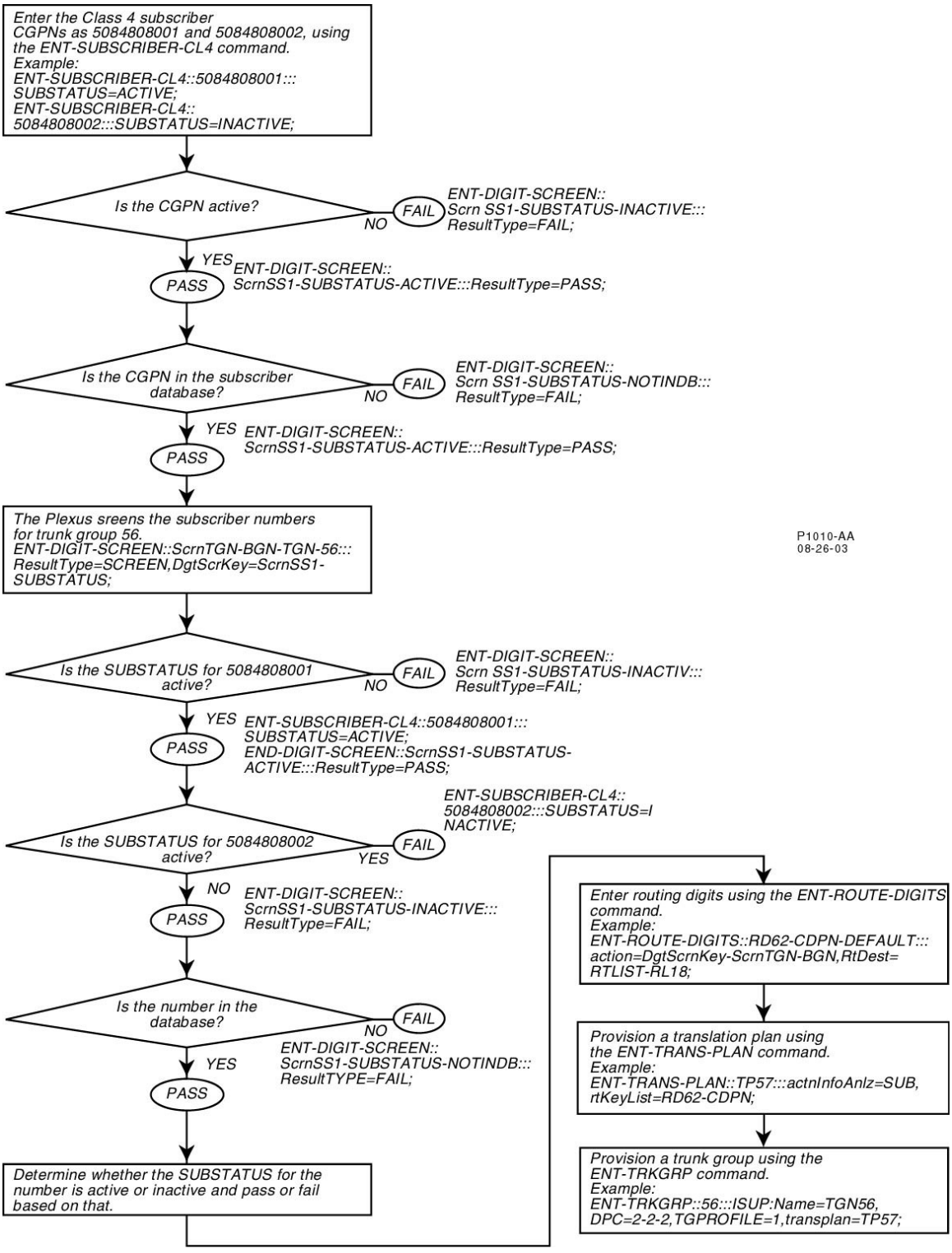
Casual vs. Non-Casual Routing on Trunk Group

Scenario: The switch enables and disables both casual and non-casual routing on a trunk group basis.

Conditions: The Calling Party Numbers (CGPNs) are equal to 5084808001 and 5084808002. The Called Party Number (CDPN) is equal to 6084808001.

By modifying the ResultType in the DIGIT-SCREEN command for SUBSTATUS, the carrier can change the decision of allowing casual routing.

Expected Result: The switch fails the calls if the CGPN is not in the subscriber database and is not in service.


Enter the Class 4 subscriber CGPNs as 5084808001 and 5084808002, using the ENT-SUBSCRIBER-CL4 command.
Example:
ENT-SUBSCRIBER-CL4::5084808001:::
SUBSTATUS=ACTIVE;
ENT-SUBSCRIBER-CL4::
5084808002:::SUBSTATUS=INACTIVE;
Is the CGPN active?
NO
FAIL
ENT-DIGIT-SCREEN::
Scrn SS1-SUBSTATUS-INACTIVE:::
ResultType=FAIL;
YES
PASS
ENT-DIGIT-SCREEN::
ScrnSS1-SUBSTATUS-ACTIVE:::ResultType=PASS;
Is the CGPN in the subscriber database?
NO
FAIL
ENT-DIGIT-SCREEN::
Scrn SS1-SUBSTATUS-NOTINDB:::
ResultType=FAIL;
YES
PASS
ENT-DIGIT-SCREEN::
ScrnSS1-SUBSTATUS-ACTIVE:::ResultType=PASS;
The Plexus sreens the subscriber numbers for trunk group 56.
ENT-DIGIT-SCREEN::ScrnTGN-BGN-TGN-56:::
ResultType=SCREEN,DgtScrKey=ScrnSS1-SUBSTATUS;
P1010-AA
08-26-03
Is the SUBSTATUS for 5084808001 active?
NO
FAIL
ENT-DIGIT-SCREEN::
Scrn SS1-SUBSTATUS-INACTIV:::
ResultType=FAIL;
YES
PASS
ENT-SUBSCRIBER-CL4::5084808001:::
SUBSTATUS=ACTIVE;
END-DIGIT-SCREEN::ScrnSS1-SUBSTATUS-ACTIVE:::ResultType=PASS;
ENT-SUBSCRIBER-CL4::
5084808002:::SUBSTATUS=I
NACTIVE;
Is the SUBSTATUS for 5084808002 active?
YES
FAIL
NO
PASS
ENT-DIGIT-SCREEN::
ScrnSS1-SUBSTATUS-INACTIVE:::
ResultType=FAIL;
Is the number in the database?
NO
FAIL
YES
PASS
ENT-DIGIT-SCREEN::
ScrnSS1-SUBSTATUS-NOTINDB:::
ResultTYPE=FAIL;
Determine whether the SUBSTATUS for the number is active or inactive and pass or fail based on that.
Enter routing digits using the ENT-ROUTE-DIGITS command.
Example:
ENT-ROUTE-DIGITS::RD62-CDPN-DEFAULT:::
action=DgtScrnKey-ScrnTGN-BGN,RtDest=
RTLIST-RL18;
Provision a translation plan using the ENT-TRANS-PLAN command.
Example:
ENT-TRANS-PLAN::TP57:::actnInfoAnlz=SUB,
rtKeyList=RD62-CDPN;
Provision a trunk group using the ENT-TRKGRP command.
Example:
ENT-TRKGRP::56:::ISUP:Name=TGN56,
DPC=2-2-2,TGPROFILE=1,transplan=TP57;

ANI Screening

Scenario: The switch supports originating ANI screening with NPA, NPA-NXX and NPA-NXX-XXXX granularity.

Conditions: In the following scenario, the Called Party Number (CDPN) NPA is 908, and the XXX is 480. The Calling Party Number NPA is 508, the XXX is 480, and the XXXX is 4001.

1. Apply ANI screening to the CDPN NPA by associating it with a treatment. For example:

   ENT-DIGIT-SCREEN::ANINPA-CDPN-UNINATNUM-908:::actn=SCREEN,DgtScrnKey=ANINPA908-CGPN;

2. Apply ANI screening to the CGPN NPA by associating it with a treatment. For example:

   ENT-DIGIT-SCREEN::ANINPA908-CGPN-UNINATNUM-508480:::actn=Treat,Treatment=Treat908;

3. Assign a treatment to a route key for an NPA CDPN. For example:

   ENT-TREATMENT::TRT908480:::treatType=REROUTE,rtKey=RTLBL1-CDPN;

4. Apply ANI screening to the CDPN NPA-NXX by associating it with a treatment. For example:

   ENT-DIGIT-SCREEN::ANINPANXXX-CDPN-UNINATNUM-908480:::actn=SCREEN,DgtScrKey=ANINPANXX-CGPN;

5. Apply ANI screening to the CGPN NPA-NXX by associating it with a treatment. For example:

   ENT-DIGIT-SCREEN::ANINPANXX-CGPN-UNINATNUM-508480:::actn=TRT908,Treatment=TRT908408;

6. Assign a treatment to a route key for an NPA-NXX CDPN. For example:

   ENT-TREATMENT::TRT908480:::treatType=REROUTE,rtKey=RTLBL1-CDPN-908;

7. Apply ANI screening to the CDPN NPA-NXX-XXXX by associating it with a treatment. For example:

   ENT-DIGIT-SCREEN::ANINPANXXX-CDPN-UNINATNUM-908480:::actn=SCREEN,DgtScrKey=ANINPANXX-CGPN;

8. Apply ANI screening to the CGPN NPA-NXX-XXXX by associating it with a treatment. For example:

ENT-DIGIT-SCREEN::ANINPANXX-CGPN-UNINATNUM-5084804001:::actn=Treat,Treatment=TRT9084808;

9. Assign a treatment to a route key for an NPA-NXX-XXXX CDPN. For example:

   ENT-TREATMENT::TRT908480:::treatType=REROUTE,rtKey=RTLBL1-CDPN;

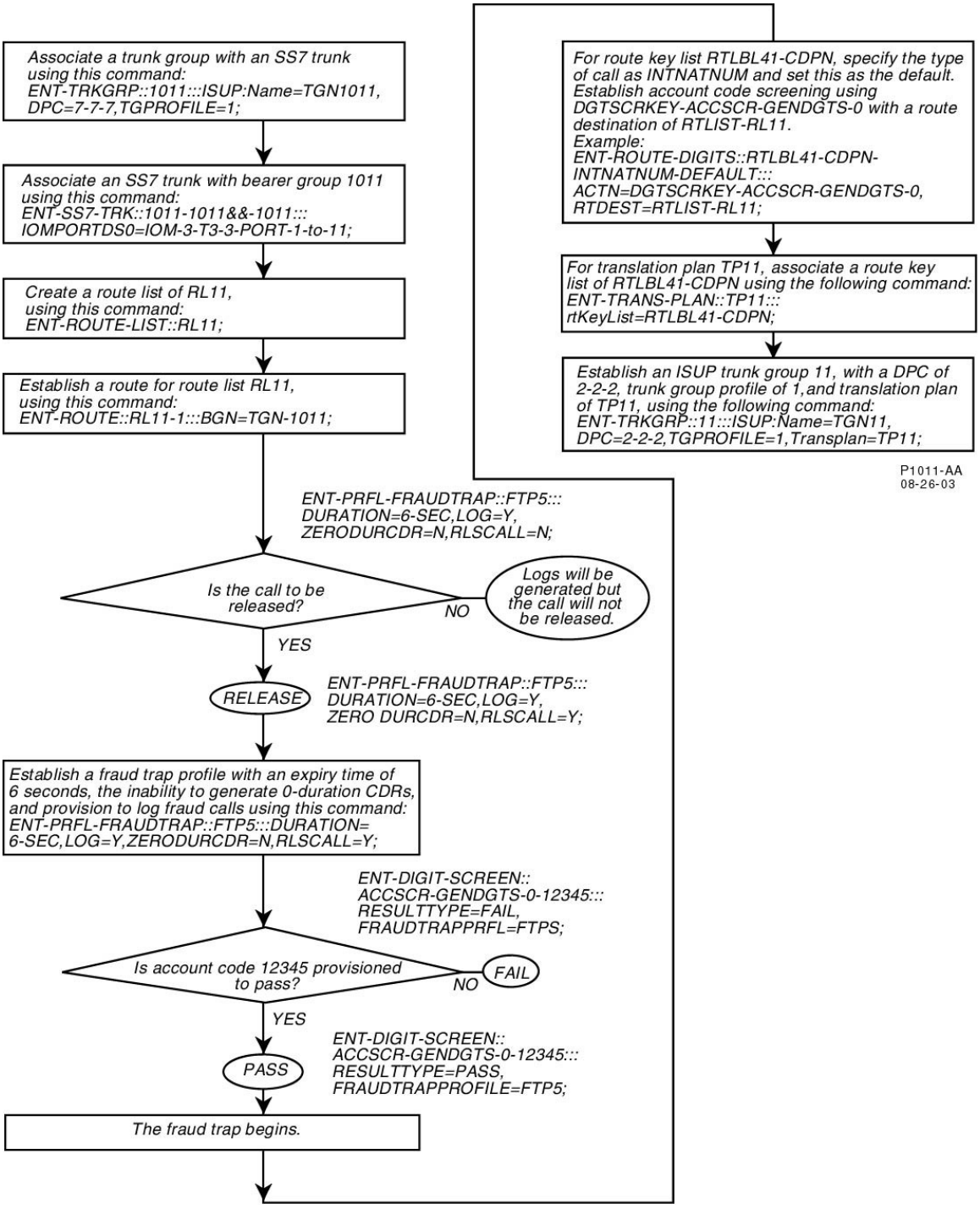
Fraud Traps

Scenario: The switch enables you to set the fraud trap on an account code basis, and keep a record of all calls in progress that meet the fraud trap criteria, enabling you to either manually release the call or set a parameter under which a call should be automatically released.

Conditions: The Carrier can release a fraud call, which is in progress by RLS-CALL, providing just the call Aid. The called number is revealed using the RTRV-FRAUDCALL command and the log for fraud call, also.

The switch allows the Carrier to set the timer in the FraudTrap Profile. After the timer expires and RELEASE=Y, the call will be released automatically. If RELEASE=N, the call will not be released.

The switch keeps record of all fraud calls. All fraud call records can be retrieved using the RTRV-FRAUDCALLS command.


Associate a trunk group with an SS7 trunk using this command: ENT-TRKGRP::1011:::ISUP:Name=TGN1011, DPC=7-7-7,TGPROFILE=1;
Associate an SS7 trunk with bearer group 1011 using this command: ENT-SS7-TRK::1011-1011&&-1011::: IOMPORTDS0=IOM-3-T3-3-PORT-1-to-11;
Create a route list of RL11, using this command: ENT-ROUTE-LIST::RL11;
Establish a route for route list RL11, using this command: ENT-ROUTE::RL11-1:::BGN=TGN-1011;
For route key list RTLBL41-CDPN, specify the type of call as INTNATNUM and set this as the default. Establish account code screening using DGTSCRKEY-ACCSCR-GENDGTS-0 with a route destination of RTLIST-RL11. Example: ENT-ROUTE-DIGITS::RTLBL41-CDPN-INTNATNUM-DEFAULT::: ACTN=DGTSCRKEY-ACCSCR-GENDGTS-0, RTDEST=RTLIST-RL11;
For translation plan TP11, associate a route key list of RTLBL41-CDPN using the following command: ENT-TRANS-PLAN::TP11::: rtKeyList=RTLBL41-CDPN;
Establish an ISUP trunk group 11, with a DPC of 2-2-2, trunk group profile of 1,and translation plan of TP11, using the following command: ENT-TRKGRP::11:::ISUP:Name=TGN11, DPC=2-2-2,TGPROFILE=1,Transplan=TP11;
P1011-AA
08-26-03
ENT-PRFL-FRAUDTRAP::FTP5::: DURATION=6-SEC,LOG=Y, ZERODURCDR=N,RLSCALL=N;
Is the call to be released?
NO
Logs will be generated but the call will not be released.
YES
RELEASE
ENT-PRFL-FRAUDTRAP::FTP5::: DURATION=6-SEC,LOG=Y, ZERO DURCDR=N,RLSCALL=Y;
Establish a fraud trap profile with an expiry time of 6 seconds, the inability to generate 0-duration CDRs, and provision to log fraud calls using this command: ENT-PRFL-FRAUDTRAP::FTP5:::DURATION= 6-SEC,LOG=Y,ZERODURCDR=N,RLSCALL=Y;
ENT-DIGIT-SCREEN:: ACCSCR-GENDGTS-0-12345::: RESULTTYPE=FAIL, FRAUDTRAPPRFL=FTPS;
Is account code 12345 provisioned to pass?
NO
FAIL
YES
PASS
ENT-DIGIT-SCREEN:: ACCSCR-GENDGTS-0-12345::: RESULTTYPE=PASS, FRAUDTRAPPROFILE=FTP5;
The fraud trap begins.

Call Processing Hierarchy

Scenario: When a call comes into the switch, the switch performs call processing on that call. The call processing scenario varies, as the call processing hierarchy changes, depending on the call processing characteristics associated with the incoming call. The following scenario provides a basic example of the switch call processing hierarchy.

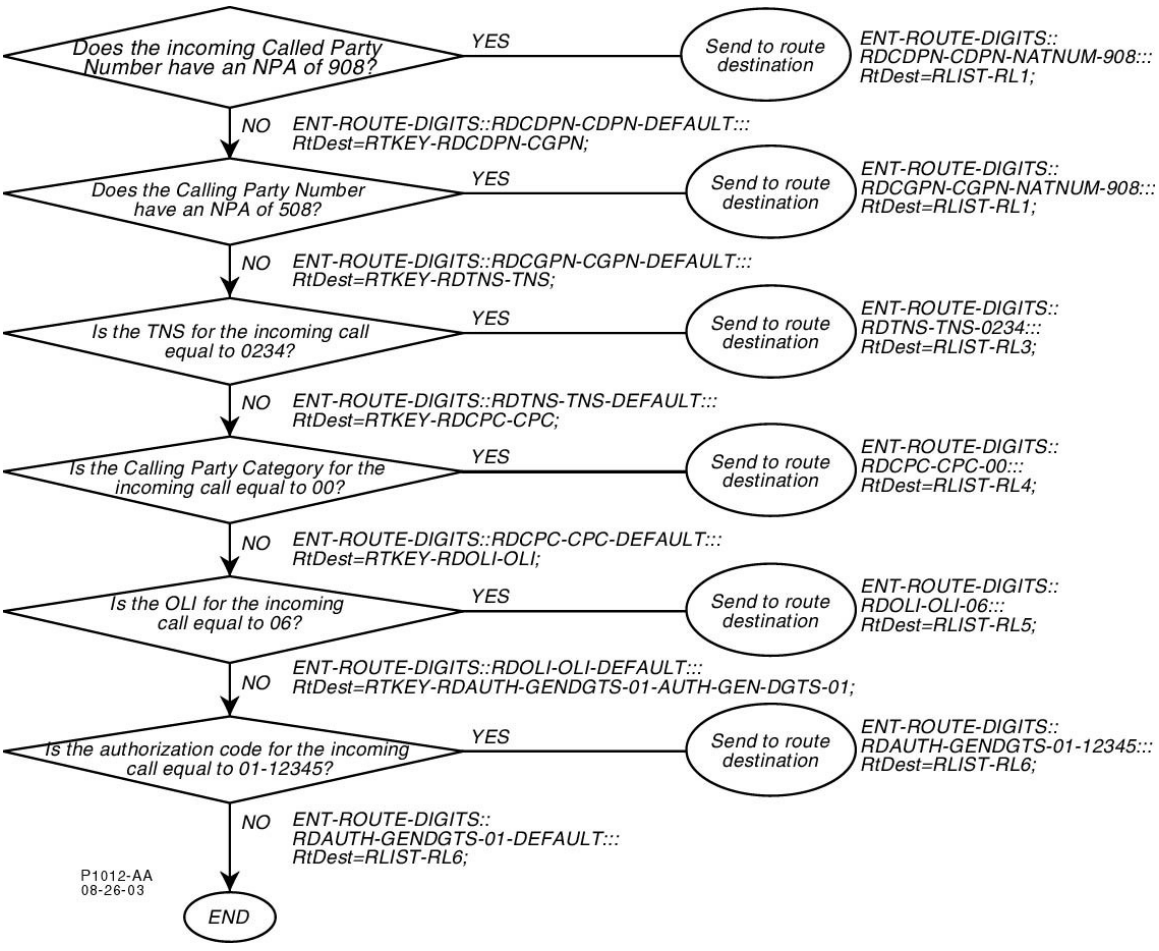
Conditions: ISUP trunk group 506 is provisioned on the switch with a DPC of 4-4-4, trunk group profile of 1 and Translation Plan of TP506. For example:

ENT-TRKGRP::506:::ISUP:Name=ICTGN506,DPC=4-4-4,TGPROFILE=1,Transplan=TP506;

Translation Plan 506 is associated with route key list RD506-CDPN. For example:

ENT-TRANS-PLAN::TP506:::RtKeyList=RD506-CDPN;

When the call comes in, the following analysis is done on that call:



AIN Feature Package

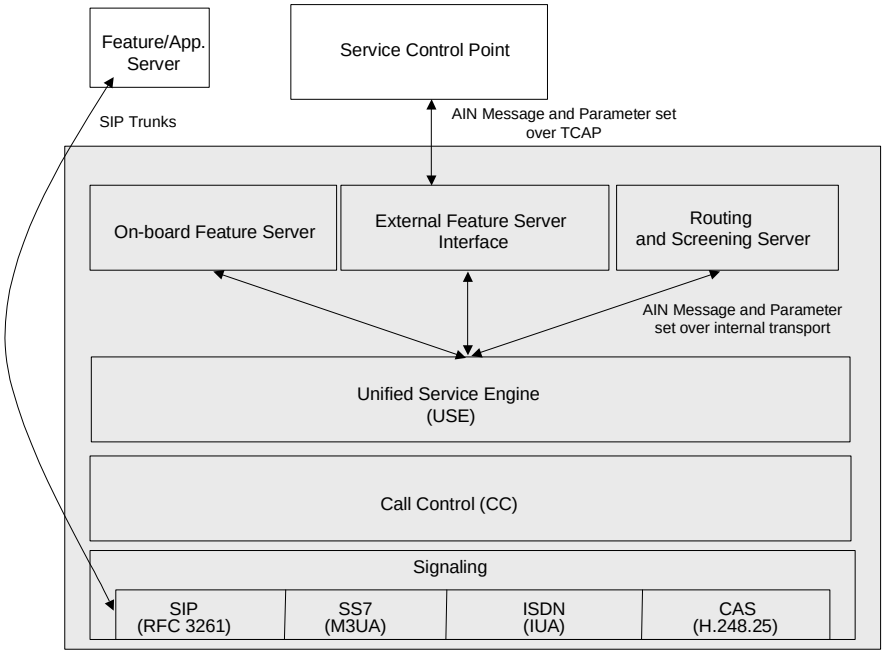
This document contains the following sections:

Scope

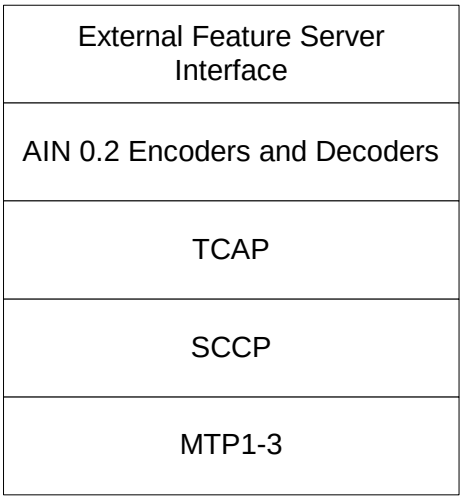
The switch's internal call processing subsystem architecture uses an AIN framework to provide the flexibility to support both internal (on-board) and external features using the AIN message and parameter set. This architecture allows the service provider to easily migrate features between on-board and external databases with just provisioning changes and without any additional software development and compilation. The switch recognizes calls that requires AIN processing without making any assumptions about the service being provided. The switch does this, after encountering an AIN trigger, by suspending call processing temporarily, then either querying its internal database or assembling and launching an external query to service logic located remotely at a Service Control Point (SCP). The subsequent database reply gives the switch information on how to continue processing the call. Some features, like CNAM (Caller Name delivery), LNP (Local Number Portability) and Toll-free, must be accessed from an SCP.

As shown in the following diagram, the Call Control (CC) and Unified Service Engine (USE) combine together to provide the entire set of AIN framework features, which includes:

- PIC(s) (Point-In-Call) in both Originating and Terminating portions of the call.
- Detection Points at above PIC(s), which can be armed as triggers statically as Trigger Detection Points (TDP(s)) or dynamically within a transaction as Event Detection Points (EDP(s)).
- Query and Response processing using both persistent and non-persistent TCAP transactions.
- Caller Interaction using on-board announcement and digit collection capabilities.
- Automatic Code Gapping.
- AIN AMA Record Generation.



The Unified Service Engine (USE) Layer manages the precedence and interaction rules for triggers used and armed by multiple features in the On-board Feature Server (OFS), or features distributed between OFS, SCP, and the Routing and Screening server. The USE layer also uses an AIN 0.2 compliant message and parameter set to interface with any of the three entities. For features residing remotely on an SCP, the External Feature Server Interface layer performs the translation of messages and parameters for transport using TCAP over SS7 as shown below.



The switch supports a subset of AIN 0.2 features for a Service Switching Point (SSP). The following sections describe the supported functionality.

AIN Triggers

Triggering is the process of identifying calls that require AIN handling. Triggers can be subscribed (line-based), group-based, or office-based. The switch supports AIN triggers including:

- Public Feature Code (subscribed)
- Specific Feature Code (subscribed)
- International Prefix (subscribed / office-based)
- Specific Digit String (office-based) and
- Local Number Portability (office-based)

The switch also supports the call-processing triggers listed below. It sends a message (with the same name as the trigger) to the SCP when it encounters one of these triggers, after which the SCP replies with an AnalyzeRoute, a Continue, or a SendToResource message.

- O_Called_Party_Busy
- O_No_Answer
- T_Busy
- T_No_Answer
- Network_Busy

These triggers allow AIN services to detect a busy condition on the originating or terminating end of a call, and to detect when the called party does not answer on the originating or terminating end of a call. These new triggers provide AIN with the capability to redirect calls on busy/no answer.

When it detects an active trigger, the switch suspends normal call processing until it completes communications with its internal database or an SCP.

The switch conforms to the following basic AIN trigger rules:

- AIN trigger points are configurable on both the line and trunk side of the switch.
- For each provisionable trigger, the *service provider* can designate whether to use external or internal processing.
- External processing is via an SCP using Transaction Capabilities Application Part (TCAP) messages.
- Point codes designating the SCP(s) to which TCAP queries will be directed are provisioned on the switch.

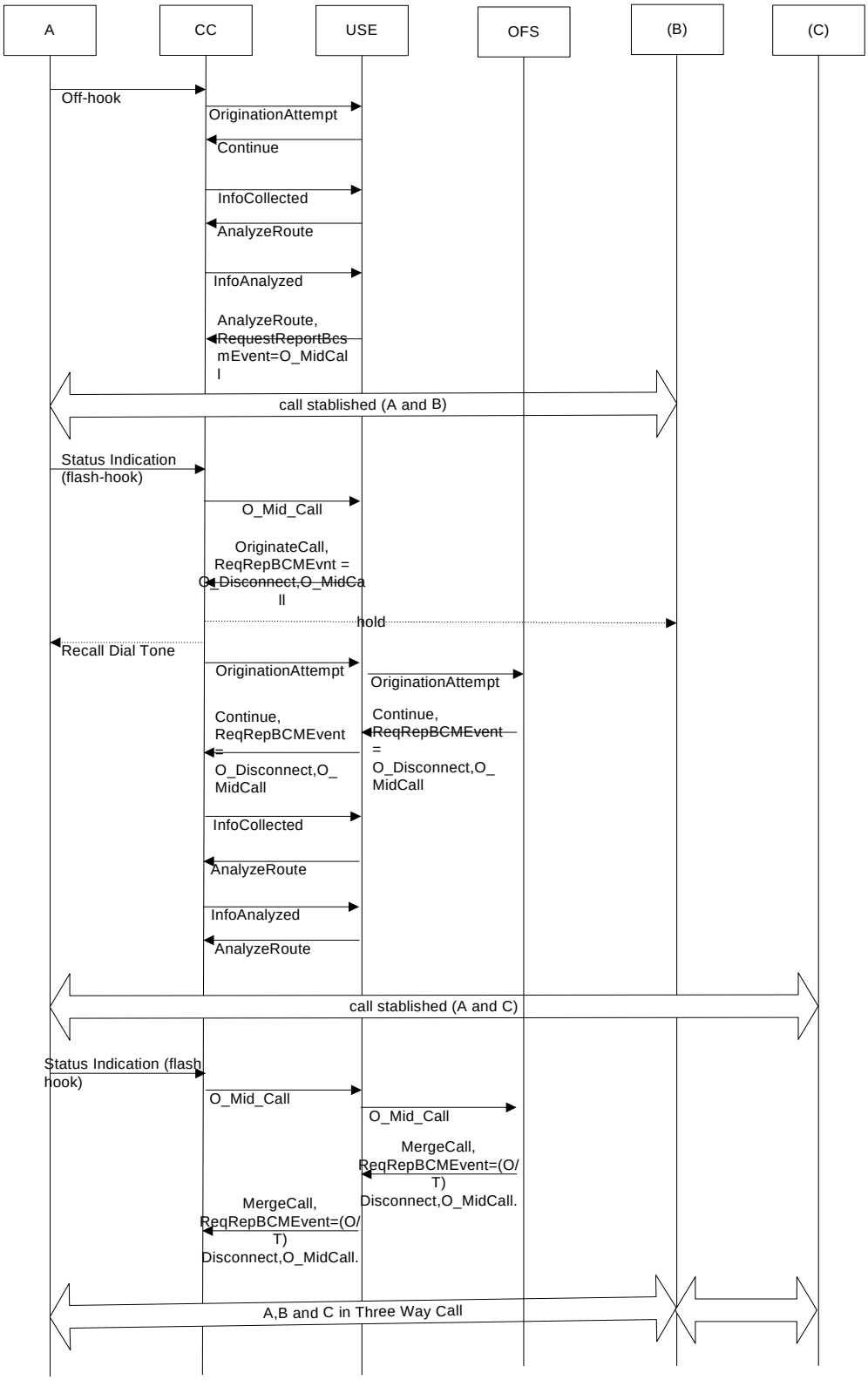
After detecting a trigger, the switch checks for the presence of applicable, active code-gapping controls to prevent SCP overload. If code-gapping controls apply, the switch gives the call final treatment; otherwise, it begins querying. Currently, the switch provides code-gapping support only for LNP and Toll-free calls.

Triggers for Internal Features

Trigger Name	Internal Features Using Trigger
Origination_Attempt	Speed Dial, Voice Mail, Add-on-Transfer-Conference, Three-way-call, Cancel Call Waiting
Info_Analyzed	Auth Codes, Remote Access to Call Forwarding, Voice Mail, Add-on-Transfer-Conference, Three-way-call, Cancel Call Waiting, Tollfree, Local Number Portability
Termination_Attempt	Anonymous Call Rejection, Call Forwarding Variable, Caller Name, Caller Number Delivery, Voice Mail
O_Mid_Call, T_Mid_Call	Add-on-transfer-conference, Three-way-call
T_Busy	Call Waiting, Call Forwarding on Busy, Voice Mail
T_No_Answer	Call Forwarding on No Answer

The message sequence diagram shown in Figure 1 illustrates the message flow between CC, USE and OFS to provide a three-way call service.

Figure 1. Message Flow Between CC, USE and OFS



Triggers for External Features

The following triggers are available for outside AIN support, at the associated "Info_Analyzed" TDP:

- Specific Digit String:
  Applies to called party numbers using NANP and can be set on three to 10 digits of an NPA-NXX-XXXX number.

- International Prefix:
  Applies to called party numbers in one of the following formats:
  - 011 + 7-15 digits
  - 01+7-15 digits
  - 101xxxx 011+7-15 digits
  - 101xxxx 01+7-15 digits

- One-Plus Prefix:
  Applies to called party numbers in one of the following formats:
  - 1+NPA-NXX-XXXX
  - 101XXXX 1+ NPA-NXX-XXXX

- Customized Dialing Plan:
  Applies when a certain 1-7 digit intercom code is dialed within a customized dialing plan.

- Operator Services:
  Applies to called party numbers in one of the following formats:
  - 0-
  - 00-
  - 101xxxx 0-
  - 101xxxx 00-
  - 0+
  - 01+
  - 101xxxx 0+
  - 101xxxx 01+

Note that although the provisionable triggers for remote features are currently a subset of the triggers supported for internal features, the development required for extending this list involves the following:

- Adding the provisioning support to expose the trigger's configuration.
- Adding the message translation code for transfer using TCAP.

Triggers armed using Next Event List

The Event Detection Point trigger events are arm(able) as requests or notifications through the RequestReportBCM message. When one of these events is detected, the switch sends the corresponding Request or Notification message to the requesting feature in the OFS or an SCP. The following EDP triggers are supported for use by remote features:

- Network_Busy
- O_Term_Seized
- O_Called_Party_Busy
- O_Answer
- O_No_Answer
- O_DTMF_Answered
- Switch_Hook_Flash
- Timeout
- O_Disconnect
- O_Disconnect_Called

AIN Messages Support

In addition to supporting the AIN messages specific to both TDP and EDP triggers mentioned above, the switch also supports the following SCP messages that affect call processing.

SSP → SCP

The following messages go from the switch to an SCP:

- Close
- Resource_Clear
- CTR_Clear

SCP → SSP

The following messages go from an SCP to the switch and are used by internal features:

- Acknowledge
- Analyze_Route
- Authorize_Termination
- Close
- Continue
- Create_Call
- Disconnect
- Disconnect_Leg
- Forward_Call
- Merge_Call
- Move_Leg

- Offer_Call
- Originate_Call
- Reconnect
- Send_To_Resource

The following messages go from an SCP to the switch and are used by external features:

- Acknowledge
- Analyze_Route
- Close
- Continue
- Disconnect
- Send_To_Resource

Again, note that the development required for extending the list of messages for support by remote features, just involves adding the message translation code for transfer using TCAP.

AIN Message Extension Flexibility

The switch can support the extension of AIN messages to overcome AIN inadequacy due to the development of new call-affecting features.

Extension Parameter

Most AIN messages have an optional parameter called "*ExtensionParameter*". This parameter allows the service provider to add parameters to messages sent between an SSP and an SCP. The AIN encoding and decoding software in the switch recognizes this as a valid optional parameter in each message. The development required to allow the use of this parameter by a custom feature in a service provider's network involves only two steps:

- Interpreting the data contained within this parameter.
- Performing the required protocol inter-working and/or call-affecting action as desired by the service provider.

Optional Parameters

The presence of optional parameters allows a protocol to be both forward and backwards compatible, as is the case with the AIN encoders/decoders used by the switch. With minor modifications to the message definitions, these AIN encoders/decoders in the switch can be updated to accept some optional parameters desired by service providers, which are otherwise not present in those messages. Again, after completing the encoder/decoder modifications, the additional development necessary to use an optional parameter by a custom feature in a service provider's network involves only two steps:

- Interpreting the data contained within this parameter.
- Performing the required protocol inter-working and/or call-affecting action as desired by the service provider.

AMA Record Generation

The switch can generate both SCP-based structures (Structure 220 and 221) and switch-based structures for calls requiring AIN interactions with an SCP. The switch selects between the two depending upon whether the "*AMAslpId*" parameter is present in the message returned by SCP. The switch supports the "Multiple Record" paradigm when exposed to multiple InfoAnalyzed triggers.

The switch currently supports recording of following AMA specific parameters that might be present in various messages from the SCP:

- AMAslpId
- AMADigitsDialedWC

AIN Queries

Querying is the process of assembling a TCAP Query message and sending it to an SCP over the Common Channel Signaling (CCS) network using SS7 signaling. The Query messages correspond to the Trigger Detection Points (TDPs): Origination_Attempt, Info_Collected, Info_Analyzed, Network_Busy, and Termination_Attempt. The content of the Query message depends on the type of trigger encountered and the parameters of the call (e.g., terminating party address and originating line information). The SCP may request the switch to obtain additional information from the caller using a TCAP Conversation with Permission message. The switch prompts (through an announcement) and collects the information from the caller (e.g., Dual-Tone Multifrequency [DTMF], dial pulse digits, or D-channel INFOrmation messages), and returns that information to the SCP in a TCAP Conversation Package. The SCP may request the switch to activate or deactivate certain triggers using a TCAP Query or Conversation Package. The switch responds with either a Response or Conversation Package, respectively, indicating whether the activation or deactivation was successful. Response processing consists of interpreting and carrying out the instructions in the TCAP Response message received from the SCP. The SCP may request the switch to route the call, redirect the call, disconnect the call, play an interactive announcement to the caller, route the call to an announcement, or provide special terminating treatment (e.g., distinctive alerting or display information). Specifically, the switch supports response processing for AnalyzeRoute, Continue, Close, Disconnect, RequestReportBCMEvent, and Send_To_Resource. The SCP Response may include a request to be notified when the call ends, in which case the switch notifies the SCP when the call is disconnected or cleared using a TCAP Unidirectional message. Additionally, the SCP may send the switch a TCAP Query message, requesting it to monitor the state of certain facilities, in which case the switch reports the state of the designated facilities using TCAP Conversation and Response messages.

You can use the EMS to provision subscribed triggers so that any calls originating from (or terminating to) the subscriber's line encounter the trigger. Office-based triggers are available to subscribers connected to the telephone switching office or who have access to the North America Numbering Plan (NANP).

Release 5.1 Enhancements

Intelligent Network Digit Modification

This feature provides the ability to support digit modification (prefixing or stripping of digits) from the Called Party Number (CdPN) field after the Intelligent Network (IN) trigger point has been reached, but before the actual IN message is sent. **Note:** "IN" is used generically and includes IN, AIN, IS41, GSM, INAP, WIN, CAMEL (all services available via ENT-LIST-AINTRIGGER).

Up to a 20 digit prefix can be inserted before the CdPN and up to 31 digits can be stripped from the CdPN (digit stripping takes place from left to right). When both digit stripping and prefixing are enabled, digit stripping takes precedence over prefixing. A commit parameter is supported that, when enabled, makes the CdPN modifications permanent and when disabled, restores the CdPN to its original value if the IN query fails.

Deployments

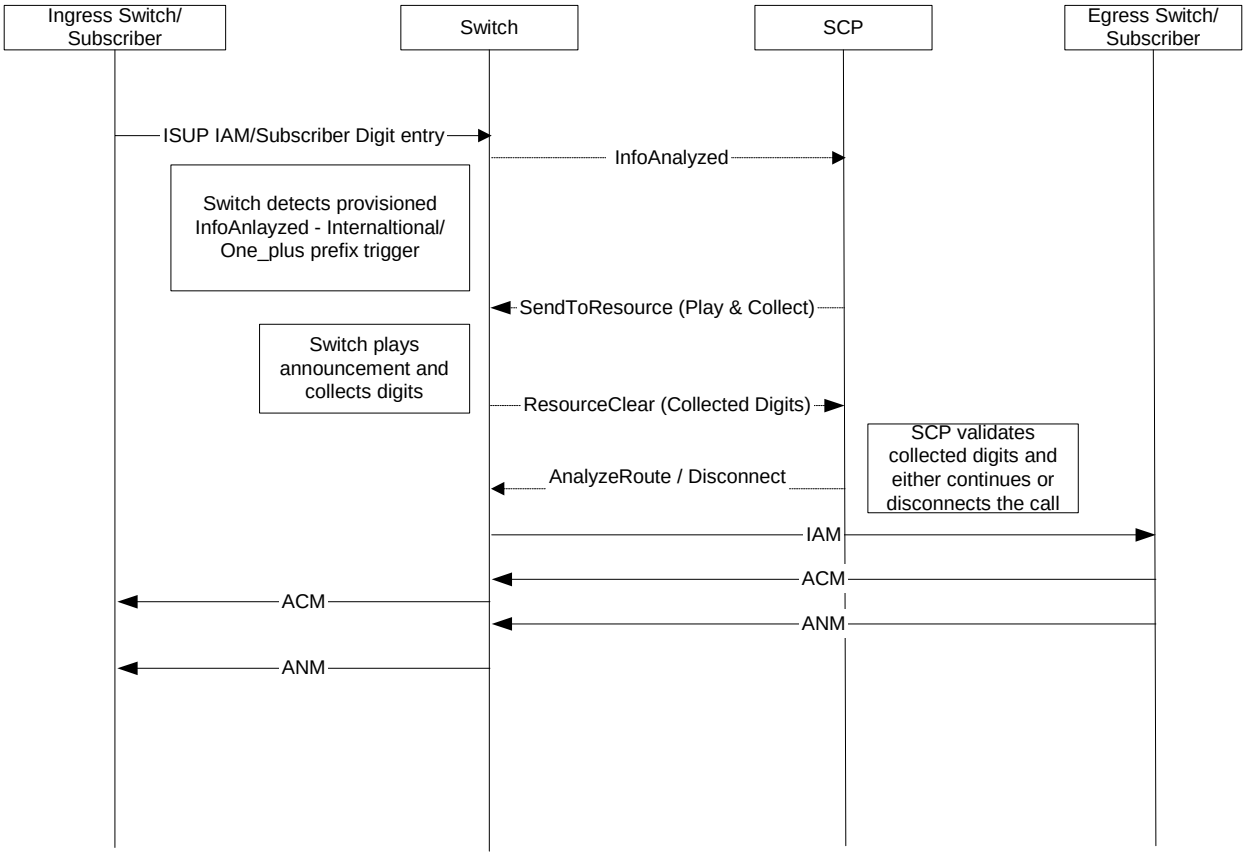
The switch can process an AIN-triggered call based on these service features:

- Authorization Code
- Terminating Toll-Free
- Call Forwarding Busy/No Answer
- Custom Dial Plan (Intercom/VPN Dialing)
- Single Call Setup and Release by Calling Party with Balance Update
- Multi-Call Setup and Release with Mid-Call Re-origination by Calling Party
- Multi-Call Setup and Release with Re-origination Using DTMF Entry After Called Party Disconnects
- Multi-Call Setup and Release with Re-origination After Called Party Disconnects
- AIN Toll-Free and Local Number Portability

Authorization Code

The switch can process an AIN-triggered call based on Authorization Code. A sample of this processing is shown in Figure 2.

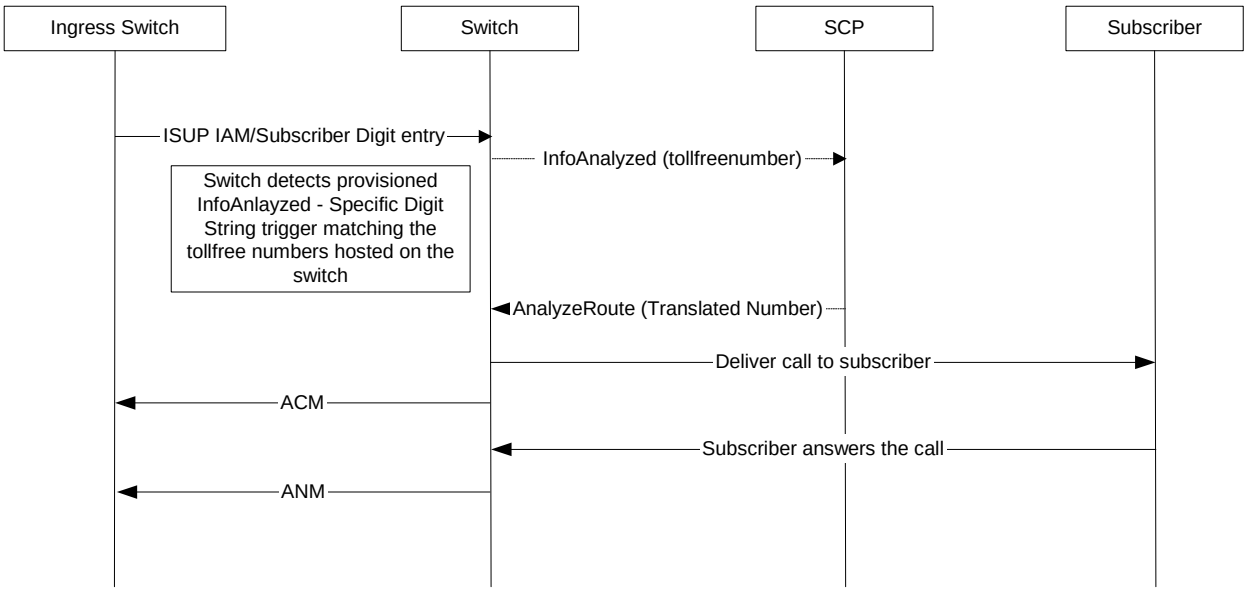
Figure 2. AIN Call Processing by Authorization Code



Terminating Toll-Free

The switch can process an AIN-triggered call based on the Terminating Toll-Free service. A sample of this processing is shown in Figure 3.

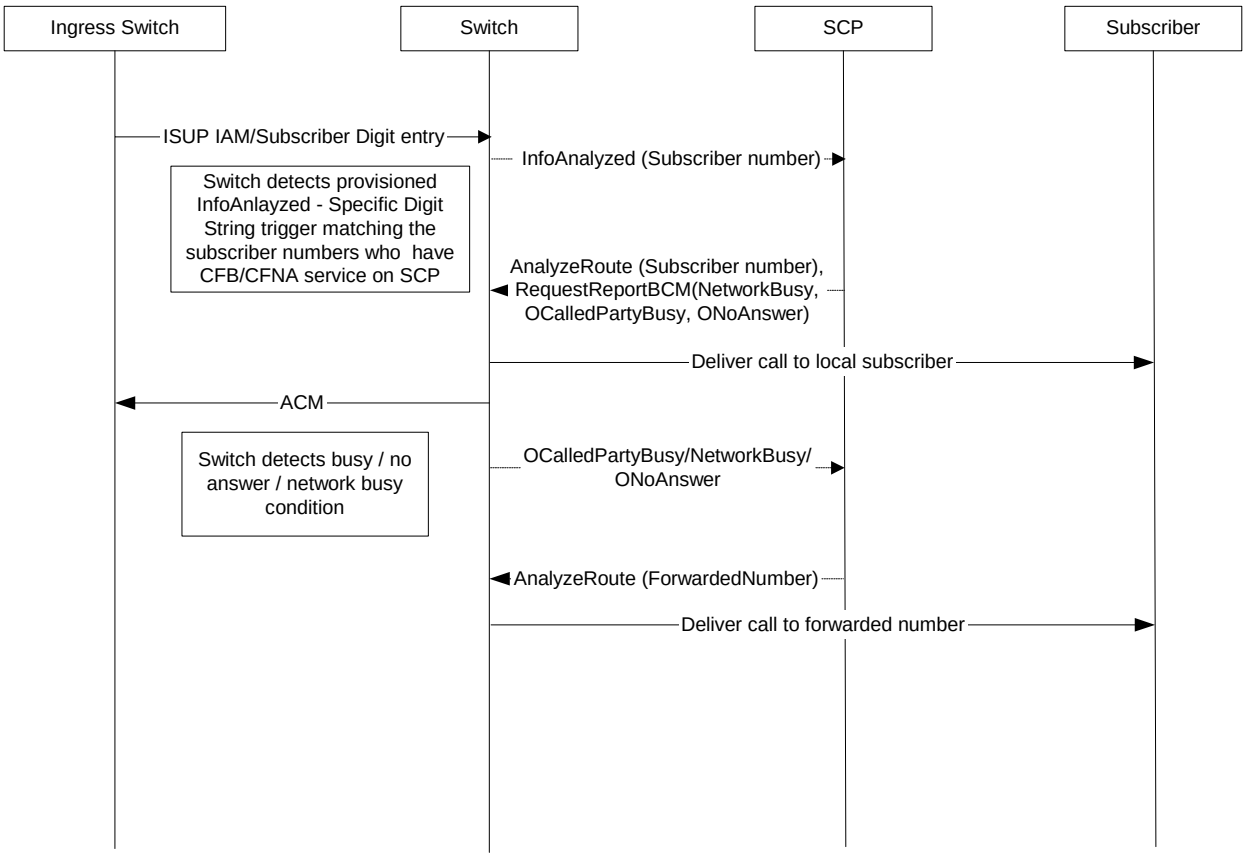
Figure 3. AIN Processing by Terminating Toll-Free Service



Call Forwarding Busy/No Answer

The switch can process an AIN-triggered call based on the Call Forwarding Busy/No Answer service. A sample of this processing is shown in Figure 4.

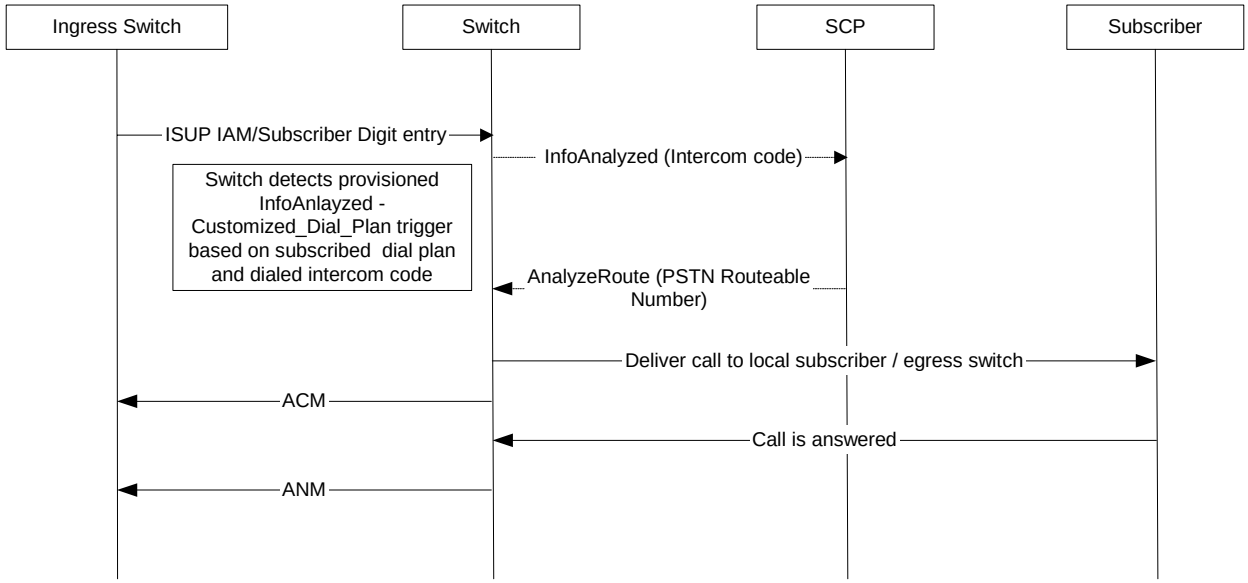
Figure 4. AIN Processing by Call Forwarding Busy/No Answer Service



Custom Dial Plan (Intercom/VPN Dialing)

The switch can process an AIN-triggered call based on Customer Dial Plan (Intercom/VPN Dialing). A sample of this processing is shown in Figure 5.

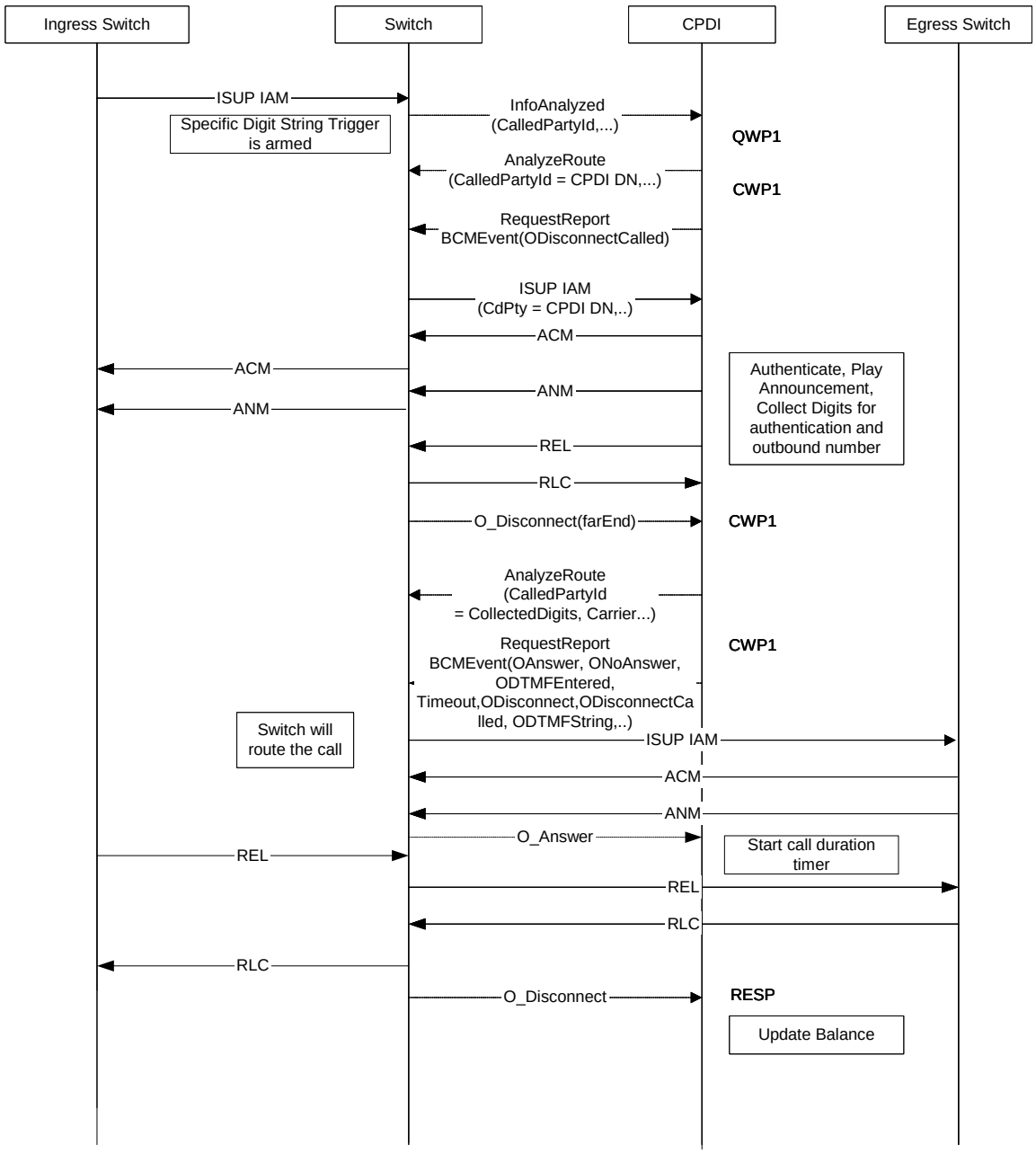
Figure 5. AIN Processing by Custom Dial Plan (Intercom/VPN Dialing)



Single Call Setup and Release by Calling Party with Balance Update

The switch can process an AIN-triggered call based on single call setup and release by calling party with a balance update. A sample of this processing is shown in Figure 6.

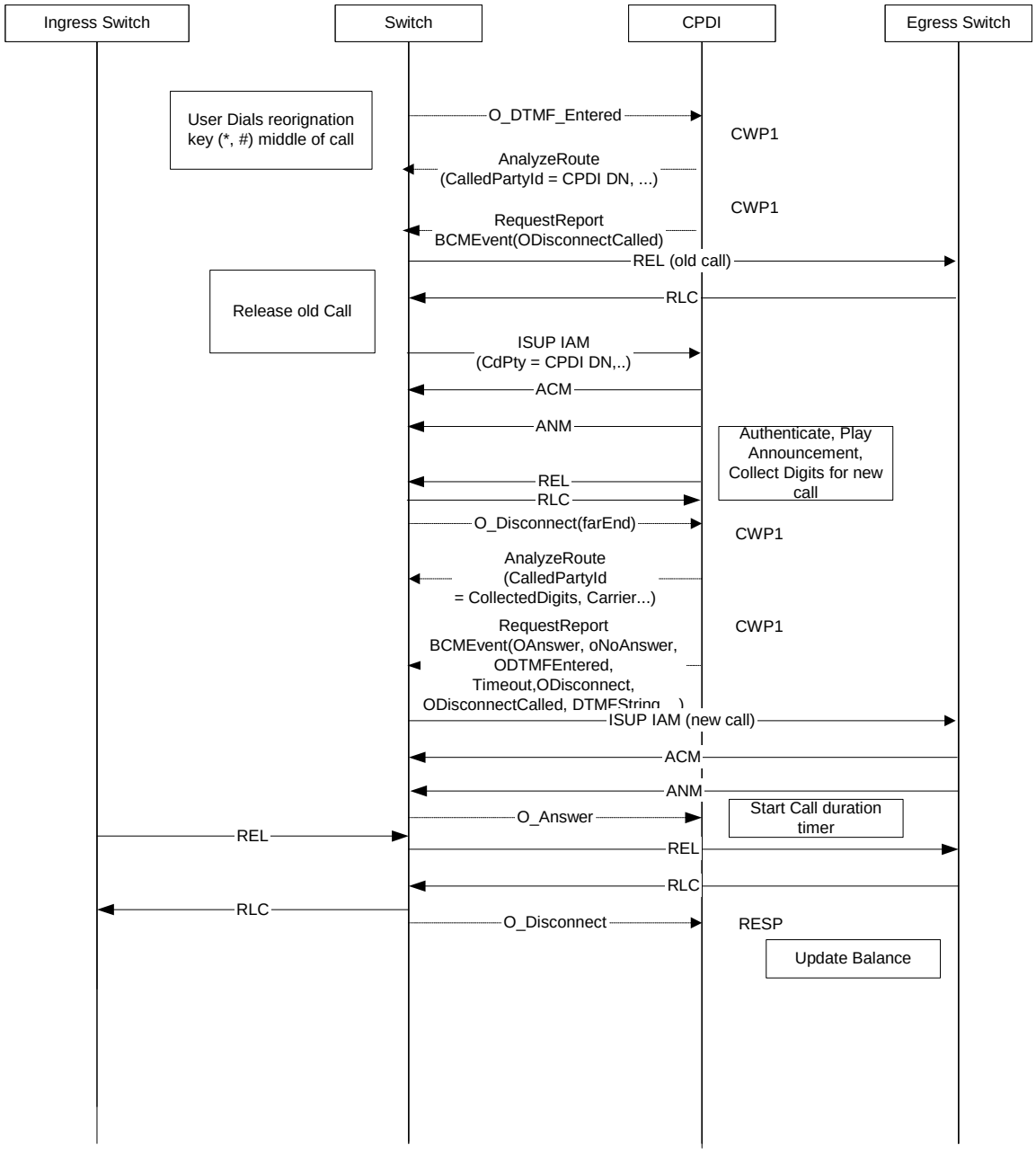
Figure 6. AIN Processing Based on Single Call Setup and Release by Calling Party with Balance Update



Multi-Call Setup and Release with Mid-Call Re-origination by Calling Party

The switch can process an AIN-triggered call based on multi-call setup and release with mid-call re-origination by calling party. A processing sample is shown in Figure 7.

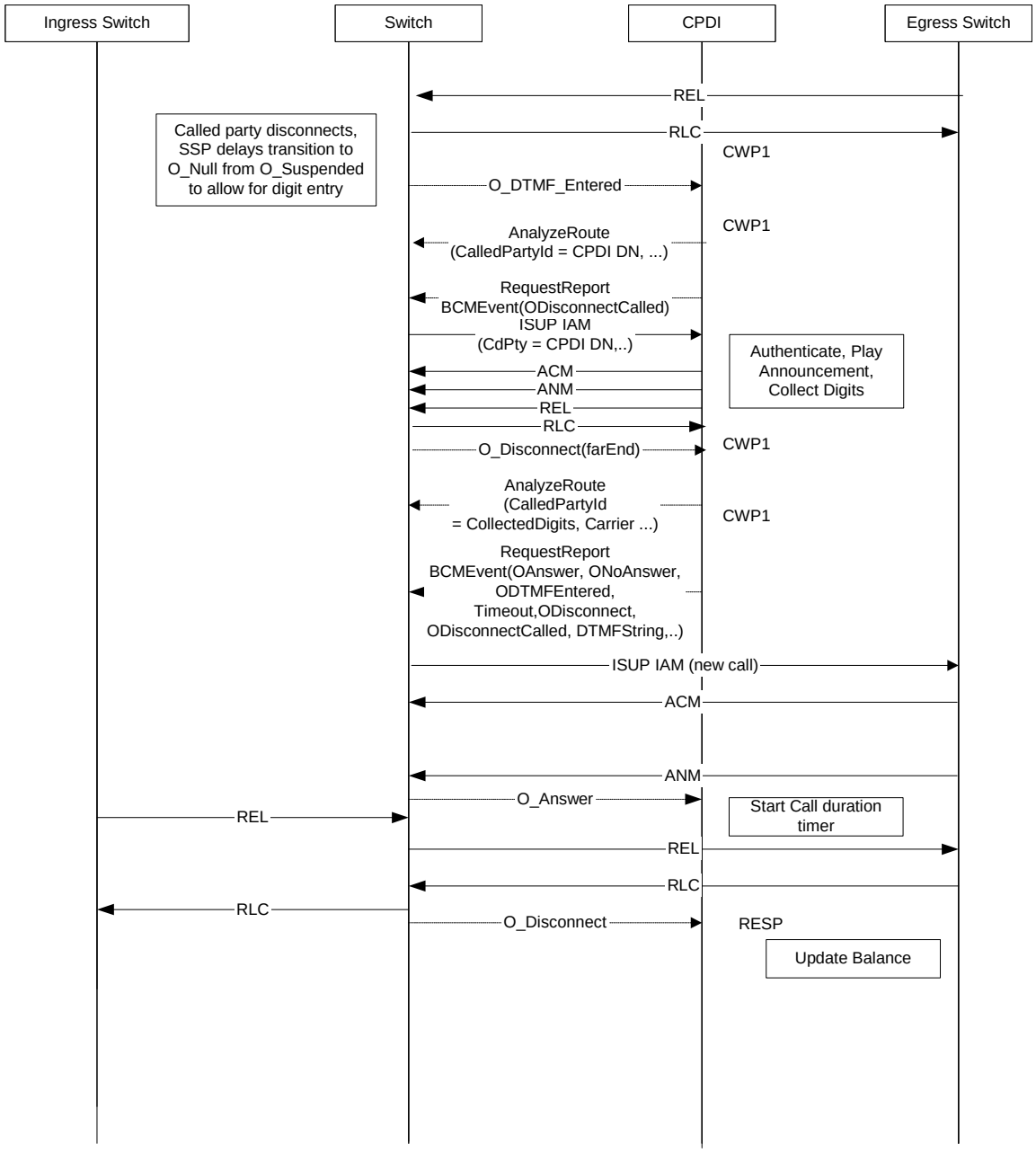
Figure 7. AIN Processing Based on Multi-Call Setup and Release with Mid-Call Re-origination by Calling Party



Multi-Call Setup and Release with Re-origination Using DTMF Entry After Called Party Disconnects

The switch can process an AIN-triggered call based on multi-call setup and release with re-origination using DTMF entry after called party disconnects. A sample of this processing is shown in Figure 8.

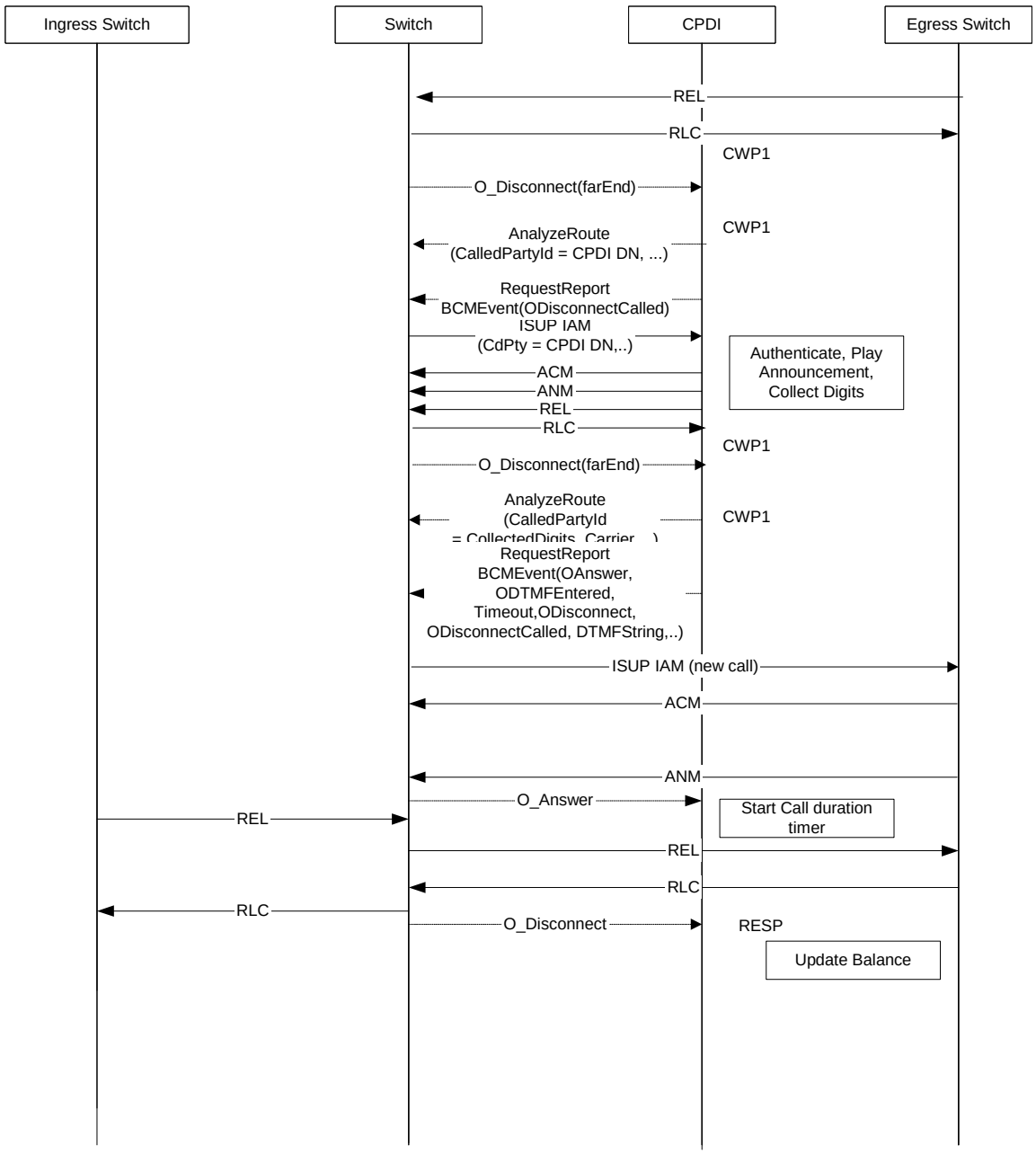
Figure 8. AIN Processing Based on Multi-Call Setup and Release with Re-origination Using DTMF Entry After called Party Disconnects



Multi-Call Setup and Release with Re-origination After Called Party Disconnects

The switch can process an AIN-triggered call based on multi-call setup and release with re-origination after called party disconnects. A sample of this processing is shown in Figure 9.

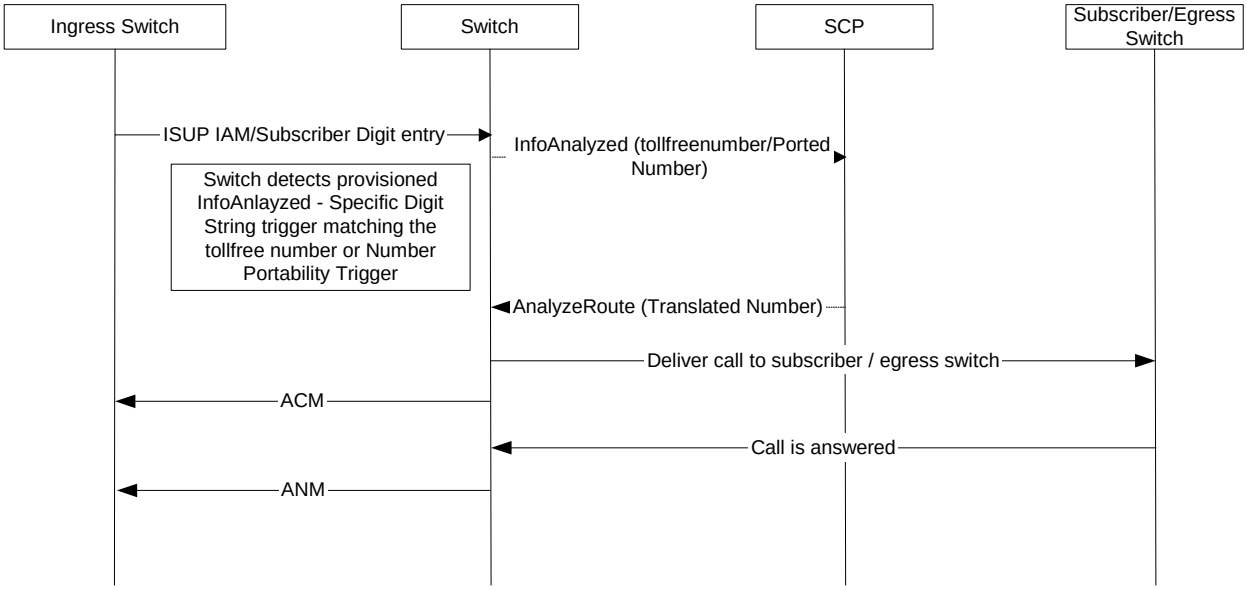
Figure 9. AIN Processing Based on Multi-Call Setup and Release with Re-origination After Called Party Disconnects



AIN Toll-Free and Local Number Portability

The switch can process an AIN-triggered call based on AIN Toll-Free and Local Number Portability. A sample of this processing is shown in Figure 10.

Figure 10. AIN Processing Based on AIN Toll-Free and Local Number Portability

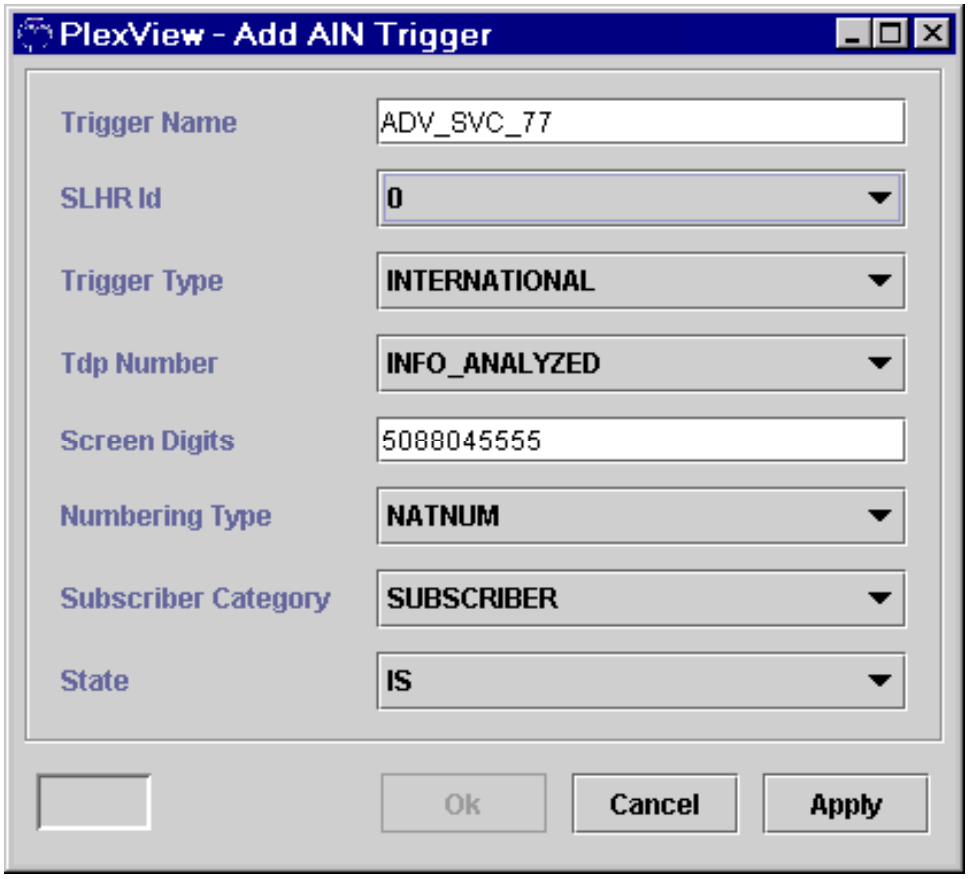


Provisioning AIN Triggers Using the PlexView® Element Management System (EMS)

You can provision the switch for AIN triggers (and services) using the PlexView EMS. You first create the trigger, using the Add AIN Trigger screen shown in Figure 11, and then provision the trigger per subscriber using the Add Subscriber → AIN Assignments screen as shown in Figure 12.

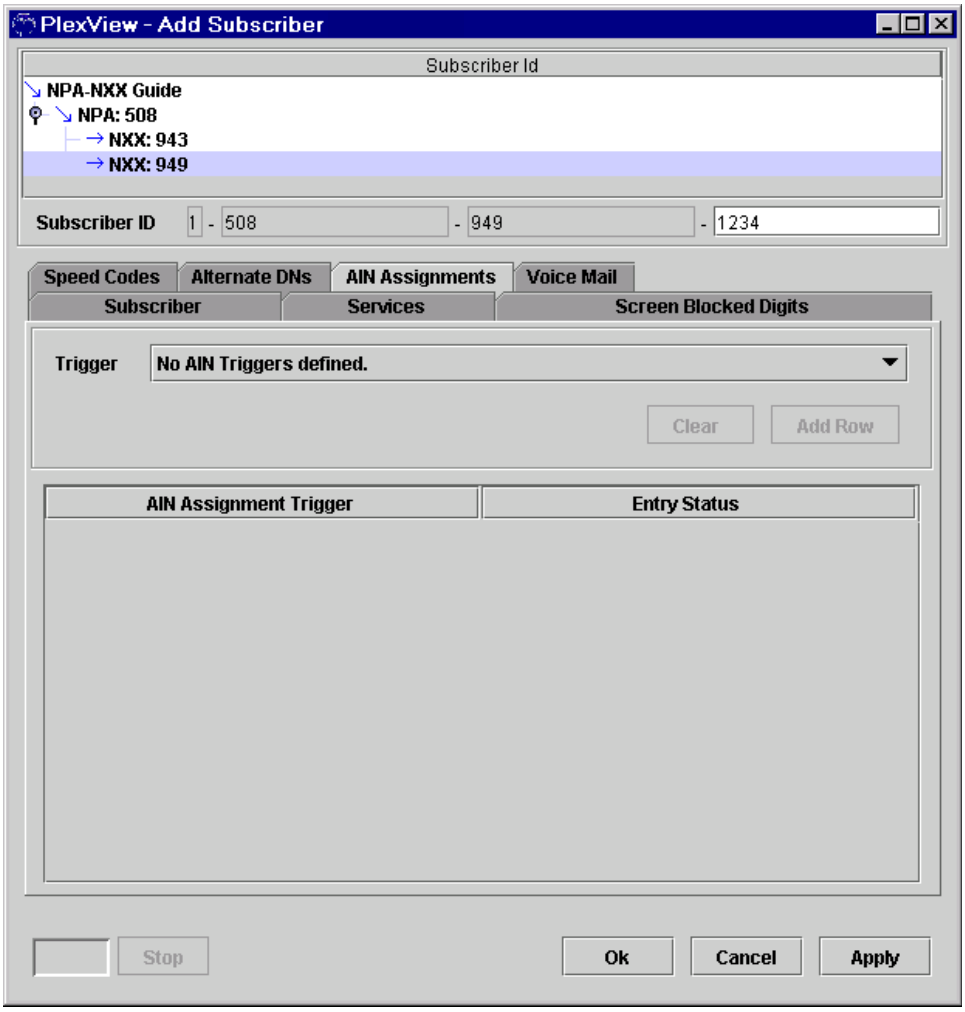
For details about provisioning AIN parameters and settings, refer to the *PlexView Element Management System (EMS) User's Guide*.

Figure 11. Add AIN Trigger



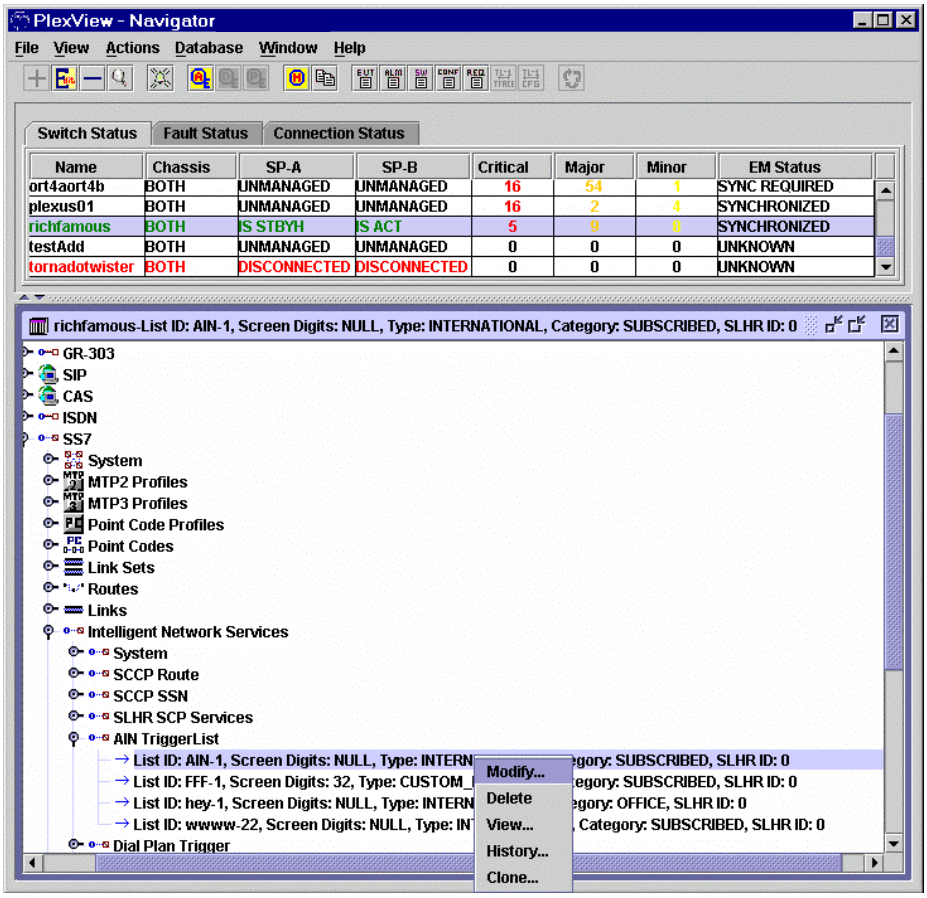
The Trigger Detection Point (TDP) number identifies the point in the basic call processing (based on the Basic Call Model), which identifies when a trigger can be detected and reported to an SCP.

Figure 12. Add Subscriber > AIN Assignments



Prior to provisioning an AIN trigger for a subscriber, you must first provision or add the AIN Trigger name located at SS7 → Intelligent Networks on the EMS Navigator. See Figure 13 for an example.

Figure 13. AIN Trigger



Related Documents

- *EMS User's Guide*

9-1-1 Service

This document contains the following sections:

9-1-1 Service Overview

What is E 9-1-1

The introduction of ANI allowed the caller's telephone number to be delivered with the call and displayed at the PSAP so that it could be used to identify the caller, and also be used for callback purposes. Having access to the caller's telephone number also meant that the caller's name and address could also automatically be made available by querying a shared ALI database. The feature that separates Basic 9-1-1 from Enhanced 9-1-1 is Selective Routing. Selective Routing is the automatic routing of a 9-1-1 call to the proper PSAP based upon the location of the caller. The introduction of ANI allowed the caller's telephone number to be delivered with the call and displayed at the PSAP so that it could be used to identify the caller, and also be used for callback purposes. Having access to the caller's telephone number also meant that the caller's name and address could also automatically be made available by querying a shared ALI database. Selective Routing is controlled by the Emergency Service Number (ESN), which is derived from the customer location. An ESN is a three to five digit number representing a unique combination of emergency service agencies (Law Enforcement, Fire and Emergency Medical Service) that serve a specific range of addresses in a particular geographical area.

Scope of this Document

This document focuses primarily on the E 9-1-1 capabilities of a Lucent switch serving as an EO or a tandem and connecting to either an E 9-1-1 tandem, or in some cases, directly to the PSAP, since the original 9-1-1 service called Basic 9-1-1 (B9-1-1) is rapidly being phased out.

Enhanced 9-1-1 in Compact Switch/Network Controller

Supported Trunk Types

All trunks and trunk groups on the Compact Switch/Network Controller (switch) support E 9-1-1 requirements for US markets, including:

- CAS
- ISUP
- SIP
- SIP-T

Dedicated and Shared Trunks

Trunk requirements reflect dedicated E 9-1-1 trunks from an EO to an E 9-1-1 tandem. When calls share trunks with non 9-1-1 calls, the Simulated Facilities Groups (SFG) feature is required.

E 9-1-1 Tandem

The term “E 9-1-1 tandem” is referenced throughout this document. The E 9-1-1 tandem carries out many specialized functions. This document addresses the switch serving as an EO or local tandem for 9-1-1- calls. But the Lucent switch does support trunking directly to PSAPs and making routing decisions about what PSAP a call should go to. Additionally, multi-party lines and coin services, each having specialized E 9-1-1-requirements, are not addressed in this document.

PSAP

A PSAP (Public Safety Answering Point) can receive calls routed by E 9-1-1 tandems or directly from switches on dedicated 911 trunks. The switch can route directly to a PSAP.

9-1-1 Operation

Figure 1 shows a representative architecture for delivering E 9-1-1 calls showing network elements, interfaces, and interworking points for the E 9-1-1 signaling architectures.

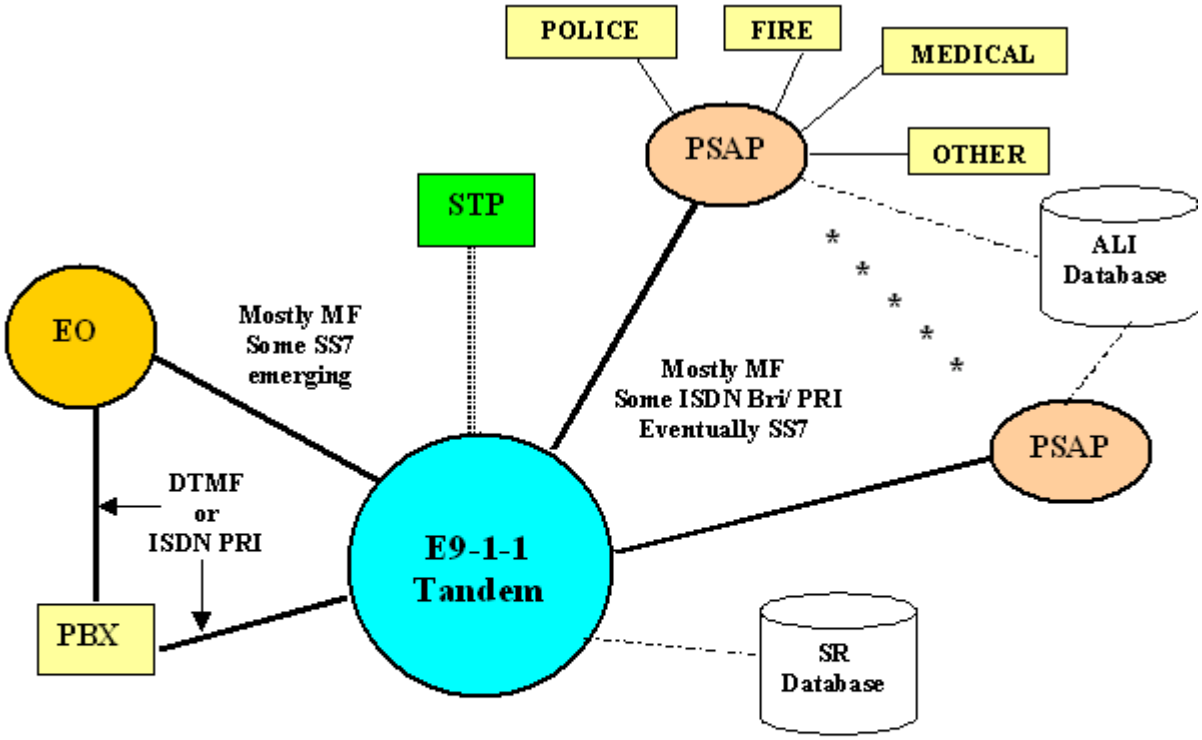
Example E 9-1-1 CALL FLOW

1. The caller dials 9-1-1 at the originating station.
2. The EO routes the call to the E 9-1-1 tandem on a dedicated MF trunk for E 9-1-1 service outpulsing the 7-digit Automatic Number Identification (ANI), which identifies the originating station. (Ten-digit ANI is an option)

   End offices are homed on at least two E 9-1-1 tandems: a primary tandem, and a secondary tandem in case the call cannot be completed to the primary tandem. The following figure does not show the secondary tandem. The EO (Lucent switch) can

route directly to the PSAP when the Selective Routing (SR) database resides in the Lucent switch. The following figure does not show that call flow.

Figure 1. E 9-1-1 Call Flow



ALI	=	Automatic Location Identification
EO	=	End Office
PBX	=	Private Branch Exchange
PSAP	=	Public Service Answering Position
SR	=	Selective Routing
STP	=	Signal Transfer Point

3. The E 9-1-1 tandem or Lucent switch determines how to properly route the call. The E 9-1-1 tandem uses the incoming trunk group identifier to determine the Numbering Plan Area (NPA). The NPA and 7-digit ANI are used in the SR database to determine the proper PSAP responsible for that originating station in the municipality.
4. The E 9-1-1 tandem or Lucent switch routes the call over dedicated trunks to the E 9-1-1 PSAP.
5. If the E 9-1-1 tandem or switch is unsuccessful in routing the call to the primary PSAP, in most cases it the can reroute the call to the designated alternate PSAP. The tandem or switch has the capability to automatically reroute calls if the first PSAP is down, due to facility outages or PSAP outages. It is also possible to set up routing to alternate PSAPs based on date and time schedules. For example, you can route calls to the designated alternate after 6 PM until 6 AM the next morning.

6. Typically, the PSAP CPE launches the ANI/ALI (Automatic Location Identification) query to get the street address (and usually name) and the closest Police, Fire, or Emergency Medical Facility for that address and delivers the data to the PSAP attendant. Mobile phone location information typically is triangulated between receiving base stations.
7. The PSAP attendant talks to the 9-1-1 caller and determines the need for Police, Fire, and/or Emergency Medical treatment and then passes the call and related location information to the proper agency (agencies) for dispatch. Whether agencies, e.g., Police, Fire or Emergency Medical can or cannot query the ALI database is determined at a state level. In some states only PSAPs can access ALI by state legislation/regulation. In other states, Police, Fire, Emergency Medical and perhaps other designated agencies can also query the ALI database.
8. If the responding PSAP determines that the call should have been sent to a different PSAP, it may reroute the call to another PSAP using the Central Office Transfer functionality at the E 9-1-1 tandem.

If the PSAP attendant gets disconnected from the caller, the PSAP attendant may make an outgoing call using the information provided to construct the 10-digit ANI for dialing.

Routing

The routing algorithm can key off the called party number (CDPN) and route the call to a dedicated 911 trunk or recursively key off the calling party number (CGPN) to determine how to route E 9-1-1 calls depending on NPA. This supports routing calls to E 9-1-1 tandems or PSAPs in environments where:

- Multiple PSAPS may serve a single NPA
- Multiple NPAs may report to a single PSAP

A call flow diagram of multi-key routing is shown in the following figure.

For 911 calls, the route can go directly to a 911 trunk or operate recursively to add the calling party information (CGPN) to its already known called party information (CDPN). Calling party information is critical for trunk selection on 911 calls..

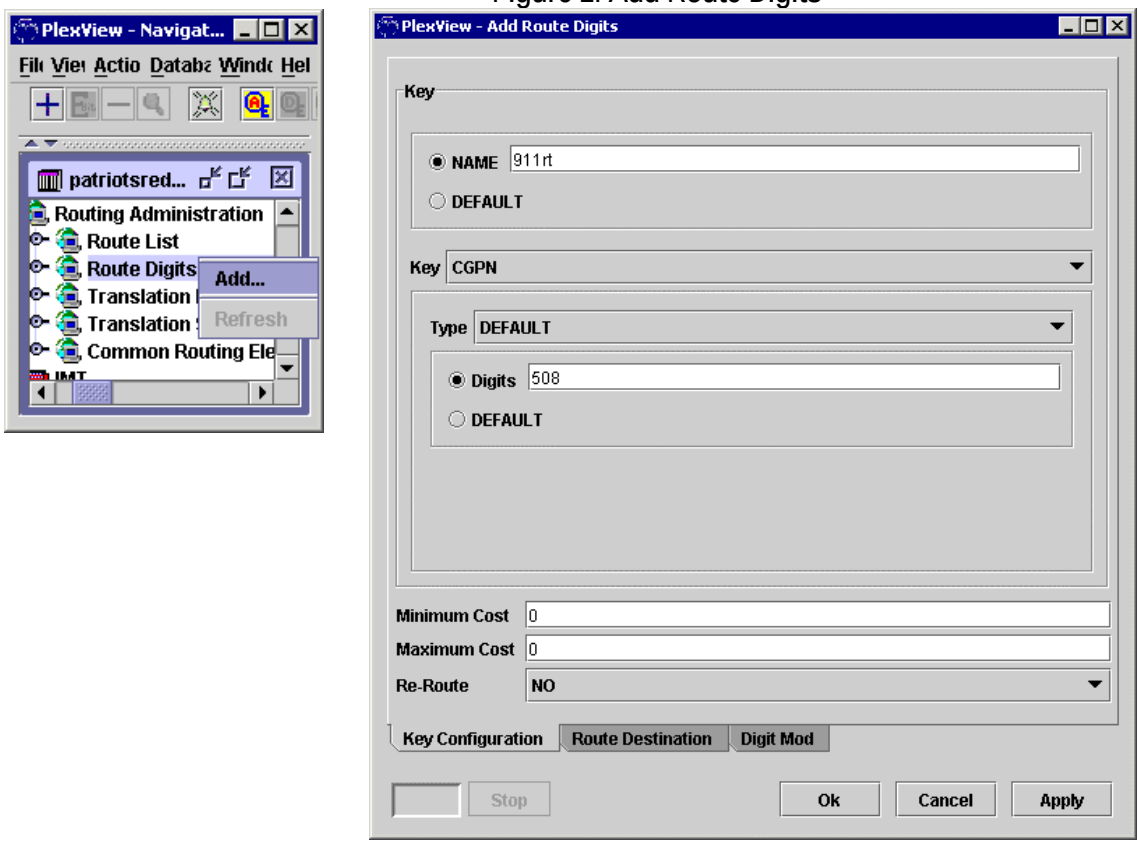
Provisioning

An example of provisioning required for multi-key routing using the PlexView Element Management System is shown here. This is not intended to show a complete or comprehensive routing example. It shows selecting 911, keying off the CDPN 911 to the CGPN route partition key, and where the router finds the appropriate CGPN NPA and routes the call to the desired trunk group.

The first command is Add Route Digits. The TL1 equivalent command is ENT-ROUTE-DIGITS. Select Add Route Digits, as shown in the following figure. In the Add Route Digits screen, set the following:

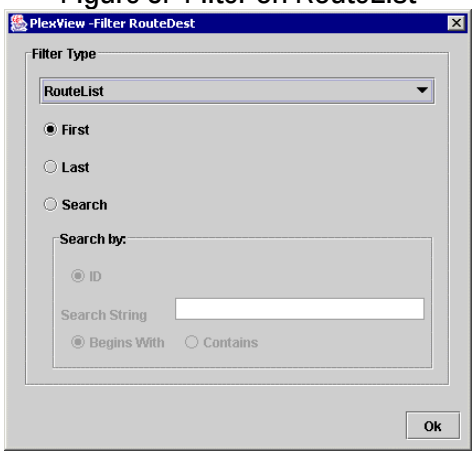
- Key off the CGPN
- Type of DEFAULT
- Digits – enter 508 (the NPA)

Figure 2. Add Route Digits



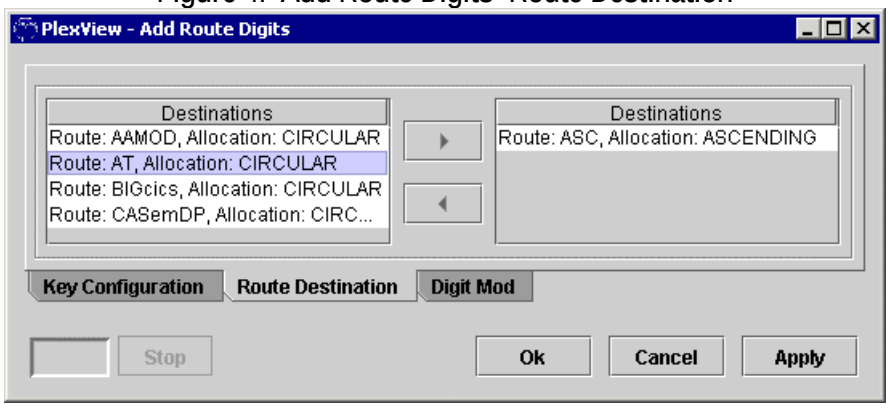
Click the Route Destination tab. In the left (available) field, right-click and select Refresh. Apply the filter as appropriate for your application. In this case, filter on RouteList. Available route lists will display.

Figure 3. Filter on RouteList



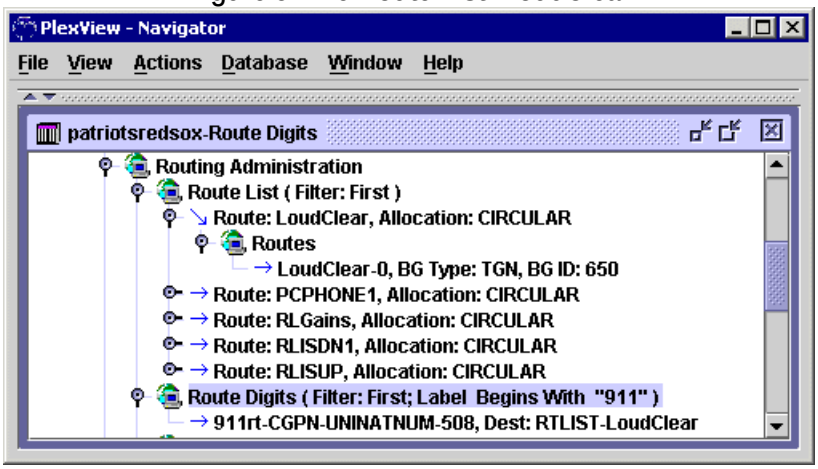
Select the appropriate 911 destination, as shown in the following figure, and select Ok.

Figure 4. Add Route Digits>Route Destination



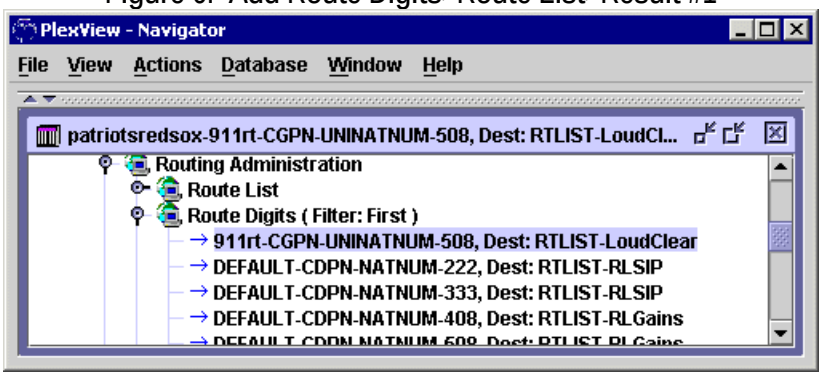
The Route List>Route>Routes>LoudClear hierarchy is shown in the following figure under Route List.

Figure 5. The Route List>LoudClear



The result of the operation is shown in the following figure.

Figure 6. Add Route Digits>Route List>Result #1

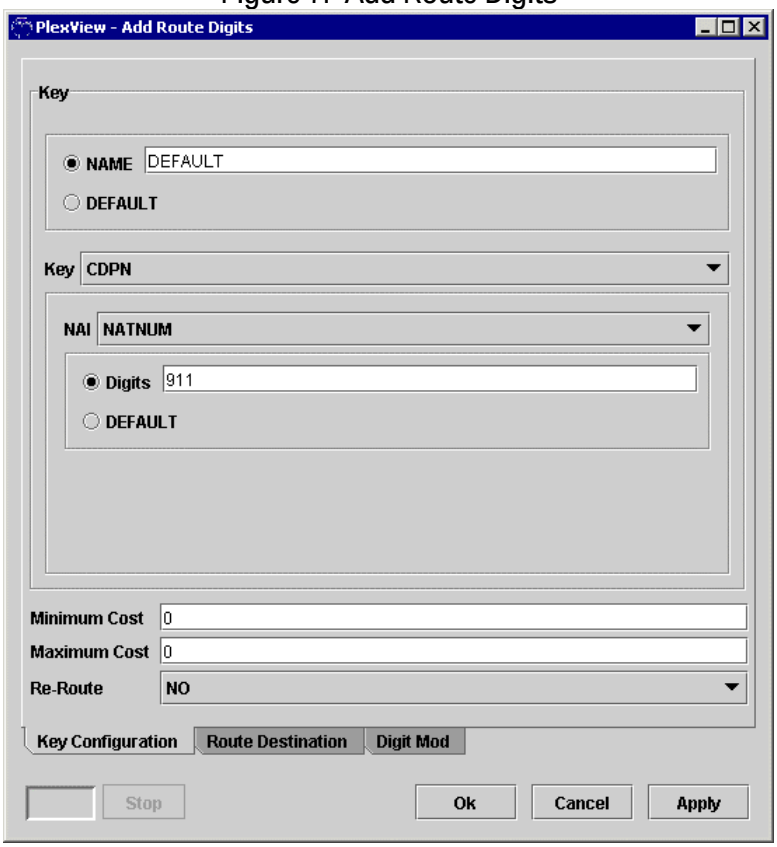


The first part of the highlighted information string shows the route name and that the route keys off CGPN, and is associated with the route list LoudClear.

For 911 calls, calling party information is required by the E 9-1-1 tandem or PSAP and has now been provided. Called party routing is also required for applications where routing decisions must be made. This information is especially true in this example where multiple NPAs use the E 911 tandem and/or PSAP and the call must contain that calling party information.

The routing algorithm operates recursively to add this information. For this example, return to the routing software and add route digits again, keying off CDPN as shown in the following figure.

Figure 7. Add Route Digits

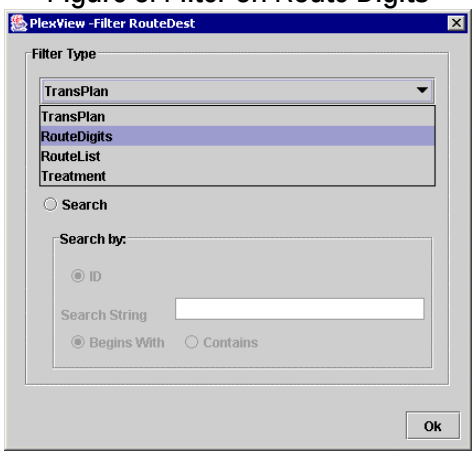


Configure the following:

- Give the route a name
- Key off CDPN
- NAI of NATNUM
- Digits – enter 911

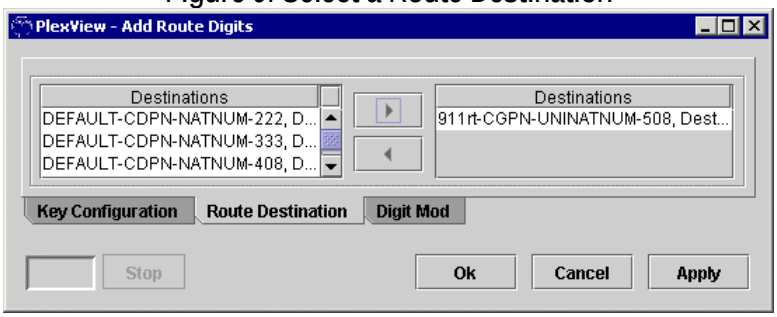
Under the Route Destination tab, right-click and select Refresh. Use the filter with a Filter Type of Route Digits to find the route for your application, as shown in the following figure.

Figure 8. Filter on Route Digits



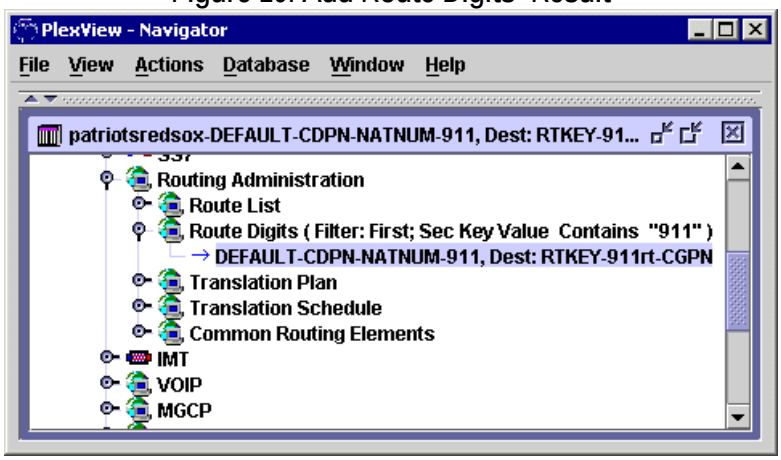
Select the appropriate destination as shown in the following figure and click Ok.

Figure 9. Select a Route Destination



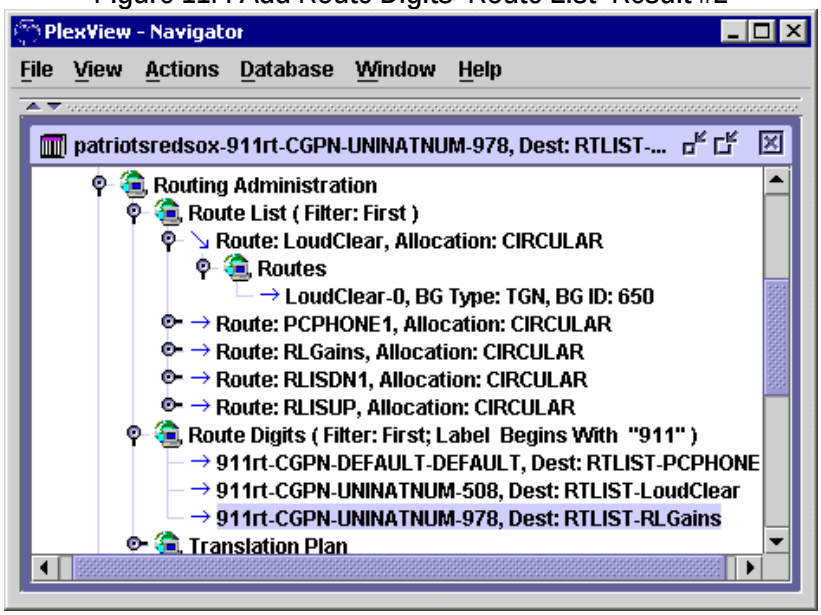
The main screen will show the new route and key, as shown in the following figure.

Figure 10. Add Route Digits>Result



If you want to have a second NPA go to the same RouteList, configure the route again, starting from Figure 2. Add Route Digits and ending with Figure 4. Add Route Digits>Route Destination. In this example the second NPA on the route list is 978. The result looks like the following figure.

Figure 11. . Add Route Digits>Route List>Result #2



This routing example now keys two NPAs to a destination. This example is complete.

Notes:

SIP Software Feature Package

This document contains the following sections:

Introduction

The Lucent switch offers SIP trunking over IP networks and also terminates SIP calls to PSTN subscribers. The switch carries calls to/from subscribers on SIP trunks. SIP subscribers are not supported on the switch itself. The SIP access interface in the switch connects to an IP feature server. The feature server controls the CPE hardware (IADs and IP phones) and provides functions such as CLASS features and IP Centrex to SIP subscribers. The switch acts as the PSTN Trunking Gateway in this application.

The SIP Software Feature Package includes the following capabilities:

- PSTN gateway for SIP initiated calls
- IP Gateway for PSTN calls
- International and inter-national voice calls over SIP trunks for toll avoidance
- Class 4 IP tandem trunking

The SIP trunking interfaces to external SIP feature servers enables the following features/services:

- IP Centrex
- Calling Card
- Unified Messaging
- Conferencing
- Call Center
- Attended or semi-attended directory assistance

Intended Audiences

This document has three intended audiences. The first audience wants high-level information on what VoIP is, what SIP is to VoIP, and how the switches support SIP. For this audience, read continuously from the beginning through the section titled SIP Trunking Applications Using the Switch.

The second audience is network engineers interested in how the switch supports SIP, what's required in the switch for SIP support, and how that support is set up. That audience should include SIP Trunking Applications, SIP Calls, and SIP Support. Also, if

interested in the mechanics of how the interfaces communicate with external servers, review the section titled Configuring SIP using the EMS or TL1, a section that is quite detailed, especially in communications protocol choices for Ethernet cards and Voice Server cards.

The third audience is interested in how switches will integrate into their networks, what interfaces are supported, and how to provision the switch to communicate with external servers and trunk SIP calls. For that audience, checking the SIP Trunking Applications section, and then moving to Switch Requirements to Support SIP, and then the Configuring SIP using the EMS or TL1 provides useful technical guidance.

SIP Overview

The Session Initiation Protocol (SIP) initiates, modifies and terminates VoIP sessions plus performs call control. It does not attempt device control for those sessions, like MGCP and Megaco do. SIP is a scalable, extensible protocol that works well with other protocols. Sessions that SIP establishes can be as simple as a two-way telephone call or they can be as complex as a collaborative multi-media conference session. As a request-response protocol, SIP closely resembles two other key Internet protocols, HTTP, the primary engine of the World Wide Web, and SMTP, the primary email protocol. Using SIP, telephony becomes another IP application and integrates easily into other Internet services. SIP has become the protocol of choice for IP signaling in VoIP applications because of its flexibility and ease of use.

Major Functions

SIP provides four basic functions:

- User location
- Feature negotiations
- Call management
- Session changes

SIP transparently supports name mapping and redirection services, supporting the implementation of ISDN and Intelligent Network telephony subscriber services. These facilities also enable personal mobility, allowing end users to originate and receive calls and access subscribed telecommunication services on any terminal in any location. The network can still identify end users as they move.

Callers and call recipients are identified by SIP addresses. When a SIP caller makes a call, the SIP phone contacts its homed server and then sends a SIP request. The most common SIP request is the invitation (INVITE). Instead of directly reaching the intended call recipient, a SIP request may be redirected or may trigger a chain of new SIP requests by proxies before reaching the recipient.

Types of Network Implementations

Peer-to-Peer VoIP

Voice over IP (VoIP) is a way of providing phone service over IP networks at prices lower than the prices offered by traditional voice service providers. Services such as Skype, created by the founders of KaZaA, offer peer-to-peer (P2P) VoIP freeware and billable premium services, with each end connecting to a PC. Free World Dialup is another example of the possibilities of P2P VoIP. This is the kind of VoIP is often hyped in the media, and these services run entirely over the IP network.

Voice over an All IP Network

Cable operators offer voice over their cable systems. Some cable modems come with Ethernet ports for phone connections. Voice over DSL broadband is also available with similar connectors. Microsoft now includes SIP in its Windows XP operating system and the company has expressed an interest in providing voice services between PCs. Though voice services over an all IP network have been around for some time, and those voice services are steadily increasing in quality, revenue opportunities have not matured and the market for all VoIP telephony has not yet reached its potential.

Voice over IP that Terminates in the PSTN

VoIP calls have to interact with the PSTN to terminate to traditional phones or cell phones. Because the PSTN is highly regulated, many features that go beyond call setup and voice quality must be dealt with before voice features are seamless on IP networks. PSTN quality offers something better than best-effort IP service. VoIP is still struggling with how to meet latency, echo cancellation, and jitter quality of the PSTN. Some other PSTN requirements include:

- Emergency (911) services
- CALEA (law enforcement monitoring)
- Directory assistance
- Life Line (works during power outages)

The telephone system is transparent to end-users. Users just dial someone and they either connect or don’t connect to them. As new users grow up with cell phones, text messaging and cell phone video, and mobility becomes more of an issue, phone and Internet services interworking will become even more important.

SIP Capabilities

SIP Trunking

The switch performs class 4 inter-machine SIP trunking and interfaces with external feature servers to assist with class 5 voice call functions for calls initiated by SIP phones to PSTN subscribers.

A SIP trunk group uses SIP call signaling protocols to establish and tear down calls. The switches support a SIP trunk interface and not SIP line interfaces. No SIP line side

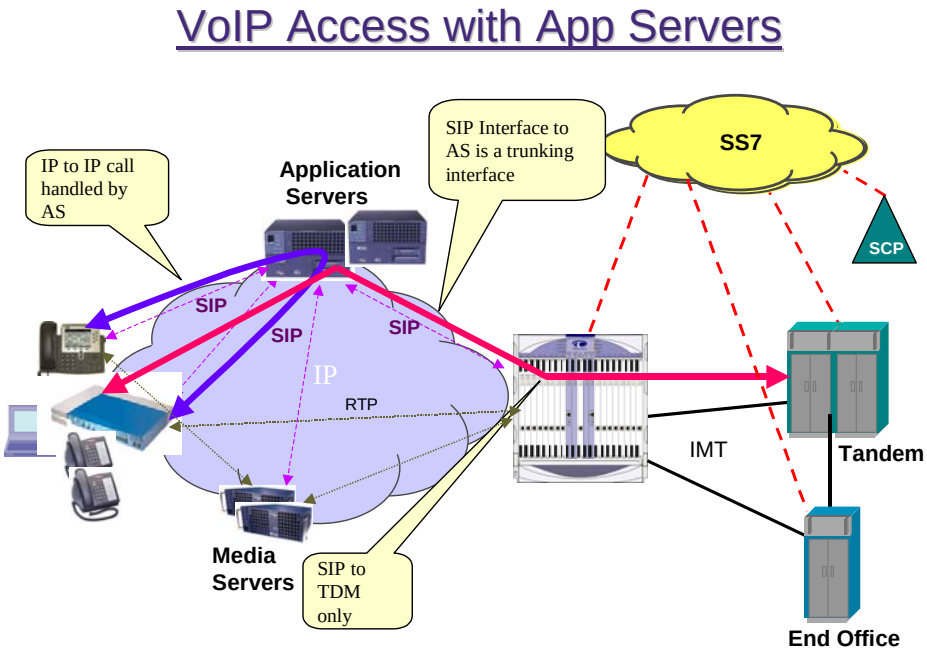
subscribers can be directly configured on the switch. Connecting with this interface is the basis for the support of the various applications such as SIP trunking for wholesaling and long distance.

SIP Subscriber Access

The SIP trunking interface can also connect to a feature server. The feature server controls the CPE hardware (IADs and IP phones) and provides features such as CLASS and IP Centrex to subscribers. The switch acts as the PSTN Trunking Gateway in this SIP application.

Another way of looking at it is that the combination of the switch and the feature server comprise a decomposed Class 5 switch. The feature server handles all calls from the SIP controlled IAD or IP phone. If the destination of the call is to another IP subscriber, it routes the call within the IP network. If the call is destined for the PSTN (based on NPA-NXX), then the call is routed via SIP to the switch for PSTN termination. The following figure shows the architecture of the switch connecting to a feature server for providing IP Centrex features and PSTN access to IP subscribers.

Figure 1 - The Switch Provides IP Centrex and PSTN Access for IP



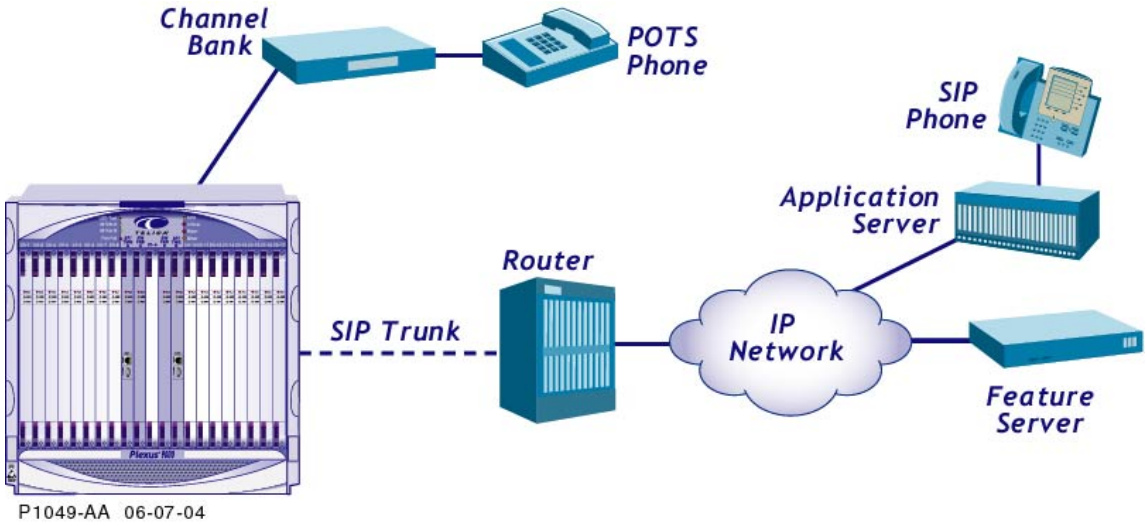
For inter-LATA, intra-LATA and international calls, the external connected server must supply a carrier ID to the switch. The switch can then route the calls by carrier.

The interface between the switch and a feature server is configured as a SIP trunk. Line side IP subscribers are supported on the feature server side of the trunk. The switch offers trunk services to the feature server, such as call routing into the PSTN, but not line features such as dial tone or CLASS features. SIP subscribers are configured outside the switch on the IP side. All subscriber specific information is passed from the feature server to theswitch in the SIP INVITE message. The switch handles the traditional PSTN functions of LNP, 8xx toll-free numbers, operator access and E-9-1-1. Since the subscribers are on the feature server, it handles obligations like CALEA features. When a SIP call for a SIP subscriber arrives at the switch, it forwards that call to the local application server, feature server, or media gateway for call setup.

SIP Trunking Applications Using the Switch

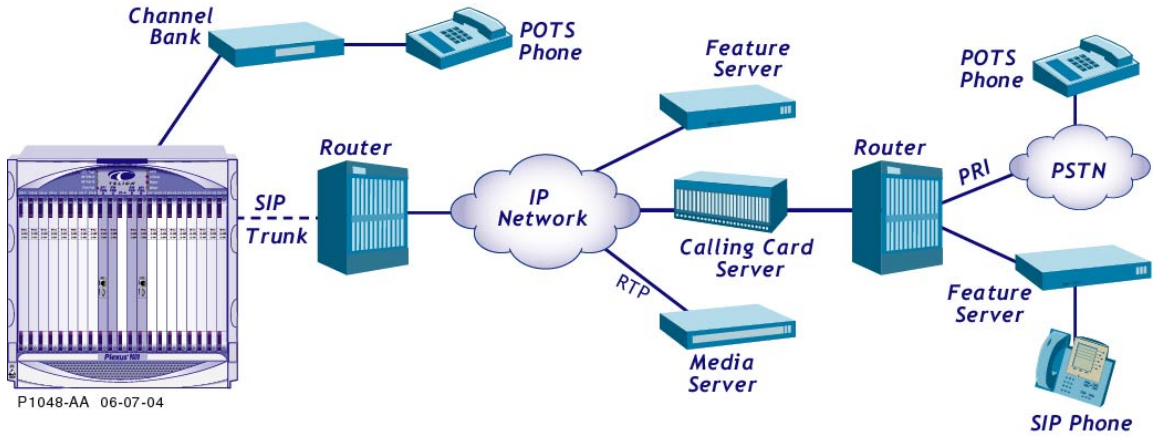
SIP trunks are typically used in IP-IP connnections, as shown in the Figure -2.

Figure -2. Intermachine IP Trunking



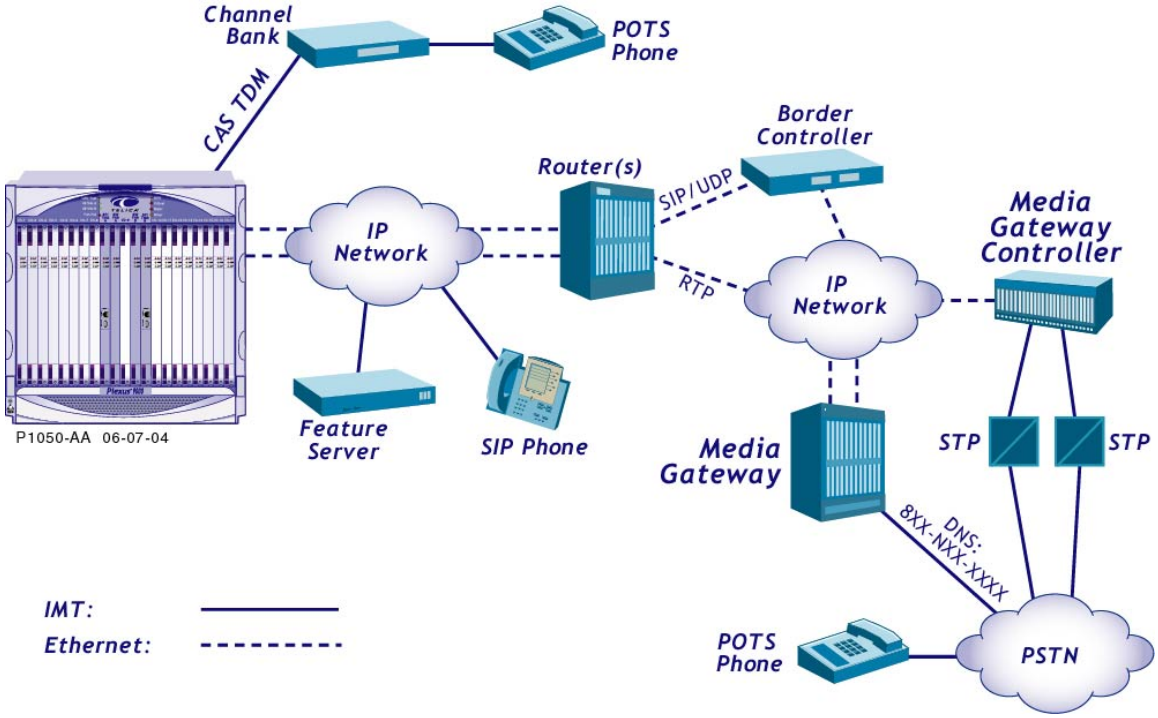
SIP trunking also supports international long distance calling, as shown in Figure 3.

Figure 3. International Long Distance



SIP trunking can be configured so the switch acts as a bridge between the PSTN and IP worlds. For example, if a calling card over PSTN service wants to interoperate with an IP based carrier, and both have existing networks, the switch in the calling card carrier's network can facilitate interoperation, as shown in the Figure 4.

Figure 4. Carrier Interoperation



SIP Calls Using the Switch

Basic SIP Call Setup

This section describes a simplified SIP call setup for a call initiated by a feature server that terminates to a PSTN TDM subscriber. It does not address IP to IP SIP calls, calls in

large networks with stateful and stateless proxies, complex call setups, multiple INVITE requests, call forking, or other call setup types.

To initiate a session from a SIP phone to a PSTN subscriber, the caller sends an INVITE request to the called party (switch subscriber). The INVITE is not routed directly to the called party, but to the SIP phone's homed server and possibly other external servers for call processing. The external server type depends on the network architecture and the size and scale of the network.

That server, or series of servers in the IP network, forwards the INVITE to other servers or, if the server knows about the called party, forwards it to the called party.

The called party is addressed as a URL, IP address, or phone number. The switch requires NPA-NXX numbers, so the feature server must be able to match the called party to a phone number. In the case of a SIP to TDM call, the phone number of the called party is used to route the call to the called party through a SIP trunk.

Coming into the switch on a SIP trunk, the call goes through the switch to the called party. The called party responds to the caller, either by answering the call, having an answering machine pick up the call or not answering at all, and the response is forwarded back on the IP network to the calling party. An acknowledgement is sent and then the bearer channel is established for voice communication. The call itself uses RTP and goes over a bearer channel that takes a different path from the setup signaling.

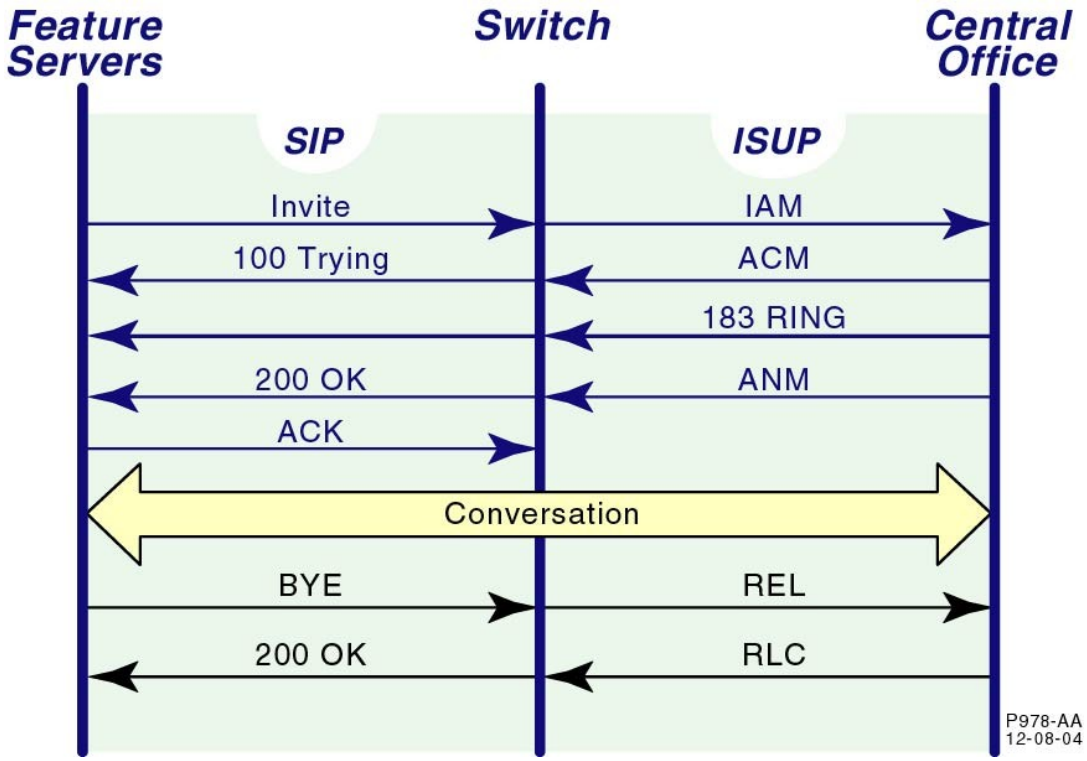
SIP Call Termination

The switch supports TDM (ISUP, ISDN, CAS) call termination from a SIP phone and feature server(s) in the IP network through the switch or vice versa. It initiates a TDM call that can terminate in a SIP network when the feature server, application server or media gateway provides the necessary call translation. That outboard server can also add CLASS features to the call.

SIP to ISUP Call INVITE

In the SIP to ISUP circuit as shown in Figure 5, an INVITE message is sent from the calling SIP phone to the feature server, and from the feature server to the local switch. The switch converts the INVITE into an IAM (initial address message). The IAM contains the destination and CIC (carrier ID code).

Figure 5. SIP and ISUP Call Setup



The called party responds to the switch with an ACM (address complete message) indicating that all addressing signals have been received and the phone is ringing. The switch sends a 100 TRYING message to the feature server, which forwards it to the SIP phone.

Between the 100 TRYING message and the first 200 OK message, the switch updates the feature server with code 183 SESSION PROGRESS (SDP-3) status messages. The feature server also forwards the 183 status messages to the SIP phone so the caller hears ringing.

When the called party answers and the phone is off hook, an ANM (answer message) is returned to the switch. The switch sends a 200 OK message to the feature server, and the feature server forwards it to the SIP phone. The SIP phone sends an ACK (acknowledge) message to the feature server. The feature server sends the ACK to the switch. The switch connects the ACK to the called party and now the two parties can communicate. The conversation is on a separate bearer channel. The SIP session setup is complete.

SIP to Switch-ISUP Call RELEASE

SIP to TDM Call RELEASE

If the SIP subscriber hangs up first, the SIP release session begins. The feature server sends a BYE message to the switch. The switch passes on an ISUP REL (release) message to the called party. The called party responds with a RLC (release complete)

message to the switch. The switch sends a 200 OK message to the feature server. The trunk and line side circuits, and the IP path all go idle and signal that they are available.

TDM to SIP Call RELEASE

If the TDM subscriber hangs up first, the ISUP REL message is interworked by the switch and converted into a SIP BYE message and sent to the feature server. The call tear-down continues with a RLC message sent and then a 200 OK message sent to the feature server, releasing the call.

Switch Requirements to Support SIP

This section describes the hardware, signaling, interfaces and configuration required to support SIP on the switch.

Required Hardware for SIP

The switch requires these cards to support SIP:

- Gigabit Ethernet IOMs
- Voice Server IOM(s)
- DS3 or DS1I/O cards (TDM IOMs)

Hardware Capacities for SIP

The three cards required for SIP have the following per card capacities:

- Gigabit Ethernet IOMs – Four Ports
- Voice Server IOM(s)
  - 2688 G.711, G.723 and G.726 Voice Channels
  - 816 G.729 Voice Channels
- DS3 or DS1I/O cards (TDM IOMs)
  - DS3 – 3 or 8 Ports
  - DS1 – 28 Ports

Required Software for SIP

SIP trunk configuration can be accessed through TL1 or the EMS (Element Management System). The EMS provides a GUI, and interacts with the switch through TL1.

Software Capacities for SIP

SIP trunks are carried over the Gigabit Ethernet interface. Up to 21,504 SIP calls can be supported on each switch.

SIP Support

SIP Support on the Switch

The switch supports an ever-increasing set of SIP features, including:

- SIP Trunking between VoIP gateways and the switch
- IP subscriber access (IAD and IP Phones) through feature servers
- SIP calling card use
- SIP calling card re-origination for Pactolus calling cards
- SIP conferencing applications
- Switch to switch IP trunking
- SIP Interworking with other protocols

Release 5.1 Enhancements

New SIP features in Release 5.1 include:

- SIP-T
- SIP P-Called-Party-ID
- SIP Domain Name with Maddr
- SIP Session Timer

SIP-T

SIP-T (SIP for Telephones) provides a framework for the integration of legacy telephony signaling into SIP messages that enables the preservation of received SS7 information within SIP requests at the originating gateway and the reuse of the SS7 information when signaling to the PSTN at the terminating gateway. In addition, SIP-T preserves the routability of SIP requests allowing a SIP request that sets up a telephone call to contain sufficient information in its headers to enable it to be appropriately routed to its destination by proxy servers within the SIP network.

The support for SIP-T, as defined in RFC3372, enables standards-based SIP bridging for the transport of call signaling information across a packet network with Lucent Compact Switches, running version 3.10.1 or later, and Lucent Network Controllers (MGCs), running version 5.1 or later.

SIP-T Feature Highlights

- Parameter Translation
  - The ISUP parameters are translated into the SIP header per RFC3398
  - The SIP header to ISUP mapping is performed per RFC3392.
  - The information from the SIP header (calling party number, called party number) overrides the equivalent parameters within the ISUP message, since these values may be changed by intermediate SIP proxies.
  - Non-ISUP ingress call legs are mapped to ISUP prior to parameter translation and message encapsulation.

- Message Mapping
  - The ISUP IAM message is carried as a MIME enclosure by the SIP INVITE request;
  - The ISUP ACM is carried as a MIME enclosure by the SIP 18x status message; and
  - The ISUP ANM message is carried as a MIME enclosure by the SIP 200 status message.
  - The ISUP REL message is carried as a MIME enclosure by the SIP BYE or CANCEL message.
    Note: ISUP-to-SIP-T-to-ISUP mid-call signaling is not supported in this version.
- Message Encapsulation
  - The encapsulation of the ISUP message within MIME enclosures is in accordance with RFC3204.
- Sending of messages
  - Supported SIP Content Negotiation Types - The sending of the following Content-types is supported for MIME-encapsulated ISUP: application/isup (Content-type: application/isup); required (Content-disposition: signal; handling=required); and optional (Content-disposition: signal; handling=optional - allows the other side to silently discard the MIME-encapsulated ISUP if it does not support it)
- Receipt of messages
  - A MIME-encapsulated ISUP message with a "415 Unsupported Media Type" is rejected if the incoming trunk group is not configured for SIP-T and the content-disposition handling is set to "required".
  - If the incoming trunk group is not configured for SIP-T and the content-disposition handling is set to "optional", the MIME-encapsulated ISUP message is silently discarded and the rest of the SIP message is processed.
  - The receipt of a SIP message from a SIP-T trunk group without a MIME encapsulated ISUP body is treated as if it were received from a SIP trunk group.
- Trunk Group Support
  - A SIP-T trunk group supports all the parameters that were previously supported by SIP trunk groups.

SIP P-Called-Party-ID

Support for the mapping of the ISUP OCN (Original Called Number) to the SIP 3GPP P-Called-Party-ID. This mapping is used in an application with feature server (e.g., Broadsoft) to provide features to a mobile wireless subscriber.

SIP Domain Name with Maddr

This feature provides a trunk group configuration option to associate a source and destination Domain Name and an Outbound-Proxy IP address with a trunk group. On the send side, the destination domain name is used to populate the host part of the Request-URI and TO header but the Outbound-Proxy IP address is still used for routing the call (sending the INVITE). The FROM header will be populated with source domain name.

On the receive side, the domain names in the Request-URI, TO and FROM headers are ignored and only the phone number part of the URL is used.

SIP Session Timer

The session timer audits active calls to make sure they have not terminated on only one side. This cleans up lost sessions and frees up system resources.

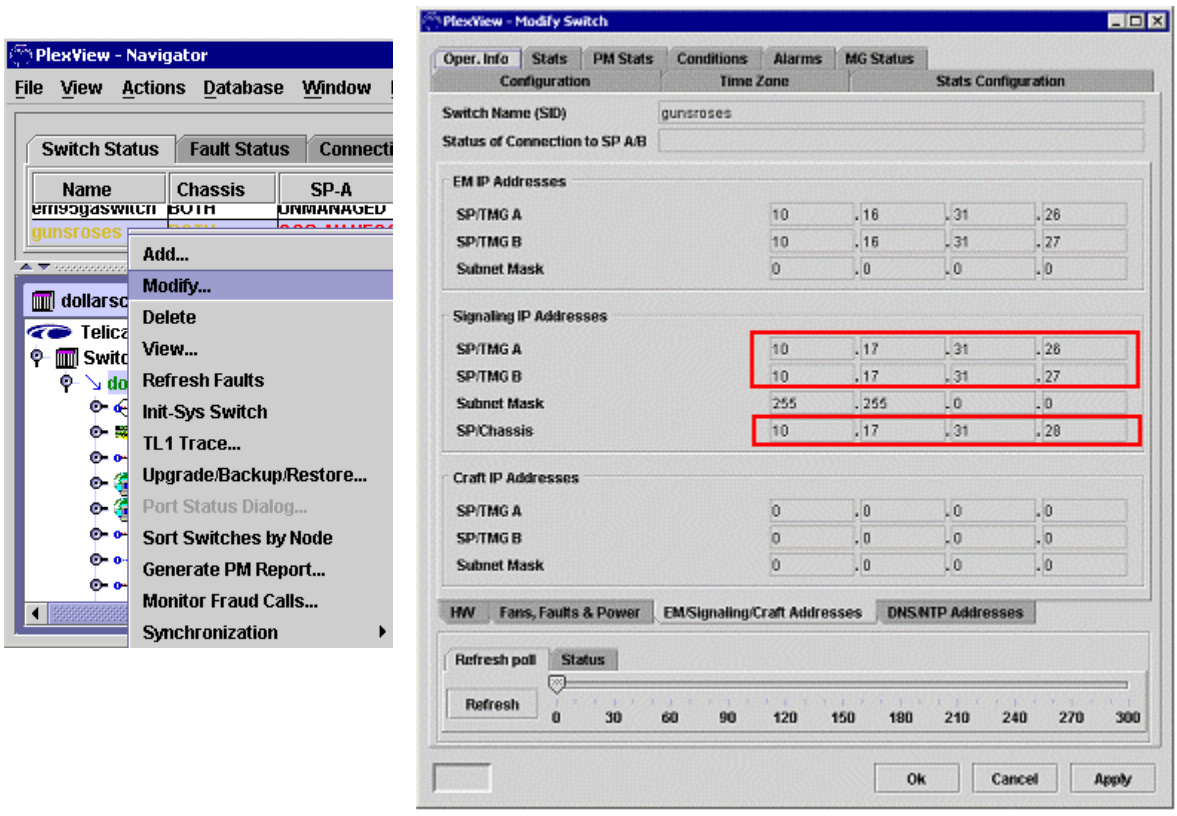
Configuring SIP using the EMS or TL1

This section presents an overview of the important things to consider when configuring SIP on the switch. Screen shots with key parameters highlighted and briefly explained are shown. This is a guideline, not a comprehensive step-by-step configuration guide.

System Processors (SP) Provisioning

IP addresses, subnet masks and routes must be configured in the System Processor (SP) modules for the signaling ports to operate. SP/TMG-A and SP/TMG-B for the signaling ports must have different addresses, with each address being specific to a signaling port. The SP/Chassis IP address is different and is reachable regardless of active SP. It is configured in devices that do not support IP failover.

Figure 6. EMS Modify SP Dialog



The equivalent TL1 commands are provided in the following table.

Table 1. TL1 Commands for Signaling IP Addresses Provisioning

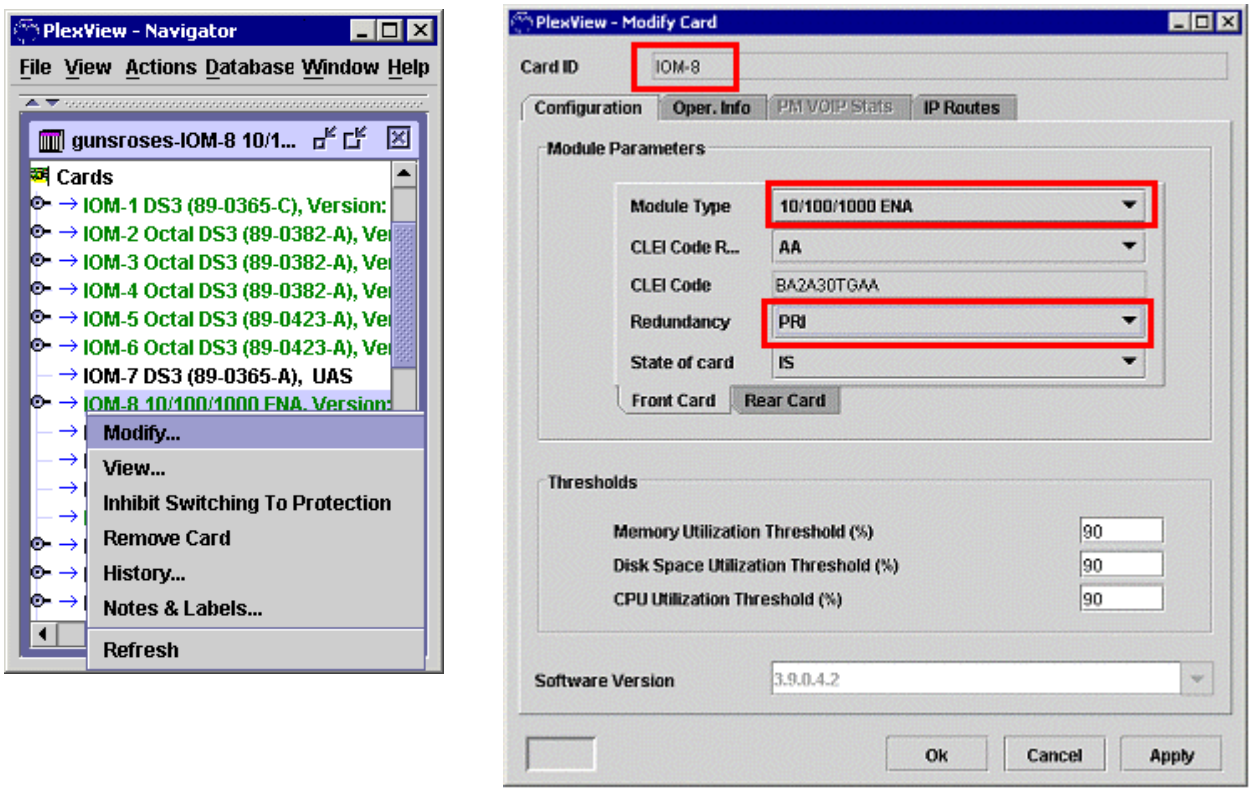
Command and Description	Definition and Parameters
ED-CHASSIS-EQPT TL1 equivalent to the red highlighted items to be configured:	Edit the Signaling IP Addresses for the SP signalingIPSPA (SP/TMG A) signalingIPSPB (SP/TMG B) SignalingIPChassis (SP/Chassis)

Ethernet IOM Provisioning

IP addresses, subnet masks and port information must be configured in the Ethernet Network Adapter IOM ports for bearer traffic.

These Ethernet IOMs reside in slot 8 and 10 of the switch. Slot 8 must be set to PRI for primary and slot 10 must be set to SEC for secondary. If a failover occurs, the IP address of the slot 8 port becomes the address of the matching slot 10 port.

Figure 7. Ethernet IOM Module Front Card



The equivalent TL1 commands are provided in the following table.

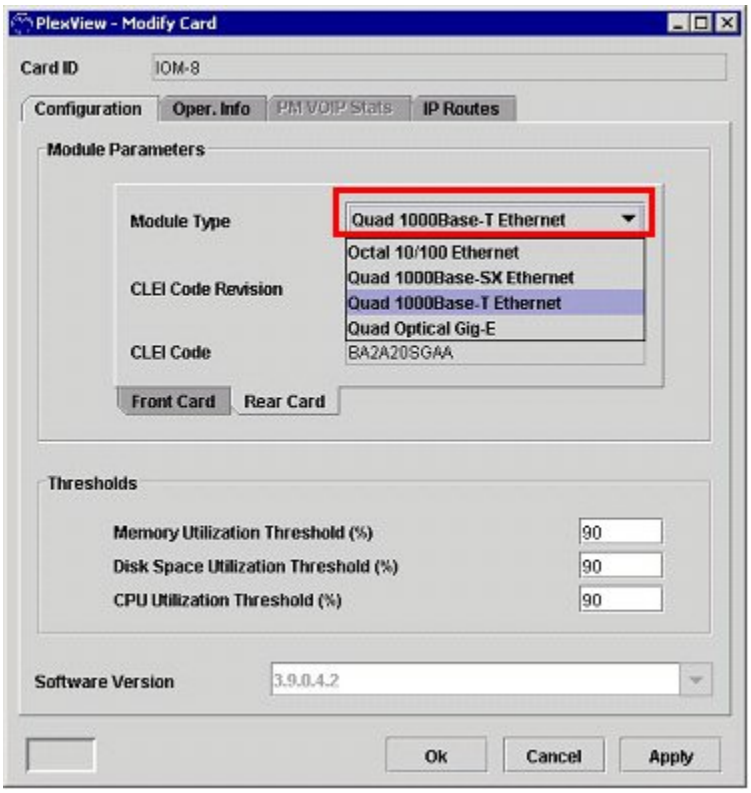
Table 2. TL1 Commands for Ethernet IOM Front and Rear Card Tabs Provisioning

Command and Description	Definition and Parameters
ED/ENT-EQPT TL1 equivalent to the red	Edit or initialize the properties of an I/O Module. IoModule (Card ID)

Command and Description	Definition and Parameters
highlighted items to be configured:	IoModuleType (Module Type) Rn (Redundancy) moduleType (Module Type from the following figure)

Click the Rear Card tab. The Ethernet Network Adapter rear card contains the actual physical interface and must be provisioned to match the physical fiber type for the software and interface to match.

Figure 8. Ethernet IOM Module Rear Card

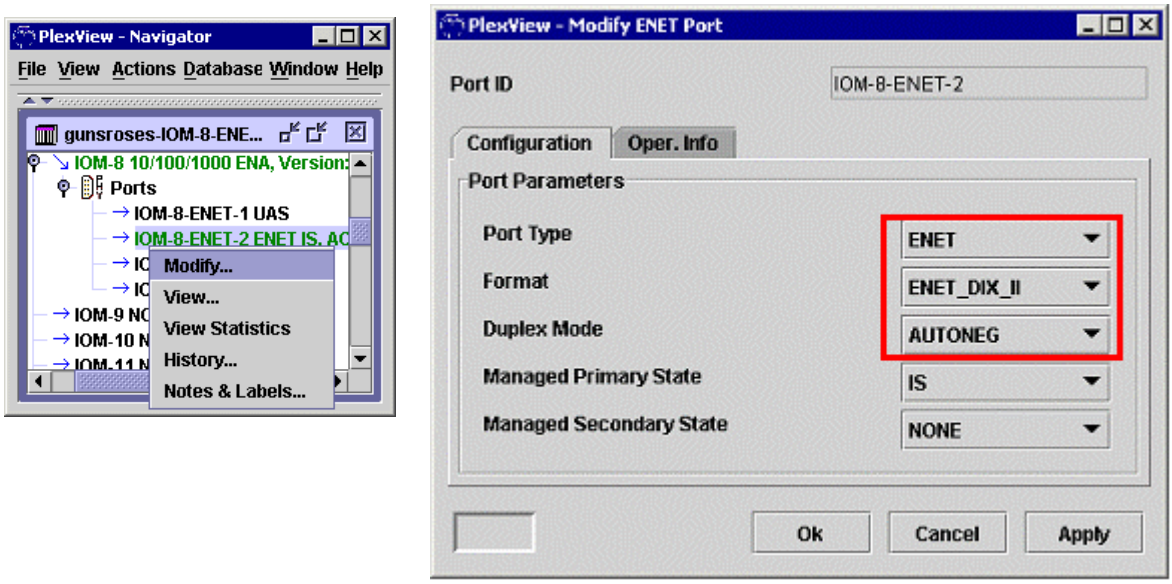


See the table in the previous section for the equivalent TL1 command.

Ethernet Ports Provisioning

All Ethernet ports must use the same settings.

Figure 9. GigE Ports



- Set the Port Type to ENET
- The Format must be ENET_DIX_II frame format or ENET_802_3. Format ENET_802_3 is also supported, but requires the AAL5 Encoding Type to be set to LLC_SNAP in VoIP system provisioning
- Set Duplex Mode to auto-negotiate (AUTONEG)
- Set the far-end Duplex Mode for Full Duplex

The equivalent TL1 commands are provided in the following table.

Table 3. TL1 Commands for Ethernet Ports Provisioning

Command and Description	Definition and Parameters
ED/ENT-ENET	Edit or establish the parameters associated with an Ethernet port on an I/O module.
TL1 equivalent to the red highlighted items to be configured:	enetID (Port Type) format (Format) mode (Duplex Mode)

Ethernet IP Address Provisioning:

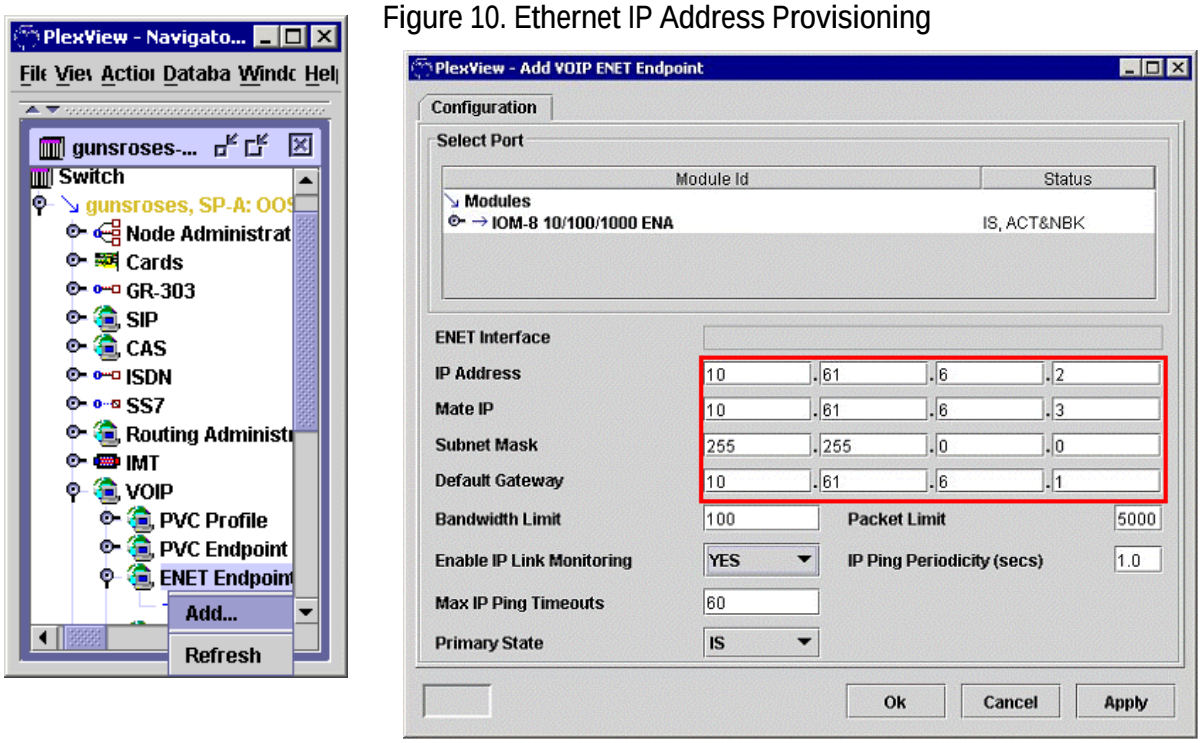
Ethernet IP Address provisioning works as follows:

- The IP Address is the IP address of the slot 8 Ethernet port
- The Mate IP address is the IP address of slot 10 corresponding port when in standby

Note: If a failover occurs, the IP address of the slot 8 port becomes the IP address of the matching slot 10 port An unsolicited ARP response will update the ARP cache of the router attached to the slot 10 Ethernet port to complete the failover update.

- The Subnet Mask determines what part of the IP address identifies the network and what part identifies the host
- The Default Gateway defines the IP address of the default router for the Ethernet port. The router should support HSRP or VRRP

Figure 10. Ethernet IP Address Provisioning



The equivalent TL1 commands are provided in the following table.

Table 4. TL1 Commands for Ethernet IP Address Provisioning

Command and Description	Definition and Parameters
ED/ENT-ENET-ENDPTVOIP	Associate an Ethernet port with an Ethernet endpoint. ED/ENT-ENET must have already been issued for this command to work.
TL1 equivalent to the red highlighted items to be configured:	ipaddress (IP Address) mateipaddress (Mate IP) subnetmask (Subnet Mask) defaultgateway (Default Gateway)

Voice Server IOM Provisioning

The primary VSM (Voice Server Module) can reside in any open slot and must be set to PRI. Slot 17 is the dedicated VSM protection slot.

Configuration Tab

The Configuration tab is the default tab when you open the IOM screen. The highlighted parameters are as follows:

- The Card ID is the slot number of the VSM
- The Module Type is the card type
- Redundancy is PRI always

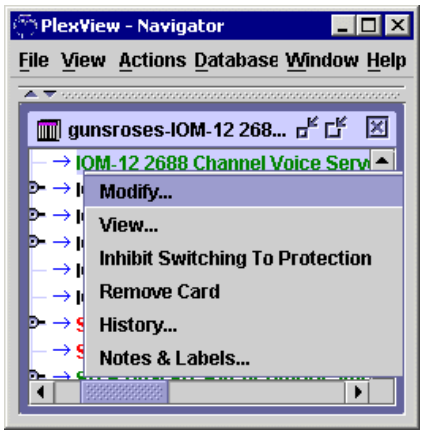
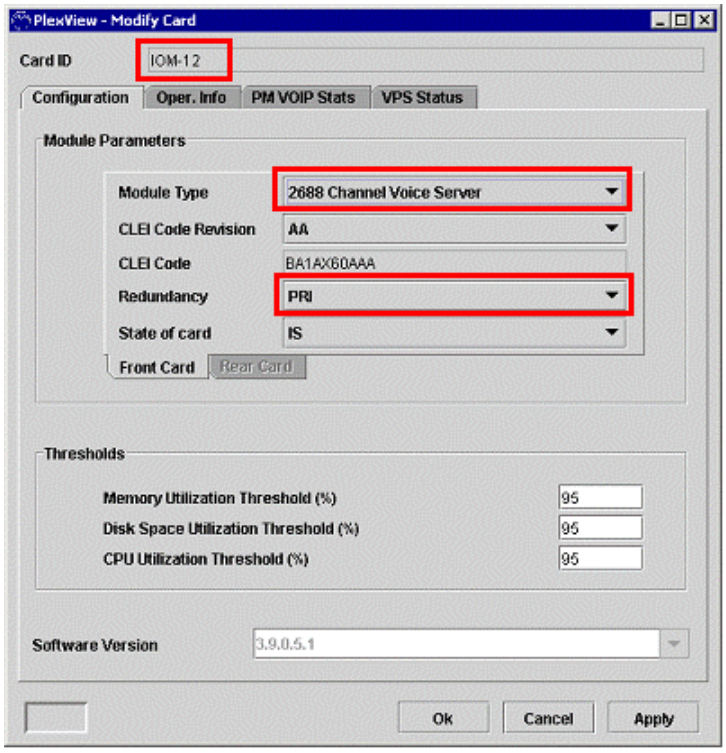


Figure 11. The Primary Voice Server Module



The equivalent TL1 commands are provided in the following table.

Table 5.TL1 Commands for Ethernet IP Address Provisioning

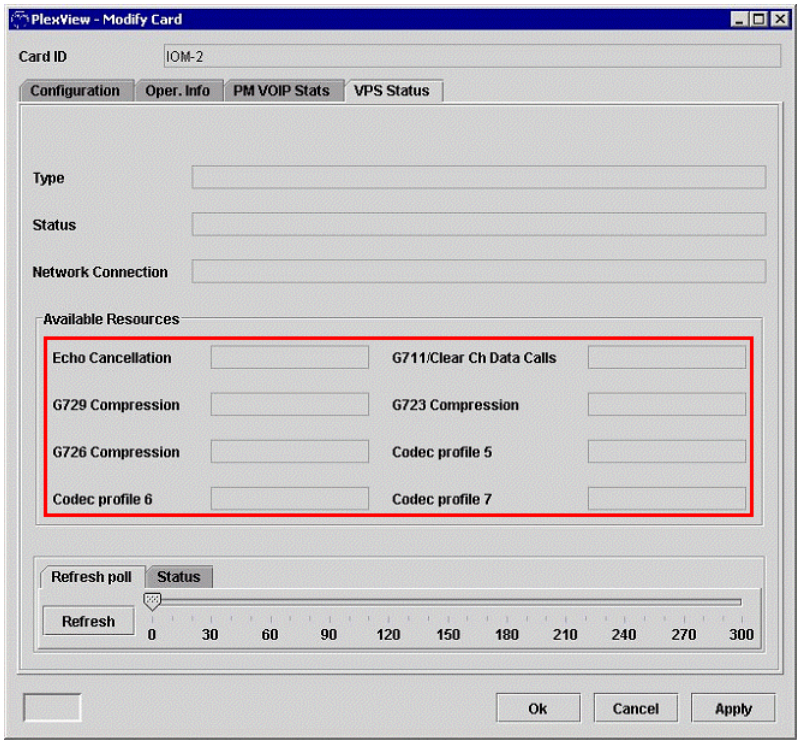
Command and Description	Definition and Parameters
ED/ENT/RTRV-EQPT TL1 equivalent to the red highlighted items to be configured:	Edit or initialize the properties of an I/O Module. IoModule (Card ID) IoModuleType (Module Type) Rn (Redundancy)

The VPS Status Tab

Click the VPS Status tab. The supported voice compression algorithms are:

- G.711 a-law/Clear Channel (µ-law to a-law conversion supported) (64k)
- G.729a (8k)
- G.726 (32k)(Cisco big endian only is supported)
- G.723.1 (6.4k)

Figure 12. Voice Compression Algorithms



The switch negotiates compression algorithms with connected devices in descending order of quality. This is set in the SDP profile, not under the VSM tab. SDP provisioning is covered later in this document.

Each VSM adds resources for IP calls and the resources vary depending on the CODEC.

CODEC	VSM2 Server Module
G.711	2688
G.723.1	672
G.729AB	816 (32 ms tail) 768 (> 32 ms tail)

Note: One G729 call on a VSM2 sets the call limits to 768 or 816 depending on the EC tail setting.

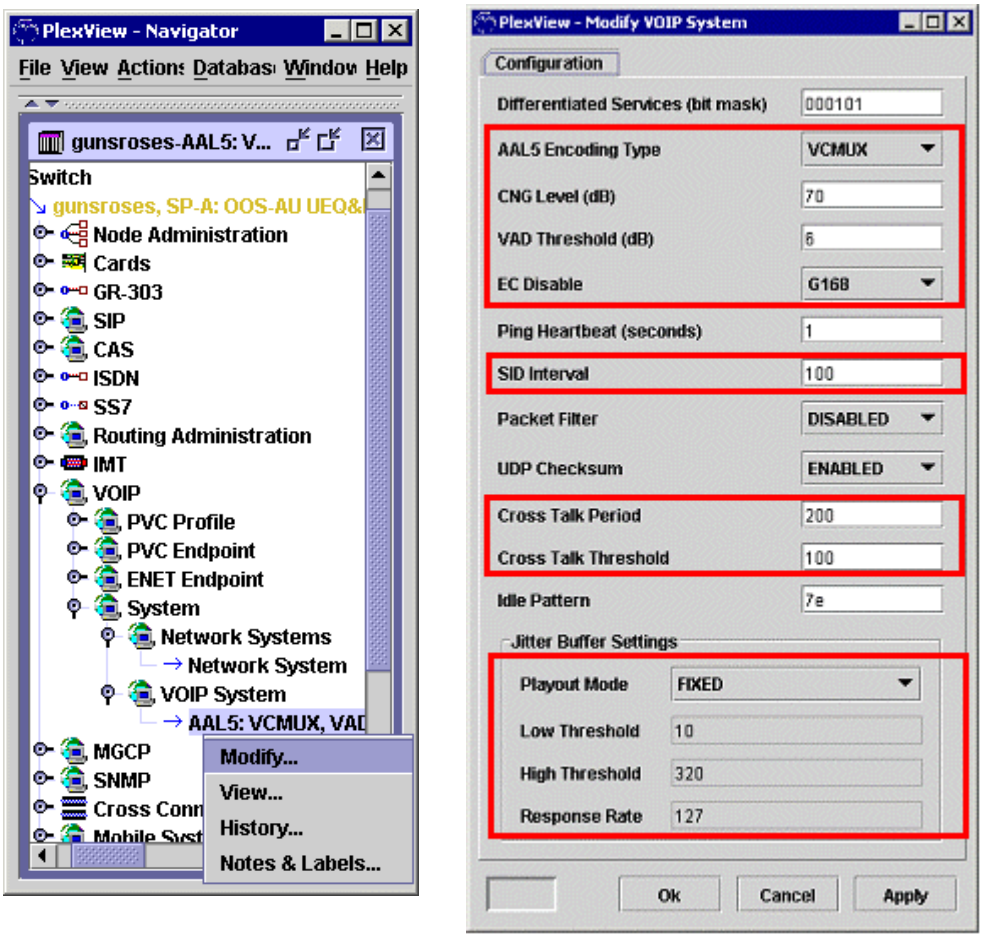
DS3 or DS1I/O cards (TDM IOMs)

Standard TDM IOM configuration is all that is required.

VoIP System Provisioning

The VoIP system comes with defaults that can be modified, as shown in the following figure.

Figure 13. VoIP System Settings



Encoding and activity levels:

- AAL5 encoding should be set to VCMUX. LLCSNAP is also supported, but all GigE ports must be provisioned as ENET_802_3 for it to work
- CNG Level (dB)(comfort noise generation) is the silence threshold before the switch generates comfort noise
- VAD Threshold (dB)(voice activity detect) is the lowest dB level of audio input considered for packetization (not silence)
- EC Disable discontinues echo cancellation. G168 is typical, G165 and G164 are also supported.
- SID Interval is the rate silence packets are transmitted at

Cross Talk levels:

IP cross talk can occur when a call terminates locally, but the remote end continues to send a packet stream. If the port is activated for a new call, two streams can be received on a switch port from different remote IP address/port combinations.

- Cross Talk Period: The number of packets received to be considered a valid VoIP stream
- Cross Talk Threshold: The number of packets from multiple sources received on a single port that will generate a cross talk event message

Jitter Buffer Settings:

Jitter buffer settings ensure that once an audio stream begins, it can be sustained even during variations in packet arrival rates. It also provides optimal performance when dealing with silence periods.

- Playout Mode identifies the jitter buffer's playout mode as fixed or adaptive
- Low Threshold is identified in milliseconds
- High Threshold is identified in milliseconds and must be higher than the low threshold
- Response Rate is the time constant. It determines the speed of adaptation with the following tradeoff: a longer time constant slows adaptation but results in a more stable jitter buffer nominal threshold variable. A shorter time constant causes faster adaptation but at the same time may result in frequent changes in the jitter buffer nominal threshold variable. For jitters in bursts, expect a better trade off when using a smaller time constant; for random jitter a longer time constant is more appropriate. The choice of optimal parameters is system dependent and should be selected based on the measure of jitter in the network. However, assuming random jitter and desire for small changes in delay over short instances, setting the value of jitBufLowThresh to "2", jitBufHighThresh to "16", and jitBufRspRt to "127" can be used as a start. The factory default is "127".

The equivalent TL1 commands are provided in the following table.

Table 6. TL1 Commands for Modifying the VOIP System

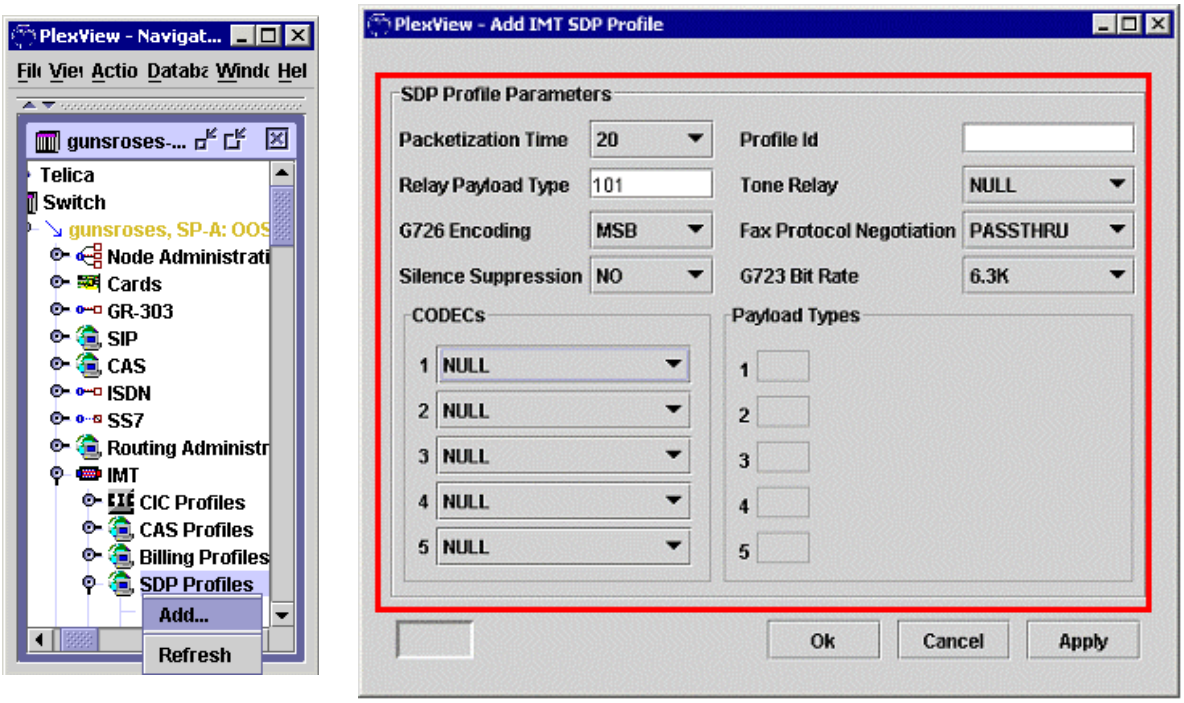
Command and Description	Definition and Parameters
ED/RTRV-VOIP-SYS	Edit general system-wide parameters for the DSP resources in the switch. Edits affect only new circuit setups after a VPS module has been removed and restored to service.

Command and Description	Definition and Parameters
TL1 equivalent to the red highlighted items to be configured:	Aal5Enc (AAL5 Encoding Type) cng (CNG Level (dB) (0, 30-77) vadThresh (VAD Threshold (dB) (Selection #) (Upper Threshold (dB)) (Lower Threshold (dB)) 1 -27 -39 2 -30 -42 3 -33 -45 4 -36 -48 5 -39 -51 6 -42 -54 7 -45 -57 8 -48 -60 9 -51 -63 10 -54 –66 ecDisable (EC Disable) sidTxInterval (SID Interval) xtalkPeriod (Cross Talk Period) xtalkThresh (Cross Talk Threshold) jitBufPlMod (Playout Mode) jitBufLowThresh (Low Threshold) jitBufHighThresh (High Threshold) jitBufRspRt (Response Rate)

Session Description Profile Provisioning

An SDP (Session Description Protocol) profile must be configured to apply to a SIP trunk. An SDP profile must have at least one codec specified for the RTP session that will be set up if the SIP call connects. Specified codecs must be contiguous and must start with codec1. The SDP Profile screen is shown in the following figure.

Figure 14. The SDP Profile Screen



- Packetization Time is the size in milliseconds of the packet containing the audio sample, or the time over which data accumulates before it is assembled into a packet. A value of NONE allows the media gateway to determine the packetization time.
- Relay Payload Type identifies the dynamic range of the RTP payload type for tone carrying packets. Each payload type is mapped to a single codec and cannot be co-assigned to another codec in the same SDP profile.
- G726 Encoding on Most Significant Bit (MSB) or Least Significant Bit (LSB)
- Silence Suppression is disabled (NO) or enabled (YES)
- Profile ID is the number of the Profile ID (1-255)
- Tone Relay determines whether to carry DTMF tones in RTP packets
- Fax Protocol Negotiation determines how to handle faxes
- G.723 Bit Rate sets G.723 for 6.3k (better fidelity) or 5.3k (bandwidth savings)
- CODECs: This section determines the hierarchical order of codec negotiation with the far-end with 1 being the highest level
- Payload Types determines the dynamic range of the RTP payload and corresponds to the codec. So Payload Type 1 would correspond to CODEC1.

The equivalent TL1 commands are provided in the following table.

Table 7. TL1 Commands for Adding an IMT SDP

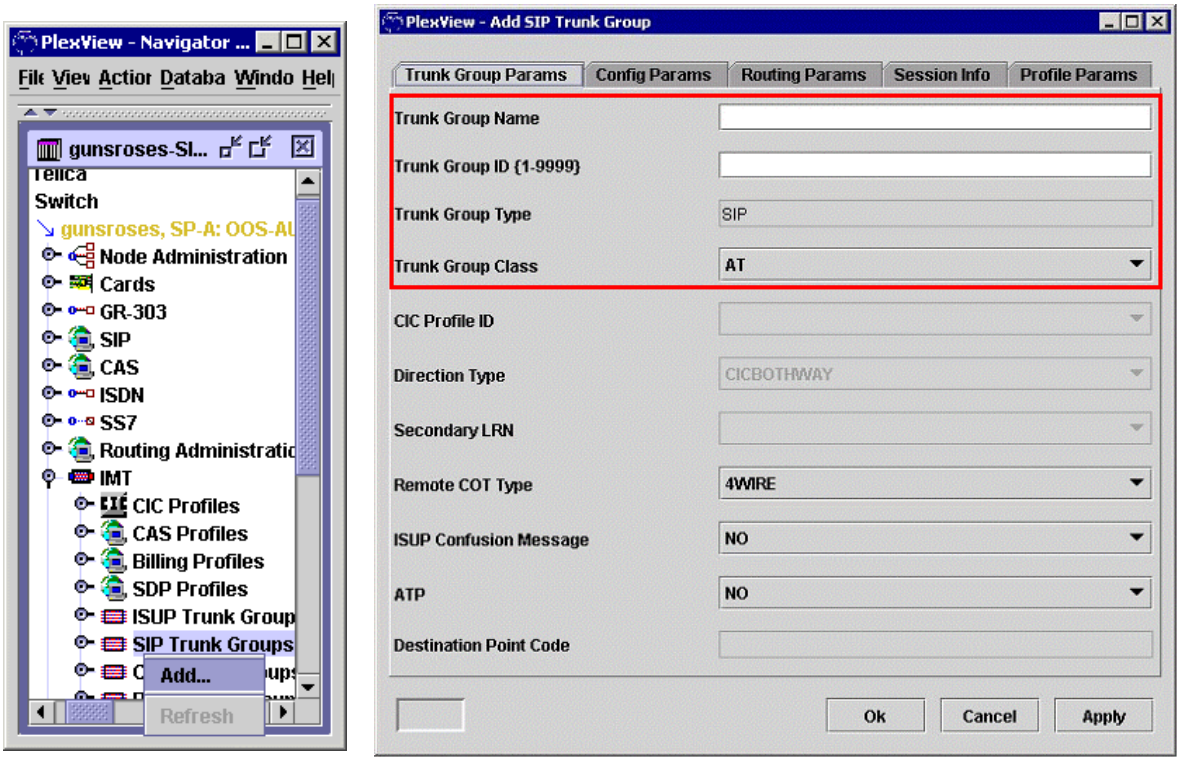
Command and Description	Definition and Parameters
ED/ENT-PRFL-SDP	Edits or establishes an SDP (Session Description Protocol) profile applicable to a SIP trunk. An SDP profile must have at least one codec specified and others must be contiguous.

Command and Description	Definition and Parameters
TL1 equivalent to the red highlighted items to be configured:	pTime (Packetization Time) relayPtype (Relay Payload Type) silSup (Silence Suppression) sdpPrflID (Profile ID) toneRelay (Tone Relay) codec1-codec5 ptype1-ptype5

SIP Trunk Group Provisioning

SIP trunk groups carry SIP calls to and from the switch. The calls are carried in RTP and are somewhat configured in the SDP profile, but the trunk groups must be fully configured for the bearer channels to work. Trunk group screens are similar for all supported trunk group types. Those menu items not relevant to SIP or SIP-T are grayed out. Also, the pull-down menu items only display selections that are relevant to SIP trunk groups. The first Add Trunk Group Params screen is shown in the following figure.

Figure 15. Add SIP Trunk Group



Initial Trunk Group Setup

This trunk group setup highlights the most important trunk group configurable parameters. Other parameters that are not highlighted must also be configured for SIP trunks.

- Assign the Trunk Group Name and ID
- The Trunk Group Type is preset before you get to this screen
- Trunk Group Class is the class of the remote switch the trunk group terminates to

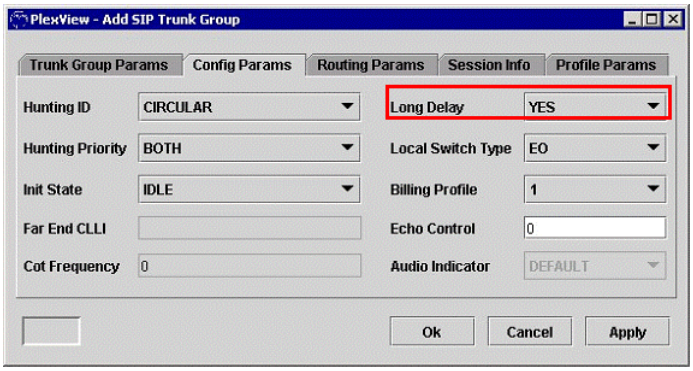
The equivalent TL1 commands are provided in the following table.

Table 8. TL1 Commands for the Initial Trunk Group Params

Command and Description	Definition and Parameters
ED/ENT-TRKGRP TL1 equivalent to the red highlighted items to be configured:	Establish a trunk group. TrkGrpName (Trunk Group Name) Tgn (Trunk Group ID) (1-9999) SigType (Trunk Group Type) TrkGrpClass (Trunk Group Class) LongDelay (Long Delay under Config Params tab) IpAddr (IP Address under Session Info tab) MaxIpCalls (Maximum IP Calls under Session Info tab)

Click the Config Params tab and the next screen appears, as shown in the following figure.

Figure 16. SIP Trunk Group Config Params

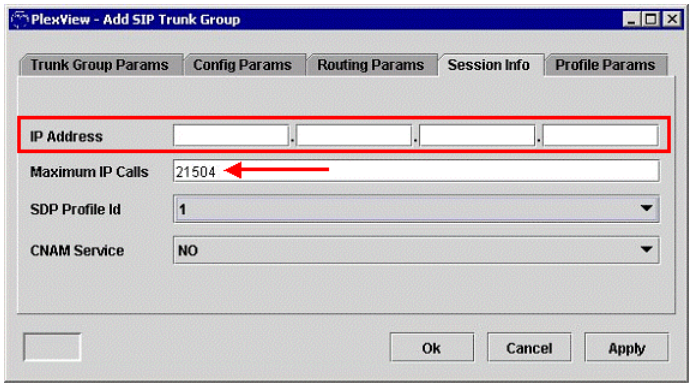


Long Delay enables echo cancellation.

Click the Session Info tab and more relevant configurable parameters appear, as shown in the following figure. They are only available when the Trunk Group Type is set to SIP.

- The IP address for this field is the IP address of the local feature server, application server, media gateway, or network server
- The Maximum IP Calls is the maximum number of calls supported on the trunk group

Figure 17. SIP Session Information

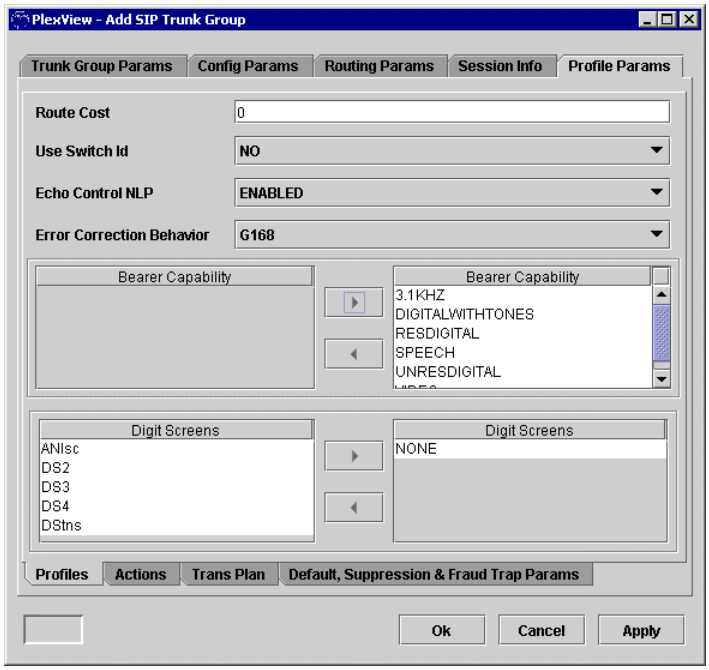


The profile parameters screen has call termination and treatment information that becomes relevant after the path of the trunk is chosen. The screen includes:

- The type of information to be carried in the bearer channel
- Digit screening
- The action to take after the trunk group is chosen
- Behavior profiles
- Translation plans
- Default profiles
- Parameter suppression profiles
- Fraud trap profiles

Many of the configurable items are under the tabs at the bottom of the screen, as shown in the following figure.

Figure 18. SIP Profile Parameters



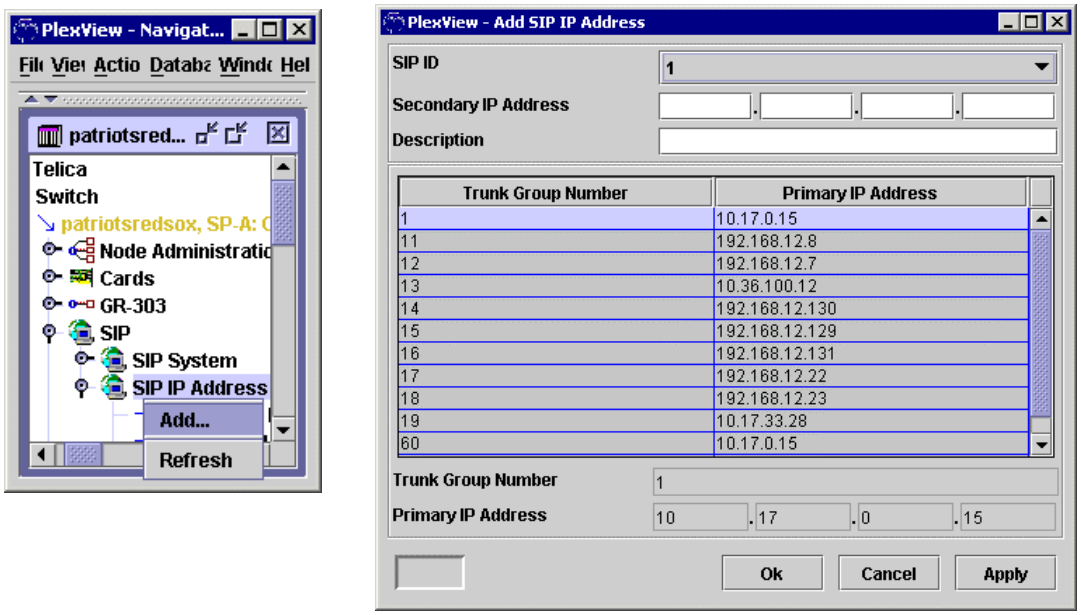
SIP IP Address Provisioning

The SIP IP Address establishes a primary and optionally a secondary IP address to access the session access node (feature server or equivalent). The SIP trunk group must be established prior to configuring the SIP IP Address. All items pertain to SIP, so no items are highlighted with a red outline.

- The SIP ID is the Session Access Node
- The Secondary IP Address optionally provides a secondary IP path to the feature server
- The Description identifies the interface
- The Trunk Group Number is the number assigned in Add SIP Trunk Group
- The Primary IP Address is the address to access the feature server.

The Add SIP IP Address screen is shown in the following figure.

Figure 19. SIP IP Address



The equivalent TL1 commands are provided in the following table.

Table 9. TL1 Commands for SIP IP Address

Command and Description	Definition and Parameters
ED/ENT-SIP-IPADDR	Edit or establish the primary and (optional) secondary IP address and description for a trunk group to a specific SIP session access node (feature server or equivalent).
TL1 equivalents to the red highlighted items to be configured:	tgnSipID (SIP ID & Trunk Group Number) secIPAddr (Secondary IP Address) description (Description) primIPAddr (Primary IP Address)

SIP System Provisioning

The SIP System node modifies the SIP stack from the system defaults for the number of supported connections and various timers. Details are beyond the scope of this document.

SIP CDR Generation with a Feature Server

When using the switch with a feature server to support enhanced IP features, two CDRs are created – one from the switch and one from the feature server. The same SIP Call ID appears on each CDR, identifying them for the same call. This facilitates billing correlation between the switch and feature server with regard to CDRs.

Related Documents

- *TL1 Commands Reference Guide*
- *EMS User's Guide*

Voice Over Packet Software Package

This document contains the following sections:

CODEC Support

The switch supports these compression/decompression (CODEC) technologies:

- G.711 µLaw (mu-Law)
- G.711 aLaw
- G.723.1
- G.726
- G.729a/b

Additionally, the switch supports these CODEC-related technologies:

- Clear-Channel Support Over Packet (X-CCD, CISCO CLEAR CHANNEL, and CLEARMODE): Clear-Channel data support lets the switch negotiate how to send restricted/unrestricted digital data over an RTP stream. Digital data in this case is potentially HDLC data received from ISDN devices.
- DTMF Relay (RFC2833): RFC-2833 describes how to send DTMF tones "out-of-band" over RTP. Support for RFC-2833 is required when the peer end-point does not have DTMF tone detectors. It requires the switch to transmit the presence of DTMF digits in the audio stream out-of-band.

These CODECs are available on each installed VSM (Voice Server Module). The switch performs CODEC negotiation during call establishment between VoIP end-points, per

RFC-3264. To establish a VoIP call, the peer end-points must have at least one common CODEC assigned to the call establishment end-point.

In the switch, CODECS are specified in preference (priority) order in Session Descriptor Protocol (SDP) profiles referenced by SIP trunks. When the switch originates a call on a SIP trunk, the first CODEC listed in the SDP profile for the trunk is the preferred CODEC that the switch wishes to use for the call. If the remote peer cannot support the preferred CODEC, due to resource limitations, but can support another CODEC in the preference list, then the remote peer responds to the switch with the next highest CODEC in the preference list that it can support and the call is established. The preference (priority) list has an effect only when the switch originates the call.

The switch supports CODEC negotiation in these situations:

- On-net (IP to IP calls), when the switch is not involved in the bearer path. The switch does not limit the CODEC negotiation, meaning that the CODEC will be negotiated between the two endpoints. In this case, the CODECs provisioned in the switch SDP profile are immaterial to the negotiation. For instance, a CODEC not supported at all by the switch could be selected by two endpoints.
- Off-net (IP to TDM or TDM to IP calls), when the switch terminates the IP flow. The switch supports CODEC priority lists on a per-trunk or per-line group basis.

Note: This priority only has effect when the switch originates the call.

The following parameters are passed as part of CODEC negotiation; however, only the CODEC is negotiated and could result in a call rejection due to unsupported CODECs. The switch complies with the requested silence suppression and packetization time.

- CODEC: G.711-aLaw, G.711-µLaw, G.723.1, G.726, G.729a and G.729b (which is G.729a with Silence Suppression)
- Packetization Time (msec): 10, 20, 30, 40 (VoIP); 60 for G.723.1 only
- Silence Suppression: on, off

Note: These silence suppression parameters are not supported: silence timer, silence preference, silence insertion descriptors, and silence fixed noise level.

- DTMF Relay (RFC2833) enable/disable: yes, no

Note: SDP parameters clock rate, bandwidth, and echo cancellation enable are not negotiated.

Clear-Channel Support Over Packet

The switch supports Clear-Channel for transporting data (64kbps unrestricted) traffic over IP (RTP). This consists of 8-bit samples with a sampling rate of 8000 Hz with no echo cancellation or silence suppression.

The typical application is for IP trunking (SIP) of ISDN or switched 56 data traffic. This consists of 8-bit samples with a sampling rate of 8000 Hz with no echo cancellation or silence suppression.

RFC2833

In release 3.8, the switch supports tone relay as defined by the IETF RFC2833 standard (Events 0-15). DTMF tones can be transported directly over the voice stream within RTP or they can be extracted out to the voice stream and encoded as RTP-named telephone events. The applications for RFC2833 are as follows:

- In a feature server environment, the switch needs to connect to a media server to provide announcements and digit collection. Some low cost media servers (e.g., software-based) do not have DTMF tone detection functions. This environment requires the switch to detect the DTMF tones and send it to the media server via RTP-named telephone events.
- In general, compressed low bit rate CODECs (G.723, G.726, G.729a) cannot transport DTMF tones reliably within the voice traffic. RFC2833 can be used to relay the DTMF tones. The alternative of up-speeding to G.711 for passing the DTMF tones is not practical due to the overhead of switching back and forth.
- In an environment where the IP network is of low quality with large jitter, long delay or high packet loss, the G.711 or G.726 CODEC may not be able to reliably transport DTMF tones. Therefore, RFC2833 may be needed to relay the DTMF tones.

Only RFC events 0-15 (DTMF tones 0-9, *, #, A-D) are supported with RFC2833. Other tones defined in RFC2833 (e.g., FAX, Modem, MF) are not supported.

How CODEC Negotiation Takes Place on the Switch

In general, CODEC negotiation involves both the switch and the far end switch suggesting the CODEC to use, then the switch attempting to achieve a match. For incoming IP calls, the switch accepts the first CODEC on the received SDP list that matches a configured CODEC in the locally configured SDP profile for that incoming trunk group. The switch rejects the call if no CODEC matches. The switch accepts silence suppression and DTMF tone relay options when they also are configured in the local SDP profile of the incoming trunk group. The switch enables DTMF tone relay when the far end requests it.

The following three tables demonstrate CODEC options between the switch and a remote endpoint. In the tables, “Signaled” identifies what either switch puts into its signaling,

whereas “TX” and “RX” identify what is actually sent and what is expected to be received. Violet fill signifies the switch; gray fill signifies the endpoint.

Table A shows the various combinations of CODECs and packet times possible when the switch originates a call. In this scenario, the switch is the “ingress” that processes a local descriptor generated from the SDP profile – there is no remote descriptor to work against.

Table A. CODEC Combinations when Originating a Call

Switch →				Endpoint				Result			
Profile		Signaled		Profile		Signaled		TX	RX	TX	RX
10ms	G.711 G.729 G.723	ptime=10	G.711 G.729	10ms	G.711 G.729 G.723	ptime=10	G.711	G.711	G.711	G.711	G.711
10ms	G.711 G.729 G.723	ptime=10	G.711 G.729	20ms	G.711 G.729 G.723	ptime=10	G.711	G.711	G.711	G.711	G.711
10ms	G.711 G.729 G.723	ptime=10	G.711 G.729	30ms	G.711 G.729 G.723	ptime=10	G.711	G.711	G.711	G.711	G.711
10ms	G.711 G.729 G.723	ptime=10	G.711 G.729	10ms	G.729 G.711	ptime=10	G.711	G.711	G.711	G.711	G.711
10ms	G.711 G.729 G.723	ptime=10	G.711 G.729	30ms	G.723 G.711	ptime=10	G.711	G.711	G.711	G.711	G.711
10ms	G.711 G.729 G.723	ptime=10	G.711 G.729	30ms	G.723 G.729 G.711	ptime=10	G.711	G.711	G.711	G.711	G.711
20ms	G.729 G.711	ptime=20	G.729 G.711	10ms	G.711 G.729 G.723	ptime=20	G.729	G.729	G.729	G.729	G.729
20ms	G.729 G.711	ptime=20	G.729 G.711	20ms	G.711 G.729 G.723	ptime=20	G.729	G.729	G.729	G.729	G.729
20ms	G.729 G.711	ptime=20	G.729 G.711	30ms	G.711 G.729 G.723	ptime=20	G.729	G.729	G.729	G.729	G.729
20ms	G.729 G.711	ptime=20	G.729 G.711	10ms	G.729 G.711	ptime=20	G.729	G.729	G.729	G.729	G.729
20ms	G.729 G.711	ptime=20	G.729 G.711	30ms	G.723 G.711	ptime=20	G.711	G.711	G.711	G.711	G.711
20ms	G.729 G.711	ptime=20	G.729 G.711	30ms	G.723 G.729 G.711	ptime=20	G.729	G.729	G.729	G.729	G.729

Table B shows the various combinations of CODECs and packet times possible when the switch receives a call. In this scenario, the switch is the "egress" that processes a local descriptor generated from the SDP profile against the remote descriptor received from the endpoint.

Table B. CODEC Combinations when Receiving a Call

Endpoint →				Switch				Result			
Profile		Signaled		Profile		Signaled		TX	RX	TX	RX
10ms	G.711 G.729 G.723	ptime=10	G.711 G.729 G.723	10ms	G.711 G.729 G.723	ptime=10	G.711	G.711 (10ms)	G.711 (10ms)	G.711 (10ms)	G.711 (10ms)
20ms	G.711 G.729 G.723	ptime=20	G.711 G.729 G.723	10ms	G.711 G.729 G.723	ptime=20	G.711	G.711 (20ms)	G.711 (20ms)	G.711 (20ms)	G.711 (20ms)
30ms	G.711 G.729 G.723	ptime=30	G.711 G.729 G.723	10ms	G.711 G.729 G.723	ptime=30	G.711	G.711 (30ms)	G.711 (30ms)	G.711 (30ms)	G.711 (30ms)
10ms	G.729 G.711	ptime=10	G.729 G.711	10ms	G.711 G.729 G.723	ptime=10	G.729	G.729 (10ms)	G.729 (10ms)	G.729 (10ms)	G.729 (10ms)
30ms	G.723 G.711	ptime=30	G.723 G.711	10ms	G.711 G.729 G.723	ptime=30	G.723	G.723 (30ms)	G.723 (30ms)	G.723 (30ms)	G.723 (30ms)
30ms	G.723 G.729 G.711	ptime=30	G.723 G.729 G.711	10ms	G.711 G.729 G.723	ptime=30	G.723	G.723 (30ms)	G.723 (30ms)	G.723 (30ms)	G.723 (30ms)
10ms	G.711 G.729 G.723	ptime=10	G.711 G.729 G.723	20ms	G.729 G.711	ptime=10	G.711	G.711 (10ms)	G.711 (10ms)	G.711 (10ms)	G.729 (10ms)
20ms	G.711 G.729 G.723	ptime=20	G.711 G.729 G.723	20ms	G.729 G.711	ptime=20	G.711	G.729 (20ms)	G.729 (20ms)	G.729 (20ms)	G.729 (20ms)
30ms	G.711 G.729 G.723	ptime=30	G.711 G.729 G.723	20ms	G.729 G.711	ptime=30	G.711	G.729 (30ms)	G.729 (30ms)	G.729 (30ms)	G.729 (30ms)
10ms	G.729 G.711	ptime=10	G.729 G.711	20ms	G.729 G.711	ptime=10	G.729	G.729 (10ms)	G.729 (10ms)	G.729 (10ms)	G.729 (10ms)
30ms	G.723 G.711	ptime=30	G.723 G.711	20ms	G.729 G.711	ptime=30	G.711	G.711 (30ms)	G.711 (30ms)	G.711 (30ms)	G.711 (30ms)
30ms	G.723 G.729 G.711	ptime=30	G.723 G.729 G.711	20ms	G.729	ptime=30	G.729	G.729 (30ms)	G.729 (30ms)	G.729 (30ms)	G.729 (30ms)

Table C shows the various combinations of CODECs and packet times possible when the switch receives a call using the remote CODEC list for preference. In this scenario, the switch is the "egress" that processes the remote descriptor received from the endpoint.

Table C. CODEC Combinations when Receiving a Call Using Remote CODEC List for Preference

Endpoint →				Switch				Result			
Profile		Signaled		Profile		Signaled		TX	RX	TX	RX
10ms	G.711 G.729 G.723	ptime=10	G.711 G.729 G.723	10ms	G.711 G.729 G.723	ptime=10	G.711	G.711 (10ms)	G.711 (10ms)	G.711 (10ms)	G.711 (10ms)
20ms	G.711 G.729 G.723	ptime=20	G.711 G.729 G.723	10ms	G.711 G.729 G.723	ptime=20	G.711	G.711 (20ms)	G.711 (20ms)	G.711 (20ms)	G.711 (20ms)
30ms	G.711 G.729 G.723	ptime=30	G.711 G.729 G.723	10ms	G.711 G.729 G.723	ptime=30	G.711	G.711 (30ms)	G.711 (30ms)	G.711 (30ms)	G.711 (30ms)
10ms	G.729 G.711	ptime=10	G.729 G.711	10ms	G.711 G.729 G.723	ptime=10	G.729	G.729 (10ms)	G.729 (10ms)	G.729 (10ms)	G.729 (10ms)
30ms	G.723 G.711	ptime=30	G.723 G.711	10ms	G.711 G.729 G.723	ptime=30	G.723	G.723 (30ms)	G.723 (30ms)	G.723 (30ms)	G.723 (30ms)
30ms	G.723 G.729 G.711	ptime=30	G.723 G.729 G.711	10ms	G.711 G.729 G.723	ptime=30	G.723	G.723 (30ms)	G.723 (30ms)	G.723 (30ms)	G.723 (30ms)
10ms	G.711 G.729 G.723	ptime=10	G.711 G.729 G.723	20ms	G.729 G.711	ptime=10	G.711	G.711 (10ms)	G.711 (10ms)	G.711 (10ms)	G.711 (10ms)
20ms	G.711 G.729 G.723	ptime=20	G.711 G.729 G.723	20ms	G.729 G.711	ptime=20	G.711	G.711 (20ms)	G.711 (20ms)	G.711 (20ms)	G.711 (20ms)
30ms	G.711 G.729 G.723	ptime=30	G.711 G.729 G.723	20ms	G.729 G.711	ptime=30	G.711	G.711 (30ms)	G.711 (30ms)	G.711 (30ms)	G.711 (30ms)
10ms	G.729 G.711	ptime=10	G.729 G.711	20ms	G.729 G.711	ptime=10	G.729	G.729 (10ms)	G.729 (10ms)	G.729 (10ms)	G.729 (10ms)
30ms	G.723 G.711	ptime=30	G.723 G.711	20ms	G.729 G.711	ptime=30	G.711	G.711 (30ms)	G.711 (30ms)	G.711 (30ms)	G.711 (30ms)
30ms	G.723 G.729 G.711	ptime=30	G.723 G.729 G.711	20ms	G.729	ptime=30	G.729	G.729 (30ms)	G.729 (30ms)	G.729 (30ms)	G.729 (30ms)

The following four tables show silence suppression options between the switch and a remote endpoint for CODECs G.711 and G.729; silence suppression is unavailable for G.723. In the tables, "Signaled" identifies what either switch puts into its signaling, whereas "TX" and "RX" identify what is actually sent and what is expected to be received. Violet fill signifies the switch; gray fill signifies the endpoint. Note that the switch properly processes incoming SID packets regardless of whether silence suppression is enabled; thus the "RX" side for the switch is always true.

Table D shows silence suppression options for G.711 when the switch originates a call.

Table D. Silence Suppression Options for G.711 when Originating

Switch →		Endpoint		Result			
Profile	Signaled	Profile	Signaled	TX	RX	TX	RX
N	N	N	N	N	Y	N	N
N	N	Y	Y	N	Y	N	N
Y	Y	Y	Y	Y	Y	Y	Y
Y	Y	N	N	N	Y	N	N

Table E shows silence suppression options for G.711 when the switch receives a call.

Table E. Silence Suppression Options for G.711 when Receiving

Endpoint →		Switch		Result			
Profile	Signaled	Profile	Signaled	TX	RX	TX	RX
N	N	N	N	N	N	N	N
N	N	Y	N	N	N	N	N
Y	Y	Y	Y	Y	Y	Y	Y
Y	Y	N	N	N	N	N	N

Table F shows silence suppression options for G.729 when the switch originates a call.

Table F. Silence Suppression Options for G.729 when Originating

Switch →		Endpoint		Result			
Profile	Signaled	Profile	Signaled	TX	RX	TX	RX
N	N	N	N	N	N	N	N
N	N	Y	Y	N	N	N	N
Y	Y	Y	Y	Y	Y	Y	Y
Y	Y	N	N	N	N	N	N

Table G shows silence suppression options for G.729 when the switch receives a call.

Table G. Silence Suppression Options for G.729 when Receiving

Endpoint →		Switch		Result			
Profile	Signaled	Profile	Signaled	TX	RX	TX	RX
N	N	N	N	N	N	N	N
N	N	Y	N	N	N	N	N
Y	Y	Y	Y	Y	Y	Y	Y
Y	Y	N	N	N	N	N	N

The following two tables demonstrate DTMF tone relay options between the switch and a remote endpoint. In the tables, violet fill signifies the switch; gray fill signifies the endpoint. "Signaled" identifies what either switch puts into its signaling, whereas "TX" and "RX" identify what is actually sent and what is expected to be received. "Inband" DTMF tone relay is voice-encoded; "Outband" DTMF tone relay is in RFC2833 tone relay RTP packets.

Table H shows DTMF tone relay options when the switch originates a call.

Table H. DTMF Tone Relay Options when Originating

Switch →		Endpoint		Result			
Profile	Signaled	Profile	Signaled	TX	RX	TX	RX
Outband	Outband	Inband	Inband	Inband	Inband	Inband	Inband
Outband	Outband	Outband	Outband	Outband	Outband	Outband	Outband
Inband	Inband	Outband	Outband	Outband	Outband	Outband	Outband
Inband	Inband	Inband	Inband	Inband	Inband	Inband	Inband

Table I shows DTMF tone relay options when the switch receives a call.

Table I. DTMF Tone Relay Options when Receiving

Endpoint →		Switch		Result			
Profile	Signaled	Profile	Signaled	TX	RX	TX	RX
Inband	Intband	Outband	Inband	Inband	Inband	Inband	Inband
Outband	Outband	Outband	Outband	Outband	Outband	Outband	Outband
Outband	Outband	Intband	Outband	Outband	Outband	Outband	Outband
Inband	Inband	Inband	Inband	Inband	Inband	Inband	Inband

TDM-VOIP Outgoing Call

For an outgoing call, the SIP (INVITE), message generated by the switch has an SDP media entry containing the offered CODECs, in preference order, with specified packet time and silence suppression state.

The SDP media entry in the corresponding Answer message received for SIP contains the CODEC selected by the remote peer for the call. The switch complies with the selection by the remote peer for CODEC, packet time, silence suppression, and Tone Relay payload type.

If the remote peer supports none of the CODECs in the initial outgoing call request, the call cannot be established and is disconnected.

TDM-VOIP Incoming Call

For an incoming call, the switch receives a proper SIP (INVITE) message with an SDP media entry containing a list of CODECs in preference order from the remote peer, as well as packet time, silence suppression and Tone Relay options.

The switch compares the received CODEC preference list against the CODEC list specified in the SDP Profile assigned to the trunk group. The switch sets up the call using the most-preferred CODEC in the preference list from the remote peer that is also common to the local SDP profile in the switch and for which the switch has sufficient resources for support. It then sends a proper SIP protocol message indicating its selection in the media entry of the SDP profile.

The switch also uses the remote peer's choice for packet time, silence suppression, and Tone Relay options in the incoming call request, if supported by the switch. For example, the switch does not currently support G.723.1 silence suppression as specified in Annex A. If the selected CODEC is G.723.1 and the remote peer requested enabling silence suppression, the switch would respond within the SDP that Annex A cannot be supported.

The previously provisioned SDP profiles (see Figure 2) for SIP calls are used to transfer the CODEC list. You assign the SDP to the SIP trunk using the screen illustrated in Figure 2.

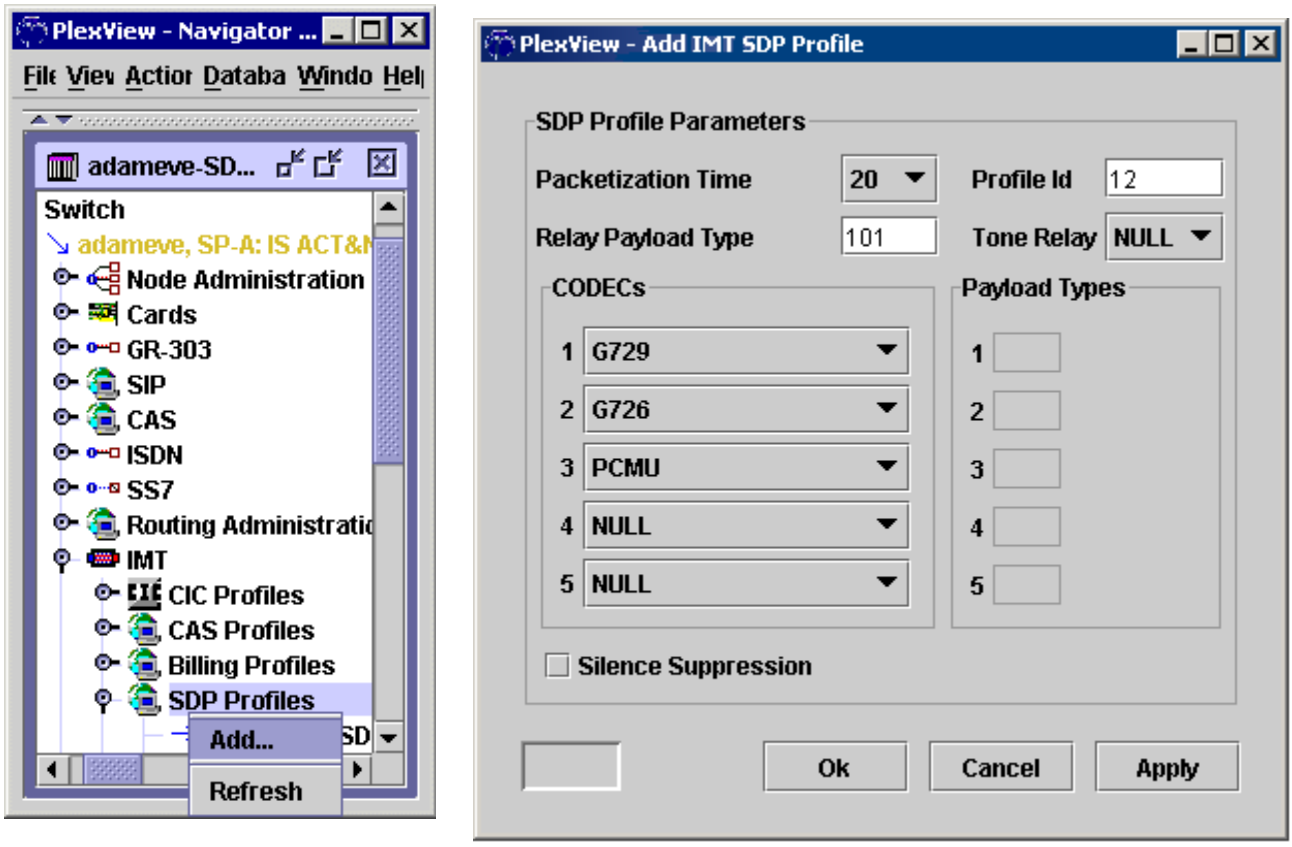
Assigning CODECs to SDP Profiles Using the EMS

To assign CODECs to SDP profiles, which are then assigned to SIP, SIP-T, ISUP, and CAS trunks, you use the PlexView EMS to first provision the SDP profile, and then to assign the profile to each trunk or line group. You use the Add IMT SDP Profile screen to add an SDP profile.

When provisioning an SDP profile, you must specify the packetization time (compression time), whether DTMF tone relay is enabled and the corresponding relay payload type, whether silence suppression is enabled, and up to five selected CODECs per SDP profile. The configurable packetization time can be set from 10 to 40 ms.

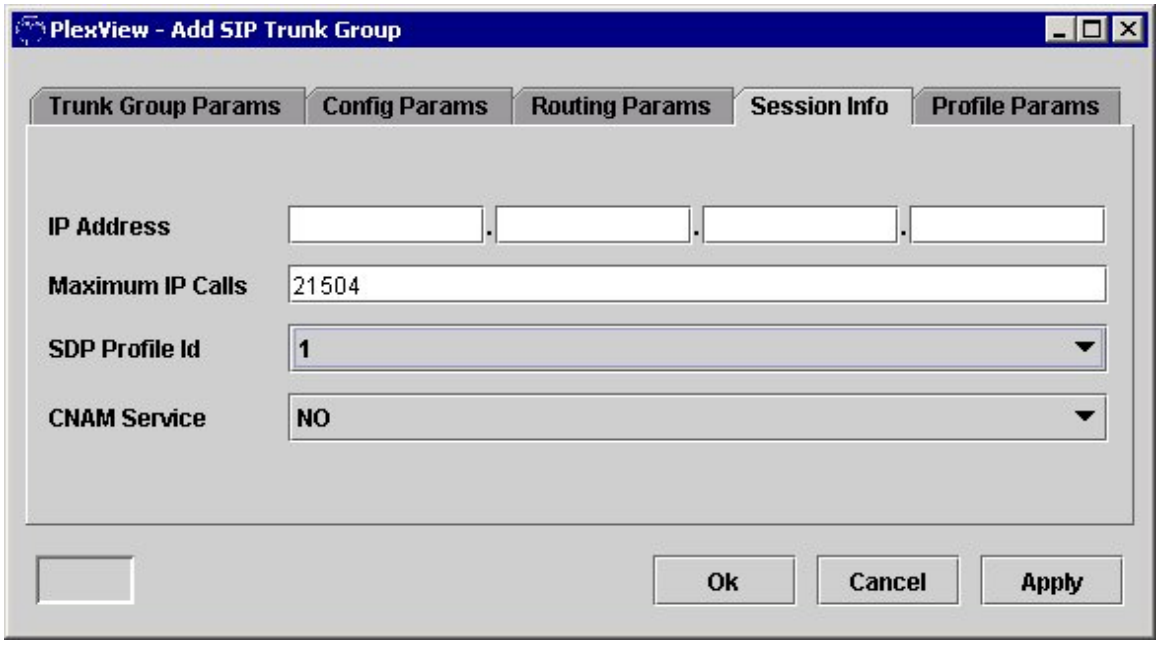
CODEC choices are PCMU (G.711-µLaw for US), PCMA (G.711-aLaw for Europe), G.723.1 (5.3k or 6.3k selectable), G.726 (MSB or LSB first, depending on the communicating device), G.729a, X-CCD (clear channel), CISCO CLEAR CHANNEL, and CLEARMODE. There are also packet type mappings for the different clear mode types. G.729b (G.729a with silence suppression), Clear Channel Support Over Packet and DTMF Relay. See Figure 1 for a sample of the EMS screen used to provision an SDP profile.

Figure 1. Add IMT SDP Profile



When provisioning trunks groups, you then assign the already provisioned SDP profile to the trunk group. For instance, to assign an SDP to a SIP trunk group, use the screen illustrated in Figure 2.

Figure 2. Add SIP or SIP-T Trunk Group, Session Info Tab, SDP Profile



SIP CODEC Negotiation

The following CODEC limitations exist for support of SIP INFO:

- The long # or double # can be detected on the packet voice stream as long as it is G.711 or G.726. It cannot be detected for G.729a or RFC2833-named telephony events.
- It is only used for transporting of the long # or double #. No other DTMF tones are supported (e.g., *).
- The switch does not support RFC2833-named telephony events; therefore, a way in which to support SIP INFO is to use the SIP SUBSCRIBE/NOTIFY messages to pass the RFC2833-named telephony events. The usage of SUBSCRIBE/NOTIFY for DTMF tone detection is also supported to eliminate the need for a Media Server to do the detection (i.e., the information is passed via the signaling path rather than the bearer).

For more information, refer to the CODEC Support section.

VoIP Diagnostics

The switch supports IP traceroute, which is a diagnostic tool used for providing a trace of the list of routers traversed to a specific destination, along with the number of hops. Traceroute is a standard IP diagnostic utility.

Related Documents

- *TL1 Commands Reference Guide*
- *Installation and Operations Manual, Vol. I*
- *Element Management System User's Guide*